Documentation
GBox Version 1.5.3.102

Documentation version : V1

Date de création : Decembre, 2023

Contents

Index **203**

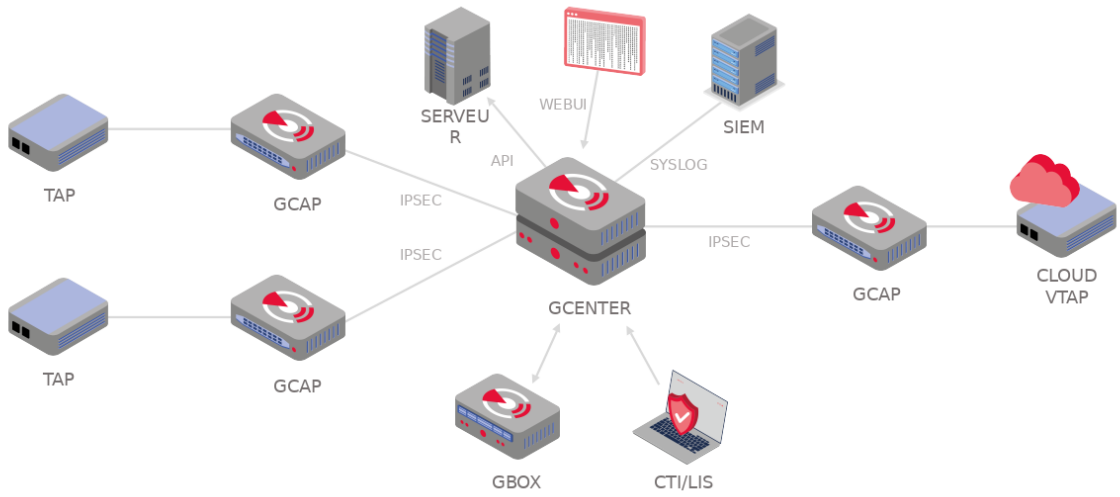
Chapter 1

Description

1.1 Introduction

La solution proposée par Gatewatcher comprend :

- un ou plusieurs GCaps
- un GCenter
- une GBox (optionnelle)



1.2 Présentation du TAP

Un TAP (Test Access Point) est un dispositif passif qui permet de surveiller un réseau informatique en recopiant certains flux qui transitent sur le réseau et en les redirigeant par exemple vers une sonde de détection (GCap).
Il est possible de connecter plusieurs TAPs à un GCap, ce dernier disposant de plusieurs interfaces de capture.

1.3 Présentation du GCap

Le GCap est une sonde de détection de type IDS.
Il permet :

- de capturer et d'analyser le trafic réseau venant des TAPs
- de générer les événements de type alertes et/ou métadonnées
- de reconstruire les fichiers présents dans le flux analysé (suivant des paramètres de type et de taille)
- de transmettre les événements et les fichiers capturés au GCenter

Pour plus d'informations, se référer à la documentation du GCap.

1.4 Présentation du GCenter

Le GCenter est le deuxième composant de la solution qui fonctionne conjointement :

- avec la sonde de détection GCap
- avec la GBox

Il a pour fonctions principales :

- le pilotage de la sonde GCap (gestion des règles d'analyse, des signatures, supervision de l'état de santé, etc)
- l'analyse approfondie des fichiers remontés par la sonde
- l'administration de la solution
- l'affichage du résultat des différentes analyses dans des tableaux de bord
- le stockage long-terme des données
- l'export des données dans des solutions tierces de type SIEM (Security Information and Event Management)

Pour plus d'informations, se référer à la documentation du GCenter.

1.5 Présentation de la GBox

La GBox est un équipement pouvant fonctionner de manière autonome ou conjointement avec le GCenter.
Cette *appliance* permet :

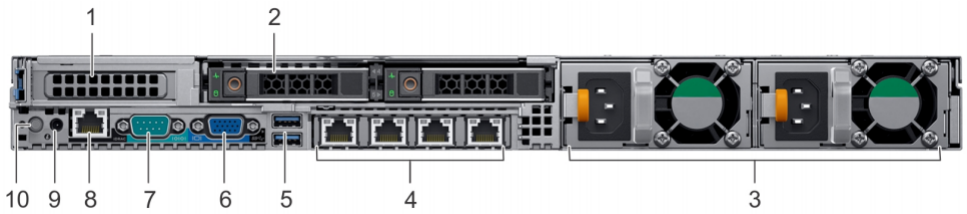
- de recevoir automatiquement des fichiers suspicieux et donc nécessitant une analyse approfondie des malwares sans avoir recours à un service externe
- d'analyser à la demande des fichiers suspicieux depuis l'interface Web UI du GCenter
- de renvoyer des rapports au GCenter pour les fichiers qui lui ont été soumis et visibles depuis l'interface Web UI du GCenter et dans celle de la GBox
- d'analyser des fichiers directement sur la Web UI de la GBox et de générer un rapport correspondant
- à l'utilisateur d'effectuer manuellement une analyse sur les noms de domaines ayant été générés par des DGA (Domain Generation Algorithm)

Elle dispose de quatre moteurs d'analyse complémentaires, permettant une analyse statique, dynamique et heuristique ainsi que la détection de *shellcode* et d'un moteur pour détecter des noms de domaines ayant été générés par des DGA
Ces moteurs d'analyse sont abordés plus en détail dans la section *Moteurs d'analyse*.

1.5.1 Modèles de serveur

Pour plus d'informations, se référer à la partie *Caractéristiques mécaniques*.

1.5.2 Liste des entrées / sorties de la GBox



La **GBox** possède :

Repère	Nom
4	Connecteur RJ-45 `GBX0` : interface de management et lien avec le **GCenter** . Connecteur RJ-45 `GBX1` : interface dédiée aux Machines Virtuelles pour l'accès Internet, l'accès des VMs de Gnest peut se faire par ce lien Connecteur RJ-45 `GBX2` : Non utilisé Connecteur RJ-45 `GBX3` : Non utilisé
5	Connecteur USB : branchement de la clé USB permettant le déchiffrement des disques (standard Linux Unified Key Setup) Connecteur USB : accès direct avec un clavier Ce mode de connexion est déprécié au profit de KVM/IDRAC/XCC et ne doit être utilisé qu'en dernier recours
6	Connecteur VGA : accès direct avec un écran. Ce mode de connexion est déprécié au profit de KVM/IDRAC/XCC et ne doit être utilisé qu'en dernier recours

Note:

Le détail des connecteurs est indiqué dans le Manuel d'installation et de maintenance Dell EMC PowerEdge R640.

1.5.2.1 Utilisation des connecteurs USB et VGA

Le branchement d'un clavier et d'un écran permet l'accès direct à l'interface console du GCenter.

Important:

Ce mode est déprécié.
Il ne doit être utilisé qu'à l'installation initiale et pour du diagnostic avancé.

1.5.2.2 Accès à l'interface de gestion et de configuration du serveur

L'accès à cette interface de gestion se fait en HTTPS :

- sur un serveur Dell, ce connecteur est appelé **iDRAC** et est noté sur le schéma **KVM/IDRAC**
- sur un serveur Lenovo, ce connecteur est appelé **TSM** : ce connecteur est identifiable grâce au symbole d'une clé anglaise présent en dessous

---

1.5.2.3 Interface réseau `Gbx0`

Cette interface permet l'administration distante au travers du protocole SSH pour l'accès :

- au menu d'installation/configuration
- à l'interface Web d'utilisation / administration

Cette interface sert aussi à l'envoi des fichiers à analyser depuis le GCenter vers la GBox.

1.5.2.4 Interface réseau `Gbx1`

Cette interface réseau permet aux machines virtuelles (sandbox) du moteur Gnest d'accéder à Internet directement ou via un proxy.
Cet accès est optionnel et doit être configuré.

1.5.2.5 Raccordement électrique

Le serveur possède deux alimentations électriques qui ont chacune la puissance nécessaire au bon fonctionnement de l'équipement.
Il est fortement recommandé de raccorder chaque alimentation sur une arrivée électrique distincte.

1.5.2.6 Connecteur USB et clé LUKS

Lors de l'installation, le contenu des disques (hors /boot) est chiffré grâce au standard LUKS.
Lors de ce processus, une clé de chiffrement unique est générée et placée sur la clé USB connectée à l'équipement.
Au démarrage, la clé USB doit impérativement être branchée sur l'équipement afin que les disques puissent être déchiffrés.
Il est fortement recommandé de faire une copie de cette clé car, en cas de défaillance, les données présentes sur les disques ne seront plus accessibles.
Une fois le système démarré, il est recommandé de retirer cette clé USB et de la placer dans un endroit sûr (ex: coffre-fort).

Chapter 2

Fonctionnement

2.1 Moteurs d'analyse

2.1.1 Présentation du moteur Grip

Le moteur d'analyse **Grip** permet une analyse statique et indique des caractéristiques du fichier.
Il ne fournit pas d'information de dangerosité ou de score de menace.
Il est cependant utile pour analyser rapidement les métadonnées d'un fichier qualifié comme *suspicious* ou *malicious*.
Il est utilisé pour avoir des informations sur le fichier en amont d'analyse plus approfondies.
Ces données sont affichées dans le rapport détaillé et plus précisément dans les sections **TOP** et **Static** (voir le *Rapport détaillé*)

Taille maximum de fichier	50 MO
Timeout d'analyse	2 minutes
Type	léger

2.1.1.1 Visualisation de l'état de Grip

La visualisation de l'état courant du moteur est donnée dans l'*Ecran `Analysers` de la Web UI*.

2.1.1.2 Mise à jour de Grip

Le moteur est mis à jour à chaque nouvelle version de la GBox.

2.1.1.3 Configuration de Grip

Le moteur n'est pas configurable.

2.1.2 Présentation du moteur Goasm

Ce moteur d'analyse permet la détection et l'analyse de **shellcodes**.
Il permet l'identification de certains encodages et permet de détailler les appels système effectués.
Ce moteur donne un score de la dangerosité potentielle et nomme le shellcode détecté.
Ces données sont affichées dans le rapport détaillé et plus précisément dans les sections **TOP**, **Shellcode** (voir le *Rapport détaillé*).

Taille maximum de fichier	50 Mo
Timeout d'analyse	4-6 minutes
Type	rapide

Goasm peut être considéré comme rapide pour des petits fichiers (< 5Mo).
En cas de gros fichiers texte (> 5 Mo), la détection prend du temps car il faut parcourir le binaire à la recherche de pattern de shellcodes.
Le timeout d'analyse interne à Goasm peut donc être atteint : 4 min.
Le timeout externe au moteur, lui, est fixé à 6 min.

En cas de timeout interne :

- il y a un message d'erreur dans la partie `` `Shellcode` `` du rapport
- le moteur arrête juste de parcourir octet par octet le fichier

En cas de timeout externe (erreur survenue ou Goasm bloqué), une erreur est présente dans le rapport mentionnant un timeout (dans ce cas, relancer l'analyse).

2.1.2.1 Visualisation de l'état courant de Goasm

La visualisation de l'état courant du moteur est donnée dans l'*Ecran `Analysers` de la Web UI*.

2.1.2.2 Mise à jour de Goasm

Le moteur est mis à jour à chaque nouvelle version de la GBox.

2.1.2.3 Configuration de Goasm

Le moteur n'est pas configurable.

2.1.3 Présentation du moteur Gmalcore

Le moteur de détection **Gmalcore** permet :

- la détection des malwares par une analyse statique et heuristique multi-moteurs en temps réel des fichiers
- l'analyse via 16 moteurs Anti-Virus
- une performance d'analyse proche de 200000 fichiers par 24h
- d'obtenir le ou les noms de la menace ainsi qu'un score de menace
- une identification rapide des menaces

Les 16 moteurs antivirus sont affichés sous le nom `engine hash` dans l'interface Web ui.

Taille maximum de fichier	50 Mo
Timeout d'analyse	2 minutes
Type	léger

Les événements générés par Gmalcore sont indiqués dans la partie `` `Heuristic` `` du rapport d'analyse de la GBox.

2.1.3.1 Visualisation de l'état de Gmalcore

La visualisation de l'état courant du moteur est donnée dans l'*Ecran `Analysers` de la Web UI*.

2.1.3.2 Mise à jour de Gmalcore

Il y a des mises à jour (Updates) pour le moteur Gmalcore.
Ces mises à jour peuvent se faire de façon manuelle ou planifiée via GUM.
Voir la section *Présentation de GUM : module dédié pour la gestion des mises à jour* et en particulier la partie *Mise à jour des signatures de détection et/ou des moteurs anti-viraux (updates)*.

2.1.3.3 Configuration de Gmalcore

La configuration de Gmalcore indique les états des moteurs (états, date de la dernière mise à jour..).
L'interface graphique de la configuration est décrite dans la partie *Ecran `Gmalcore configuration`*.
La mise en œuvre de la configuration de Gmalcore est donnée dans la *Procédure de configuration du moteur Gmalcore*.

2.1.4 Présentation du moteur Gnest

Le moteur d'analyse **Gnest** permet une analyse dynamique.
Il exécute le fichier dans une machine virtuelle (sandbox) et analyse son comportement.
Suite à cela, il est possible d'extraire les données générées lors de l'analyse comme un *dump* de la mémoire, les chaînes de caractères extraites, ou une capture des communications réseau (pcap).
Dans le cas d'un fonctionnement connecté au GCenter, ce moteur est utile pour analyser en profondeur un fichier qualifié de *suspicious* ou *malicious*, lors d'une seconde analyse d'un fichier.
Cette analyse est plus lente et requiert un opérateur de niveau confirmé afin d'analyser les résultats produits.

Ces données sont affichées dans le *Rapport détaillé* et plus précisément dans les sections **TOP**, **Iocs**, **Ttps**, **Overview**, **Signatures** et **Process Tree**.

Taille maximum de fichier	50Mo
Timeout d'analyse	1 heure
Type	lent

2.1.4.1 Visualisation de l'état de Gnest

La visualisation de l'état courant du moteur est donnée dans l'*Ecran `Analysers` de la Web UI*.

2.1.4.2 Mise à jour de Gnest

Il y a des mises à jour (Updates) pour le moteur Gnest via des paquets.
Ces mises à jour peuvent se faire de façon manuelle ou planifiée via GUM.
Voir la section *Présentation de GUM : module dédié pour la gestion des mises à jour* et en particulier la partie *Mise à jour des signatures de détection et/ou des moteurs anti-viraux (updates)*.

2.1.4.3 Configuration de Gnest

La configuration de Gnest consiste :

- gérer et configurer des machines virtuelles.
  L'interface graphique de la gestion des machines virtuelles est décrite dans l'*Ecran `Gnest configuration`*.
  La mise en œuvre est donnée dans la *Procédure de configuration du moteur Gnest*.
- autoriser les machines virtuelles à avoir une interface réseau vers Internet (voir paragraphe ci-après)

L'utilisation de Gnest dans les modèles et en particulier le paramétrage de Gnest dans ces modèles permet :

- le choix de la machine virtuelle active
- l'activation de l'interface réseau de la VM
- la configuration de la durée maximum de l'exécution dans la VM
- l'activation ou non du dump mémoire à la fin des analyses réalisées par Gnest

L'interface graphique de la gestion des modèles est décrite dans l'*Ecran `Admin/Templates` de la Web UI*.
La mise en œuvre est donnée dans la *Procédure de configuration du moteur Gnest*.

2.1.4.4 Configuration des services Sandbox

La configuration consiste à :

- activer ou désactiver l'interface de sortie vers Internet
- configurer cette interface (adresse IP...)
- configurer un proxy pour accéder à Internet

Cette configuration est fait par la commande `services` du menu de configuration accessible par l'utilisateur setup.
L'interface graphique est décrite dans la partie *Commande `Services`*.

Important:

Ce proxy est indépendant du proxy accessible par la Web UI (celui-ci sert uniquement à l'installation de logiciel).

2.1.5 Présentation du moteur Gdgadetect

2.1.5.1 Présentation de l'algorithme DGA

La **GBox** embarque un moteur capable de détecter des noms de domaines ayant été générés par des DGA (Domain Generation Algorithm).
La présence de noms de domaines générés par DGA sur un réseau est un fort indicateur de compromission.
En effet, les logiciels malveillants peuvent utiliser des requêtes HTTP vers des noms de domaine générés automatiquement, afin de contacter leurs serveurs de commande et de contrôle (aussi appelés CnC, C&C ou C2).
Ces noms de domaine ont des propriétés différentes des noms de domaines légitimes.
Les approches classiques de détection comme les listes noires ne sont pas pertinentes dans le cas de domaines renouvelés en permanence.
Les simples calculs d'entropie génèrent une grande quantité de faux positifs.

2.1.5.2 Analyse

Le Machine Learning est basé sur un modèle pré-entraîné, dont l'architecture est basée sur un réseau de neurones profond de type LSTM (Long Short Term Memory networks).

2.1.5.3 Affichage des alertes DGA

L'analyse se fait dans la page `` `Quick analysis` ``.
En fonction du résultat, une icône verte ou rouge indique si c'est un DGA ou non.

2.1.5.4 Visualisation de l'état de Gdgadetect

La visualisation de l'état courant du moteur est donnée dans l'*Ecran `Analysers` de la Web UI*.

2.1.5.5 Mise à jour de Gdgadetect

Le moteur ne reçoit pas de mise à jour.

2.1.5.6 Configuration de Gdgadetect

Le moteur n'est pas configurable.

2.2 Gestion du logiciel GBox

2.2.1 Présentation de GUM : module dédié pour la gestion des mises à jour

La gestion des mises à jour s'effectue via le module nommé **GUM** (**G** atewatcher **U** pdate **M** anager). GUM permet :

- l'installation des **Upgrades** : ce sont les **mises à niveau** (opération à faire manuellement)
- l'installation des **Updates** : ce sont les **mises à jour des signatures de détection et/ou des moteurs anti-viraux**.
  le processus d'installation peut être manuel ou planifié
  Les mises à jour **Updates** n'existent que pour les moteurs Gmalcore et Gnest.
- la partie Hotfix pour l'installation des **Hotfix** : ce sont les **correctifs manuels qui modifient la solution sans avoir à procéder à un upgrade complet de la solution**
- la partie Configuration de GUM pour configurer la planification des paquets **Update**
  Pour plus d'informations, voir la *Configuration de GUM*.

La gestion des mises à jour est indiquée dans les Notes de version. Pour plus d'informations, voir la *Note de version*.
Les différentes mises à jour existantes sont :

Type de mise à jour	Pour faire quoi?	Comment	Voir pour plus d'information	Voir la procédure
Upgrade	Montée de version	Manuellement	*Mise à niveau (Upgrade)*	*Installation d'une mise à niveau (upgrade)*
Update	Mise à jour des signatures de détection et/ou des moteurs anti-viraux uniquement pour les moteurs Gmalcore et Gnest	Manuellement	*Mise à jour des signatures de détection et/ou des moteurs anti-viraux (updates)*	*Installation manuelle d'une mise à jour des signatures (update)*
		Automatiquement		*Configuration de la mise à jour automatique via GUM*
Hotfix	Application de correctif	Manuellement	*Application d'un correctif (Hotfix)*	*Installation d'un correctif (Hotfix)*

2.2.2 Mise à niveau (Upgrade)

La mise à niveau (ou upgrade) de la GBox est une montée de version et modifie de façon importante la solution.
Lors de l'application d'une mise à jour système, il sera nécessaire de redémarrer ce dernier manuellement à la fin de l'opération
Une mise à niveau incrémente le numéro de version comme par exemple 2.3.5.101 vers 2.3.5.102.

Note:

Les mises à niveau sont effectuées manuellement par l'administrateur de la solution ; aucune automatisation n'est possible dans le menu GUM.

Note:

Il est nécessaire pour l'administrateur de prendre connaissance de la Note de versions avant d'effectuer une montée de version.

Note:

Il existe aussi des paquets de montée de version incluant directement les correctifs présents dans les hotfix.
Cela permet de ne pas avoir à appliquer l'ensemble des hotfix après l'installation d'une appliance.

L'interface graphique est décrite dans l'*Ecran `Admin-GUM - Upgrade` de la legacy Web UI*.
Pour la mise en œuvre, voir l'*Installation d'une mise à niveau (upgrade)*.

2.2.2.1 Cas de mise à jour mineure

Par exemple, pour le passage de la v2.3.5.101 à la 2.3.5.101-hf1, il existe deux manières d'effectuer la mise à jour système :

- en appliquant uniquement le correctif HF1
- en effectuant une mise à niveau (Upgrade)

Ces deux solutions sont équivalentes.

2.2.2.2 Dans le cas d'une mise à jour majeure

Par exemple, pour le passage de la v2.3.5.101 vers la 2.3.5.102, seule la mise à niveau est applicable.
Pour la mise en œuvre, voir l'*Installation d'une mise à niveau (upgrade)*.

2.2.2.3 Chemin de mise à niveau

La règle générale concernant les chemins de mise à jour est qu'il est nécessaire d'être sur le dernier correctif avant de réaliser une montée de version.
Dans le cas contraire, cela sera notifié dans la Note de versions de la version concernée.

2.2.3 Mise à jour des signatures de détection et/ou des moteurs anti-viraux (updates)

Les mises à jour de signatures ou **updates** correspondent aux mises à jour des moteurs de détection de la GBox.
Il existe 3 types de paquets de mise à jour :

- les paquets Gmalcore (*latest_malcore*) : ces paquets contiennent uniquement les mises à jour des moteurs et des bases des antivirus utilisés par Malcore
- les paquets sandbox (*latest_sandbox*) : ces paquets contiennent des mises à jour des signatures et des modules utilisés par les sandbox du moteur Gnest
- les paquets complets (*latest_full*) : ces paquets sont une combinaison des 2 précédents paquets

Ces paquets peuvent être installés de façon :

- manuelle. Dans ce cas, l'interface graphique à utiliser est décrite dans l'*Ecran `Admin-GUM - Updates` de la legacy Web UI*.
  Pour la mise en œuvre, voir la procédure d'*Installation manuelle d'une mise à jour des signatures (update)*
- automatique. Cette planification doit être configurée.
  Cette configuration est décrite dans la *Configuration de GUM*.
  L'interface graphique à utiliser est décrite dans l'*Ecran `Admin-GUM - Config` de la legacy Web UI*.
  Pour la mise en œuvre de la planification , voir la procédure de *Configuration de la mise à jour automatique via GUM*.

2.2.4 Application d'un correctif (Hotfix)

Le hotfix permet d'appliquer un ou plusieurs correctifs sans avoir à procéder à un mise à niveau complète de la solution.
De ce fait, le redémarrage n'est pas nécessaire.
L'application d'un correctif doit être effectuée dans l'ordre (par exemple v102 -> v102-hf1 -> v102-hf2 -> ...).

Note:

Dans la majorité des cas, les correctifs ne nécessiteront pas de redémarrage du service web.

L'interface graphique est décrite dans l'*Ecran `Admin-GUM - Hotfix` de la legacy Web UI*.
Pour la mise en œuvre, voir la procédure d'*Installation d'un correctif (Hotfix)*.

2.2.5 Configuration de GUM

La configuration de GUM consiste à configurer la planification des paquets de mise à jour (**updates**).
Les éléments à configurer sont :

- l'activation de cette fonctionnalité
- le mode de mise à jour
- les informations de la planification (jour, heure et fréquence)
- l'adresse du dépôt où télécharger les paquets
- l'authentification d'accès à ce dépôt

L'interface graphique est décrite dans l'*Ecran `Admin-GUM - Config` de la legacy Web UI*).
Pour la mise en œuvre, voir la procédure de *Configuration de la mise à jour automatique via GUM*.

2.2.5.1 Différents modes de mises à jour

Les modes peuvent être :

- mise à jour **Online** : les paquets sont téléchargés directement sur Internet depuis les sites GATEWATCHER
- mise à jour **Local** : les paquets sont téléchargés depuis un dépôt local

---

2.2.5.1.1 Mise à jour Online

La mise à jour **Online** se fait automatiquement depuis le site https://update.gatewatcher.com/ et https://gupdate.gatewatcher.com.

2.2.5.1.2 Mise à jour Local

Afin de répondre à des contraintes de sécurité particulières, la GBox est capable d'aller chercher ses mises à jour sur un dépôt local préalablement configuré pour recevoir les paquets.
Ce dépôt local est défini dans l'*Ecran `Admin-GUM - Config` de la legacy Web UI*.

2.2.6 Note de version

Les notes de version (ou *Release Note*) contiennent la liste des changements apportés par la version donnée, la liste des problématiques connues mais également des notes importantes liées au processus d'upgrade.
Les notes de version sont référencées dans le tableau suivant.

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/

2.3 Utilisation des données

Pour que la solution TRACKWATCH / AIONIQ puisse fonctionner correctement, la GBox travaille avec des fichiers de logs.
Lors d'un problème bloquant, il est nécessaire d'accéder aux journaux de la solution afin de résoudre ce dernier.
Ces informations sont utilisées pour le diagnostic en collaboration avec le support de GATEWATCHER.

La fonction de diagnostic permet :

- de générer les fichiers de logs puis
- de les télécharger afin d'analyse par le support de GATEWATCHER

Le fichier d'export de log peut être protégé par un mot de passe (uniquement connu par le support de GATEWATCHER).
L'interface graphique de la fonction de diagnostic est décrite dans l'*Ecran `Admin-GBox - Diagnostics` de la Web UI*.
Pour la mise en œuvre, voir la procédure de *Génération et téléchargement des fichiers pour le diagnostic*.

2.4 La gestion des archives

2.4.1 Fonctionnement

L'objet de l'analyse est de déterminer si l'archive contient des fichiers malveillants.
La GBox extrait les archives soumises pour analyse.
Le fonctionnement est le suivant :

- soumission d'une archive (somme des fichiers archivés de moins de 50Mo)
- l'utilisateur peut fournir le mot de passe de l'archive via l'interface graphique ou l'api (il faut que le mot de passe soit le même à tous les niveaux de l'archive)
- la GBox tente d'extraire l'archive avec le mot de passe :
  - avec une protection contre les zipbombes
  - avec une protection contre les archives malicieuses
  - si l'archive extraite fait plus de 50Mo, l'extraction est stoppée et un message d'erreur est retourné indiquant un fichier trop gros: rien ne sera analysé
  - si l'archive est trop profonde par rapport à la profondeur configurée dans la GBox, l'analyse porte sur les fichiers correspondants à la profondeur, configurée (3 niveaux max : zip de zip au maximum)
  - si le mot de passe ne correspond pas, un message d'erreur est retourné
  - si l'archive contient trop de fichiers par rapport à ce qui a été configuré dans la GBox (10 fichiers max), un message d'erreur est retourné: rien n'est analysé
- une analyse "parente" est créée, elle représente le fichier d'archive (avec son empreinte et l'empreinte de l'analyse) et pointe vers les analyses "enfant" (image de rapport de parent plus bas)
  - elle n'a pas état du moteur d'analyse, car rien n'est analysé
  - elle a juste un résultat global
  - elle n'affiche pas le contenu des erreurs des enfants
- une analyse "enfant" est créée par fichier enfant trouvé dans l'archive, elle est liée à l'analyse parente (image de rapport d'analyse enfant plus bas)
- quand toutes les analyses "enfant" sont finies, l'analyse parente est mise à jour
  - son score équivaut au maximum du score des "enfants"
  - son état équivaut à l'état global des "enfants"
    - si 1 ou + "enfant" "en cours", alors l'analyse parente est "en cours"
    - si 1 ou + "enfant" "en erreur", alors "en erreur"
    - si tous les "enfants" sont "finis" sans erreurs alors "fini"
- il n'y a pas de PDF ou de rapport regroupant tous les enfants, il faut regarder sur chaque analyse enfant pour avoir le rapport

2.4.2 Formats supportés

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

2.4.3 Définition du mot de passe des archives

Le mot de passe pour l'analyse d'une archive avec mot de passe se définit dans l'*Ecran `New analysis` de la Web UI*.

2.5 Fichiers analysables par la GBox

2.5.1 Types de fichiers supportés

- .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 (géré comme une archive)
- .tar

2.5.2 Types de fichiers non supportés

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

2.5.3 Taille

La taille du fichier que l'utilisateur charge ne doit pas dépasser 50Mo.

2.5.4 Droits

L'utilisateur doit être membre du groupe **Operators** pour pouvoir analyser les fichiers.

2.6 Gestion des GApps

Les GApps représentent les différents services.
Il peut être nécessaire dans certains cas de devoir les redémarrer : se référer à la procédure de la *Commande `Gapps`*.

Pour le service Malcore, il est possible de forcer le redémarrage ou la réinstallation.
Pour les services Sandbox du moteur Gnest, il est possible de gérer l'interface réseau de sortie vers Internet.
Pour l'ensemble de ces services, se référer à la procédure de la *Commande `Services`*.

2.7 Résultats et rapports d'analyse

2.7.1 Liste de rapports d'analyse

Les résultats des analyses sont représentés sous forme de liste (mis à jour toutes les 30 secondes) où chaque ligne correspond à une analyse avec, entre autres :

- les caractéristiques du fichier
- un score d'analyse globale
- le nom de la menace
- le statut global de l'analyse (Done ou Error)

L'ensemble des informations ainsi que l'interface graphique sont donnés dans l'*Ecran `Reports` de la Web UI*.
De plus, sont présents :

- un lien vers le rapport au format pdf
- un lien vers le détail du rapport

Pour la procédure d'analyse d'un rapport, voir la *Procédure rapide pour analyser un fichier*.

2.7.2 Détails du rapport

Le rapport d'analyse comporte toutes les informations extraites du fichier soumis par les différents moteurs d'analyse.
Le rapport comprend :

- un résumé de l'analyse indiquant le score de menace, les moteurs impliqués, l'état global (sain, suspect ou malicieux)
- ainsi que les informations sur l'analyse en elle-même (nom du template, identifiant de l'analyse et date) et le fichier (nom, hash)

Trois boutons sont présents :

- `SAMPLE` pour télécharger le fichier analysé
- `REPORT` pour télécharger le rapport au format PDF
- `RETRY` pour rejouer l'analyse de ce fichier (avec ce template ou un autre)

L'ensemble des informations composant le rapport et la présentation de l'interface graphique sont donnés dans le paragraphe *Rapport détaillé*.

2.8 API

2.8.1 Présentation

L'API (Application Programming Interface) est l'ensemble des endpoints (appelés aussi ressources ou fin d'URL).
Chacun de ces endpoints permet d'effectuer une action sur la GBox et retourner des informations et ceci sans avoir à passer par l'interface graphique GBox.
Ceci facilite le partage et l'intégration de fonctionnalités et des données de la GBox dans des architectures existantes.

Chacun de ces endpoints a une syntaxe simple.
Ces endpoints sont prédéterminées : la liste de ces endpoints est limitée et est affichée par thème (analysers...).

Note:

La liste des endpoints est donnée dans le paragraphe *Liste des endpoints*.

L'exécution de ces endpoints peut se faire :

- via SWAGGER (*Utilisation via l'interface graphique swagger*) :
  ceci permet l'utilisation des endpoints et de comprendre son paramétrage et pouvoir tester son exécution et d'analyser ses résultats
- via CURL (*Utilisation via CURL*) : ceci permet d'exécuter directement une requête Curl et de ne pas passer par l'interface graphique

---

2.8.2 Utilisation via l'interface graphique swagger

Chaque endpoint de l'API :

- effectue une opération précise. Son nom et sa description sont indiquées dans l'interface graphique (ou dans la liste *Liste des endpoints*)
- effectue une méthode parmi les quatre possibles : GET (Obtenir), DELETE (Supprimer), POST (Publier), PUT (Modifier)
- a besoin de droits d'authentification qui sont les mêmes que pour l'interface graphique (Operators ou Administrators)
- peut avoir besoin de paramètres de fonctionnement (entrée et /ou sortie) : par exemple, dans le cas d'un filtre, la valeur de ce filtre doit être indiquée.

Toutes ces informations sont visibles dans l'interface graphique swagger et sont donc, la documentation de l'ensemble de nos endpoints API.
La description d'interface graphique swagger est donnée dans la *Présentation de l'interface API GBOX*.
Pour la mise en œuvre de l'interface swagger, voir la procédure d'*Utilisation d'un endpoint API*.

Cette interface permet de :

- avoir la liste des endpoints existants (listés par thème)
- avoir le détail des paramètres éventuels pour l'exécution d'un endpoint
- avoir des informations sur le résultat attendu (modèle des données et un exemple avec des valeurs par défaut)
- exécuter des requêtes
- récupérer la commande Curl équivalente à la requête via l'API

2.8.3 Utilisation via CURL

Il est possible d'exécuter un endpoint par une commande curl.
Cette commande est accessible via l'interface graphique swagger après avoir sélectionné le endpoint, entrer les paramètres éventuels puis lancer l'exécution du endpoint.
La commande curl est affichée dans la zone `Responses`.

Note:

Envoi d'une requête pour lister les moteurs de la GBox (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"
```

où x.x.x.x est l'adresse IP de la Gbox.

2.8.4 Authentification et accès à l'API GBox

L'accès à l'interface graphique swagger se fait via l'interface GBox puis appui sur le bouton `API`.
L'authentification sur la GBox permet l'accès à l'API GBox (pour plus d'infos, voir le paragraphe *Barre de titre*).
L'utilisation de requête curl nécessite que l'authentification se fasse dans la requête.
Cette authentification se fait à l'aide des couples nom/mot de passe ou des tokens définis dans l'*Ecran `Admin-GBox - Accounts` de la Web UI*.

Chapter 3

Caractéristiques

3.1 Caractéristiques mécaniques

REFERENCE	DIMENSIONS (H x L x P)	RACKAGE	POIDS (KG)
GBOX	42,8 x 482 x 705,05mm	1 U	21,9

3.2 Caractéristiques électriques

REFERENCE	STOCKAGE LOCAL (SSD)	STOCKAGE BACKUP	EXTENSION STOCKAGE	ALIMENTATION ELECTRIQUE
GBOX	2x 960GB RAID1	2x 4 TB RAID1	Contacter GATEWATCHER	2 x 750W

3.3 Caractéristiques fonctionnelles

REFERENCE	FONCTION
GBOX	Analyse proche de 200000 fichiers par 24h

Chapter 4

Présentation des comptes

4.1 Liste des comptes

Il y a deux interfaces graphiques pour l'utilisateur :

- le menu de configuration (GUI)
- l'interface web (Web UI)

Pour chacune des deux interfaces graphiques, des comptes utilisateurs existent.

4.2 Présentation du compte setup du menu de configuration

4.2.1 Compte du menu de configuration

L'utilisateur à utiliser est : **setup**.
Le mot de passe par défaut est : **default**.

4.2.2 Principes associés

4.2.2.1 Mode d'authentification

L'authentification d'un utilisateur s'effectue par un couple identifiant / mot de passe.

4.2.2.2 Gestion des mots de passe

Il est possible de changer le mot de passe du compte **setup** depuis la GUI.
Voir la rubrique *Commande `Password`*.

4.2.3 Fonctions autorisées au compte setup

Depuis le compte **setup**, il est possible d'utiliser l'ensemble du menu de configuration (GUI).
Le menu de configuration est décrit dans la *Présentation du menu de configuration*.
Les fonctions autorisées sont décrites dans les *Cas d'utilisation du menu de configuration: compte setup*.

4.3 Présentation des comptes de l'interface web et de leurs gestions

L'interface web permet d'accéder à :

- la création de modèles d'analyse
- l'analyse des fichiers
- l'accès et la gestion des rapports d'analyse
- la gestion des utilisateurs et des groupes associés
- l'historique des authentifications, des créations/suppressions de compte et des changements de droits sur la plate-forme

---

4.3.1 Comptes, groupes et droits de l'interface web

Il est possible de créer des comptes utilisateurs ayant chacun des droits différents.
Ces droits sont définis par des groupes.
Chaque utilisateur peut donc appartenir à un ou plusieurs groupes et donc hérite des droits du groupe.

Dans l'interface web, il existe deux types de groupes donc de droits différents :

- Operators
- Administrators

Des comptes génériques ont été définis avec des niveaux de droits listés ci-après :

Compte...	Type de droits ou groupe	Destiné à un...
`operator`	Operators	analyste
`administrator`	Administrators	administrateur
`admin`	Operators et Administrators	accès à toutes les fonctionnalités de l'analyste et de l'administrateur

---

4.3.2 Fonctions autorisées pour les membres du groupe Operators

Les membres du groupe **Operators** ont accès aux fonctions de détection et des rapports correspondants.
A contrario, les menus dédiés à l'administration de l'équipement ne seront pas accessibles.

4.3.3 Fonctions autorisées pour les membres du groupe Administrators

Les membres du groupe **Administrators** ont accès aux fonctions d'administration de l'équipement.
A contrario, les menus dédiés à l'exploitation de l'équipement ne seront pas accessibles.

4.3.4 Fonctions autorisées au compte admin

Depuis le compte **admin**, il est possible d'accéder à l'ensemble des fonctionnalités présentes.

4.3.5 Tableaux récapitulatifs des droits par groupe

4.3.5.1 Accès aux icônes

Icône	Description	Membres du groupe Operators	Membres du groupe Administrators
bouton de changement de thème	Changement du thème courant Voir la *Barre de titre*	accès	accès
API	Interface Gatewatcher API Voir l'*Accès à l'interface Gatewatcher API*	accès limité	accès
bouton du compte courant	Gestion du compte courant Voir la *Gestion du compte courant, membre du groupe Operators*	accès, voir la *Gestion du compte courant, membre du groupe Operators*	accès, voir la *Gestion du compte courant, membre du groupe Administrators*

4.3.5.2 Accès aux commandes du Menu Général

Menu	Description	Operator	Administrator
logo GATEWATCHER Home	Page `home` ,vue générale du GCenter, Voir l'*Ecran `Home` de la Web UI*	accès	pas accès
`New analysis`	Page `New analysis` Voir l'*Ecran `New analysis` de la Web UI*	accès	pas accès
`Reports`	Page `Reports` Voir l'*Ecran `Reports` de la Web UI*	accès	pas accès
`Templates`	Page `Templates` Voir l'*Ecran `Admin/Templates` de la Web UI*	pas accès	accès
`Analysers`	Page `Analysers` Voir l'*Ecran `Analysers` de la Web UI*	pas accès	accès
Admin	Menu des fonctions d'administration, voir le tableau ci-après	pas accès	accès

4.3.5.3 Accès aux commandes du Menu Admin : a revoir

Sous menu	Description	Operator	Administrator
GUM commande Config	page `GUM configuration` de l'Interface traditionnelle Voir l'*Ecran `Admin-GUM - Config` de la legacy Web UI*	pas accès	accès
GUM commande Updates	Interface traditionnelle page `Updates` Voir l'*Ecran `Admin-GUM - Updates` de la legacy Web UI*	pas accès	accès
GUM commande Hotfix	Interface traditionnelle page `Hotfix` Voir l'*Ecran `Admin-GUM - Hotfix` de la legacy Web UI*	pas accès	accès
GUM commande Upgrade	Interface traditionnelle page `Hotfix` Voir l'*Ecran `Admin-GUM - Upgrade` de la legacy Web UI*	pas accès	accès
GBox commande Diagnostics	Interface traditionnelle page `Diagnostics` Voir l'*Ecran `Admin-GBox - Diagnostics` de la Web UI*	pas accès	accès
GBox commande Accounts	Interface traditionnelle page `Accounts` Voir l'*Ecran `Admin-GBox - Accounts` de la Web UI*	pas accès	accès
GBox commande Users management	Interface traditionnelle page `Users management` Voir l'*Ecran `Admin-GBox- Users management` de la Web UI*	pas accès	accès
GBox commande Configuration	Interface traditionnelle page `Configuration` Voir l'*Ecran `Admin-GBOX-Configuration` de la Web UI :*	pas accès	accès

4.3.6 Principes associés

4.3.6.1 Mode d'authentification

L'authentification d'un utilisateur s'effectue avec un identifiant et un mot de passe.

4.3.6.2 Gestion des mots de passe

Le compte courant gère son propre mot de passe mais potentiellement aussi d'autres comptes en fonction des droits données par son groupe.
Le détail est donné dans le tableau ci-après :

Utilisateur	peut modifier le mot de passe du		
	groupe Operators	groupe Administrators	admin
compte operator	uniquement son propre compte	Non	Non
membre du groupe Administrators	X	X	X
compte type admin	X	X	X

4.3.6.2.1 Modification de son propre mot de passe

L'interface graphique est décrite dans le paragraphe *Barre de titre*.
Pour un mot de passe du groupe Operators, voir la procédure de *Modification du mot de passe du compte courant*.
Pour un mot de passe du groupe Administrators, voir la procédure de *Modification du mot de passe du compte courant*.

4.3.6.2.2 Gestion par l'administrateur des mots de passe des autres comptes

L'interface graphique est décrite dans l'*Ecran `Admin-GBox - Accounts` de la Web UI*.
Pour la mise en œuvre, voir la procédure de *Réinitialisation du mot de passe d'un utilisateur*.

4.3.6.3 Gestion de la politique des mots de passe

Les mots de passe saisis doivent correspondre à une politique de gestion des mots de passe.
La politique comprend deux catégories :

- les paramètres généraux
- les paramètres spécifiques des mots de passe

Ces paramètres généraux sont :

- la durée de validité
- l'enregistrement des hashes des mots de passe précédents

Ces paramètres spécifiques sont les critères que doivent contenir les mots de passe (minuscule, majuscule...).

Paramètre	Valeur par défaut
Présence d'au moins une majuscule	activé
Présence d'au moins un chiffre (0 à 9)	activé
Longueur minimum du mot de passe	8 caractères
Présence d'au moins une minuscule	activé
Présence d'au moins un symbole (c.a.d ni un chiffre ni une lettre)	activé

4.3.7 Création d'utilisateurs locaux

En plus des comptes génériques, il est possible de créer des comptes utilisateurs ayant chacun des droits différents.
L'interface graphique permettant la création des utilisateurs est faite dans l'*Ecran `Admin-GBox-Users management` de la Web UI*.
Pour la mise en œuvre, voir :

- la *Création d'un utilisateur local*
- la *Modification de certaines informations d'un utilisateur local*
- la *Suppression d'un utilisateur*

4.3.8 Principe de l'audit trail

La solution enregistre les différentes actions effectuées dans l'interface web au fil du temps, ceci afin d'en assurer la traçabilité.
Cette traçabilité est effectuée pour :

- la connexion ou déconnexion des utilisateurs
- la création et la suppression de compte
- la modification des permissions d'un compte

4.3.8.1 Fonction historique des authentifications

L'historique de toutes les authentifications sur la GBox est disponible.
Pour voir la présentation de l'interface graphique, se référer à la *Partie `Authentications history` du sous menu `Accounts`*.
Pour la mise en œuvre, voir la *Visualisation de l'historique des authentifications*.

4.3.8.2 Fonction historique de toutes les créations ou suppressions

L'historique de toutes les créations ou suppressions des utilisateurs de la GBox est disponible.
Pour voir la présentation de l'interface graphique, se référer à la *Partie `Creations/Deletions history` du sous menu `Accounts`*.
Pour la mise en œuvre, voir la *Visualisation de l'historique des créations ou suppressions des utilisateurs*.

4.3.8.3 Fonction historique de toutes les modifications des droits des utilisateurs

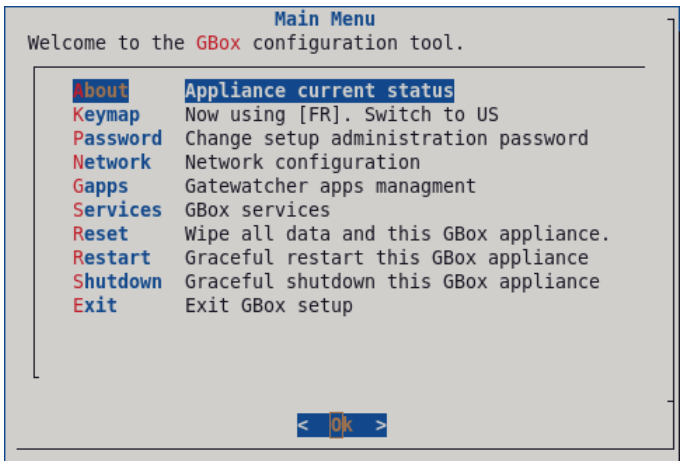
L'historique de toutes les permissions des utilisateurs sur la GBox est disponible.
Pour voir la présentation de l'interface graphique, voir la *Partie `Permissions history` du sous menu `Accounts`*.
Pour la mise en œuvre, voir la *Visualisation de l'historique de toutes les modifications des droits des utilisateurs*.

Chapter 5

Présentation des interfaces graphiques

5.1 Présentation du menu de configuration

Le menu de configuration est affiché.



Chacune des commandes présentes permet d'effectuer une action.
Ces commandes sont détaillées dans le tableau ci-dessous (y compris les liens vers les procédures correspondantes).

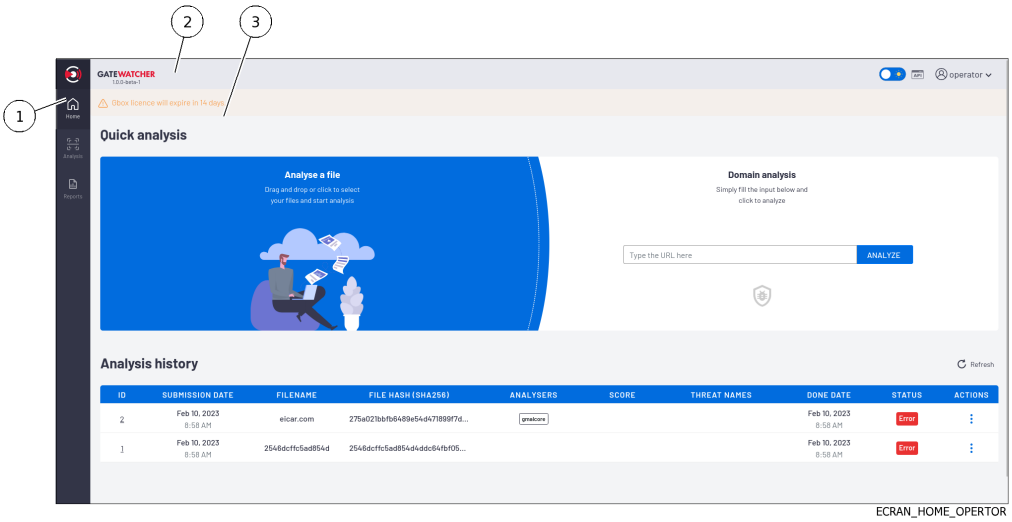
Choix	Touche raccourci	Explication	Voir
About	A	Informations générales sur la GBox (nom, version, adresse IP...)	la *Commande `About`*
Keyboard	K	Permet de changer la langue du clavier (choix US ou FR)	la *Commande `Keymap`*
Password	P	Permet de modifier le mot de passe du compte **setup**	la *Commande `Password`*
Network	N	Permet de visualiser et / ou de modifier la configuration réseau	la *Commande `Network`*
Gapps	G	Permet de redémarrer les applications de la GBox	la *Commande `Gapps`*
Services	S	Permet de redémarrer ou de remettre à défaut certains services	la *Commande `Services`*
Reset	R	Permet de permet d'effacer les données et de remettre la GBox dans son paramétrage "sortie d'usine"	la *Commande `Reset`*
Restart	R	Permet de redémarrer proprement la GBox	la *Commande `Restart`*
Shutdown	S	Permet d'éteindre la GBox	la *Commande `Shutdown`*
Exit	E	Permet de fermer le menu de configuration	la *Commande `Exit`*

5.2 Interface graphique niveau Operators via le navigateur Web

5.2.1 Présentation de l'interface graphique Web UI au niveau Operators

Important:

Dans cette partie, sont décrits les éléments graphiques accessibles aux membres du groupe Operators.



ECRAN_HOME_OPERTOR

L'écran est composé de trois parties :

Repère	Nom	Description
1	La *Barre de navigation*	Affiche les icônes utilisées pour accéder aux principales fonctions
2	La *Barre de titre*	Donne un accès direct à certaines fonctions (recherche, thème visuel...)
3	L' *Ecran central*	Affiche l'écran sélectionné par appui sur l'icône de la barre de navigation

5.2.1.1 Barre de navigation

La barre de navigation est composée de boutons pour accéder aux différentes fonctions suivantes.

Repère	Nom du bouton	Affiche
1	Logo GATEWATCHER	l'*Ecran `Home` de la Web UI* : correspond au tableau de bord principal Cette page permet d'effectuer rapidement une analyse et d'afficher l'historique des rapports effectués
2	`Home`	
3	`Analysis`	l'*Ecran `New analysis` de la Web UI* : la page `New Analysis` permet : • de configurer rapidement une analyse (sélection du modèle, saisie du mot de passe et activation du forçage) • d'effectuer l'analyse et de visualiser son rapport
4	`Reports`	l'*Ecran `Reports` de la Web UI* : correspond à la liste des rapports effectués

5.2.1.2 Barre de titre

La barre de titre est située et est composée des éléments suivants :

BARRE_TITRE_OPERATOR

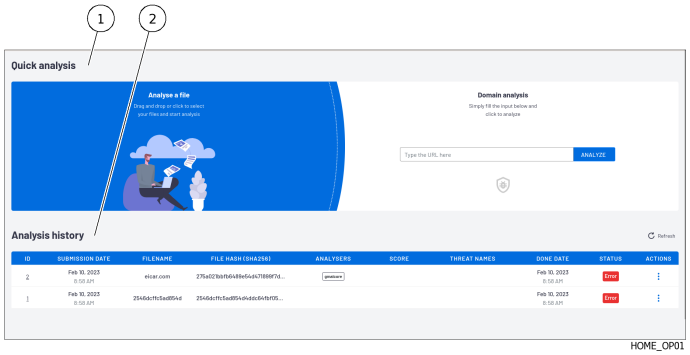
Repère	Nom	Description
1	Logo GATEWATCHER	Si appui alors retour à l'écran `Home`
2	Bouton de changement thème	Permet de changer le thème courant : choix (clair ou foncé)
3	Bouton API	Basculement vers l'interface GATEWATCHER API UI
4	Bouton du compte courant	Gestion du compte courant

5.2.1.3 Ecran central

L'écran central affiche les informations sélectionnées par un bouton de la barre de navigation.
Par défaut, c'est l'écran `Home` qui est affiché : se référer à l'*Ecran `Home` de la Web UI*.

5.2.2 Ecran `Home` de la Web UI

Après appui sur l'un des boutons `HOME` ou `GATEWATCHER` de la barre de navigation, l'écran `Home` est affiché.
Il comprend les éléments suivants :



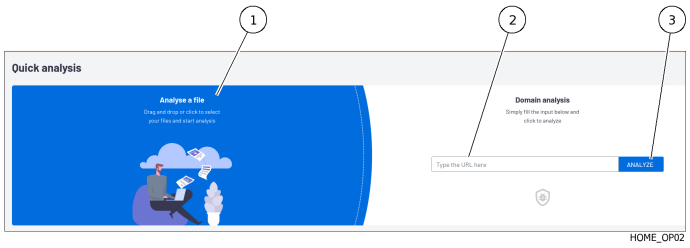
HOME_OP01

Repère	Nom
1	*Zone `Quick analysis`*
2	*Zone `Analysis history`*

5.2.2.1 Zone `Quick analysis`

Cette zone permet d'effectuer rapidement :

- soit le chargement d'un ou des fichiers depuis le PC de l'utilisateur vers la GBox (en utilisant la zone `Analyse a file`) et de lancer une analyse dont le résultat est indiqué dans un rapport
  Cette analyse sera effectuée avec le modèle par défaut défini par un membre du groupe Administrators.
  Si les fichiers sont compressés avec un mot de passe alors il faut utiliser l'*Ecran `New analysis` de la Web UI*.
- soit l'analyse un domaine (en utilisant la zone `Domain analysis`)

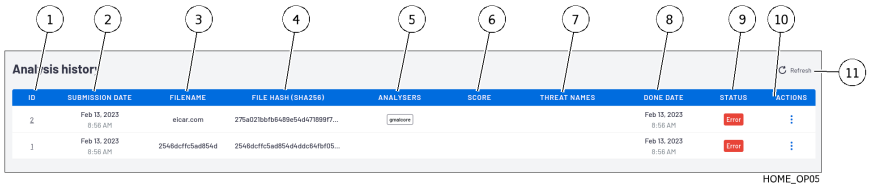


Repère	Nom
1	Zone pour déposer un fichier à analyser
2	Zone de saisie de l'URL du domaine à analyser
3	Bouton d'exécution de l'analyse du domaine

Pour analyser un fichier, voir la *Procédure rapide pour analyser un fichier*.
Pour analyser un domaine, voir la *Procédure rapide pour analyser un domaine*.

5.2.2.2 Zone `Analysis history`

Cette zone permet d'afficher l'historique des analyses effectuées.



Les analyses sont triées dans l'ordre :

- de la date du champ `DONE DATE`
- en l'absence d'informations de ce champ
  - du champ `STATUS` : d'abord les états `New` puis `In progress` puis `Done` ou `Error`

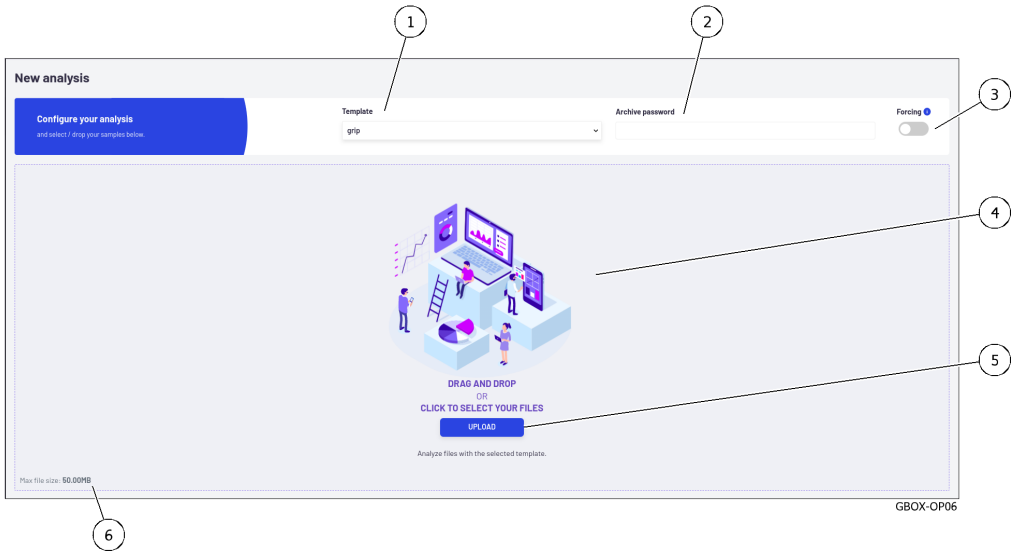
Chaque ligne correspond à une analyse différente et les informations de chaque analyse sont présentées et détaillées dans le tableau ci-après.

Repère	Nom	Description
1	`ID`	Numéro de l'analyse. Les rapports listés sont triés du plus récent au plus ancien Cliquer sur ce champ ouvre la page `Analysis report` de ce rapport
2	`SUBMISSION DATE`	Date et heure de la soumission de l'analyse
3	`FILENAME`	Nom du fichier analysé Cliquer sur ce champ copie ce nom dans le presse papier
4	`FILE HASH (SHA256)`	SHA256 du fichier Cliquer sur ce champ copie ce hash dans le presse papier
5	`ANALYSERS`	Indique le nom du (ou des) moteur qui a servi à l'analyse
6	`SCORE`	Score (Threat score) d'analyse globale calculé à partir du score d'analyse retourné par les différents moteurs
7	`THREAT NAMES`	Nom de la menace retournée par le module gmalcore (ou n/a) Cliquer sur ce champ copie ce hash dans le presse papier
8	`DONE DATE`	Date et heure de fin de l'analyse
9	`STATUS`	Etat global de l'analyse (Done, In Progress, In queue ou Error) Dans le cas d'une erreur, des informations complémentaires sont disponibles dans le rapport de l'analyse
10	`ACTIONS`	Actions possibles à effectuer : téléchargement du rapport au format pdf

Le bouton (11) permet le rafraîchissement de l'écran.
Pour la mise en œuvre, voir la *Procédure d'analyse du contenu d'un rapport*.

5.2.3 Ecran `New analysis` de la Web UI

Après appui sur le bouton `Analysis` de la barre de navigation, l'écran `New analysis` est affiché.
Il comprend les éléments suivants :



Repère	Nom	description
1	`Template`	Sélection du modèle à utiliser pour l'analyse
2	`Archive password`	Champ de saisie du mot de passe des fichiers compressés
3	`Forcing`	Sélecteur pour forcer la réanalyse et ne pas tenir compte des résultats existants
4	`DRAG AND DROP`	Zone pour déposer un fichier à analyser / zone de rapports des fichiers analysés
5	`UPLOAD`	Bouton pour ouvrir une fenêtre pour charger un (ou des) fichier(s) à analyser
6	`Max file size`	Information indiquant que la taille du fichier est limité à 50MO

Cette zone permet :

- le chargement d'un fichier depuis le PC de l'utilisateur vers la GBox (soit par un glissé / déposé ou par la sélection dans une fenêtre) puis
- l'analyse de ce fichier et d'afficher le résultat dans un rapport

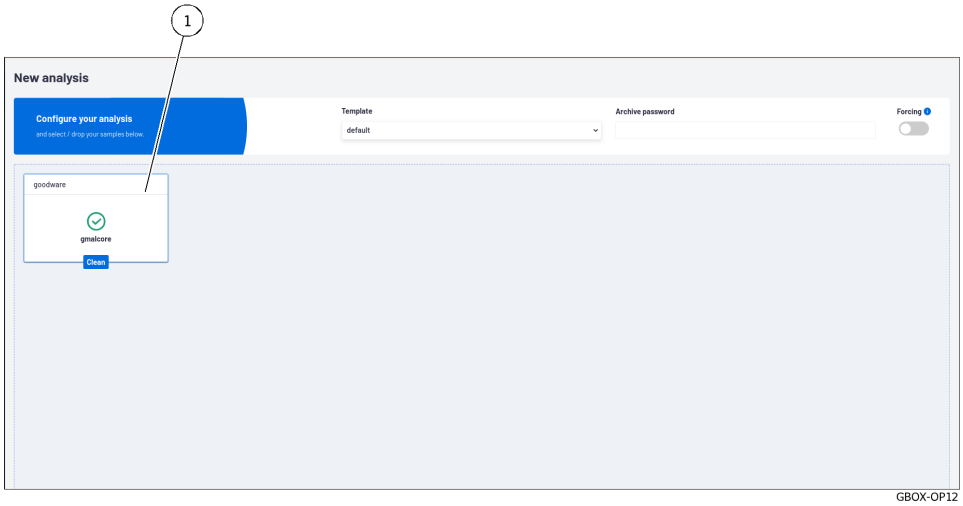
Les caractéristiques des fichiers à analyser sont décrites dans les *Fichiers analysables par la GBox*.
Les caractéristiques des fichiers compressés à analyser sont décrites dans *La gestion des archives*.
Pour la mise en œuvre, voir la *Procédure d'analyse d'un fichier dans l'écran `New analysis`*.

Note:

La sélection d'un fichier ainsi que le choix d'un modèle (Template) sont obligatoires.
Utiliser la fonction `Forcing` est optionnel.
La taille du fichier à analyser ne doit pas dépasser 50MO.
L'utilisateur doit avoir les droits **Operator** pour pouvoir analyser les fichiers.

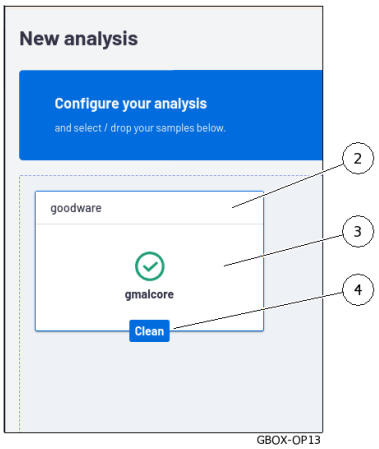
5.2.3.1 Zone d'affichage des rapports

Une fois une analyse faite, la zone (4) de la fenêtre `New analysis` affiche autant de rapports réduits (1) que de fichiers analysés.



GBOX-OP12

5.2.3.1.1 Rapport réduit



GBOX-OP13

Le rapport réduit (1) affiche :

- le nom du fichier analysé (2)
- le résultat de l'analyse (coche = ok) et le nom du moteur utilisé (ici le moteur Gmalcore), repère (3)
- le statut du résultat (4), dans cet exemple `clean`

5.2.3.1.2 Rapport complet

Cliquer sur le rapport réduit :

- ouvre sa version détaillée
- supprime le rapport réduit de la fenêtre
- enregistre le rapport dans la fenêtre rapport

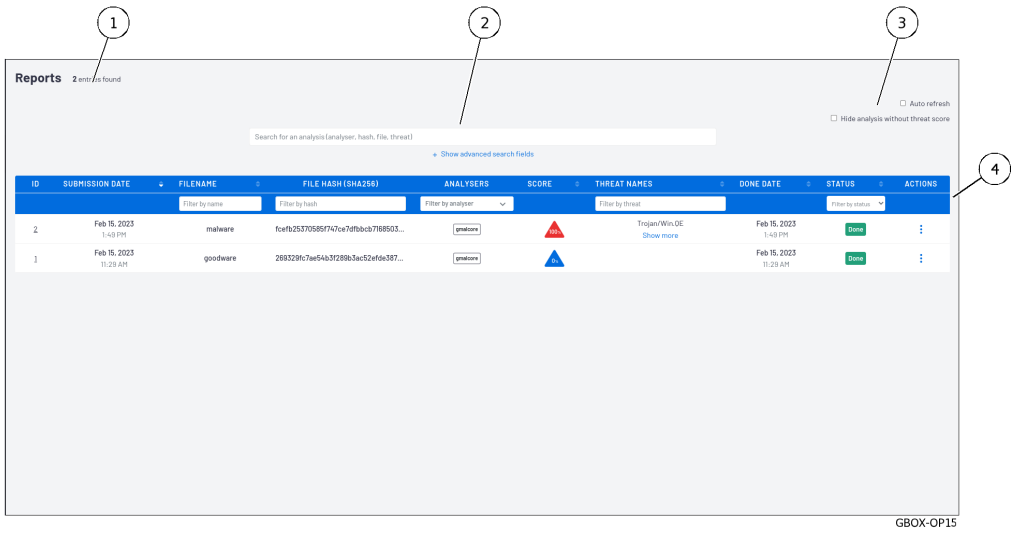
Pour plus d'informations sur les rapports, se référer à l'*Ecran `Reports` de la Web UI*.

5.2.4 Ecran `Reports` de la Web UI

5.2.4.1 Présentation de l'écran `Reports`

Après appui sur le bouton **`Reports`** de la barre de navigation, l'écran **`Reports`** est affiché.
Cet écran permet :

- de visualiser les rapports afin de pouvoir analyser les résultats
- les filtrer
- exporter des rapports en format pdf
- de télécharger le fichier analysé

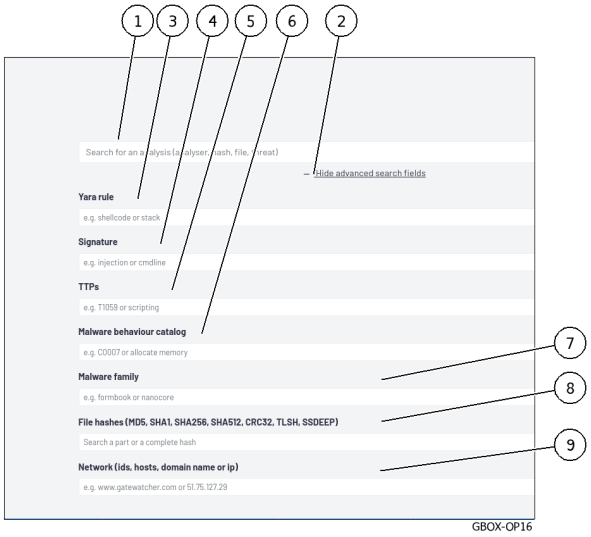


Il comprend les éléments principaux suivants :

Repère	Nom
1	Nombre de rapports présents dans l'historique (ici 2)
2	Zone permettant la recherche dans les rapports
3	Zone de configuration
4	Zone détaillée des rapports

5.2.4.2 Zone permettant la recherche

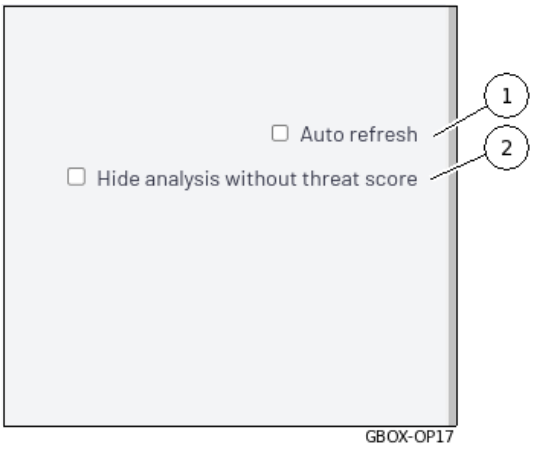
Cette zone permet de filtrer les rapports à l'aide des critères suivants.



Repère	Champ	Description
1	`Search for an analysis`	Filtre les rapports en fonction de la saisie. Le filtree se fait sur les champs `FILENAME`, `FILE HASH (SHA256)`, `THREAT NAMES`)
2	`Hide advanced search fields`	Montre / cache les champs de recherche avancés
3	`Yara rule`	Règle Yara (par exemple shellcode ou stack)
4	`Signature`	Signature (par exemple injection ou cmdline)
5	`TTPs`	Tactique, Technique, Procédure (par exemple T1059 ou script)
6	`Malware behaviour catalog`	Catalogue des comportements malveillants (par exemple C0007 ou allocation mémoire)
7	`Malware family`	Famille de logiciels malveillants (par exemple formware ou nanocore)
8	`File Hashes`	Tout ou partie du hash de fichiers (MD5, SHA1, SHA256, SHA512, CRC32, TLSH, SSDEEP)
9	`Network`	Paramètre réseau (ids, hosts, domain name or ip)

5.2.4.3 Zone de configuration

Cette zone permet de configurer l'affichage des rapports.



Repère	Nom	Description
1	`Auto refresh`	Rafraîchissement automatique
2	`Hide analysis without threat score`	Masque l'analyse sans score de menace

Note:

Si la GBox reçoit directement les fichiers sans passer par un GCenter alors les fichiers analysés avec un score nul peuvent être considérés comme sains pour le moteur utilisé.

Si la GBox reçoit les fichiers venant d'un GCenter alors les fichiers analysés ont été considérés comme suspicieux.

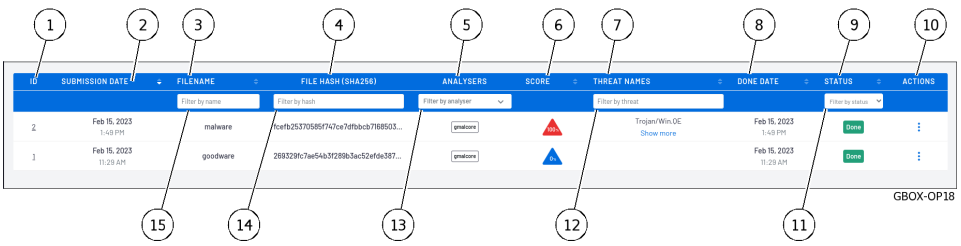
Le fait qu'ils aient un score nul ne suffit pas pour être considéré comme sain.

Un analyste doit regarder les rapports et tenir compte des moteurs utilisés (et non utilisés !) lors de l'analyse.

5.2.4.4 Zone des rapports

Cette zone permet d'afficher les détails des analyses effectuées.

Chaque ligne correspond à une analyse différente et les informations de cette analyse sont présentées et détaillées dans le tableau ci-après.



Note:

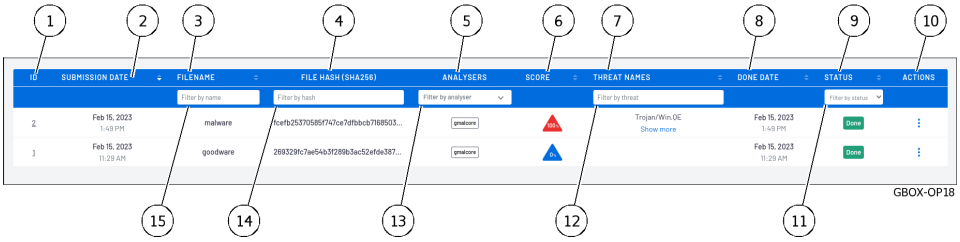
Les informations listées dans le tableau ci-dessous sont les mêmes champs que dans les rapports de l'écran `Home`.

Repère	Nom	Description
1	`ID`	Numéro de l'analyse. Les rapports listés sont triés du plus récent au plus ancien Cliquer sur ce champ ouvre la page `Analysis report` de ce rapport
2	`SUBMISSION DATE`	Date et heure de la soumission de l'analyse
3	`FILENAME`	Nom du fichier analysé Cliquer sur ce champ copie ce nom dans le presse papier
4	`FILE HASH (SHA256)`	SHA256 du fichier Cliquer sur ce champ copie ce hash dans le presse papier
5	`ANALYSERS`	Indique le nom du (ou des) moteur qui a servi à l'analyse
6	`SCORE`	Score (Threat score) d'analyse globale calculé à partir du score d'analyse retourné par les différents moteurs
7	`THREAT NAMES`	Nom de la menace retournée par le module gmalcore (ou n/a) Cliquer sur ce champ copie ce hash dans le presse papier
8	`DONE DATE`	Date et heure de fin de l'analyse
9	`STATUS`	Etat global de l'analyse (Done, In Progress, In queue ou Error) Dans le cas d'une erreur, des informations complémentaires sont disponibles dans le rapport de l'analyse
10	`ACTIONS`	Actions possibles à effectuer : téléchargement du rapport au format pdf

Les champs ci-dessous sont les champs supplémentaires permettant de faire le filtrage des rapports.

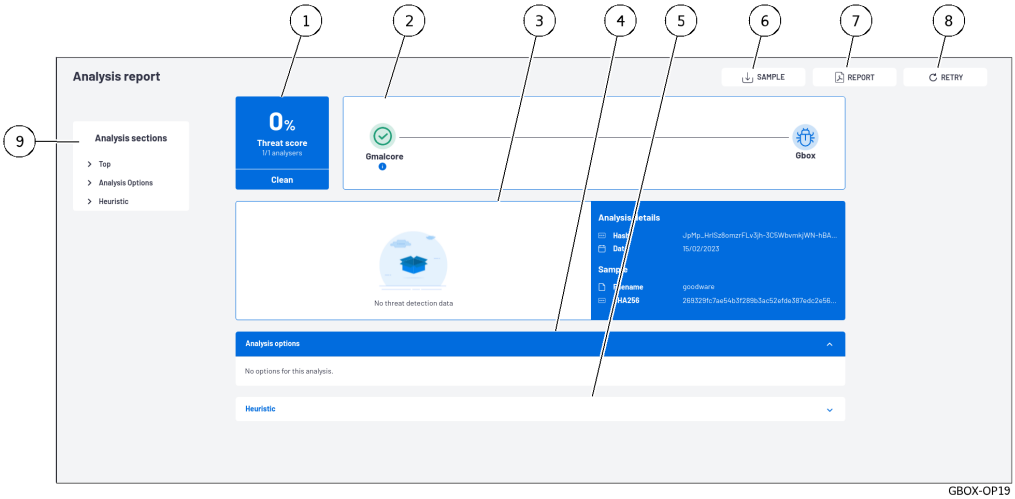
Repère	Nom	Description
11	`Filter by status`	Permet de filtrer les rapports avec ce statut à sélectionner dans la liste
12	`Filter by threat`	Permet de filtrer les rapports avec ce nom de menace à saisir
13	`Filter by analyser`	Permet de filtrer les rapports avec un nom de moteur à sélectionner dans la liste
14	`Filter by hash`	Permet de filtrer les rapports avec ce hash à saisir
15	`Filter by name`	Permet de filtrer les rapports avec le nom de fichier à saisir

5.2.4.5 Rapport détaillé



GBOX-OP18

Après appui sur l'ID (1) d'un rapport, le rapport détaillé est affiché.



GBOX-OP19

En fonction des moteurs sélectionnés dans le modèle lors de l'analyse, certaines informations peuvent être affichées. Elles sont indiquées au cas par cas.

Dans l'exemple ci-dessus, le rapport a été fait avec un modèle avec uniquement le moteur Gmalcore actif.

Le rapport d'analyse comporte toutes les informations extraites du fichier soumis aux différents moteurs d'analyse.

5.2.4.5.1 Informations présentes dans ce rapport

Les informations présentes dans ce rapport sont :

Repère	Description
1	Résumé du résultat de l'analyse indiquant : • le résultat (Threat Score) de l'analyse globale calculé à partir du score d'analyse retourné par les différents moteurs de Gmalcore - de 0% pour un fichier déclaré sain par le moteur utilisé - à 100 % valeur max pour un fichier déclaré malicieux • le nombre de moteur moteur impliqué (ici 1/1 analysers) • l'état global (sain, suspect ou malicieux) : ici Clean ou sain Un score n'est donné que pour les moteurs Gmalcore et Goasm
2	Résumé des étapes de l'analyse : • la liste des moteurs utilisés : ici Gmalcore • le résultat du chargement du fichier pour chacun des moteurs : ici pour Gmalcore, la coche indique que le chargement s'est bien passé • coté droit, le résultat de l'analyse : ici l'icône signifie OK
3	Informations comprenant : • un graphique (voir la note ci-dessous) • sur l'analyse (hash et date) • sur le fichier (nom, sha256)
4 et 5	Sections d'analyse optionnelles. Ces informations dépendent du moteur dans le modèle. Dans cet exemple, seules les sections `` `Analysis options` `` et `` `Heuristic` `` sont affichées. Cette rubrique peut être pliée / dépliée
	Informations sur l'analyse heuristique (5) : cette rubrique peut être pliée / dépliée Cette rubrique indique le résultat pour chacun des moteurs (ici les 16 moteurs du moteur Gmalcore)
6	Bouton `` `SAMPLE` `` qui permet de télécharger le fichier analysé. Le fichier téléchargé est compressé et protégé par un mot de passe (le mot de passe est **infected**) Une fois décompressé, le fichier analysé a une extension .sample
7	Bouton `` `REPORT` `` qui permet de télécharger le rapport en format pdf
8	Bouton `` `RETRY` `` qui permet de rejouer l'analyse de ce fichier (avec ce template ou un autre)
9	La section `` `Analysis sections` `` comprend des raccourcis pour ouvrir ces sections et recentrer l'affichage Ces sections donnent le détail des analyses venant des moteurs définis dans le modèle d'analyse. Ces informations permettent à un analyste d'avoir une idée plus précise de l'anatomie et du comportement du fichier lors de son ouverture/exécution Dans cet exemple, seules les sections `` `Top` ``, `` `Analysis options` `` et `` `Heuristic` `` sont affichées. Suivant la combinaison de moteurs utilisés, certaines sections peuvent être absentes de cette liste : le détail est donné dans le tableau ci-dessous

suite sur la page suivante

Table 1 – suite de la page précédente

Repère	Description
	Bouton `ALL ARTEFACTS` permet de télécharger les artefacts issus de l'analyse (dump mémoire, capture réseau (pcap), chaînes de caractères détectées) Cette section permet également de supprimer les artefacts. Ce bouton n'est présent que si le moteur Gnest est actif.

5.2.4.5.2 Liste des sections présentes dans la section `Analysis sections`

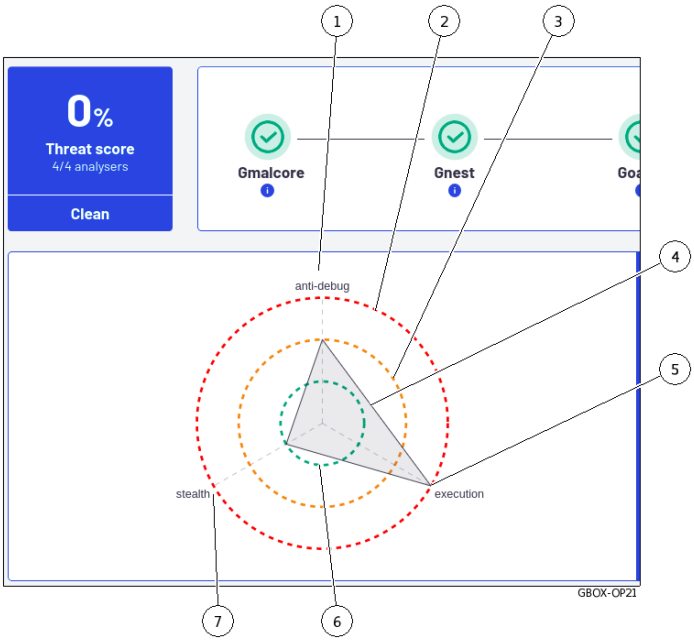
Table2: Liste des sections présentes dans `Analysis sections`

Titre de la section	Description	Est activé par le moteur
`Top`	Raccourci vers la partie supérieure du rapport soient les parties (1) à (3)	Tous les moteurs
`Analysis options`	Valeurs des options utilisées pour l'analyse	Grip et Gnest
`Iocs`	Liste des actions effectuées (fichiers, base de registres, réseau, processus...)	GNEST
`Ttps`	Les TTPs analysent le fonctionnement d'un acteur malveillant, elles décrivent comment les cyberattaquants orchestrent, exécutent et gèrent les attaques opérationnelles. Les TTPs contextualisent une menace. Elles révèlent les étapes ou les actions prises par des acteurs malveillants lors de de l'exfiltration de données par exemple.	GNEST
`Static`	Métadonnées	GRIP
`Overview`	Informations sur le fichier (taille, différents hash, type...)	GNEST
`Heuristic`	Liste des moteurs (Entry#x) et nom de la menace retournée par le module Gmalcore (ou n/a)	Gmalcore
`Shellcode`	Résultat de la détection de shellcode	GOASM
`Signatures`	Liste des signatures yara correspondant au fichier analysé	Gnest
`Process Tree`	Représentation graphique de l'arbre de processus	Gnest

5.2.4.5.3 Détails du graphique

Note:

Le graphique est disponible uniquement si Gnest fait partie du modèle (les données nécessaires au graphique sont retournées par ce moteur).



Ce graphique permet d'avoir un visuel sur la dangerosité du fichier analysé :

- la catégorie de la dangerosité est définie par les axes (1) (5) et (7) : titres et nombre d'axe sont donnés par les moteurs
- le niveau de la dangerosité est donné par les cercles concentriques.
- le cercle central (6) indique le niveau *sain*
- le cercle milieu (3) indique le niveau *suspicieux*
- le cercle externe (2) indique le niveau *malicieux*

La synthèse pour le fichier se lit sur les sommets de la forme représentée (4).
Dans l'exemple affiché, le sommet (5) indique que le fichier est :

- malicieux dans l'axe `execution` (5)
- suspicieux dans l'axe `antidebug` (1)
- sain dans l'axe `stealth` (7)

Pour l'analyse d'un rapport, voir la *Procédure d'analyse du contenu d'un rapport*.

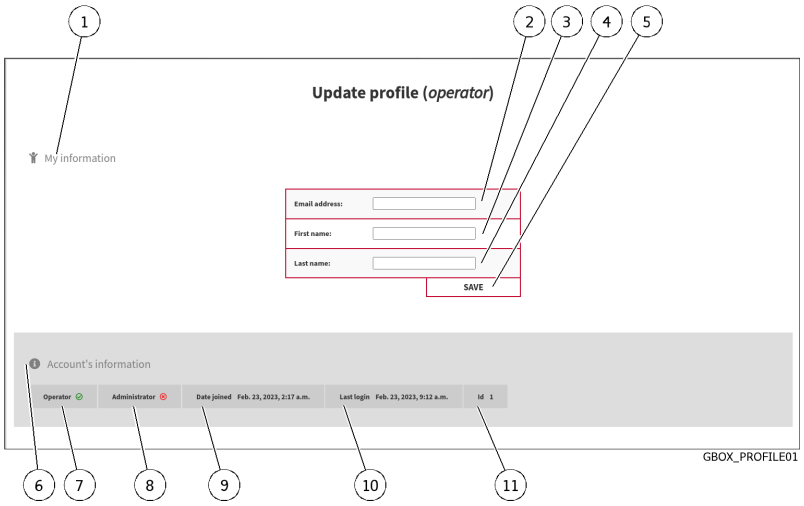
5.2.5 Gestion du compte courant, membre du groupe Operators

Après appui sur le bouton de gestion du compte courant (4), trois commandes sont disponibles :

- la commande `Edit profile` : voir l'*Ecran `Update profile`*
- la commande `Change password` : voir l'*Ecran `Change Password`*
- la commande `Logout` : voir la *Commande Logout*

5.2.5.1 Ecran `Update profile`

Après avoir cliqué sur la commande `Edit profile`, l'écran `Update profile` est affiché :

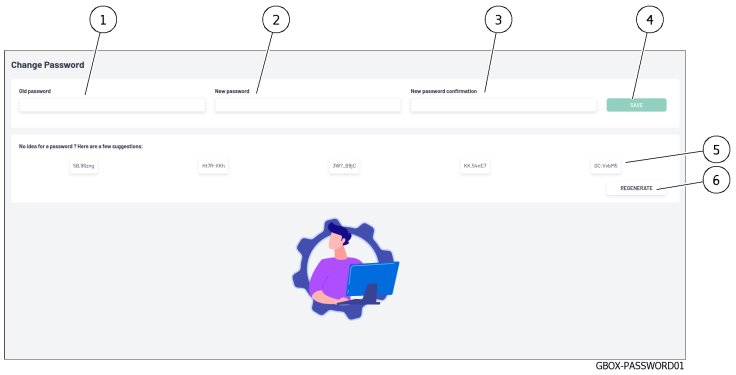


Repère	Nom	Description
1	`My information`	Zone listant les informations du compte courant
2	`Email address`	Adresse email de l'utilisateur courant
3	`First name`	Prénom de l'utilisateur courant
4	`Last name`	Nom l'utilisateur courant
5	`SAVE`	Bouton de sauvegarde de la saisie.
6	`Account's information`	Zone listant les informations de gestion du compte courant
7	`Operator`	Appartenance au groupe Operators (coche indique l'appartenance, la croix la non appartenance)
8	`Administrator`	Appartenance au groupe Administrators (coche indique l'appartenance, la croix la non appartenance)
9	`Date joined`	Date et heure de la création du compte courant
10	`Last login`	Date et heure de la dernière connexion du compte courant
11	`ID`	Numéro identifiant le compte

Pour la mise en œuvre, voir la procédure de *Modification de certaines informations de l'utilisateur courant*.

5.2.5.2 Ecran `Change Password`

Après avoir cliqué sur la commande `Change password`, l'écran `Change Password` est affiché :



Cet écran permet de changer le mot de passe du compte courant.
Cette politique de mot de passe est décrite dans la *Gestion de la politique des mots de passe*.

Repère	Nom	Description
1	`Old password`	Zone de saisie de l'ancien mot de passe
2	`New password`	Zone de saisie du nouveau mot de passe
3	`New password confirmation`	Zone de saisie de la confirmation du nouveau mot de passe
4	`SAVE`	Bouton de sauvegarde de la saisie
5	`No idea for a password ?` `Here are a few suggestions`	Cinq mots de passe sont proposés
6	`REGENERATE`	Bouton de regénération de nouveaux mots de passe

Pour la mise en œuvre, voir la procédure de *Modification du mot de passe du compte courant*.

5.2.5.3 Commande Logout

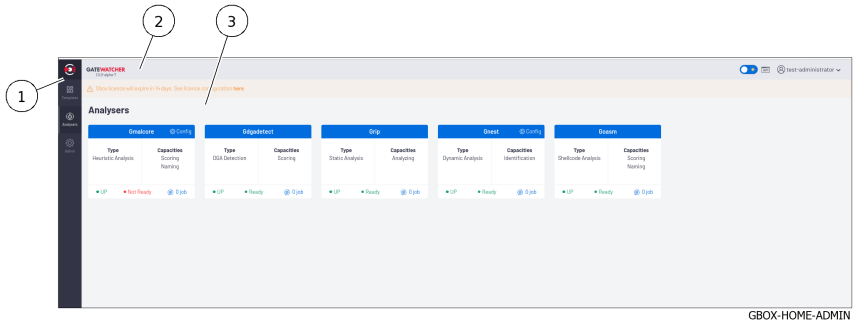
Après avoir cliqué sur la commande `Logout`, l'utilisateur courant est immédiatement déconnecté.
L'écran de connexion est affiché.
Pour la mise en œuvre, voir la procédure de *Déconnexion de l'interface web de la GBox*.

5.3 Interface graphique niveau Administrators via le navigateur Web

5.3.1 Présentation de l'interface graphique Web UI au niveau Administrators

Important:

Dans cette partie, sont décrits les éléments graphiques accessibles aux membres du groupe Administrators.



GBOX-HOME-ADMIN

L'écran est composé de trois parties :

Repère	Nom	Description
1	La *Barre de navigation*	Affiche les icônes utilisées pour accéder aux principales fonctions
2	La *Barre de titre*	Donne un accès direct à certaines fonctions (recherche, thème visuel...)
3	L'*Ecran central*	Affiche l'écran sélectionné par appui sur l'icône de la barre de navigation

5.3.1.1 Barre de navigation

La barre de navigation est composée de boutons pour accéder aux différentes fonctions.

GBOX_ICONE_

Repère	Nom du bouton	Affiche
1	Logo GATEWATCHER	L'*Ecran `Analysers` de la Web UI*
2	`Template`	L'*Ecran `Admin/Templates` de la Web UI*
3	`Analysers`	L'*Ecran `Analysers` de la Web UI* : • de faire rapidement une analyse d'un fichier • de visualiser l'historique des analyses
4	`Admin`	Voir le *Menu Admin*

5.3.1.2 Barre de titre

La barre de titre est située et est composée des éléments suivants :

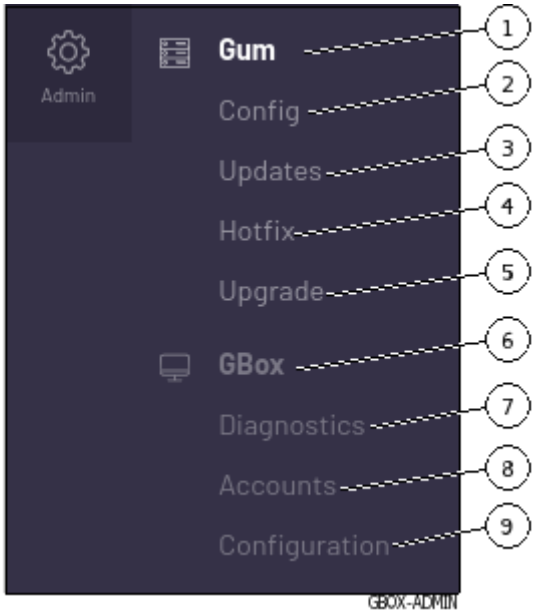
Repère	Nom	Description
1	Logo GATEWATCHER	Si appui alors retour à l'écran `Home`
2	Bouton de changement thème	Permet de changer le thème courant : choix (clair ou foncé)
3	Bouton API	Basculement vers l'interface GATEWATCHER API UI
4	Bouton du compte courant	Gestion du compte courant

5.3.1.3 Ecran central

L'écran central affiche les informations sélectionnées par un bouton de la barre de navigation.
Par défaut, c'est l'écran `Home` qui est affiché : se réferer à l'*Ecran `Analysers` de la Web UI*.

5.3.1.4 Menu Admin

Le menu est composé des éléments suivants :



Repère	Nom du menu	Nom de la commande	Affiche
1	Menu `GUM`	comprend les commandes suivantes :	
2		• `Config`	*Ecran `Admin-GUM - Config` de la legacy Web UI*
3		• `Updates`	*Ecran `Admin-GUM - Updates` de la legacy Web UI*
4		• `Hotfix`	*Ecran `Admin-GUM - Hotfix` de la legacy Web UI*
5	Menu `GBox`	comprend les commandes suivantes :	
6		• `Diagnostics`	*Ecran `Admin-GBox - Diagnostics` de la Web UI*
7		• `Accounts`	*Ecran `Admin-GBox - Accounts` de la Web UI*
8		• `Configuration`	*Ecran `Admin-GBox- Users management` de la Web UI*

5.3.2 Présentation de l'interface graphique Web traditionnelle (legacy Web UI)

5.3.2.1 Présentation de l'interface

Cette interface est l'interface traditionnelle de la solution, appelée aussi **legacy Web UI**.
Elle est composée de l'ensemble des menus de configuration.
Lors de la connexion web :

- si le compte utilisé fait partie du groupe **Operators** alors l'interface qui s'affiche est l'interface principale Web UI : l'utilisateur n'a pas accès à l'interface traditionnelle.
- si le compte utilisé fait partie du groupe **Administrators** alors l'interface qui s'affiche est l'interface principale Web UI.

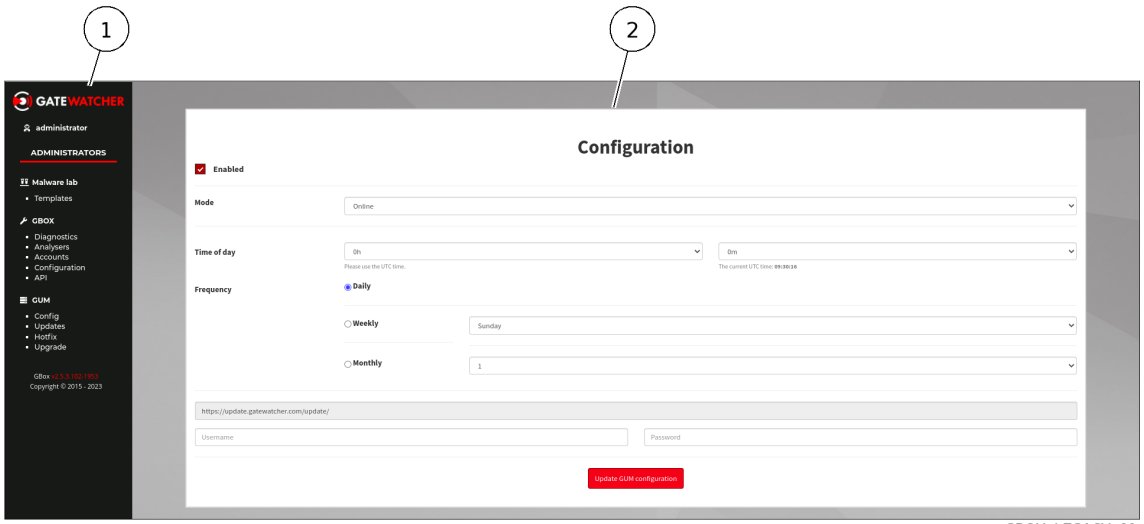
L'interface traditionnelle (legacy Web UI) est utilisée pour certaines fonctions.

Note:

Dans chacune des interfaces, il y a les mêmes commandes dans le menu qui permettent donc à l'utilisateur de lancer n'importe quelle commande quelle que soit l'interface active.

Commande du menu administrator	Interface Web ui	Interface legacy Web ui
Templates	Actif	
Analysers	Actif	
Admin	dépend de la commande est détaillé plus loin	

5.3.2.2 Description de l'interface traditionnelle



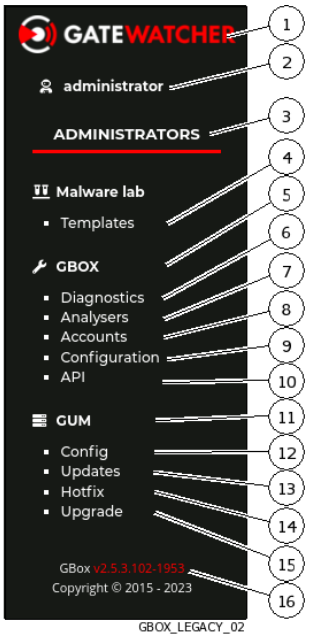
GBOX_LEGACY_01

L'écran est composé de deux parties :

Repère	Nom	Description
1	*Barre de navigation de l'interface traditionnelle*	Affiche les menus et commandes d'accès aux principales fonctions
2	*Ecran central de l'interface traditionnelle*	Affiche l'écran sélectionné par appui sur une commande de la barre de navigation. Chaque écran est nommé comme la commande associée : exemple écran `Diagnostics`

5.3.2.2.1 Barre de navigation de l'interface traditionnelle

La barre de navigation est composée de boutons pour accéder aux différentes fonctions.



GBOX_LEGACY_02

Repère	Nom	Affiche	
1	Logo GATEWATCHER	L'utilisation du bouton permet de revenir à : • l'écran `Quick analysis` pour le compte avec les droits Operators • l'écran `Analysers` pour le compte avec les droits Administrators	
2	Utilisateur courant	Indique le nom de l'utilisateur courant. L'utilisation du bouton affiche les commandes `Èdit profile`, `Change passord` et `logout` pour se déconnecter.	
3	`ADMINISTRATORS`	Cette section permet d'accéder à l'ensemble des menus d'administration. Cette section comprend les éléments suivants :	
4		La commande `Template` permet de d'accéder au menu de gestion des modèles (*Ecran `Admin/Templates` de la Web UI*)	
5		Le menu `GBox` permet d'administrer la GBox. Il est composé de :	
6			• la commande `Diagnostics` permet de générer et d'exporter les journaux systèmes du GCenter en vue d'une analyse par le support de GATEWATCHER (*Ecran `Admin-GBox - Diagnostics` de la Web UI*)
7			• la commande `Analysers` permet d'accéder à la gestion des moteurs d'analyse (*Ecran `Admin-GBox - Diagnostics` de la Web UI*)

suite sur la page suivante

Table 3 – suite de la page précédente

Repère	Nom	Affiche	
8			• la commande `Accounts` permet de gérer l'authentification sur la GBox avec une authentification locale (*Ecran `Admin-GBox - Accounts` de la Web UI*)
9			• la commande `uration` permet de gérer la configuration globale de la GBox (proxy, certificat, licence, etc) (*Ecran `Admin-GBox- Users management` de la Web UI*)
10			• la commande `API` permet d'accéder à la page Swagger de l'API de la GBox (*Accès à l'interface Gatewatcher API*)
11		Le menu `GUM` permet de configurer le système de mise à jour de logiciel. Il comprend les commandes suivantes :	
12			• la commande `Config` permet d'automatiser les mises à jour des moteurs (*Ecran `Admin-GUM - Config` de la legacy Web UI*)
13			• la commande `Updates` permet de mettre à jour la solution via un update (*Ecran `Admin-GUM - Updates` de la legacy Web UI*)
14			• la commande `Hotfix` permet d'appliquer un correctif (*Ecran `Admin-GUM - Hotfix` de la legacy Web UI*)
15			• la commande `Upgrade` permet de mettre à niveau la solution (*Ecran `Admin-GUM - Upgrade` de la legacy Web UI*)
16		GBox v2.5.3.102-1953. Dans ce champ, la version de la GBox est affichée (ici v2.5.3.102-1953)	

5.3.2.3 Ecran central de l'interface traditionnelle

L'écran central affiche les informations sélectionnées par un bouton de la barre de navigation.

5.3.3 Accès à l'interface Gatewatcher API

L'interface API permet d'interagir avec les endpoints API disponibles.
L'accès à cette interface est disponible dans le barre de titre de l'interface principale.

Après avoir cliqué sur le bouton (3), un nouvel onglet s'ouvre avec l'interface API.
Dans cette interface, l'ensemble des endpoints API sont disponibles et utilisables.
L'utilisation des différents endpoints est soumise aux mêmes droits que dans les interfaces Web.

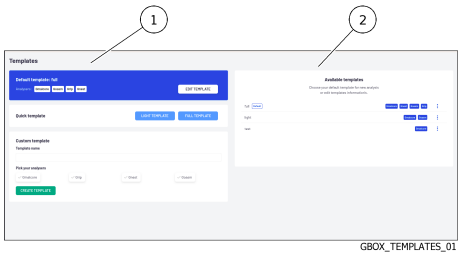
Note:

Une fonctionnalité nécessitant des droits administrateurs ne pourra être utilisée par un utilisateur n'ayant que les droits opérateurs.

Pour plus d'informations sur l'interface API, se référer à l'*Interface graphique API*.

5.3.4 Ecran `Admin/Templates` de la Web UI

Après appui sur la commande `Templates`, l'écran suivant est affiché.

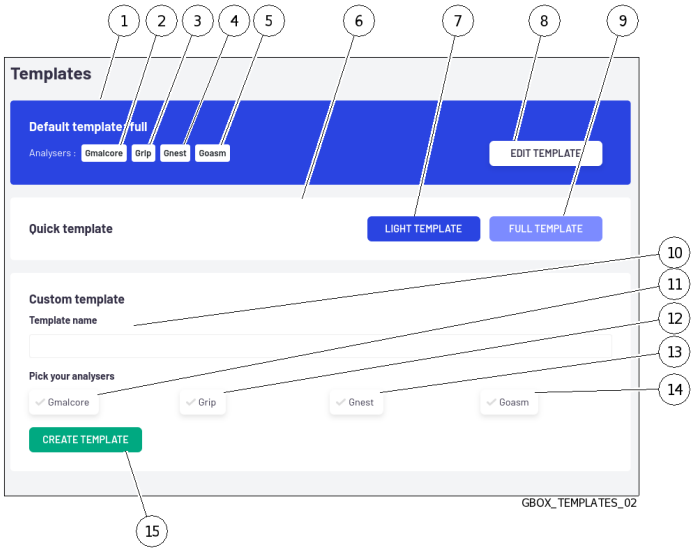


Repère	Zone	Fonction
1	Création de modèles	Cette zone permet de créer des modèles (templates) utilisables pour l'analyse des fichiers accessibles à l'opérateur
2	Gestion de modèles	Cette zone (`Available templates`) permet de gérer les modèles existants

---

5.3.4.1 Zone Création de modèles

La zone de création des modèles comprend 2 parties.



Cette zone comprend :

- partie `Defaut template` et `Quick template` : *La partie Création du modèle par défaut*
- partie `Custom template` : *La partie Création d'un modèle personnalisé*

Pour la mise en œuvre, voir la procédure de *Création d'un modèle d'analyse*.

5.3.4.1.1 La partie Création du modèle par défaut

Cette partie est composée des parties `Defaut template` et `Quick template`.
Elle permet de paramétrer les modèles qui pourront devenir le modèle par défaut utilisé par l'opérateur dans la recherche de menaces.
La phase de création de ces modèles se fait à l'aide des éléments décrits ci-dessous.

Astuce:

La phase du choix du modèle par défaut parmi les modèles présents se fait dans la zone `Available templates`.

Important:

Il est indispensable d'avoir au minimum un modèle défini afin que les opérateurs puissent effectuer des analyses.

Repère	Nom	Fonction
1	`Default template`	Cette zone permet de définir le modèle par défaut (`Default template`) Si un modèle par défaut est défini, alors son nom est affiché. Dans cet exemple, `Default template : full` signifie que le nom du modèle par défaut est full Si aucun modèle par défaut n'est défini alors le message suivant est affiché : `Default template : No default template` Les moteurs définis dans le modèle par défaut sont listés : dans cet exemple, ce sont les items (2) à (5)
2		• Dans cet exemple, le moteur (Analyser) `Gmalcore` est visible et donc actif dans le modèle par défaut.
3		• Dans cet exemple, le moteur (Analyser) `Grip` est visible et donc actif dans le modèle par défaut
4		• Dans cet exemple, le moteur (Analyser) `Gnest` est visible et donc actif dans le modèle par défaut
5		• Dans cet exemple, le moteur (Analyser) `Goasm` est visible et donc actif dans le modèle par défaut
8		• Le bouton `EDIT TEMPLATE` permet d'editer le modèle par défaut. Il est possible de changer les moteurs actifs, de les configurer
6	`Quick template`	Cette zone permet rapidement un modèle en cliquant uniquement sur un des 2 boutons suivants :
7		• le bouton `LIGHT TEMPLATE` crée un modèle avec uniquement les moteurs Gmalcore et Goams d'où le terme modèle léger.
9		• le bouton `FULL TEMPLATE` crée un modèle avec les moteurs actifs d'où le terme modèle complet. Les paramètres des moteurs Grip et Gnest sont les paramètres par défaut. La liste des paramètres par défaut est donnée plus loin.

Note:

Il ne peut y avoir qu'un seul modèle nommé `light` et un seul modèle nommé `full`.

5.3.4.1.2 La partie Création d'un modèle personnalisé

Repère	Nom	Fonction
10	`Template name`	Cette zone permet de définir le nom d'un modèle personalisé Le type de modèle en cours est listé. Dans cet exemple, `Default template : full` signifie que le modèle en cours est du type complet (full)
11	`Gmalcore`	Permet d'activer le moteur Gmalcore. Dans l'exemple, le moteur Gmalcore est inactif
12	`Grip`	Permet d'activer le moteur Grip. Dans l'exemple, le moteur Grip est inactif
13	`Gnest`	Permet d'activer le moteur Gnest. Dans l'exemple, le moteur Gnest est inactif
14	`Goasm`	Permet d'activer le moteur Goasm. Dans l'exemple, le moteur Goasm est inactif
15	`CREATE TEMPLATE`	Le bouton `EDIT TEMPLATE` ouvre une fenêtre de paramétrage du modèle à créer avec les options préselectionnées

---

5.3.4.1.2.1 Paramètres de Grip

Le moteur Grip doit être configuré en sélectionnant le type d'analyse (`Analysis type`): {light|heavy} pour déterminer les données extraites du fichier analysé.

Note:

L'analyse par défaut est : light

Données extraites	light	heavy
taille de l'archive	X	X
librairies utilisées	x	x
informations sur le point d'entrée (entrypoint) du binaire	x	x
informations générales	x	x
chaînes de caractères		x
imports / exports		x
sections du binaire		x

5.3.4.1.2.2 Paramètres de Gnest

Le moteur Gnest doit être configuré pour ce modèle :

Paramètre	Signification	Valeurs	Valeurs par défaut
`VM`	Choix de la VM active. Seule la VM sélectionnée est activée dans ce modèle Les paramètres suivant concernent uniquement la VM sélectionnée ou toutes les VMs (choix `any`)	any ou default	any
`Analysis duration`	Durée maximum de l'exécution dans la VM	100s à 300 s	100s
`Network`	Activation de l'interface réseau de la VM	None ou Internet	None
`Memory dump`	Active ou non le dump mémoire à la fin des analyses réalisées par Gnest Danger, utilisation élevée du disque : Le dump mémoire est téléchargeable depuis la page **Reports - List all** à partir des artefacts de l'analyse	No ou Yes	No

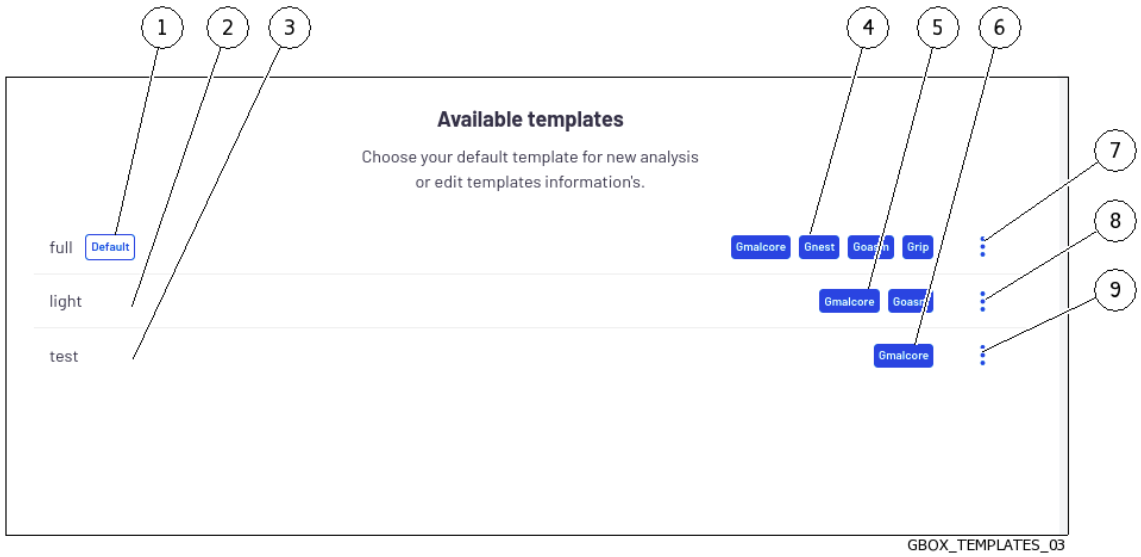
Avertissement:

L'activation de l'option `Memory dump` implique la sauvegarde sur disque de l'intégralité de la mémoire (4Go).

Afin d'éviter de saturer l'espace disque, il est préférable d'activer cette option sur des modèles spécifiques et non sur le modèle par défaut.

Il est cependant possible de supprimer ces dumps via la suppression des artefacts disponibles dans les rapports ou via l'API.

5.3.4.2 Zone Gestion de modèles



La zone Gestion des modèles permet de gérer les modèles existants.

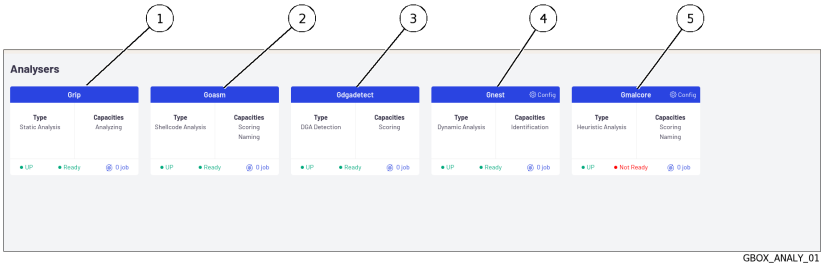
Repère	Nom	Fonction
1	`full`	Ce modèle dont le nom est full est défini comme celui par defaut (présence du champ `Default`)
4		Liste des moteurs actifs dans ce modèle (ici, dans le cas du modele complet, tous les moteurs sont actifs)
7		Menu de gestion de ce modèle (dans le cas du modèle par défaut seule la commande `Edit` est disponible)
2	`light`	Ce modèle est celui dont le nom est `light`
5		Liste des moteurs actifs dans ce modèle (ici, dans le cas du modele léger, seuls les moteurs Gmalcore et Goasm sont actifs)
8		Menu de gestion de ce modèle : les commandes `Set as default`, `Edit` et `Remove` sont disponibles
3	`test`	Ce modèle est un exemple de modèle personnalisé
6		Liste des moteurs actifs dans ce modèle (ici, dans le cas du modele léger, seuls les moteurs Gmalcore et Goasm sont actifs)
9		Menu de gestion de ce modèle : les commandes `Set as default`, `Edit` et `Remove` sont disponibles

Un modèle d'analyse peut-être supprimé en cliquant sur le bouton `Remove`.
Lors de la suppression d'un modèle d'analyse, les analyses lancées avec ce modèle sont conservées, ainsi que le nom du modèle au moment de sa suppression.
Pour la mise en œuvre, voir la procédure de *Gestion des modèles d'analyse*.

5.3.5 Ecran `Analysers` de la Web UI

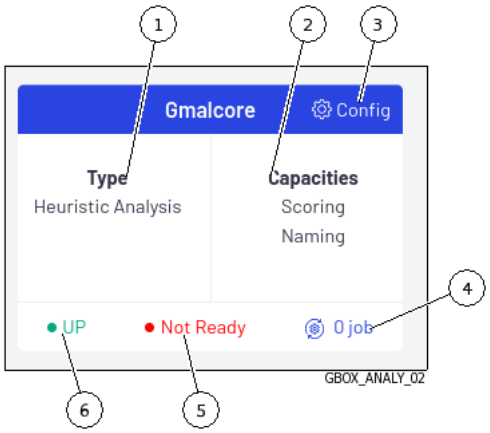
Cet écran affiche les états des différents moteurs d'analyse.

Après appui sur la commande `Analysers`, l'écran suivant est affiché.



Repère	Moteur	Fonction du moteur
1	*Moteur Grip*	Analyse statique
2	*Moteur Goasm*	Détection des shellcodes
3	*Moteur Gdgadetect*	Détection de noms de domaine
4	*Moteur Gnest*	Analyse dynamique dans une machine virtuelle
5	*Moteur Gmalcore*	Analyse statique et heuristique

Pour chacun des moteurs, les informations suivantes sont affichées :


1
2
3
Gmalcore
Config
Type
Heuristic Analysis
Capacities
Scoring
Naming
4
UP
Not Ready
0 job
GBOX_ANALY_02
6
5

Repère	Nom	Moteur Grip	Moteur Goasm	Moteur Gdgadetect	Moteur Gnest	Moteur Gmalcore
1	Type	Analyse statique	Détection des shellcodes	Détection de noms de domaine générés par des DGA (Domain Generation Algorithm)	Exécute le fichier dans une machine virtuelle et analyse son comportement	Analyse statique et heuristique multi-moteurs
2	Capacités	Analyse	Donne un score de la dangerosité potentielle et nomme le shellcode détecté	Donne un score de compromission	Nomme le problème détecté	Donne un score de la dangerosité potentielle et nomme le problème détecté
3	Config	Non configurable donc ce champ n'est pas affiché			Gestion des machines virtuelles (ajout, suppression, historisation)	Gestion des moteurs de Gmalcore
4	x jobs : nombre de tâches en cours (statut de l'analyse NEW + IN PROGRESS)	Nombre de tâches en attente de traitement				
5	Capacité à effectuer des analyses	Ce moteur n'a pas d'exigences donc toujours à l'état `ready`			Le moteur est à l'état `ready` s'il y a le même nombre de VM dans la GBox et dans CAPE (le moteur d'analyse dynamique)	Le moteur est à l'état `ready` si tous les moteurs sont installés et l'API est up
6	Etat du moteur	UP : l'api du moteur est en écoute : DOWN : l'api du moteur est non actif				

Astuce:

Si l'état du moteur (Grip, Goasm, Gdgadetect ou Gnest) est `DOWN`, attendre un moment.
Si le moteur reste dans l'état `DOWN`, contacter le support de Gatewatcher.

Astuce:

Si l'état du moteur Gmalcore est `DOWN`, redémarrer le service Malcore (ou Réinstaller le service Malcore): voir la *Commande `Services`*.
Si le moteur reste dans l'état `DOWN`, contacter le support de Gatewatcher.
L'état `Not Ready` pour le moteur **Gmalcore** ne signifie pas forcément que ce dernier n'est pas en capacité d'effectuer des analyses mais indique qu'au moins un des 16 moteurs antivirus n'est pas à jour ou est hors service.

5.3.5.1 Moteur Grip

Il est cependant utile pour analyser rapidement les métadonnées d'un fichier qualifié comme *suspicious* ou *malicious*.
Il est utilisé pour avoir des informations sur le fichier en amont d'analyse plus approfondies.
Ces données sont affichées dans le rapport détaillé et plus précisément dans les sections **TOP** et **Static** (voir le *Rapport détaillé*)

Taille maximum de fichier	50 MO
Timeout d'analyse	2 minutes
Type	léger

5.3.5.1.1 Visualisation de l'état de Grip

5.3.5.2 Moteur Goasm

Ce moteur d'analyse permet la détection et l'analyse de **shellcodes**.
Il permet l'identification de certains encodages et permet de détailler les appels système effectués.
Ce moteur donne un score de la dangerosité potentielle et nomme le shellcode détecté.
Ces données sont affichées dans le rapport détaillé et plus précisément dans les sections **TOP**, **Shellcode** (voir le *Rapport détaillé*).

Taille maximum de fichier	50 Mo
Timeout d'analyse	4-6 minutes
Type	rapide

Goasm peut être considéré comme rapide pour des petits fichiers (< 5Mo).
En cas de gros fichiers texte (> 5 Mo), la détection prend du temps car il faut parcourir le binaire à la recherche de pattern de shellcodes.
Le timeout d'analyse interne à Goasm peut donc être atteint : 4 min.
Le timeout externe au moteur, lui, est fixé à 6 min.

En cas de timeout interne :

- il y a un message d'erreur dans la partie `Shellcode` du rapport
- le moteur arrête juste de parcourir octet par octet le fichier

En cas de timeout externe (erreur survenue ou Goasm bloqué), une erreur est présente dans le rapport mentionnant un timeout (dans ce cas, relancer l'analyse).

5.3.5.3 Moteur Gdgadetect

5.3.5.3.1 Présentation de l'algorithme DGA

La **GBox** embarque un moteur capable de détecter des noms de domaines ayant été générés par des DGA (Domain Generation Algorithm).
La présence de noms de domaines générés par DGA sur un réseau est un fort indicateur de compromission.
En effet, les logiciels malveillants peuvent utiliser des requêtes HTTP vers des noms de domaine générés automatiquement, afin de contacter leurs serveurs de commande et de contrôle (aussi appelés CnC, C&C ou C2).
Ces noms de domaine ont des propriétés différentes des noms de domaines légitimes.
Les approches classiques de détection comme les listes noires ne sont pas pertinentes dans le cas de domaines renouvelés en permanence.
Les simples calculs d'entropie génèrent une grande quantité de faux positifs.

5.3.5.3.2 Analyse

Le Machine Learning est basé sur un modèle pré-entraîné, dont l'architecture est basée sur un réseau de neurones profond de type LSTM (Long Short Term Memory networks).

5.3.5.3.3 Affichage des alertes DGA

L'analyse se fait dans la page `Quick analysis`.
En fonction du résultat, une icône verte ou rouge indique si c'est un DGA ou non.

5.3.5.4 Moteur Gnest

Le moteur d'analyse **Gnest** permet une analyse dynamique.
Il exécute le fichier dans une machine virtuelle (sandbox) et analyse son comportement.
Suite à cela, il est possible d'extraire les données générées lors de l'analyse comme un *dump* de la mémoire, les chaînes de caractères extraites, ou une capture des communications réseau (pcap).
Dans le cas d'un fonctionnement connecté au GCenter, ce moteur est utile pour analyser en profondeur un fichier qualifié de *suspicious* ou *malicious*, lors d'une seconde analyse d'un fichier.

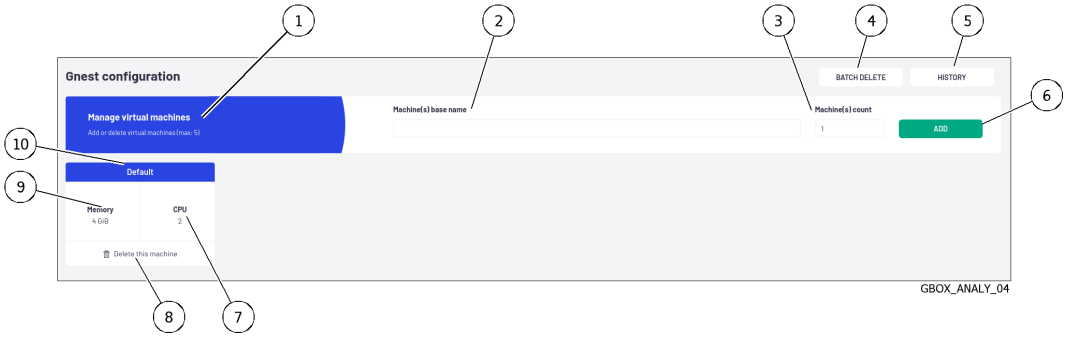
Cette analyse est plus lente et requiert un opérateur de niveau confirmé afin d'analyser les résultats produits.

Ces données sont affichées dans le *Rapport détaillé* et plus précisément dans les sections **TOP**, **Iocs**, **Ttps**, **Overview**, **Signatures** et **Process Tree**.

Taille maximum de fichier	50Mo
Timeout d'analyse	1 heure
Type	lent

5.3.5.5 Ecran `Gnest configuration`

Cet écran permet de gérer les machines virtuelles du moteur Gnest.
Après appui sur le lien du moteur Gnest, l'écran suivant est affiché.



Repère	Description	
1	Zone `Manage virtual machines` : cette zone permet de créer de nouvelles machines virtuelles Cette zone comprend :	
2	• `Machine(s) base name`	Nom de base de la (ou des) machine(s) virtuelle(s) (VM)
3	• champ `Machine(s) count`	Nombre de machine(s) à créer
6	• bouton `ADD`	Lance la création de machine(s) virtuelle(s)
4	Bouton `BATCH DELETE`	Permet de supprimer une ou plusieurs VM
5	Bouton `HISTORY`	Affiche la fenêtre de l'historique de la gestion des VMs
10	Nom `Default` : machine virtuelle existante et nom de la machine par défaut. Elle comprend les informations suivantes	
9	• champ `Memory`	Valeur de la quantité de mémoire attribué à la VM
7	• champ `CPU`	Valeur de la quantité de processeur attribuée à la VM
8	• bouton `Delete this machine`	Supprime la machine sélectionnée

L'ajout / suppression de VMs attend que les analyses Gnest en cours soient finies et bloque les prochaines analyses.
Cependant, si le modèle d'une VM est supprimé alors que des jobs sont en attente, ceux-ci passeront en erreur.
La mise en œuvre est donnée dans la *Procédure de configuration du moteur Gnest*.

5.3.5.6 Moteur Gmalcore

- la détection des malwares par une analyse statique et heuristique multi-moteurs en temps réel des fichiers
- l'analyse via 16 moteurs Anti-Virus
- une performance d'analyse proche de 200000 fichiers par 24h
- d'obtenir le ou les noms de la menace ainsi qu'un score de menace
- une identification rapide des menaces

Les 16 moteurs antivirus sont affichés sous le nom `engine hash` dans l'interface Web ui.

Taille maximum de fichier	50 Mo
Timeout d'analyse	2 minutes
Type	léger

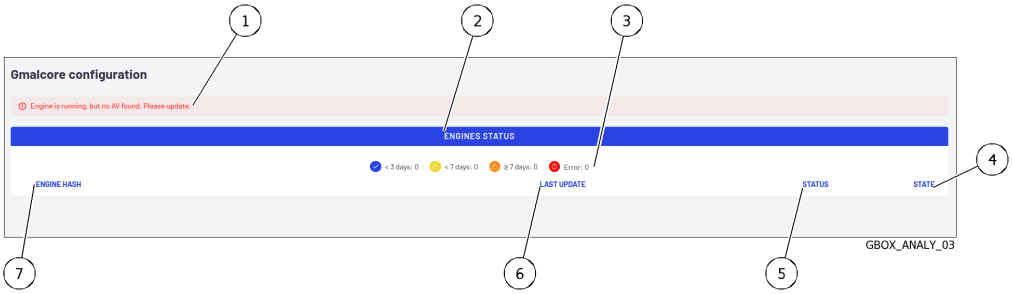
Les événements générés par Gmalcore sont indiqués dans la partie `Heuristic` du rapport d'analyse de la GBox.

5.3.5.7 Ecran `Gmalcore configuration`

Cet écran donne les informations de la configuration du moteur Gmalcore :

- l'état des moteurs Gmalcore
- la date de la dernière mise à jour installée

Après appui sur le lien `Config` du moteur Gmalcore, l'écran suivant est affiché.

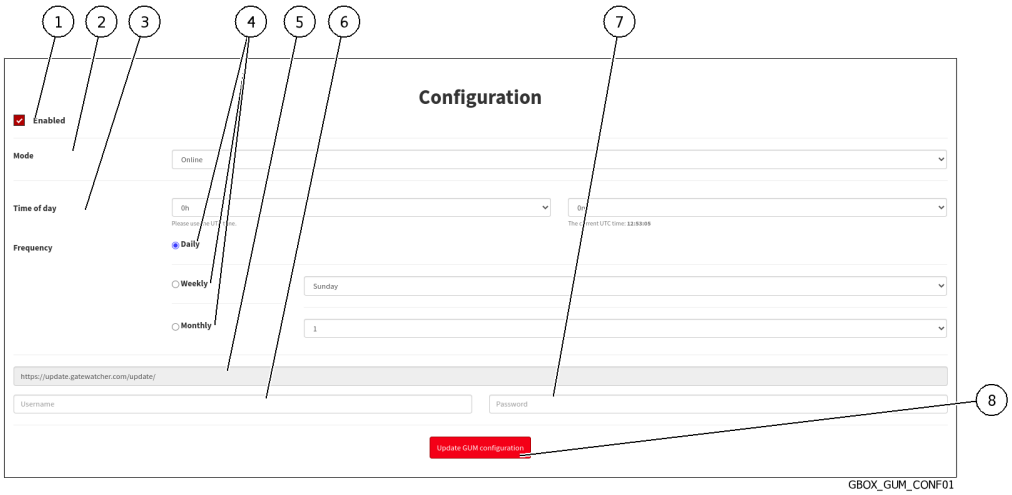


Repère	Moteur	Fonction
1	Message de l'état de la configuration	`Engine is running, but no AV found. Please update.` : nécessite l'installation d'une mise à jour des moteurs Gmalcore
2	`ENGINES STATUS`	Cette zone permet d'afficher l'état des moteurs antivirus avec les informations suivantes :
3		• icônes de couleurs. Chaque moteur est précédé d'une icône indiquant l'ancienneté de la mise à jour des signatures des moteurs
7		• `ENGINE HASH`. Les 16 moteurs antivirus sont affichés sous le nom "engine hash"
6		• `LAST UPDATE`. Date de la dernière mise à jour (update)
5		• `STATUS`. Icône indiquant l'état et ancienneté de la dernière mise à jour
4		• `STATE`. Etat du moteur (PRODUCTION, DOWNLOADED...)

La mise en œuvre de la configuration de Gmalcore est donnée dans la *Procédure de configuration du moteur Gmalcore*.

5.3.6 Ecran `Admin-GUM - Config` de la legacy Web UI

Après appui sur la commande `Config` du menu `GUM`, l'écran suivant est affiché.



Repère	Nom	Fonction
1	`Enabled`	Active la possibilité d'effectuer des mises à jour en mode local ou online
2	`Mode`	Permet de sélectionner le type de mode de mises à jour (local ou en ligne). Le mode Online permet de faire les mises à jour de manière automatique (à partir des serveurs de Gatewatcher) Le mode local permet de faire les mises à jour à partir d'un dépôt local.
3	Champ `Time of day`	Choix de l'heure de la mise à jour
4	Boutons `Daily`, `Weekly`, `Monthly`	Choix de la périodicité du déclenchement des mises à jour.
5	Champ source des mises à jour	En mode Online, ce champ est automatiquement renseigné En mode Local, ce champ doit contenir l'adresse IP ou le FQDN de l'adresse du dépôt local
6	Champ `Username`	En mode Online, champ pour le login pour se connecter aux serveurs Gatewatcher En mode local, champ pour le login au dépôt local
7	Champ `Password`	En mode Online, champ pour le mot de passe pour se connecter aux serveurs Gatewatcher En mode Local, champ pour le mot de passe au dépôt local
8	Bouton `Update GUM configuration`	Met à jour la configuration de GUM

Cet écran permet de configurer la planification automatique des mises à jour.
Ces mises à jour peuvent être faites :

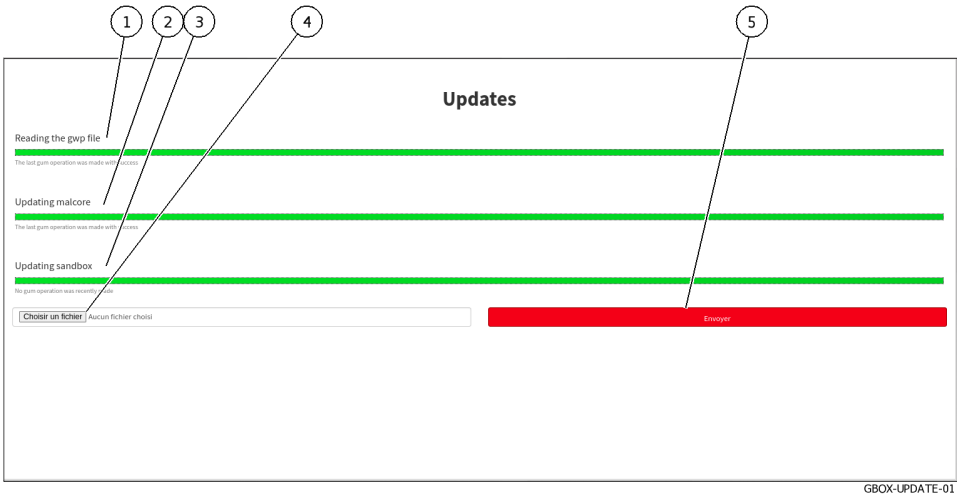
- par le mode Online
  Si besoin, configurer un proxy (voir la procédure de *Configuration d'un proxy*)
  Le mode online permet de faire les mises à jour de manière automatique (à partir d'Internet).
  Le champ URL sera automatiquement renseigné. Les packages de mise à jour sont récupérés depuis les serveurs Gatewatcher https://update.GATEWATCHER.com/update/.
- par le mode Local
  Si besoin, configurer un proxy (voir la procédure de *Configuration d'un proxy*)
  Le mode Local permet de faire les mises à jour à partir d'un dépôt local préalablement configuré pour télécharger les paquets depuis les serveurs Gatewatcher https://update.GATEWATCHER.com/update/.
  Ce dépôt local est défini dans l'*Ecran `Admin-GUM - Config` de la legacy Web UI*.

Un compte intelligence sera nécessaire pour que le téléchargement du package de mise à jour puisse se faire depuis le site.
Dans le cas du mode `online`, ce couple utilisateur et mot de passe doivent être renseignés dans les champs `Username` et `Password` situés sous l'adresse.

Pour la mise en œuvre, se référer à la *Configuration de la mise à jour automatique via GUM*.

5.3.7 Ecran `Admin-GUM - Updates` de la legacy Web UI

Après appui sur la commande `Updates` du menu `GUM`, l'écran suivant est affiché.



Repère	Nom	Fonction
1	`Reading the gwp file`	Barre de progression de la vérification de l'intégrité d'un paquet chargé
2	`Updating malcore`	Barre progression de la mise à jour du moteur Malcore / Etat de la dernière mise à jour
3	`Updating sandbox`	Barre progression de la mise à jour du moteur Gnest/ Etat de la dernière mise à jour
4	Bouton `Parcourir`	Permet de sélectionner un paquet de mise à jour
5	Champ `Envoyer`	Déclenche l'installation du paquet de mise à jour

Les mises à jour de signatures ou **updates** correspondent aux mises à jour des moteurs de détection de la GBox.
Il existe 3 types de paquets de mise à jour :

- les paquets Gmalcore (*latest_malcore*) : ces paquets contiennent uniquement les mises à jour des moteurs et des bases des antivirus utilisés par Malcore
- les paquets sandbox (*latest_sandbox*) : ces paquets contiennent des mises à jour des signatures et des modules utilisés par les sandbox du moteur Gnest
- les paquets complets (*latest_full*) : ces paquets sont une combinaison des 2 précédents paquets

Cet écran permet de visualiser l'historique et l'état de l'installation :

- pour les paquets téléchargés de façon planifiée

- pour les paquets téléchargés de façon manuelle

En cas de mise à jour d'un paquet :

- la barre de progression du champ `Reading the gwp file` commence sa progression : ceci signifie que le fichier a été téléchargé et le système contrôle son intégrité
- la barre de progression du champ `Updating malcore` commence sa progression : ceci correspond au traitement des fichiers du moteur Malcore
- la barre de progression du champ `Updating sandbox` commence sa progression : ceci correspond au traitement des mises à jour des signatures et des modules utilisés par la sandbox

Pour utiliser un fichier de paquet depuis le PC distant, utiliser le bouton (4) `Parcourir`.

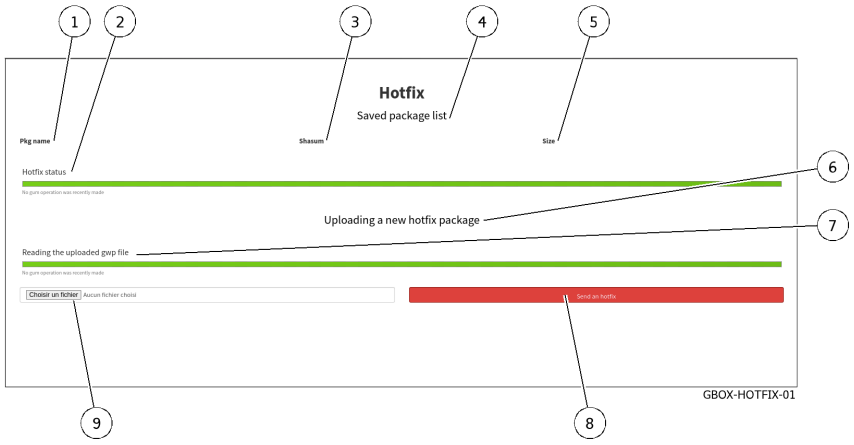
Important:

Dans ce cas, il faut sélectionner un fichier de package GWP et uniquement ceux des moteurs de la solution.
Les packages de type correctif (hotfix) et mise à niveau (upgrade) ne fonctionneront pas dans cet écran.

Pour la mise en œuvre, voir la procédure d'*Installation manuelle d'une mise à jour des signatures (update)*.

5.3.8 Ecran `Admin-GUM - Hotfix` de la legacy Web UI

Après appui sur la commande `Hotfix` du menu `GUM`, l'écran suivant est affiché.



L'écran `Hotfix` contient les éléments suivants :

Repère	Nom	Fonction
4	Zone `Saved package lists` qui comprend...	Liste des correctifs téléchargés mais en attente d'application. Après installation, la liste est purgée Après installation, le hotfix apparait dans le numéro du logiciel gbox (repère 16 dans la *Barre de navigation de l'interface traditionnelle*)
1	• Champ `Pkg Name`	Nom du paquet de logiciels
2	• Champ `Update status`	Barre de progression de l'application d'un correctif / Etat de la dernière application du paquet
3	• Champ `Shasum`	Shasum sha256 du fichier
5	• Champ `Size`	Taille du fichier
6	Zone `Uploading a new hotfix package` qui comprend...	Zone permettant l'installation manuelle d'un paquet
7	• Champ `Reading the uploaded gwp file`	Barre de progression de la vérification de l'intégrité du paquet / Etat de la dernière vérification
8	• Bouton `Send an hotfix`	Déclenche l'installation du correctif
9	• Bouton `Choisir un fichier`	Permet de sélectionner un paquet

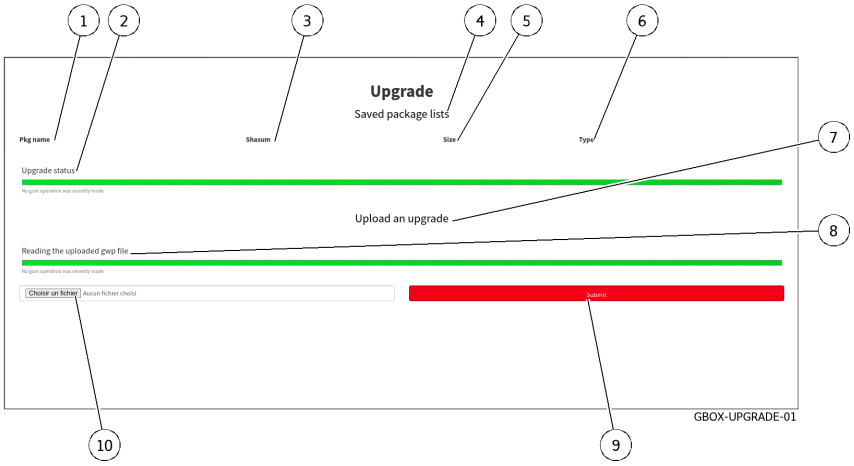
Important:

Il faut sélectionner un fichier de paquet gwp et uniquement ceux de type Hotfix.
Les paquets des autres types ne fonctionneront pas dans cette interface.

Pour plus d'information, voir l'*Application d'un correctif (Hotfix)*.
Pour la mise en œuvre, voir la procédure d'*Installation d'un correctif (Hotfix)*.

5.3.9 Ecran `Admin-GUM - Upgrade` de la legacy Web UI

Après appui sur la commande `Upgrade` du menu `GUM`, l'écran suivant est affiché.



L'écran `Upgrade` contient les éléments suivants :

Repère	Nom	Fonction
4	Zone `Saved package lists` qui comprend	Historique des paquets de logiciels
1	• Champ `Pkg Name`	Nom du paquet de logiciels
2	• Champ `Upgrade status`	Barre de progression de l'application d'une mise à niveau / Etat de la dernière application du paquet
3	• Champ `Shasum`	Shasum sha256 du fichier
5	• Champ `Size`	Taille du fichier
6	• Champ `Type`	Type
7	Zone `Upload an upgrade` qui comprend	Zone permettant l'installation manuelle d'un paquet
8	• Champ `Reading the uploaded gwp file`	Barre de progression de la vérification de l'intégrité du paquet / Etat de la dernière vérification
9	• Bouton `Submit`	Déclenche l'installation du paquet
10	• Bouton `Choisir un fichier`	Permet de sélectionner un paquet

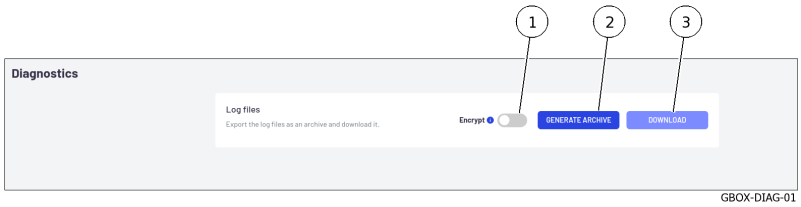
Important:

Il faut sélectionner un fichier de paquet GWP et uniquement ceux de type mise à niveau.
Les paquets des autres types ne fonctionneront pas dans cette interface.

Pour plus d'information, voir la *Mise à niveau (Upgrade)*.
Pour la mise en œuvre, voir la procédure d'*Installation d'une mise à niveau (upgrade)*.

5.3.10 Ecran `Admin-GBox - Diagnostics` de la Web UI

Après appui sur la commande `Diagnostics` du menu `GBox`, l'écran suivant est affiché.
Cet écran permet d'exporter les fichiers log et les télécharger.



Repère	Nom	Fonction
1	`Encrypt`	Crypter les fichiers logs
2	`GENERATE ARCHIVE`	Bouton de génération du fichier compressé `Log files`
3	`DOWNLOAD`	Bouton de téléchargment du fichier `Log files`

Le fichier d'export de log est crypté, seul le support de GATEWATCHER peut la déchiffrer.
Pour plus de détails sur la gestion des données, voir le paragraphe *Utilisation des données*.
Pour la mise en œuvre, voir la procédure de *Génération et téléchargement des fichiers pour le diagnostic*.

5.3.11 Ecran `Admin-GBox - Accounts` de la Web UI

Après appui sur la commande `Accounts` du menu `Admin-GBox`, l'écran `Accounts management` est affiché et permet :

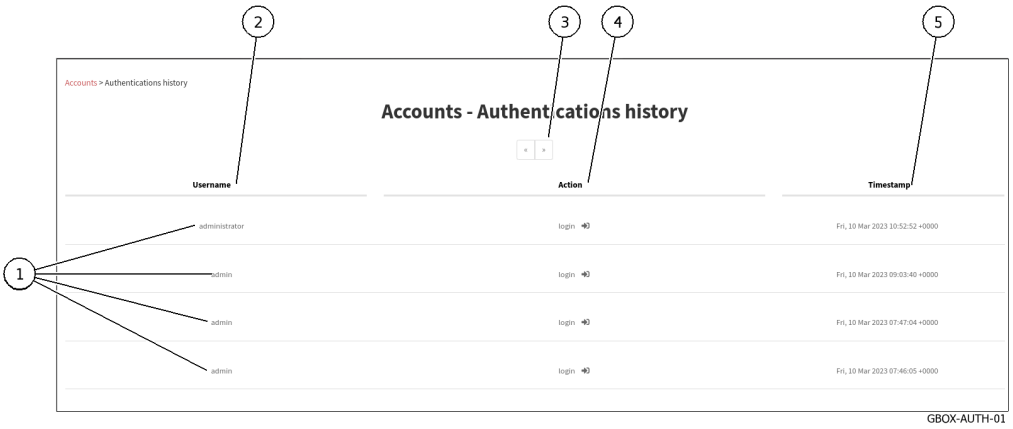
- la gestion des utilisateurs et des rôles associés
- l'affichage de l'historique des authentifications, des permissions et de la gestion utilisateur

Cet écran comprend les parties suivantes :

Partie	Fonction	se référer à
`Authentications history`	Historique de toutes les authentifications	*Partie `Authentications history` du sous menu `Accounts`*
`Creations/ Deletions history`	Historique de toutes les créations ou suppressions des utilisateurs	*Partie `Creations/Deletions history` du sous menu `Accounts`*
`Permissions history`	Historique de toutes les permissions des utilisateurs	*Partie `Permissions history` du sous menu `Accounts`*
`Users management`	Création de nouvel utilisateur et gestion des utilisateurs existants	*Ecran `Admin-GBox- Users management` de la Web UI*
`API tokens`	Création de token et gestion des tokens existants	*Partie `API tokens` du sous menu `Accounts`*

5.3.11.1 Partie `Authentications history` du sous menu `Accounts`

La fenêtre **`Authentications history`** affiche l'historique de toutes les authentifications sous forme d'un timestamp au format [**jour , xx mois année hh : mm : ss**].



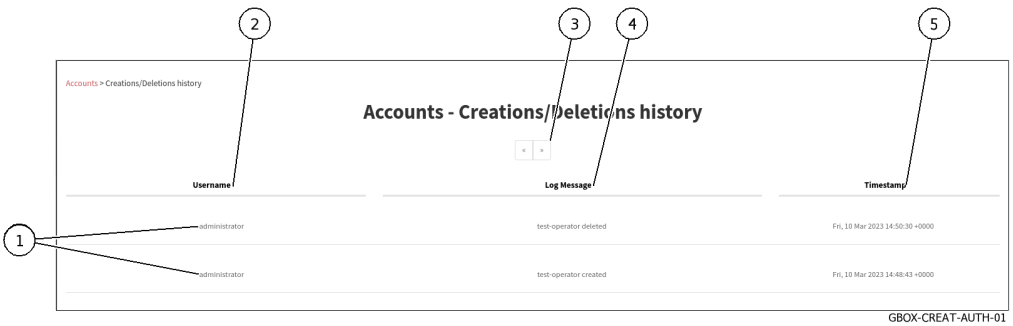
Cette fenêtre affiche les connexions (1) dans l'ordre du plus récent au plus ancien.
Les flèches (3) permettent de naviguer entre les différentes pages.
Pour chaque connexion, les informations suivantes sont affichées :

- champ **`Username`** (2) : nom de la personne qui s'est connecté / déconnecté
- champ **`Action`** (4) : login ou logout
- champ **`timestamp`** (5) : date et heure des connexions / déconnexions au format (**jj , mm aaaa hh : mm : ss**)

Pour la mise en œuvre, voir la procédure de *Visualisation de l'historique des authentifications*.

5.3.11.2 Partie `Creations/Deletions history` du sous menu `Accounts`

La fenêtre **`Creations/Deletions history`** affiche l'historique de toutes les créations ou suppressions des utilisateurs.
Toutes les modifications faites par un compte administrateur sur un utilisateur sont affichées.



Cette fenêtre affiche les créations ou suppressions (1) dans l'ordre du plus récent au plus ancien.
Les flèches (3) permettent de charger la page suivante.

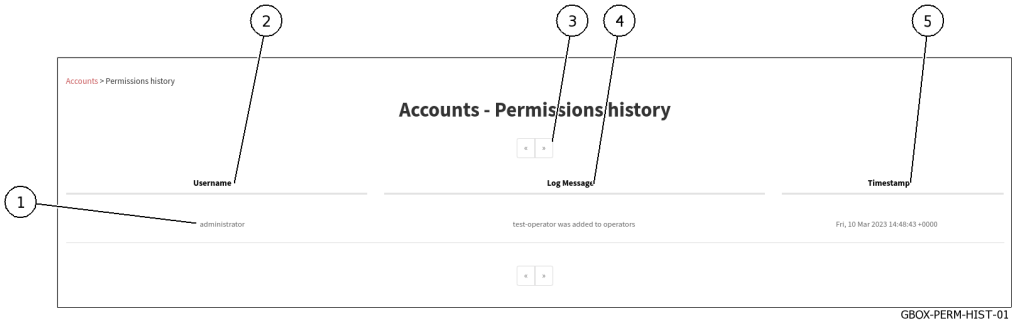
Pour chaque connexion, les informations suivantes sont affichées :

- champ `Username` (2) : nom de la personne qui a créé/supprimé le compte
- champ `Log Message` (4) : le nom du compte suivi de l'action (created or deleted)
- champ `timestamp` (5) : date et heure des connexions / déconnexions au format (**jj** , **mm aaaa hh** : **mm** : **ss**)

Pour la mise en œuvre, voir la procédure de *Visualisation de l'historique des créations ou suppressions des utilisateurs*.

5.3.11.3 Partie `Permissions history` du sous menu `Accounts`

La fenêtre `Permissions history` affiche historique de toutes les modifications des droits des utilisateurs.



Cette fenêtre affiche les modifications des droits (1) dans l'ordre du plus récent au plus ancien.
Les flèches (3) permettent de charger la page suivante.
Pour chaque connexion, les informations suivantes sont affichées :

- champ `Username` (2) : le nom de l'administrateur qui a modifié les droits du compte
- champ `Log Message` (4) : le nom du compte dont les droits ont été modifiés et l'action faite. Les modifications de droit s'effectue en changeant l'appartenance à tel ou tel groupe.
- champ `timestamp` (5) : date et heure des modifications au format (**jj** , **mm aaaa hh** : **mm** : **ss**)

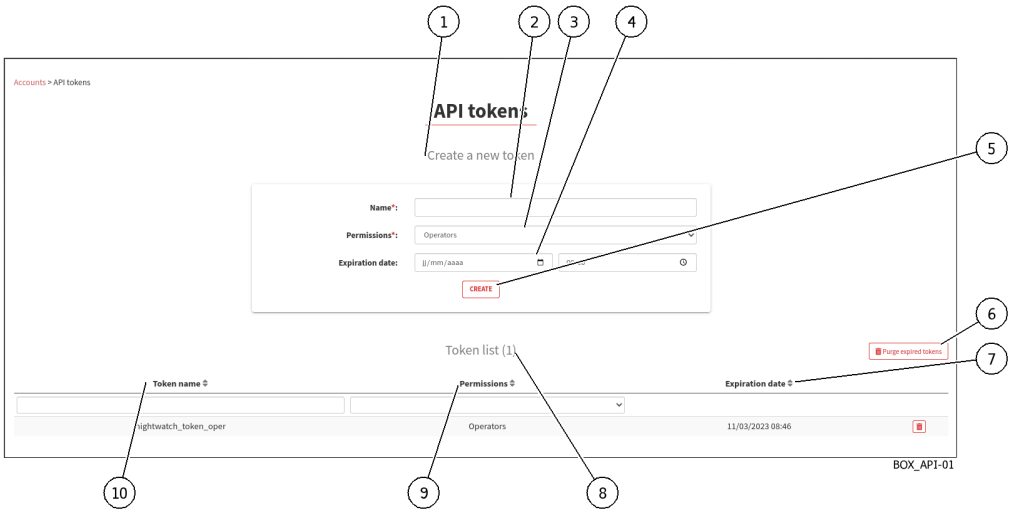
Pour la mise en œuvre, voir la procédure de *Visualisation de l'historique de toutes les modifications des droits des utilisateurs*.

5.3.11.4 Partie `Users management` du sous menu `Accounts`

Se référer à l'*Ecran `Admin-GBox- Users management` de la Web UI*

5.3.11.5 Partie `API tokens` du sous menu `Accounts`

L'écran **`API tokens`** gère les tokens d'accès des API.



Repère	Zone	Elément
1	**`Create a new token`** : zone pour ajouter un nouvel token d'accès d'API	
2		**`Name`** : champ pour saisir le nom du nouveau token
3		**`Permissions`** : champ pour sélectionner le compte et donc des droits du nouveau token
4		**`Expiration date`** : champ pour saisir la date d'expiration du nouveau token
5		**`CREATE`** : bouton pour ajouter le nouveau token
8	**`Token list`** : zone pour afficher la liste des tokens existants	
6		**`Purge expired tokens`** : bouton pour puger les tokens expirés
10		**`Name`** : champ pour afficher le nom du token
9		**`Permission`** : champ pour afficher le compte et donc des droits
7		**`Expiration`** : champ pour afficher la date d'expiration

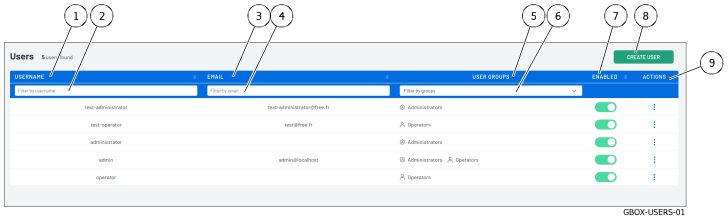
Pour la mise en œuvre, voir la procédure de *Création ou suppression d'un token d'accès d'un API*.

5.3.12 Ecran `Admin-GBox- Users management` de la Web UI

Cet écran permet :

- la gestion des utilisateurs existants et des rôles associés
- la création de nouveaux utilisateurs

Après appui sur la commande **`Users management`** du menu **`Admin-GBox`**, l'écran suivant est affiché.
Cet écran permet la gestion des utilisateurs existants.
La fenêtre **`Users`** comprend :



Repère	Nom	Description
1	`USERNAME`	Champ indiquant le nom de l'utilisateur
3	`EMAIL`	Champ indiquant l'adresse mail
5	`USER GROUPS`	Champ indiquant le groupe (Operators ou Administrators) ou les deux
7	`ENABLED`	Active ou désactive le compte
8	`CREATE USER`	Bouton d'affichage de la fenêtre `Create user` détaillée ci-après
9	`ACTIONS`	Actions possibles pour chacun des comptes présents : édition, suppression, initialisation du mot de passe

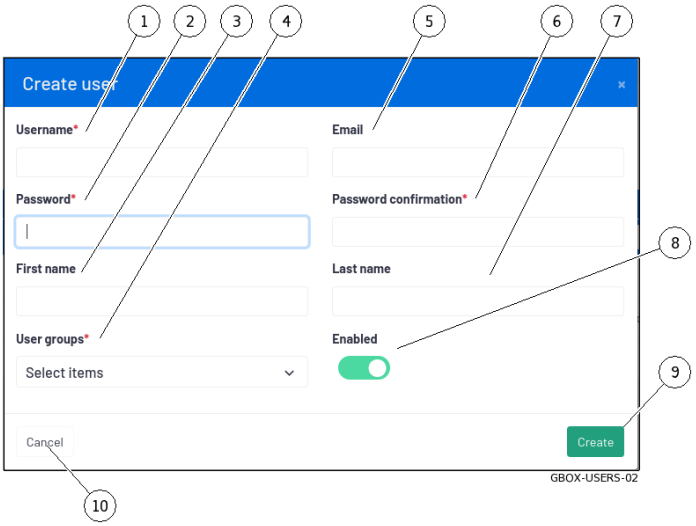
Les champs ci-dessous sont les champs supplémentaires permettant de faire le filtrage des comptes existants.

Repère	Nom	Description
2	`Filter by username`	Permet de filtrer les comptes avec ce nom à saisir
4	`Filter by email`	Permet de filtrer les comptes avec cet émail à saisir
6	`Filter by groups`	Permet de filtrer les comptes avec ce groupe à sélectionner

Pour la mise en œuvre de l'initialisation du mot de passe d'un utilisateur, voir la procédure de *Réinitialisation du mot de passe d'un utilisateur*.
Pour la mise en œuvre de la suppression d'un utilisateur, voir la *Suppression d'un utilisateur*.
Pour la mise en œuvre de la modification de certaines informations d'un utilisateur local, voir la *Modification de certaines informations d'un utilisateur local*.

5.3.12.1 Fenêtre `Create user`

Après appui sur le bouton `Create User`, cette fenêtre est affichée et permet la création d'utilisateur.



Repère	Nom	Description
1	`Username`	Nom complet du nouvel utilisateur. N'utiliser que les lettres non sensibles à la casse, virgule, point, apostrophe ou tiret.
2	`Password`	Mot de passe Ce mot de passe doit obligatoirement contenir un minimum de sept caractères (ou **8**).
3	`First name`	Prénom de l'utilisateur : champ optionnel
4	`Users groups`	Permet de sélectionner le groupe (Operators ou Administrators) ou les deux
5	`Email`	Adresse mail : champ optionnel
6	`Password confirmation`	Mot de passe identique au champ `Password`
7	`Last name`	Nom de l'utilisateur : champ optionnel
8	`Enabled`	Active ou désactive le compte
9	`Create`	Bouton de création de l'utilisateur avec les paramètres saisis

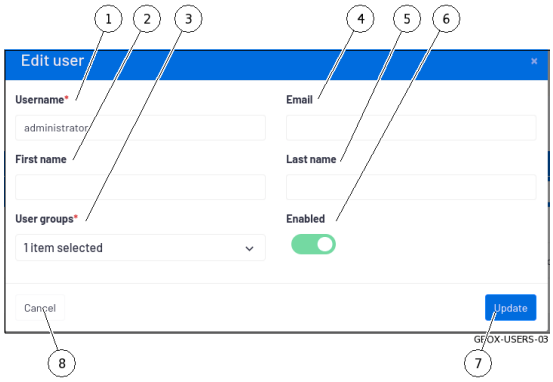
Note:

Se référer au paragraphe *Fonctions autorisées pour les membres du groupe Operators* et *Fonctions autorisées pour les membres du groupe Administrators*

Pour la mise en œuvre, voir la procédure de *Création d'un utilisateur local*.

5.3.12.2 Fenêtre `Edit user`

Après appui sur la commande `Edit` du menu `ACTIONS`, cette fenêtre est affichée et permet l'édition d'un utilisateur.



Repère	Nom	Description
1	`Username`	Nom complet du nouvel utilisateur. N'utiliser que des lettres, des virgules, des points, des guillemets ou des tirets. des lettres, des chiffres et des caractères (@/./+/-/-/_).
2	`First name`	Prénom de l'utilisateur : champ optionnel
3	`Users groups`	Permet de sélectionner le groupe (Operators ou Administrators) ou les deux
4	`Email`	Adresse mail : champ optionnel
5	`Last name`	Nom de l'utilisateur : champ optionnel
6	`Enabled`	Active ou désactive le compte
7	`Update`	Bouton de mis à jour des paramètres saisis
8	`Cancel`	Bouton d'annulation

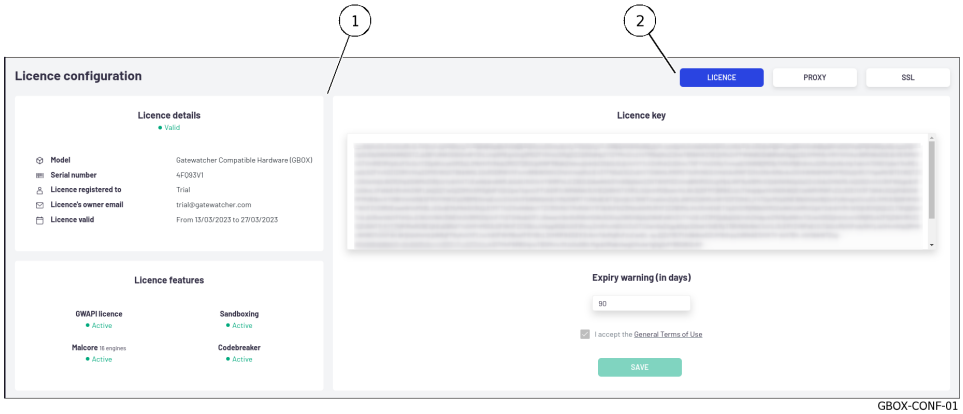
Pour la mise en œuvre, voir la *Modification de certaines informations d'un utilisateur local*.

5.3.13 Ecran `Admin-GBOX- Configuration` de la Web UI :

Cet écran permet :

- la visualisation des informations sur la licence en cours, d'en vérifier la validité et des fonctionnalités disponibles
- la configuration du serveur mandataire (ou proxy) afin de récupérer les mise à jour via celui-ci et d'un dépôt local
- la configuration du certificat SSL (Secure Socket Layer)

Après appui sur la commande `Configuration` du menu `Admin-GBox`, l'écran suivant est affiché.
La fenêtre comprend :



GBOX-CONF-01

Repère	Description
1	*Zone d'affichage de l'écran `Configuration`* : le contenu dépend du choix sélectionné par appui sur l'un des boutons (2)
2	*Sélecteur de tableau de bord de l'écran `Configuration`* : comprend trois boutons de choix

---

5.3.13.1 Sélecteur de tableau de bord de l'écran `Configuration`

Le sélecteur comprend les boutons suivants :

Nom	Description
`LICENCE`	Visualisation des informations sur la licence en cours, d'en vérifier la validité et des fonctionnalités disponibles
`PROXY`	Configuration du serveur mandataire (ou proxy)
`SSL`	Configuration du certificat SSL (Secure Socket Layer)

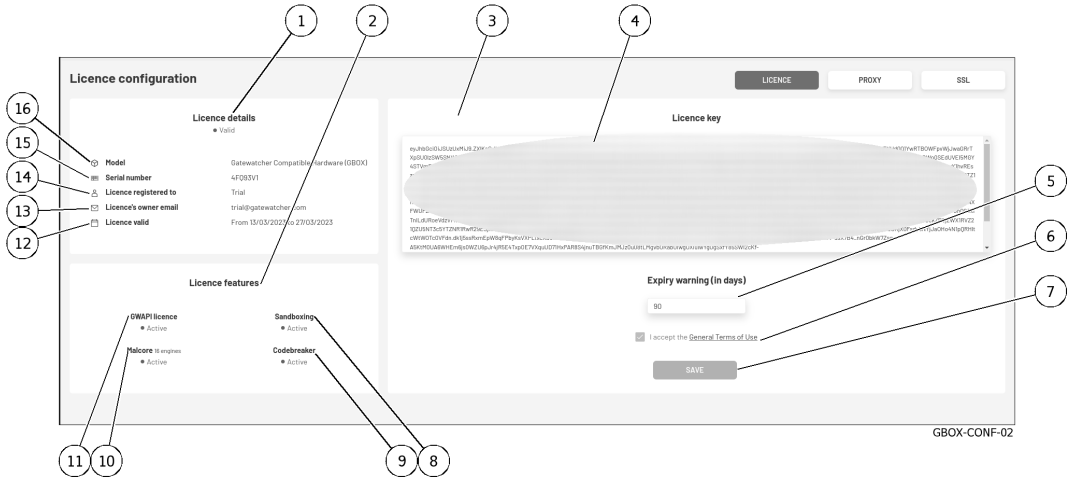
5.3.13.2 Zone d'affichage de l'écran `Configuration`

Cette zone affiche les informations de l'écran correspondant au bouton utilisé dans le sélecteur de tableau de bord.
Trois écrans sont accessibles :

- *Ecran `Licence configuration`*
- *Ecran `Proxy settings`*
- *Ecran `SSL settings`*

5.3.13.2.1 Ecran `Licence configuration`

Après avoir cliqué sur le bouton `LICENCE`, l'écran suivant est affiché :



Cet écran est composé de trois parties :

- la partie `Licence key` : permet de saisir la licence et le délai du message d'alarme
- la partie `Licence features`: permet de visualiser les fonctionnalités activées dans cette licence
- la partie `Licence details` : permet d'obtenir des informations sur le matériel pour lequel cette licence a été émise via son modèle et son numéro de série, mais également la période de validité de celle-ci et l'adresse de contact associée et le type de licence

La partie `License key` (3) contient les éléments suivants :

Repère	Nom	Fonction
4	Champ `License key`	Saisie de la clé de licence
5	Champ `Expiry warning (in days)`	Saisie du nombre de jours du message d'alarme expiration de la licence de la licence
6	Champ `I accept the General Terms of Use`	Sélection de l'acceptation des conditions d'utilisation
7	Bouton `SAVE`	Sauvegarde les paramètres courants

La partie `License features` (2) contient les éléments suivants :

Repère	Nom	Fonction
8	Champ `Sandboxing`	Information sur l'activation du moteur Gnest (sandboxing)
9	Champ `Codebreaker`	Information sur l'activation du moteur Codebreaker autre nom du moteur Goasm
10	Champ `Malcore engines`	Information sur l'activation du moteur Malcore (nombre de moteurs)
11	Champ `GWAPI licence`	Information sur l'activation de GWAPI

La partie `License details` (1) contient les éléments suivants :

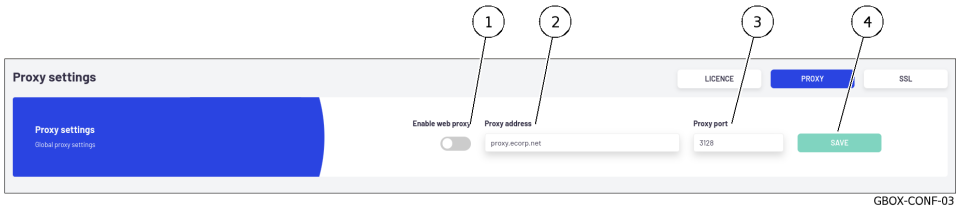
Repère	Nom	Fonction
12	Champ `License valid`	Date d'enregistrment de la licence et durée restante
13	Champ `License's owner email`	Email du propriétaire de la licence
14	Champ `License registered to`	Enregistrement de la licence
15	Champ `Serial Number`	Information sur le serveur
16	Champ `Model`	Type de matériel (**a completer**)

Pour la mise en œuvre de la Modification de la licence, voir la procédure de *Modification de la licence*.

5.3.13.2.2 Ecran `Proxy settings`

La GBox offre la possibilité de configurer un serveur mandataire (ou proxy) afin de récupérer les updates (mise à jour de signatures) via celui-ci.

Après avoir cliqué sur le bouton `PROXY`, l'écran suivant est affiché :



GBOX-CONF-03

La partie `Proxy settings` contient les éléments suivants :

Repère	Nom	Fonction
1	Sélecteur `Enable Web Proxy`	Active/Désactive l'utilisation du proxy
2	Champ `Proxy address`	Définit l'adresse du serveur mandataire sous forme d'adresse IP ou de FQDN
3	Champ `Proxy port`	Sélectionne le port d'écoute du proxy (1-65535)
4	Bouton `SAVE`	Sauvegarde les paramètres courants

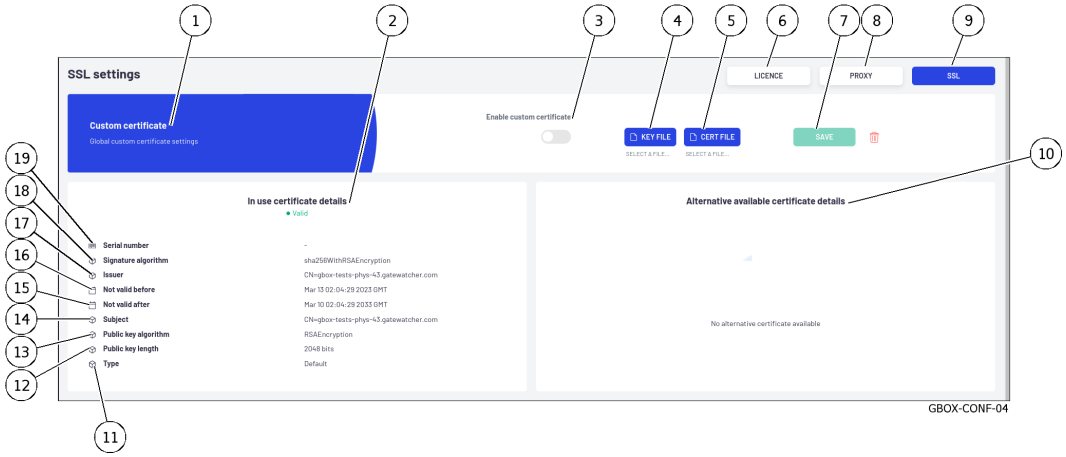
Pour la mise en œuvre, voir la procédure de *Configuration d'un proxy*.

5.3.13.2.3 Ecran `SSL settings`

Cette partie permet de visualiser le certificat SSL (Secure Socket Layer) et un certificat personnalisé de la GBox. Il est possible de sélectionner un des deux certificats.

Le certificat généré atteste de l'identité de la GBox et permet de chiffrer les données échangées.

Après avoir cliqué sur le bouton `SSL`, l'écran suivant est affiché :



Cet écran est composé des zones :

- *Zone `In use certificate details`* (2)
- *Zone `Custom Certificate`* (1)
- *Zone `Alternative available certificate details`* (10)

Pour la mise en œuvre, voir la procédure de *Mise en place d'un certificat SSL*.

5.3.13.2.3.1 Zone `In use certificate details`

Cette zone (2) permet d'obtenir des informations sur le certificat en cours d'utilisation.
Cette zone contient les éléments suivants :

Repère	Nom	Fonction
2	Champ `In use certificate details`	Affiche les informations sur le certificat. La validité de ce certificat est précisé
19	Champ `Serial number`	Numéro de série unique attribué par l'autorité de certification qui a émis le certificat
18	Champ `Signature algorithm`	Algorithme de signature du certificat (sha256WithRSAEncryption par exemple)
17	Champ `Issuer`	Emetteur du certificat
16	Champ `Not valid before`	Date du début de la validité
15	Champ `Not valid after`	Date de fin de la validité
14	Champ `Subject`	L'objet (domaine pour lequel le certificat est émis)
13	Champ `Public key algorithm`	Algorithme de chiffrement utilisé pour les échanges entre le serveur et le client
12	Champ `Public key length`	Longueur de la clé publique (2048bits par exemple)
11	Champ `Type`	Type

5.3.13.2.3.2 Zone `Custom Certificate`

La zone (1) permet d'utiliser un certificat spécifique.
Pour cela il suffit de charger la clé privée et le certificat au format PEM.
La zone `Custom Certificate` contient les éléments suivants :

Repère	Nom	Fonction
3	Sélecteur `Enable Custom Certificate`	Si actif alors sélection d'un certicat personnalisé (alternative) Si non actif alors sélection du certicat courant (in use)
4	Bouton `KEY FILE`	Sélection de la clé privée à utiliser
5	Champ `CERT FILE`	Sélection du certificat (Clé publique) associé à la clé privée
7	Bouton `SAVE`	Sauvegarde les paramètres courants

5.3.13.2.3.3 Zone `Alternative available certificate details`

La zone (1) permet d'utiliser un autre certificat.
Pour cela il suffit de charger la clé privée et le certificat au format PEM.
La zone `Alternative available certificate details ` contient les informations de ce certificat alternatif.

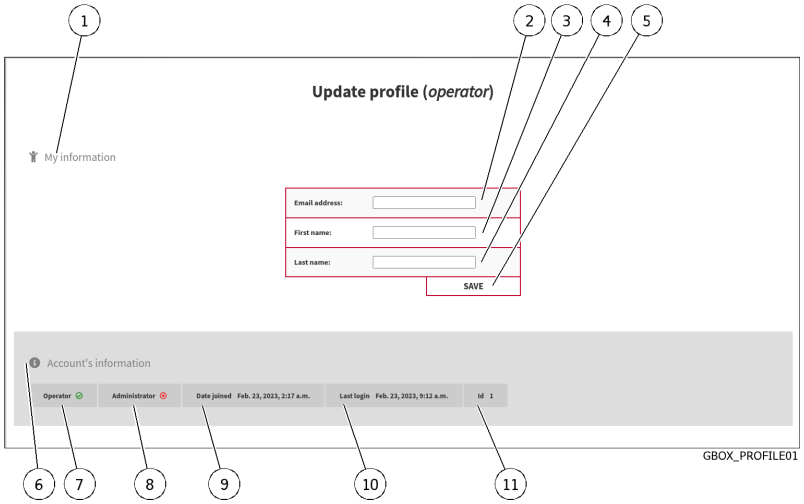
5.3.14 Gestion du compte courant, membre du groupe Administrators

Après appui sur le bouton de gestion du compte courant (4), trois commandes sont disponibles :

- la commande `Edit profile` : voir l'*Ecran `Update profile`*
- la commande `Change password` : voir l'*Ecran `Change Password`*
- la commande `Logout` : voir la *Commande Logout*

5.3.14.1 Ecran `Update profile`

Après avoir cliqué sur la commande `Edit profile`, l'écran `Update profile` est affiché :

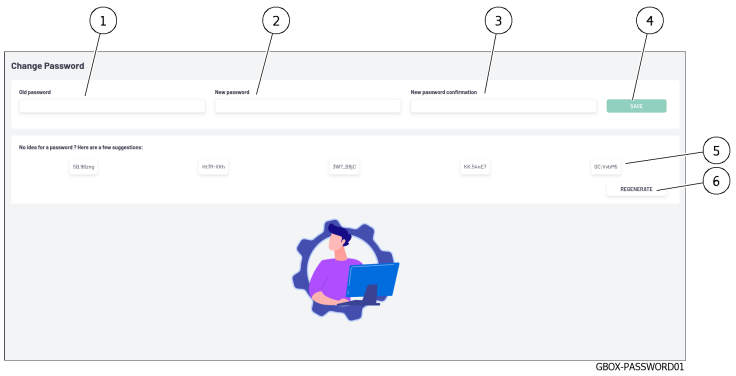


Repère	Nom	Description
1	`My information`	Zone listant les informations du compte courant
2	`Email address`	Adresse email de l'utilisateur courant
3	`First name`	Prénom de l'utilisateur courant
4	`Last name`	Nom l'utilisateur courant
5	`SAVE`	Bouton de sauvegarde de la saisie.
6	`Account's information`	Zone listant les informations de gestion du compte courant
7	`Operator`	Appartenance au groupe Operators (coche indique l'appartenance, la croix la non appartenance)
8	`Administrator`	Appartenance au groupe Administrators (coche indique l'appartenance, la croix la non appartenance)
9	`Date joined`	Date et heure de la création du compte courant
10	`Last login`	Date et heure de la dernière connexion du compte courant
11	`ID`	Numéro identifiant le compte

Pour la mise en œuvre, voir la procédure de *Modification de certaines informations de l'utilisateur courant*.

5.3.14.2 Ecran `Change Password`

Après avoir cliqué sur la commande **`Change password`**, l'écran **`Change Password`** est affiché :



Cet écran permet de changer le mot de passe du compte courant.

Cette politique de mot de passe est décrite dans la *Gestion de la politique des mots de passe*.

Repère	Nom	Description
1	`Old password`	Zone de saisie de l'ancien mot de passe
2	`New password`	Zone de saisie du nouveau mot de passe
3	`New password confirmation`	Zone de saisie de la confirmation du nouveau mot de passe
4	`SAVE`	Bouton de sauvegarde de la saisie
5	`No idea for a password ?` `Here are a few suggestions`	Cinq mots de passe sont proposés
6	`REGENERATE`	Bouton de regénération de nouveaux mots de passe

Pour la mise en œuvre, voir la procédure de *Modification du mot de passe du compte courant*.

5.3.14.3 Commande Logout

Après avoir cliqué sur la commande `Logout`, l'utilisateur courant est immédiatement déconnecté.
L'écran de connexion est affiché.
Pour la mise en œuvre, voir la procédure de *Déconnexion de l'interface web de la GBox*.

5.4 Interface graphique API

5.4.1 Présentation de l'interface API GBOX

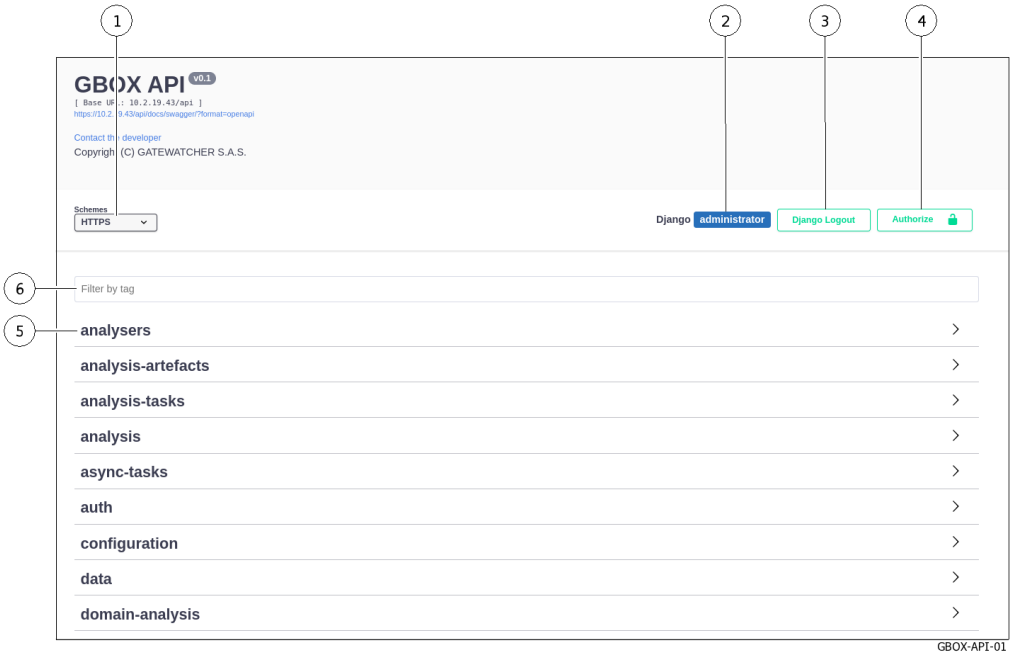
L'interface API permet :

- d'afficher la liste par thème des endpoints existants
- de pouvoir filtrer cette liste
- de connaître toutes les informations de chaque endpoint
- d'exécuter le endpoint,
- de connaître sa commande curl
- de connaître sa requête URL

Note:

L'interface graphique GBox API est nommée swagger.

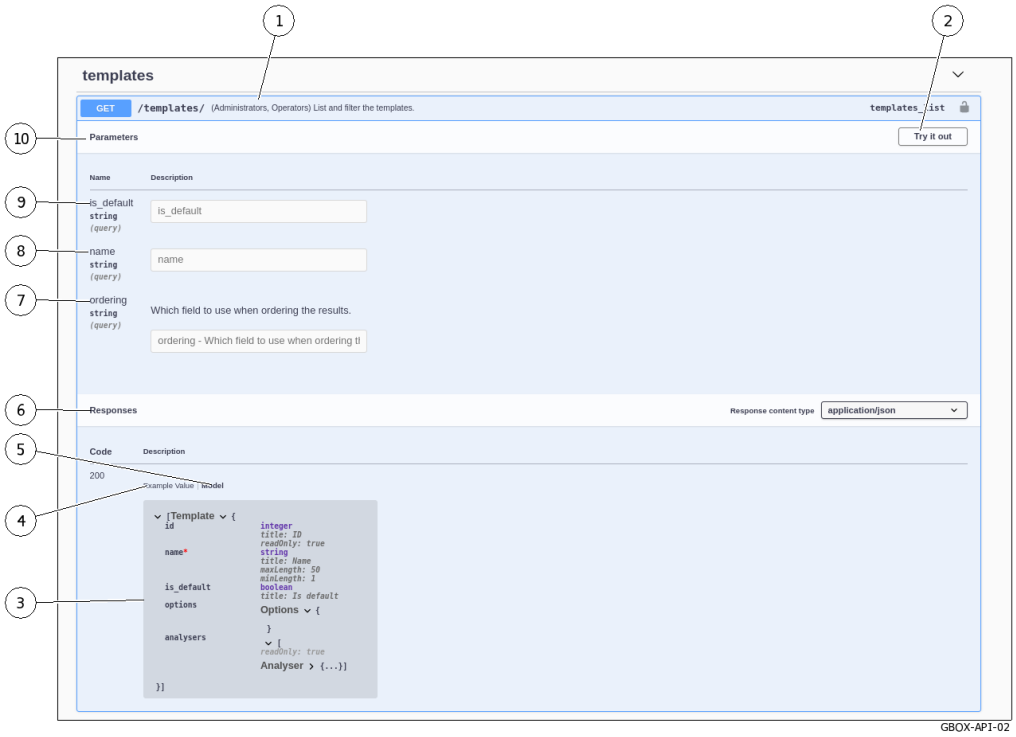
Après appui sur le bouton `API` de la barre de titre, l'écran suivant est affiché.
La fenêtre comprend :



Repère	Description
1	`Schemes` : paramètre indiquant le protocole utilisé (HTTPS)
2	Nom du compte courant : ici compte administrator
3	Bouton `Django Logout`: permet de sortir de l'interface graphique API
4	Bouton `Authorize`: permet de définir l'authentification nécessaire dans les commandes curl
5	Les endpoints sont triés par thème (tag)
6	Champ de filtration : permet de filtrer les thèmes

5.4.1.1 Détail pour un endpoint

Les informations affichées pour un endpoint sont les suivantes :



Repère	Description
1	Ligne de titre. Elle comprend l'action (ici GET), le nom du endpoint (ici /template), les accès (ici Administrators et Opertors), la description du endpoint
2	Bouton `Try it out` : exécute le endpoint avec les paramètres courants
10	Zone `Parameters`: affiche les paramètres optionnelles ou obligatoires pour exécuter la requête. Pour connaître les paramètres obligatoires, se référer à la zone (6). Cette zone comprend :
9	• Paramètre `is_default` : permet de sélectionner le template par défaut. Paramètre `true` à saisir.
8	• Paramètre `name` : définit le nom du modèle dont les informations doivent être récupérées. A regarder dans la fenêtre `Model` pour le type (ici string) et si le paramètre est obligatoire (ici * = obligatoire).
7	• Champ `ordering` : saisir le nom du champ qui sert à ordonner la réponse.
6	Zone `Responses` : zone qui affiche des informations en fonction si le bouton `Try it out` a été activé ou non

Note:

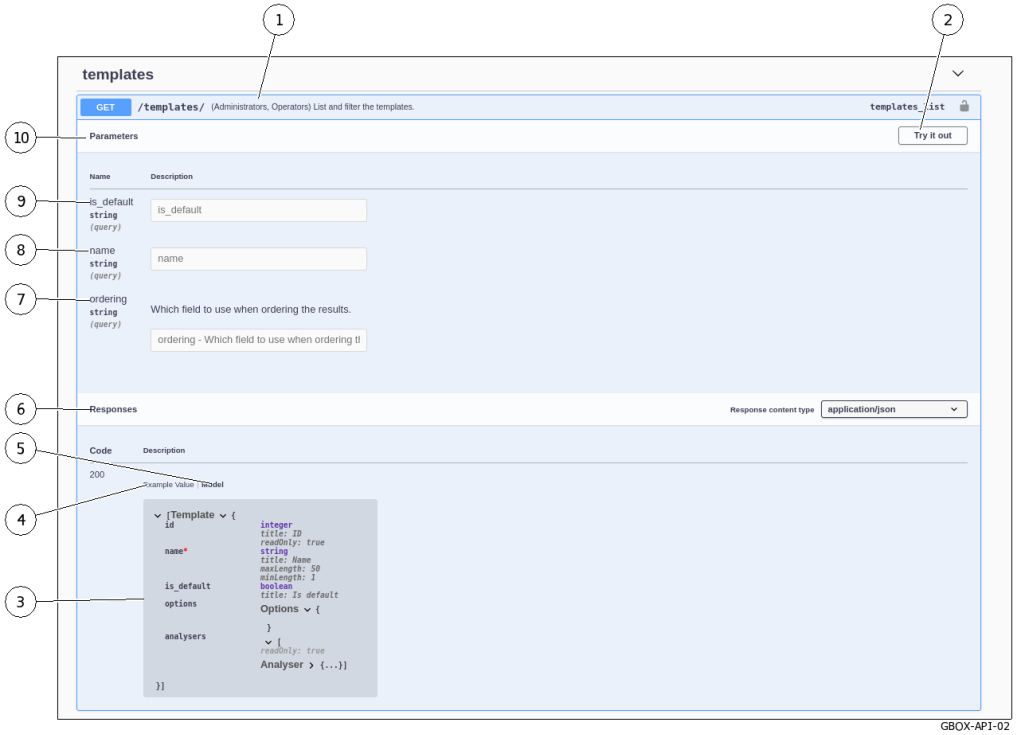
Si un paramètre est obligatoire, un astérisque avec indication `required` est affiché.

Note:

Dans cet écran, il n'est pas possible de saisir les paramètres. Pour cela, il faut exécuter la requête.

5.4.1.1.1 Zone `Responses` si le bouton `Try it out` est non activé

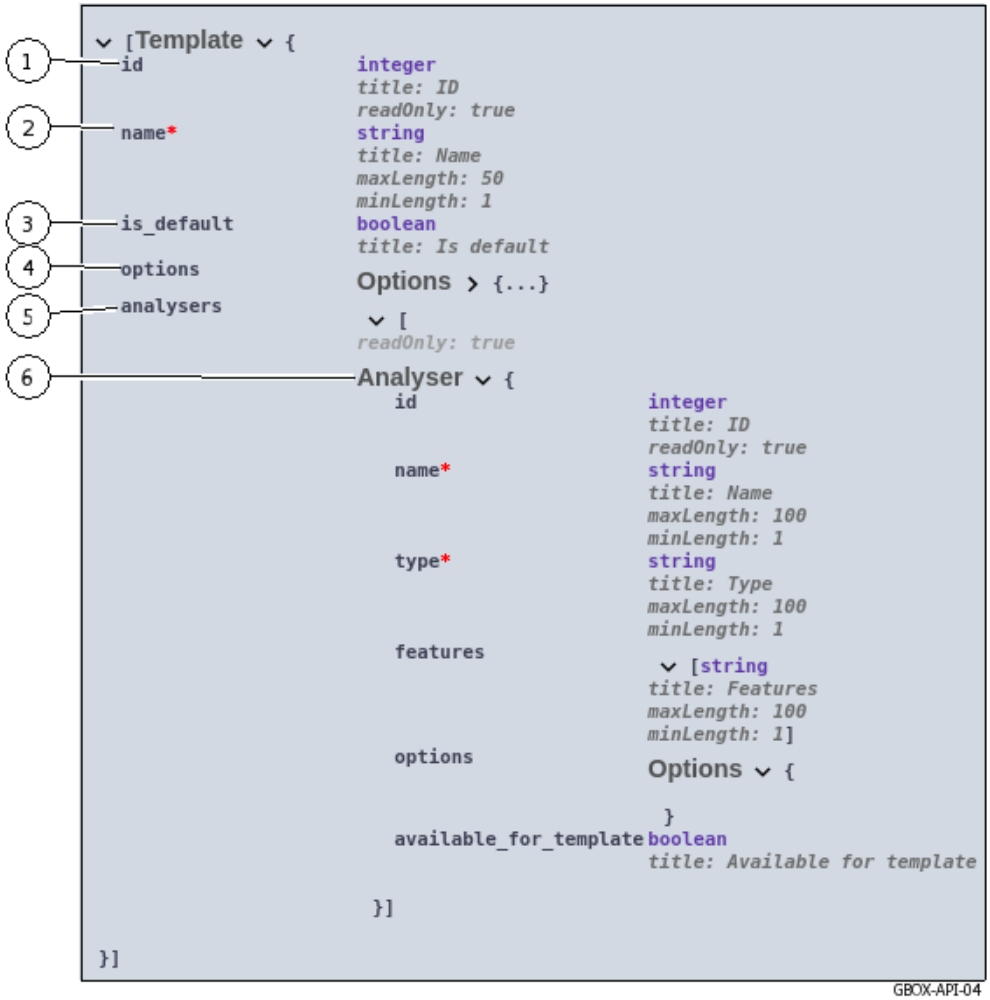
Si le bouton **`Try it out`** est non activé alors la zone **`Responses`** contient les informations de la réponse attendue :



Repère	Description
5	lien **`Model`** : en cliquant sur ce texte, la fenêtre (3) affiche le modèle de la réponse attendue
4	lien **`Example Value`** : en cliquant sur ce texte, la fenêtre (3) affiche un exemple de la réponse attendue avec des valeurs pour exemple. Les valeurs sont, pour le type **integer** (valeur 0), pour le type string (valeur = string), pour le type **boolean** (valeur = true)
3	Champ de visualisation : contient le contenu sélectionné par l'option active (4) ou (5). Un exemple de contenu est donné ci dessous.

5.4.1.1.1.1 Exemple de modèle de sortie

Le modèle de sortie donne la structure des données qui seront affichées en sortie donc après exécution de la requête.



Repère	Description
1	`id` : numéro du modèle. Pour ce paramètre, ses caractéristiques sont indiquées (type, titre...).
2	`name` : nom du modèle. Pour ce paramètre, ses caractéristiques sont indiquées (type, titre, longueur...).
3	`is_defaut` : champ définissant si le modèle courant est le modèle par défaut. La réponse est un booléen (valeur true/false).
4	`options` : champ définissant les options éventuelles.
5	`analysers` : champ définissant les informations de l'ensemble des moteurs.
6	`Analyser` : champ définissant les informations d'un seul moteur.

5.4.1.1.2 Exemple avec des valeurs par défaut

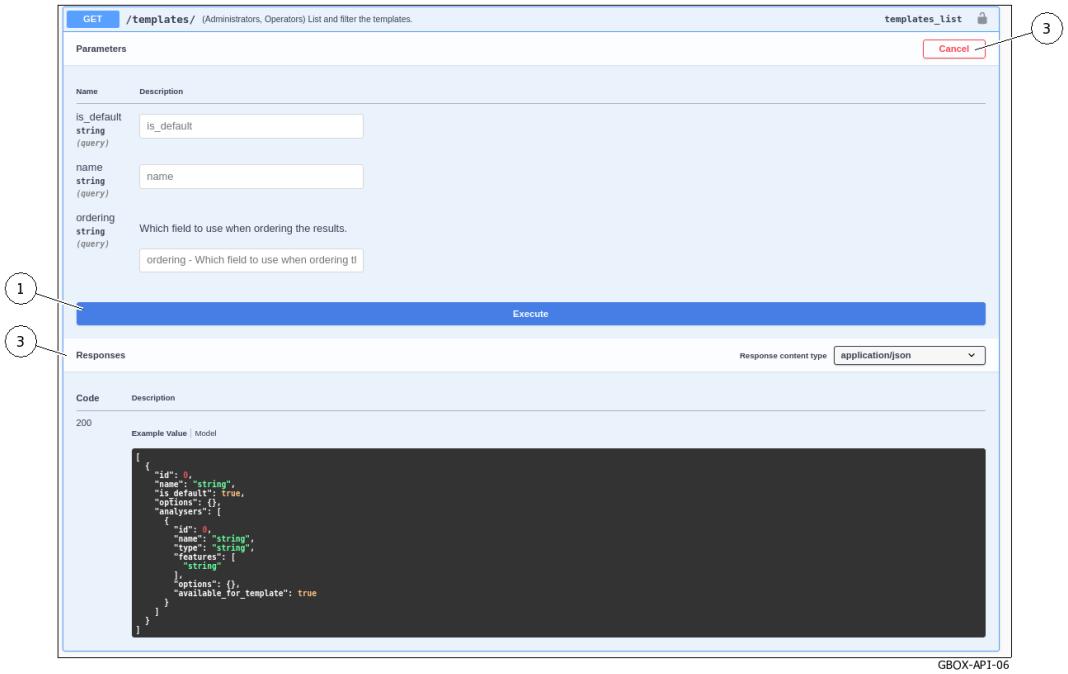
Dans cet exemple, les informations sont affichées avec les valeurs par défaut suivantes :

- les paramètres de type **integer** sont affichés avec le nombre `0`
- les paramètres de type **string** sont affichés avec le texte `string`
- les paramètres de type **booléen** sont affichés avec le texte `true`

Le repérage est le même que dans le modèle de sortie.

5.4.1.1.3 Zone `Responses` si le bouton `Try it out` est activé

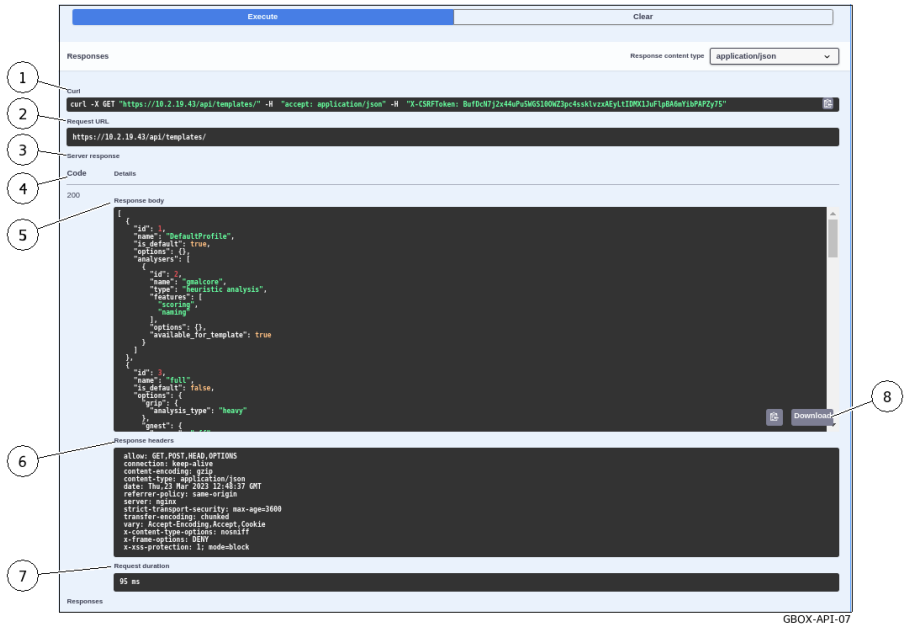
Après avoir cliqué sur le bouton `Try it out`, la zone de saisie des paramètres est activée.
L'écran suivant est affiché :



GBOX-API-06

Repère	Description
1	Bouton `Execute` : permet d'exécuter la requête avec les paramètres courants
2	Bouton `Cancel` : annule la requête
3	La zone `Responses`` n'a pas changé

Après avoir cliqué sur le bouton `Execute`, la requête est lancée et la fenêtre suivante est affichée.



GBOX-API-07

Repère	Description
1	Bouton `Clear` : permet de revenir à l'état avant exécution
2	Zone d'affichage `Curl` : affiche la requête Curl
3	Zone d'affichage `URL` : affiche la requête URL
4	`Code` : si code 200 alors exécution ok. Si le message `code 400 Undocumented Error Bad Request` est affiché, vérifier que les paramètres obligatoires soient bien saisis.
6	`id 1` : modèle numéro 1
7	`Name gmalcore` : moteur id 2 Gmalcore
8	`id 3` : modèle numéro 3
9	`Responses headers` : zone détaillant l'entête de la réponse
10	`Request duration` : valeur en ms de la durée de la requête

5.4.2 Liste des endpoints

Note:

Dans le tableau ci-après la légende est :

- Ope : Rôle Operators
- Adm : Rôle Administrators
- WAuth : Without Authentication
- AUser : Authenticated User

Theme	Nom	Verbe	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

suite sur la page suivante

Table 4 – suite de la page précédente

Theme	Nom	Verbe	Role	Description
Analysis	/analysis/{id}/retry/	POST	Ope	Retry the analysis with the given template
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

suite sur la page suivante

Table 4 – suite de la page précédente

Theme	Nom	Verbe	Role	Description
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.
users-history	/users-history/authentication/	GET	Adm	List and filter the user authentication history
users-history	/users-history/authentication/{id}/	GET	Adm	Retrieve an 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 an 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 an user permission history
users	/users/	GET	Adm	List and filter the users
users	/users/	POST	Adm	Create an 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

Cas d'utilisation

6.1 Introduction

L'utilisation de la Box est décrite au travers de cas d'utilisation listés pour les différents types d'utilisateurs.

6.1.1 Cas d'utilisation : membre du groupe Operators

Pour l'utilisation de la GBox, il est nécessaire d'utiliser l'interface WEB avec un compte membre du groupe **Operators**.
Les tableaux listés dans la section *Comment utiliser la GBox : niveau Operators* permettent d'avoir une vision générale sur les actes courants.

6.1.2 Cas de configuration : compte setup

Pour la configuration initiale de la GBox et pour faire des configurations ou vérifications avancées, il est nécessaire d'utiliser l'interface de configuration avec le compte **setup**.
Les tableaux listés dans la section *Comment administrer la GBox : niveau setup ou Administrators* permettent d'avoir une vision générale sur les actes courants d'administrations.

6.1.3 Cas d'administration : membre du groupe Administrators

Pour l'administration de la GBox, il est nécessaire d'utiliser l'interface WEB avec un compte membre du groupe **Administrators**.
Les tableaux listés dans la section *Comment administrer la GBox : niveau setup ou Administrators* permettent d'avoir une vision générale sur les actes courants.

6.2 Comment se connecter à la GBox

L'accès peut être fait :

- soit par une *Connexion directe devant le serveur*
- soit par une *Connexion à distance en HTTP via l'iDRAC (iDRAC pour un serveur DELL)*
- soit par une *Connexion à distance au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*
- soit par une *Connexion distant au menu de configuration en SSH*
- soit par une *Connexion via un navigateur Web*

L'accès au menu de configuration pour gérer la GBox peut être fait à distance via une connexion SSH ou HTTP.

Note:

La liste des connecteurs physiques à utiliser a été décrite dans la *Présentation de la GBox*.

6.2.1 Connexion directe devant le serveur

La première connexion peut s'effectuer par une connexion directe (avec clavier et écran).
Cela est nécessaire lorsque la configuration réseau n'est pas encore effectuée (ou en cas de non connaissance de l'adresse réseau).
Cette connexion n'est pas la façon nominale d'accéder à l'équipement mais permet de configurer la connexion réseau de l'iDRAC entre autres.
Les accès ultérieurs se feront généralement à distance.

Note:

L'identifiant et le mot de passe par défaut sont indiqués dans la documentation du fabricant du serveur.

Pour la mise en œuvre réservée au compte **setup**, se référer à la *Connexion directe au menu de configuration avec clavier et écran*.

6.2.2 Connexion à distance en HTTP via l'iDRAC (iDRAC pour un serveur DELL)

L'accès distant se fait en utilisant :

- la connexion réseau connectée sur le port iDRAC
- un navigateur Web

Cet accès nécessite :

- la connaissance du nom et mot de passe d'accès à l'iDRAC (accès à l'iDRAC)
- la configuration réseau a été faite (adresse IP de l'iDRAC connue)

Depuis la page Web de l'iDRAC, il est possible de :

- visualiser les ressources matérielles, leur état et la configuration BIOS
- interagir avec le serveur pour l'allumer, l'éteindre ou le redémarrer
- se connecter en mode console

Cette connexion n'est pas la façon nominale d'accéder à l'équipement mais permet d'y accéder en cas de problèmes.
L'accès aux fonctionnalités avancées (accès console..) nécessite l'achat d'une licence spécifique.
Pour plus d'informations, veuillez contacter le support ou un responsable commercial de Gatewatcher.

Pour la mise en œuvre réservée au compte **setup**, se référer à l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*.

6.2.3 Connexion à distance au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série

L'accès distant se fait en utilisant :

- la connexion réseau connectée sur le port iDRAC
- un outil de connexion via SSH

Cet accès nécessite :

- la connaissance du nom et mot de passe d'accès à l'iDRAC (accès à l'iDRAC)
- la configuration réseau a été faite (adresse IP de l'iDRAC connue)

Depuis l'interface, il est possible de :

- de visualiser les messages du système d'exploitation
- se connecter en console à la GBox

Cette connexion n'est pas la façon nominale d'accéder à l'équipement mais permet d'y accéder en cas de problèmes.

Pour la mise en œuvre réservée au compte **setup**, se référer à l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*.

6.2.4 Connexion distant au menu de configuration en SSH

L'accès distant depuis un ordinateur distant à l'équipement se fait de façon sécurisée en utilisant un tunnel SSH.
Cette connexion est la façon nominale d'accéder au menu de configuration de l'équipement.

Pour la mise en œuvre réservée au compte **setup**, se référer à l'*Accès au menu de configuration en SSH*.

6.2.5 Connexion via un navigateur Web

L'accès distant depuis un ordinateur distant à l'équipement se fait en utilisant un navigateur Web.
Cette connexion est la façon nominale d'accéder à l'interface Web de l'équipement.
Pour la mise en œuvre, se référer à la *Connexion à l'interface web via un navigateur internet*.

6.3 Comment se connecter au GCenter

L'accès distant au GCenter se fait via un navigateur Web pour pouvoir associer le GCenter et la GBox.
Pour plus d'informations, se référer à la documentation du GCenter.

6.4 Comment utiliser la GBox : niveau Operators

6.4.1 Accéder à la GBox

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes	Réservé au groupe
Connexion à la GBox via un navigateur Web	1	*Connexion à l'interface web via un navigateur internet*	tous les comptes

---

6.4.2 Analyser un fichier

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Procédure rapide pour analyser un fichier	1	*Procédure rapide pour analyser un fichier*
	2	*Procédure d'analyse du contenu d'un rapport*
Procédure rapide pour analyser un domaine	1	*Procédure rapide pour analyser un domaine*
	2	*Procédure d'analyse du contenu d'un rapport*
Procédure d'analyse d'un fichier dans l'écran `New analysis`	1	*Procédure d'analyse d'un fichier dans l'écran `New analysis`*
	2	*Procédure d'analyse du contenu d'un rapport*
Procédure d'analyse des rapports de la page Reports	1	*Procédure d'analyse de la liste des rapports de page Reports*

6.4.3 Gérer le compte courant

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Modification du mot de passe du compte courant	1	*Modification du mot de passe du compte courant*
Modification de certaines informations de l'utilisateur courant	1	*Modification de certaines informations de l'utilisateur courant*

6.5 Comment administrer la GBox : niveau setup ou Administrators

6.5.1 Accéder à la GBox

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes	Réservé au groupe
Première connexion par une connexion directe	1	*Connexion directe au menu de configuration avec clavier et écran*	setup
Connexion à distance en HTTP via l'iDRAC	1	*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*	setup
Connexion à distance au menu de configuration en SSH via l'interface iDRAC	1	*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*	setup
Connexion directe au menu de configuration en SSH	1	*Accès au menu de configuration en SSH*	setup
Connexion à la GBox via un navigateur web	1	*Connexion à l'interface web via un navigateur internet*	tous les comptes

---

6.5.2 Configurer la GBox

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
La première installation	1	Procédure de *Configuration de la GBox lors de la première connexion*
	2	Procédure de *Mise en exploitation d'une GBox*
Configuration du clavier	1	Utilisation de la *Commande `Keymap`*
Modification de la licence	1	Procédure de *Modification de la licence*
Mise en exploitation d'une GBox	1	Procédure de *Mise en exploitation d'une GBox*
Modification du certificat SSL	1	Procédure de *Mise en place d'un certificat SSL*

6.5.3 Gérer les comptes de la Web UI

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Création d'un utilisateur local	1	*Création d'un utilisateur local*
Modification de certaines informations d'un utilisateur local	1	*Modification de certaines informations d'un utilisateur local*
Modification du mot de passe du compte courant	1	*Modification du mot de passe du compte courant*
Réinitialisation du mot de passe d'un utilisateur local	1	*Réinitialisation du mot de passe d'un utilisateur*
Suppression d'un utilisateur local	1	*Suppression d'un utilisateur*
Visualisation de l'historique des authentifications	1	*Visualisation de l'historique des authentifications*
Visualisation de l'historique des créations ou suppressions des utilisateurs	1	*Visualisation de l'historique des créations ou suppressions des utilisateurs*
Visualisation de l'historique de toutes les modifications des droits des utilisateurs	1	*Visualisation de l'historique de toutes les modifications des droits des utilisateurs*

6.5.4 Gérer le compte setup du menu de configuration

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Modification du mot de passe du compte setup	1	*Accès au menu de configuration en SSH*
	2	Utiliser la commande *Commande `Password`*

6.5.5 Gérer le réseau

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Visualisation de la configuration courante de la GBox	1	*Procédure d'accès au sous-menu `Network Setup`*
	2	*Procédure de visualisation de la configuration courante*
Visualisation de la configuration de chaque interface réseau	1	*Procédure d'accès au sous-menu `Network Setup`*
	2	*Procédure de visualisation de l'état des interfaces réseau*
Modification des paramètres généraux de la GBox	1	*Procédure d'accès au sous-menu `Network Setup`*
	2	*Procédure de modification des paramètres généraux de la GBox*
Gestion des paramètres de l'interface réseau de management GBx0	1	*Procédure d'accès au sous-menu `Network Setup`*
	2	Appliquer la *Procédure de modification des paramètres des interfaces réseaux* pour l'interface GBx1
	3	*Procédure de prise en compte des modifications*
Configuration de l'interface réseau GBx1 des machines virtuelles de Gnest à Internet	1	*Procédure d'accès au menu `Services`*
	2	*Procédure d'accès aux services Sandbox du moteur Gnest*
	3	*Procédure d'activation de la connexion internet*
	4	*Procédure d'accès au sous-menu `Network Setup`*
	5	Appliquer la *Procédure de modification des paramètres des interfaces réseaux* pour l'interface GBx1
	6	*Procédure de prise en compte des modifications*
	7	Activer l'option `Network` dans les paramètres de Gnest dans les modèles de Malware : pour cela se référer à la *Procédure de modification d'un modèle existant*

6.5.6 Gérer les moteurs d'analyse

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Configuration du moteur Gnest (modification du nombre de machines virtuelles)	1	*Procédure de configuration du moteur Gnest*
	2	Modification de modèles existants pour prendre en compte cette nouvelle configuration : *Procédure de configuration du moteur Gnest*
Configuration du moteur Gmalcore	1	*Procédure de configuration du moteur Gmalcore*
	2	Modification de modèles existants pour prendre en compte cette nouvelle configuration : *Procédure de configuration du moteur Gmalcore*
Surveillance des moteurs d'analyse	1	*Procédure de surveillance des moteurs d'analyse*

6.5.7 Gérer le serveur GBox

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Quitter la session en cours ou quitter la session SSH	1	Utiliser la *Commande `Exit`*
Système : redémarrer la GBox	1	Utiliser la *Commande `Restart`*
Système : éteindre la GBox	1	Utiliser la *Commande `Shutdown`*
Effacer les données et de remettre la GBox dans son paramétrage sortie d'usine	1	Utiliser la *Commande `Reset`*
Services Malcore : forcer le redémarrage ou la réinstallation	1	Utiliser la *Commande `Services`*
Redémarrer les applications	1	Utiliser la *Commande `Gapps`*

6.5.8 Gérer les modèles d'analyse

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Créer de nouveaux modèles	1	*Création d'un modèle d'analyse*
Gérer les modèles	1	*Gestion des modèles d'analyse*

6.5.9 Surveiller la GBox

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Surveillance : téléchargement des fichiers pour le diagnostic	1	*Génération et téléchargement des fichiers pour le diagnostic*

6.5.10 Utiliser l'API

Pour effectuer la tâche suivante	#	Effectuer successivement les procédures suivantes
Connexion à l'interface Web via un navigateur internet	1	*Connexion à l'interface web via un navigateur internet*
Création ou suppression d'un token d'accès d'un API	1	*Création ou suppression d'un token d'accès d'un API*
Utilisation d'un endpoint API	1	*Utilisation d'un endpoint API*

6.5.11 Gérer le logiciel via GUM

Pour effectuer la tâche suivante	Effectuer successivement les procédures suivantes	
Mettre à jour des moteurs (updates)	1	Si besoin, configurer le proxy (mode local) : voir la procédure de *Configuration d'un proxy*
	2	Selon le mode (local ou online), appliquer la procédure correspondante *Configuration de la mise à jour automatique via GUM*
	3	Vérifier le bon fonctionnement de la mise à jour avec l'*Installation manuelle d'une mise à jour des signatures (update)*
Installation d'un patch correctif (Hotfix)	1	*Installation d'un correctif (Hotfix)*
Installation d'une mise à niveau (upgrade)	1	*Installation d'une mise à niveau (upgrade)*

Chapter 7

Cas d'utilisation du menu de configuration: compte setup

7.1 Connexion directe au menu de configuration avec clavier et écran

7.1.1 Introduction

La première connexion peut s'effectuer par une connexion directe (avec clavier et écran).
Cela est nécessaire lorsque la configuration réseau n'est pas encore effectuée (ou en cas de non connaissance de l'adresse réseau).
Cette connexion n'est pas la façon nominale d'accéder à l'équipement mais permet de configurer la connexion réseau de l'iDRAC entre autres.
Les accès ultérieurs se feront généralement à distance.

Note:

L'identifiant et le mot de passe par défaut sont indiqués dans la documentation du fabricant du serveur.

7.1.2 Opérations préliminaires

- Connecter les câbles d'alimentation.
- Connecter les câbles réseau (voir la *Présentation de la GBox*).

7.1.3 Procédure pour connecter l'écran et clavier

- Connecter l'écran sur le connecteur VGA.
- Connecter le clavier sur un des connecteurs USB.
- Mettre sous tension le serveur.

7.1.4 Procédure pour connaître (ou modifier) les paramètres réseau de l'iDRAC via le BIOS

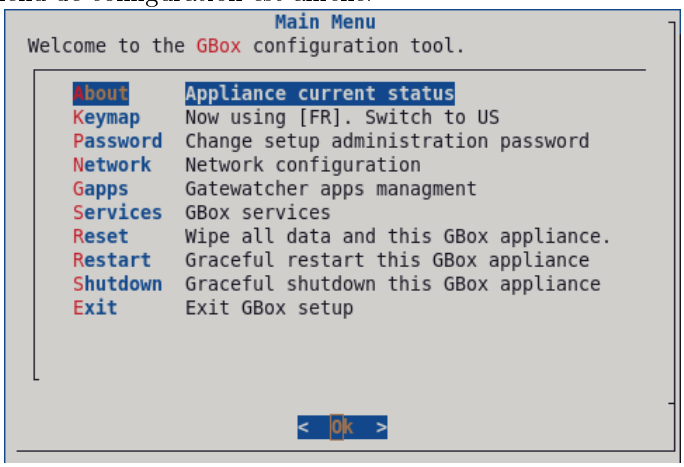
- Appuyer sur **F2** pendant l'auto-test de démarrage (POST).
- Sur la page `` `System Setup Main Menu` `` (menu principal de la configuration du système), cliquer sur `` `iDRAC Settings` `` (Paramètres iDRAC).

  La page `` `iDRAC settings` `` s'affiche.
- Cliquer sur `` `Network` ``.

  La page `` `IDRAC Settings. Network` `` s'affiche.
- Noter les paramètres réseaux dans les paramètres `` `Network Settings` `` ou modifier ces paramètres.
- Après avoir noté la configuration réseau, sortir du BIOS.
- Cliquer successivement sur le bouton `` `Back` `` puis sur le bouton `` `Finish` ``.
- Dans la fenêtre `` `Warning` `` demandant de sauvegarder les modifications, cliquer sur le bouton `` `No` ``.
- Dans l'écran `` `System Setup` ``, cliquer sur le bouton `` `Finish` ``.
- Dans la fenêtre `` `Warning` `` demandant de confirmer la sortie, cliquer sur le bouton `` `Yes` ``.

  Le serveur redémarre...
- Débrancher les écrans et clavier si nécessaire.

  Le menu de configuration est affiché.



Note:

Appuyer sur la première lettre d'une commande pour accéder rapidement à celle-ci.
Appuyer sur le bouton `` `OK` `` pour valider le choix sélectionné.

7.2 Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)

7.2.1 Introduction

L'accès distant se fait en utilisant :

- la connexion réseau connectée sur le port iDRAC
- un navigateur Web

Cet accès nécessite :

- la connaissance du nom et mot de passe d'accès à l'iDRAC (accès à l'iDRAC)
- la configuration réseau a été faite (adresse IP de l'iDRAC connue)

Depuis la page Web de l'iDRAC, il est possible de :

- visualiser les ressources matérielles, leur état et la configuration BIOS
- interagir avec le serveur pour l'allumer, l'éteindre ou le redémarrer
- se connecter en mode console

Cette connexion n'est pas la façon nominale d'accéder à l'équipement mais permet d'y accéder en cas de problèmes.
L'accès aux fonctionnalités avancées (accès console..) nécessite l'achat d'une licence spécifique.
Pour plus d'informations, veuillez contacter le support ou un responsable commercial de Gatewatcher.

7.2.2 Opérations préliminaires

- Effectuer la configuration réseau de l'iDRAC (voir la procédure de *Connexion directe au menu de configuration avec clavier et écran*).

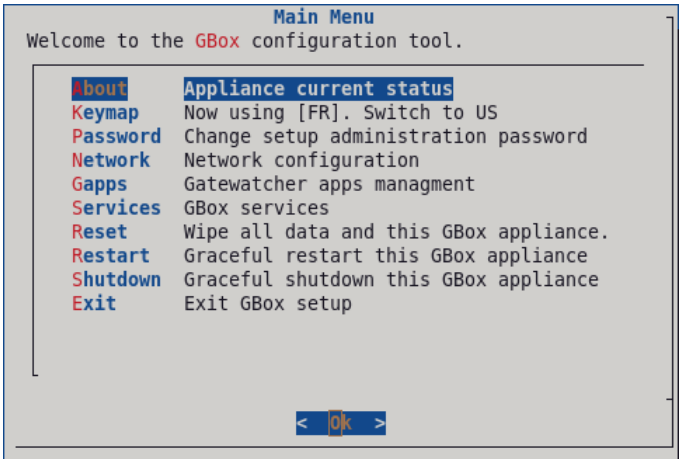
7.2.3 Procédure

- Sur l'ordinateur distant, ouvrir un navigateur internet.
- Saisir l'URL : https://iDRAC-IP-address

> **Note:**
> iDRAC-IP-address est l'adresse IP de l'interface iDRAC de la GBox .

- Valider.
  La fenêtre `Login` est affichée.
- Entrer les paramètres demandés :
  - `Username` : identifiant
  - `Password` : mot de passe de l'identifiant saisi
  - `Domain` : sélectionner `This IDRAC`
- Cliquer sur le bouton `Log In`.
- Lancer la console virtuelle (zone `Virtual console`, bouton `Launch Virtual console`).
  A la suite de cette action, une nouvelle page s'ouvre et il sera possible d'interagir avec l'équipement.

Le menu de configuration est affiché.



Note:

Appuyer sur la première lettre d'une commande pour accéder rapidement à celle -ci.
Appuyer sur le bouton `OK` pour valider le choix sélectionné.

7.3 Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série

7.3.1 Introduction

L'accès distant se fait en utilisant :

- la connexion réseau connectée sur le port iDRAC
- un outil de connexion via SSH

Cet accès nécessite :

- la connaissance du nom et mot de passe d'accès à l'iDRAC (accès à l'iDRAC)
- la configuration réseau a été faite (adresse IP de l'iDRAC connue)

Depuis l'interface, il est possible de :

- de visualiser les messages du système d'exploitation
- se connecter en console à la GBox

Cette connexion n'est pas la façon nominale d'accéder à l'équipement mais permet d'y accéder en cas de problèmes.

7.3.2 Opérations préliminaires

- Effectuer la configuration réseau de l'iDRAC (voir la procédure de *Connexion directe au menu de configuration avec clavier et écran*).

7.3.3 Procédure sur le PC distant sous Linux

- Ouvrir une invite de commande.
- Entrer la commande `` `ssh identifiant@adresse_ip` ``.
  Par exemple, `` `ssh setup@x.x.x.x` `` où
  - `` `setup` `` est l'identifiant et
  - x.x.x.x est l'adresse IP du port iDRAC
- Valider la commande.
- Entrer le mot de passe de l'identifiant saisi.
- Appuyer sur `` `Enter` ``.
- Entrer la commande suivante `` `racadm>>console com2` ``.
- Valider.
  Le système affiche désormais l'interface graphique de l'équipement.

7.3.4 Procédure sur le PC distant sous Windows

- Ouvrir un logiciel client SSH, type Putty.
- Entrer l'adresse IP de l'interface iDRAC puis valider.
- Entrer la commande suivante `` `racadm>>console com2` ``.
- Valider.
  Le système affiche désormais l'interface graphique de l'équipement.

7.4 Accès au menu de configuration en SSH

7.4.1 Introduction

L'accès distant depuis un ordinateur distant à l'équipement se fait de façon sécurisée en utilisant un tunnel SSH.
Cette connexion est la façon nominale d'accéder au menu de configuration de l'équipement.

7.4.2 Opérations préliminaires

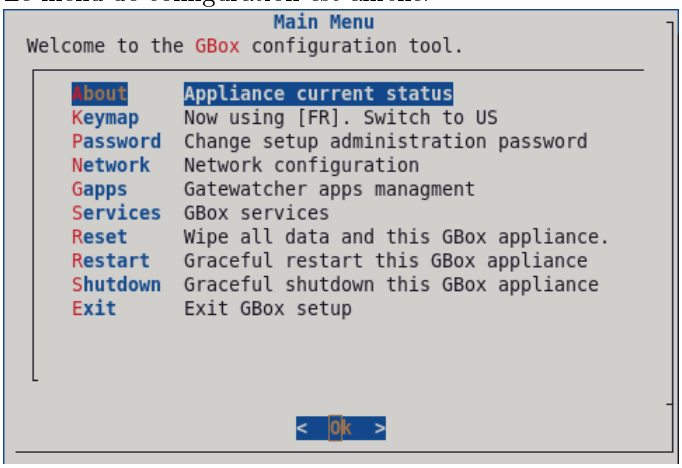
- Effectuer une première connexion (voir la procédure de *Connexion directe au menu de configuration avec clavier et écran*).
- Connaître le nom de la GBox ou son adresse IP.

7.4.3 Procédure sur le PC distant sous Linux

- Ouvrir une invite de commande.
- Entrer la commande `ssh identifiant@adresse_ip_GBox` ou `ssh identifiant@FQDN_GBox`.
  Par exemple, `ssh setup@gGBox` où :
  - l'identifiant est `setup` et
  - le FQDN est `GBox`
- Valider la commande.
- Entrer le mot de passe.

7.4.4 Procédure sur le PC distant sous Windows

- Ouvrir un logiciel client SSH, type Putty.
- Entrer l'adresse IP de l'interface GBox puis valider.
- Entrer l'identifiant et le mot de passe.
  Le menu de configuration est affiché.



Note:

Appuyer sur la première lettre d'une commande pour accéder rapidement à celle -ci.
Appuyer sur le bouton `OK` pour valider le choix sélectionné.

7.5 Commande `About`

7.5.1 Introduction

La commande `About` affiche les informations :

- `GBox Name` : nom de la GBox
- `Version` : version du logiciel
- `IP Address` : adresse IP de l'interface réseau active
- `Subnet Mask` : masque de sous réseau de l'interface réseau active
- `Default Gateway` : passerelle par défaut

7.5.2 Prérequis

- Utilisateur : setup

7.5.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.5.4 Procédure

Le menu de configuration est affiché.

- Sélectionner la ligne `About` ou appuyer sur la lettre **A**.
- Appuyer sur le bouton `OK`.
  La fenêtre `About` est affichée et montre les informations de la GBox.

```
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:

Les informations affichées sont une exemple..

- Appuyer sur la touche `OK` pour revenir au menu.

7.6 Commande `Keymap`

7.6.1 Introduction

La commande `Keymap` permet de changer la langue du clavier (choix US ou FR).

7.6.2 Prérequis

- Utilisateur : setup

7.6.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.6.4 Procédure

Le menu de configuration est affiché.
Le système indique :

  - la configuration courante
  - et, s'il y a appui sur la ligne, le basculement sur l'autre langue.

    Par exemple : la ligne `` `Keymap` `` indique : `` `Now using [US]. Switch to FR` ``.
    Dans ce cas, la langue courante du clavier est US.

- Sélectionner la ligne `` `Keymap` `` ou appuyer sur la lettre **K**.
- Appuyer sur le bouton `` `OK` ``.
  Le système change la langue du clavier.
  La ligne `` `Keymap` `` est mise à jour : `` `Now using [FR]. Switch to US` ``
- Appuyer sur la touche `` `OK` `` pour revenir au menu.

7.7 Commande `` `Password` ``

7.7.1 Introduction

La commande `` `Password` `` permet de modifier le mot de passe du compte **setup**.

7.7.2 Prérequis

- Utilisateur : setup

7.7.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.7.4 Procédure

Le menu de configuration est affiché.

- Sélectionner la ligne `` `Password` `` ou appuyer sur la lettre **P**.
- Appuyer sur le bouton `` `OK` ``.
  La fenêtre `` `About to change the setup administration password` `` s'affiche.
  Le message suivant est affiché :

```
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?
```

- Appuyer sur le bouton `` `Yes` `` pour changer le mot de passe ou le bouton `` `No` `` pour annuler.
- Si le bouton `` `Yes` `` a été appuyé, le message suivant est affiché : `` `New Password for setup` ``.
  - Entrer le mot de passe courant puis valider.
  - Entrer à nouveau le mot de passe courant puis valider.
    Après acceptation, le message suivant est affiché `` `Password successfully changed` ``.
  - Cliquer sur le bouton `` `OK` ``.
    En cas d'erreur, le message suivant est affiché : `` ` Do you want to retry?` ``
- Sélectionner le bouton `` `Yes` `` pour relancer la procédure de changement de mot de passe ou le bouton `` `No` `` pour annuler.

7.8 Commande `` `Network` ``

7.8.1 Introduction

Les informations de la configuration réseau sont :

- des paramètres généraux :
  - nom (hostname)
  - nom du domaine (domain name)
  - serveurs DNS (primaire et secondaire)
  - serveurs NTP (primaire et secondaire)
  - nom de l'interface activée
- des paramètres de chaque interface réseau :
  - adresse IP
  - masque
  - passerelle
  - table routage

La commande `` `Network` `` permet d'accéder au sous-menu `` `Network Setup` `` :

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

Chacune de ces commandes est détaillée dans le tableau suivant :

Menu	Fonction	Voir procédure
`Show current configuration`	Visualiser la configuration courante : le DNS, domaine, informations des interfaces réseau GBx (0 à 3), le hostname, le NTP	*Procédure de visualisation de la configuration courante*
`Show interface status`	Visualiser l'état des interfaces réseau adresse MAC, état du carrier, vitesse, le type de connexion	*Procédure de visualisation de l'état des interfaces réseau*
`Hostname, domain, DNS, NTP`	Modification des paramètres généraux de la GBox : DNS, domaine, hostname, NTP	*Procédure de modification des paramètres généraux de la GBox*
`Configure interfaces`	Modification des paramètres des interfaces réseaux : pour chaque interface réseau, adresse MAC, état du carrier, vitesse, le type de connexion	*Procédure de modification des paramètres des interfaces réseaux*
`Apply Network Config`	Appliquer la configuration courante sur les interfaces réseaux	*Procédure de prise en compte des modifications*

7.8.2 Prérequis

- Utilisateur : setup

7.8.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.8.4 Procédure d'accès au sous-menu `Network Setup`

Le menu de configuration est affiché.

- Sélectionner la ligne `Network` ou appuyer sur la lettre **N**.
  Le sous-menu `Network Setup` est affiché :

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

7.8.5 Procédure de visualisation de la configuration courante

Le sous-menu `Network Setup` est affiché.

- Sélectionner la ligne `Show current configuration` ou appuyer sur la lettre **S**.
- Appuyer sur le bouton `OK`.
  La fenêtre `Current Network Configuration` est affichée :

```
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
```

Cette fenêtre affiche :

- le DNS
- le nom du domaine
- pour chaque interface réseau gbx(0 à 3),
  - l'adresse IP
  - le masque
  - le sous réseau
  - la table de routage
  - l'information interface active ou non
- le hostname de la GBox
- le NTP

- Appuyer sur le bouton `Back` pour revenir au menu précédent.

7.8.6 Procédure de visualisation de l'état des interfaces réseau

Le sous-menu `Network Setup` est affiché.

- Sélectionner la ligne `Show interface status` ou appuyer sur la lettre **S** jusqu'à sélectionner cette commande.
- Appuyer sur le bouton `OK`.
  La fenêtre suivante est affichée :

```
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
```

  Cette fenêtre affiche pour chaque interface réseau (gbx) :

  - son nom (colonne `name`)
  - son adresse MAC (colonne `Address`)
  - la présence de la porteuse (colonne `Carrier`) : UP ou DOWN
  - la vitesse (colonne `Speed`)
  - le type de connexion (colonne `Type`)

- Si besoin, cliquer sur le bouton `refresh`.
- Appuyer sur le bouton `Back` pour revenir au menu précédent.

7.8.7 Procédure de modification des paramètres généraux de la GBox

Le sous-menu `Network Setup` est affiché.

- Sélectionner la ligne `hostname, domain, DNS, NTP` ou appuyer sur la lettre **S** jusqu'à sélectionner cette commande.
- Appuyer sur le bouton `OK`.
  La fenêtre suivante est affichée :

```
Configure GBox Network

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

(suite sur la page suivante)

(suite de la page précédente)

```
NTP Server (primary)   :  192.168.1.251
NTP Server (secondary) :  ``
```

Note:

Seul le point décimal est accepté dans la saisie de l'adresse IPv4.

- Si besoin, modifier les valeurs.
- Appuyer sur le bouton `Ok` pour valider les informations ou sur le bouton `Cancel` pour revenir au menu précédent.
- Appliquer les modifications (voir la *Procédure de prise en compte des modifications*).

7.8.8 Procédure de modification des paramètres des interfaces réseaux

Le sous-menu `Network Setup` est affiché.

- Sélectionner la ligne `Configure interfaces` ou appuyer sur la lettre **C** jusqu'à sélectionner cette commande.
- Appuyer sur le bouton `OK`.
  La fenêtre suivante est affichée :

```
Choose an interface

 gbx 0 :  192.168.1.43
 gbx 1 :
```

- Sélectionner une interface (ici gbx 0 ou 1) ou cliquer sur le bouton `Cancel` pour revenir au menu précédent.
  La fenêtre suivante est affichée (par exemple gbx 0) :

```
Configure gbx0

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

Note:

Seul le point décimal est accepté dans la saisie de l'adresse IPv4

- Si besoin, modifier les valeurs.
- Appuyer sur le bouton `Ok` pour valider les informations ou sur le bouton `Return` pour revenir au menu précédent.
- Appuyer sur le bouton `Return` pour revenir au menu précédent.
- Appliquer les modifications (voir la *Procédure de prise en compte des modifications*).

7.8.9 Procédure de prise en compte des modifications

Le sous-menu `Network Setup` est affiché.

- Sélectionner la ligne `Apply Network Config` ou appuyer sur la lettre **A** jusqu'à sélectionner cette commande.
- Appuyer sur le bouton `OK`.
  Les modifications sont prises en compte.
  La liste des paramètres est affichée et un état par type de paramètre est affichée.
  Un compte rendu global est affichée à la fin (DONE = ok).
  Une barre de progression est affichée.
- Quand les modifications sont appliquées, appuyer sur le bouton Entrée du clavier pour revenir au menu précédent.
  Le menu de configuration est affiché.

7.9 Commande `Gapps`

7.9.1 Introduction

La commande `Gapps Management` permet de redémarrer les applications de la GBox.
Les services déployant l'application web, les bases de données et les moteurs d'analyse sont redémarrés.

Important:

Cette option est à utiliser avec précaution.

7.9.2 Prérequis

- Utilisateur : setup

7.9.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.9.4 Procédure

Le menu de configuration est affiché.

- Sélectionner la ligne `Gapps` ou appuyer sur la lettre **G**.
- Appuyer sur le bouton `OK`.
  La fenêtre `Gapps` est affichée :

```
Restart   Restart the Gapps
```

- Sélectionner la ligne `Restart Restart the Gapps` ou appuyer sur la lettre **R** .
- Appuyer sur le bouton `OK`.
  Le système affiche la fenêtre `Restarting Gbox stack`.
  Un message indiquant le redémarrage en cours.
- Attendre l'affichage du message `Gbox stack successfully restarted`.
- Appuyer sur le bouton `OK`.
- Appuyer sur la touche `Return` pour revenir au menu principal.

7.10 Commande `Services`

7.10.1 Introduction

La commande `Services` permet de :

- pour le service Malcore : forcer le redémarrage ou la réinstallation
- pour les services Sandbox :

- activation ou désactivation de l'interface réseau de connexion à Internet
- possibilité de configurer cette interface (adresse IP...)
- configurer un proxy

7.10.2 Prérequis

- Utilisateur : setup

7.10.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.10.4 Procédure d'accès au menu `Services`

Le menu de configuration est affiché.

- Sélectionner la ligne `Services` ou appuyer sur la lettre **S**.
- Appuyer sur le bouton `OK`.
  La fenêtre `Services` suivante est affichée :

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

Chacune de ces commandes est détaillée dans le tableau suivant :

Commande	Fonction	Voir
`Malcore service`	Accès au service du moteur Malcore	*Procédure d'accès au service du moteur Malcore*
`Sandbox services`	Accès aux services Sandbox du moteur Gnest	*Procédure d'accès aux services Sandbox du moteur Gnest*

7.10.5 Procédure d'accès au service du moteur Malcore

La fenêtre `Services` suivante est affichée.

- Sélectionner la ligne `Malcore service` ou appuyer sur la lettre **M**.
- Cliquer sur le bouton `OK`.
  La fenêtre `Malcore Services Manager` est affichée :

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

Chacune de ces commandes est détaillée dans le tableau suivant :

Commande	Fonction
`Restart Malcore forcefully`	Force le redémarrage du service Malcore : à utiliser en cas de blocage
`Reinstall Malcore service`	Réinstaller le service Malcore

- Pour forcer le redémarrage du service :
  - Sélectionner la commande `Restart Malcore forcefully` et valider.
    La fenêtre `Restart Malcore forcefully` est affichée.
  - Attendre l'affichage du message `Malcore successfully restarted`.
  - Cliquer sur le bouton `OK`.
- Pour réinstaller le service :
  - Sélectionner la commande `Reinstall Malcore service` et valider.
    La fenêtre `About to reinstall malcore` est affichée.

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

  - Cliquer sur le bouton `OK`.
    La fenêtre `About to reinstall malcore` est affichée.
  - Attendre l'affichage du message `Malcore successfully restarted`.
  - Cliquer sur le bouton `OK`.
- Appuyer sur la touche `OK` pour revenir au menu principal.

7.10.6 Procédure d'accès aux services Sandbox du moteur Gnest

La fenêtre `Services` suivante est affichée.

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

- Sélectionner la ligne `Sandbox services` ou appuyer sur la lettre **S**.
- Cliquer sur le bouton `OK`.
  La fenêtre `Sandbox Services Manager` est affichée :

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

Note:

L'activation de la connexion Internet est utilisée par les machines virtuelles de Gnest.
Toutefois cette activation doit être faite aussi dans la configuration des modèles d'analyse : la mise en œuvre est donnée dans la *Procédure de configuration du moteur Gnest*.

Chacune de ces commandes est détaillée dans le tableau suivant :

Commande	Fonction	Voir procédure
`Enable internet ouput`	Activer la connexion Internet	*Procédure d'activation de la connexion internet*
`Disable internet ouput`	Désactiver la connexion Internet	*Procédure de désactivation de la connexion internet*

7.10.6.1 Procédure d'activation de la connexion internet

- Sélectionner la commande `Enable internet ouput` et valider.
  Le menu `Enable internet output` est affichée.

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

Chacune de ces commandes est détaillée dans le tableau suivant :

Commande	Fonction	Voir procédure
`` `Internet output interface` ``	Sélection de l'interface physique de la GBox connectée physiquement à Internet (gbx1 à 3)	*Procédure d'activation de la connexion internet*
`` `Proxy configuration` ``	Configurer un proxy d'accès à Internet	*Procédure d'accès aux services Sandbox du moteur Gnest*
`` `Apply internet configuration` ``	Appliquer la configuration Internet	*Procédure d'accès aux services Sandbox du moteur Gnest*

- Pour choisir une interface pour la sortie vers internet :
  - Sélectionner la commande `` `Internet output interface` `` et valider.
    La fenêtre `` `Choose an interface` `` est affichée.
  - Sélectionner une interface (par exemple gbx1) puis appuyer sur la touche `` `OK` ``.
    Le message suivant est affiché : `` `you either have to configure gbx1 or choose another interface` ``.
  - Appuyer sur la touche `` `OK` `` pour configurer l'interface sélectionnée (ici gbx1).
    Le message suivant est affiché : `` `Internet ouput successfully configured` ``.
  - Appuyer sur la touche `` `OK` `` pour revenir au menu précédent.
  - Appuyer sur la touche `` `Return` `` pour revenir au menu précédent.
- Pour configurer un proxy :
  - Sélectionner la commande `` `Proxy configuration` `` et valider.
    La fenêtre `` `Proxy configuration` `` est affichée.
  - Saisir l'adresse IP.
  - Saisir le port.
  - Appuyer sur la touche `` `OK` `` pour valider la saisie.
  - Appuyer sur la touche `` `OK` `` pour revenir au menu précédent.
  - Appuyer sur la touche `` `Return` `` pour revenir au menu précédent.
- Pour appliquer les modifications de la configuration réseau :
  - Sélectionner la commande `` `Apply internet configuration` `` et valider.
    Plusieurs messages apparaissent puis le menu `` `Enable internet output` `` est affiché.
  - Appuyer sur la touche `` `OK` `` pour revenir au menu précédent.
  - Appuyer sur la touche `` `Return` `` pour revenir au menu précédent.

7.10.6.2 Procédure de désactivation de la connexion internet

- Sélectionner la commande `` `Disable internet ouput` `` et valider.
  La fenêtre `` `Disable internet output` `` est affichée.

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

- Cliquer sur le bouton `` `Yes` `` pour désactiver l'interface connecté vers internet.
- Attendre l'affichage du message `` `Ìnternet ouput successfully disabled` ``.
- Appuyer sur la touche `` `OK` `` pour revenir au menu précédent.
- Appuyer sur la touche `` `Return` `` pour revenir au menu précédent.
- Appuyer sur la touche `` `Return` `` pour revenir au menu précédent.

7.11 Commande `Reset`

7.11.1 Introduction

La commande `Reset` permet d'effacer les données et de remettre la GBox dans son paramétrage "sortie d'usine".
L'ensemble des configurations et des données sont effacées.

7.11.2 Prérequis

- Utilisateur : setup

7.11.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.11.4 Procédure

Le menu de configuration est affiché :

- Sélectionner la ligne `Reset` ou appuyer sur la lettre **A**.
- Appuyer sur le bouton `OK`.
  La fenêtre `Reset GBox Appliance` est affichée :

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

- Appuyer sur :
  - le bouton `Yes` pour continuer
  - le bouton `No` pour annuler

7.12 Commande `Restart`

7.12.1 Introduction

La commande `Restart` permet de redémarrer proprement la GBox.

7.12.2 Prérequis

- Utilisateur : setup

7.12.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.12.4 Procédure

Le menu de configuration est affiché.

- Sélectionner la ligne `Restart` ou appuyer sur la lettre **R**.
- Appuyer sur le bouton `OK`.
  La fenêtre `Rebooting` est affichée :

```
Rebooting in 10 seconds
You can still abort reboot by pressing <ESC> or <Cancel> button.
```

- Appuyer sur :
  - le bouton `Reboot now` pour revenir au menu.
  - le bouton `Cancel` pour annuler le redémarrage.

7.13 Commande `Shutdown`

7.13.1 Introduction

La commande `Shutdown` permet d'éteindre la GBox.

7.13.2 Prérequis

- Utilisateur : setup

7.13.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.13.4 Procédure

Le menu de configuration est affiché.

- Sélectionner la ligne `Shutdown` ou appuyer sur la lettre **S**.
- Appuyer sur le bouton `OK`.
  La fenêtre `Shutdown` est affichée :

```
Shutdowning in 10 seconds
You can still abort reboot by pressing <ESC> or <Cancel> button.
```

- Appuyer sur :
  - le bouton `Shutdown now` pour revenir au menu
  - le bouton `Cancel` pour annuler l'arrêt

7.14 Commande `Exit`

7.14.1 Introduction

La commande `Exit` permet de fermer le menu de configuration.

7.14.2 Prérequis

- Utilisateur : setup

7.14.3 Opérations préliminaires

Suivant le cas :

- soit utiliser l'*Accès au menu de configuration en SSH*
- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

7.14.4 Procédure

Le menu de configuration est affiché.

- Sélectionner la ligne `` `Exit` `` ou appuyer sur la lettre **E**.
- Appuyer sur le bouton `` `OK` ``.

Note:

Si la connexion à la GBox est distante, elle sera fermée.
Si la connexion est faite via l'IDrac, le menu se ferme et la page de connexion s'affiche.

Chapter 8

Cas d'utilisation groupe Operators

8.1 Connexion à l'interface web via un navigateur internet

8.1.1 Introduction

Cette procédure décrit la connexion depuis un ordinateur distant à l'interface Web de la GBox.
Cette connexion est la façon nominale d'accéder à l'interface Web de l'équipement.

8.1.2 Prérequis

- Utilisateur : tout utilisateur

8.1.3 Opérations préliminaires

- Connaître le nom de la GBox ou son adresse IP.

8.1.4 Procédure

Sur le PC distant :

- Ouvrir un navigateur Web
- Entrer l'adresse IP ou le FQDN de la GBox
- Valider
  La fenêtre de connexion est affichée.
- Entrer l'identifiant
- Entrer le mot de passe
- Valider
  L'interface graphique est affichée.

8.2 Analyses avec la GBox

8.2.1 Procédure rapide pour analyser un fichier

8.2.1.1 Introduction

L'écran `Quick analysis` permet à un opérateur :

- de soumettre un (ou des fichiers) via l'interface Web de la GBox afin qu'il soit analysé
- de visualiser le rapport d'analyse
  Cette analyse est faite par le(s) moteur(s) défini(s) configuré(s) dans le modèle par défaut.
  L'analyse se fait systèmatiquement avec le modèle par défaut.
  Il n'est pas possible de tester des fichiers possédant un mot de passe. Pour cela, il faut utiliser l'écran `New Analysis` (voir *Procédure d'analyse d'un fichier dans l'écran `New analysis`*).

Note:

Les modèles sont gérés par l'administrateur.

Note:

Attention la taille maximale du fichier ne doit pas dépasser 50MO par défaut.
Il n'y a pas de limitation du nombre d'analyse de fichiers.

L'interface graphique est décrite dans l'*Ecran `Home` de la Web UI*.

8.2.1.1.1 Types de fichiers supportés

- .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 (géré comme une archive)
- .tar

8.2.1.1.2 Types de fichiers non supportés

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

8.2.1.1.3 Fichiers compressés

Concernant les fichiers compressés analysés par le moteur Malcore :

- le nombre de fichiers contenus dans une archive est limité et est modifiable (50 est la valeur par défaut)
- le nombre de fois que le fichier est compressé est limité (niveau de récursivité max) et est modifiable (5 est la valeur par défaut)
- si les fichiers sont protégés par un mot de passe, celui-ci doit être déclaré dans les réglages globaux

Ces réglages ne sont accessibles qu'aux membres du groupe Administrators.

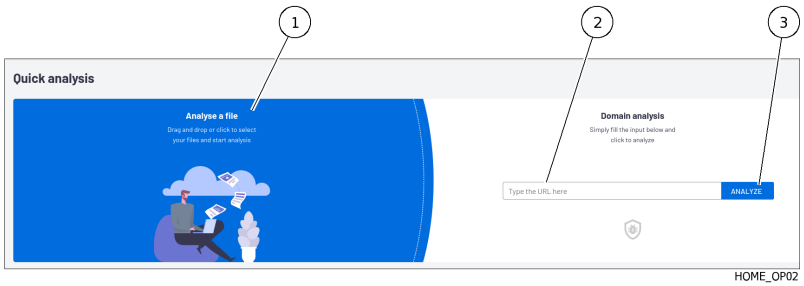
8.2.1.2 Prérequis

- Utilisateur : membre du groupe **Operators**

8.2.1.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

8.2.1.4 Procédure pour analyser un fichier

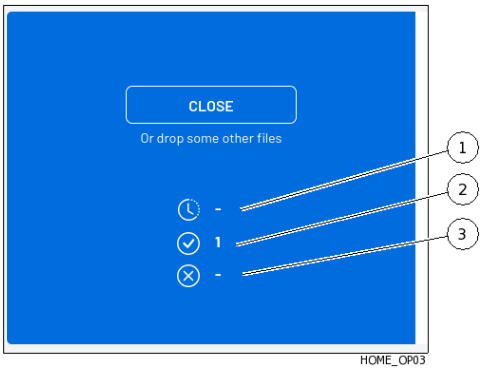


HOME_OP02

- Déposer le fichier souhaité dans la zone `Analyse a file`.
  ou
- Cliquer sur cette zone afin d'envoyer le fichier suspect.
  L'analyse est automatiquement lancée et le résultat est affiché automatiquement dans un rapport la zone `Analysis history`.

8.2.1.5 Procédure pour analyser les informations du télechargement

Le compte rendu du chargement est affiché dans la fenêtre suivante :



Repère	Nom
1	Icône reflétant le temps de chargement
2	Nombre total de fichiers téléchargés
3	Erreur lors du téléchargement

- Analyser la valeur des champs (1) à (3) avec les informations suivantes :
- Si l'icône (1) indique un nombre, attendre la fin du téléchargement.
  Le nombre décroit.
  Un message est affiché pour indiquer la fin du téléchargement.
- L'icône (2) a pour valeur le nombre total de fichiers téléchargés tant que la page courante est active.
- L'icône (3) a pour valeur :
  - 0 : aucune erreur n'est détectée durant le téléchargement
  - 1 ou plus : au moins une erreur est arrivée

8.2.1.6 Procédure pour analyser le rapport

Chaque fichier analysé fait lieu d'un rapport qui est affiché dans la zone `` `Analysis history` ``.

Note:

Si un répertoire contenant des fichiers a été déposé alors un rapport différent est créé pour chaque fichier de ce répertoire.
Si un fichier compréssé a été déposé alors un rapport différent est créé pour chaque fichier contenu dans ce fichier compressé.

Les résultats des analyses sont représentés sous forme de liste (mis à jour toutes les 30 secondes) dans la zone `` `Quick analysis` `` où chaque ligne correspond à une analyse d'un fichier différent.
Cette liste est limitée aux 10 derniers fichiers analysés.
Les différents champs affichés sont décrits dans la *Zone `Analysis history`*.

- Analyser les rapports.
  Pour cela, se référer à la *Procédure d'analyse du contenu d'un rapport*.

8.2.2 Procédure rapide pour analyser un domaine

8.2.2.1 Introduction

La GBox permet à un opérateur d'analyser un domaine après la saisie de son URL.
L'interface graphique est décrite dans l'*Ecran `Home` de la Web UI*.

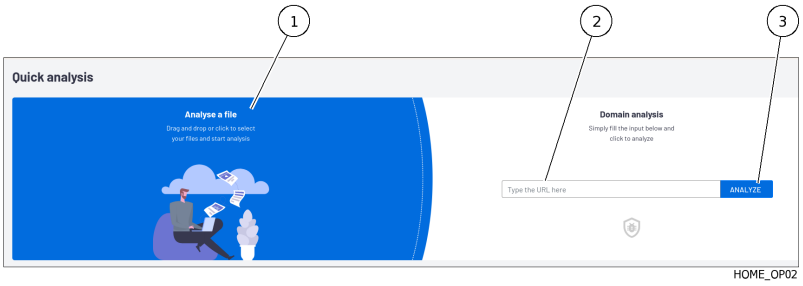
8.2.2.2 Prérequis

- Utilisateur : membre du groupe **Operators**

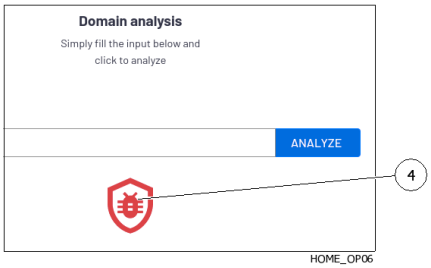
8.2.2.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

8.2.2.4 Procédure



- Saisir l'URL du domaine à analyser dans le champ (2).
- Cliquer sur le bouton `Analyse` (3).
  L'analyse est automatiquement lancée et le résultat est affiché et c'est le rôle de l'icône (4).



Icône	Signification
Rouge	Danger
Autre	Pas danger

Il n'y a pas de rapport généré lors de cette analyse.

8.2.3 Procédure d'analyse d'un fichier dans l'écran `New analysis`

8.2.3.1 Introduction

L'écran `New analysis` permet à un opérateur :

- de soumettre un (ou des fichiers) via l'interface Web du GCenter afin qu'il soit analysé
- de visualiser le rapport d'analyse

  Le moteur utilisé est celui défini dans le champ `Template`.

  Pour un fichier compressé et protégé par un mot de passe, le champ `Archive password` permet de le saisir afin d'analyser le contenu.

  Le sélecteur `Forcing` permet d'ignorer les éventuels résultats existants pour ce fichier avec ce modèle.

Note:

Attention la taille maximale du fichier ne doit pas dépasser 50MB par défaut. Il n'y a pas de limitation du nombre d'analyses de fichiers.

L'interface graphique est décrite dans l'*Ecran `New analysis` de la Web UI*.

8.2.3.1.1 Types de fichiers supportés

- .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 (géré comme une archive)
- .tar

8.2.3.1.2 Types de fichiers non supportés

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

8.2.3.1.3 Fichier compressés

Les caractéristiques des fichiers compressés à analyser sont décrites dans *La gestion des archives*.
Concernant les fichiers compressés analysés par Malcore :

- le nombre de fichiers contenus dans une archive est limité et est modifiable (50 est la valeur par défaut).
- le nombre de fois que le fichier est compressé est limité (niveau de récursivité max) et est modifiable (5 est la valeur par défaut).
- si les fichiers sont protégés par un mot de passe, celui-ci doit être déclaré dans les réglages globaux.

Ces réglages ne sont accessibles qu'aux membres du groupe Administrators.

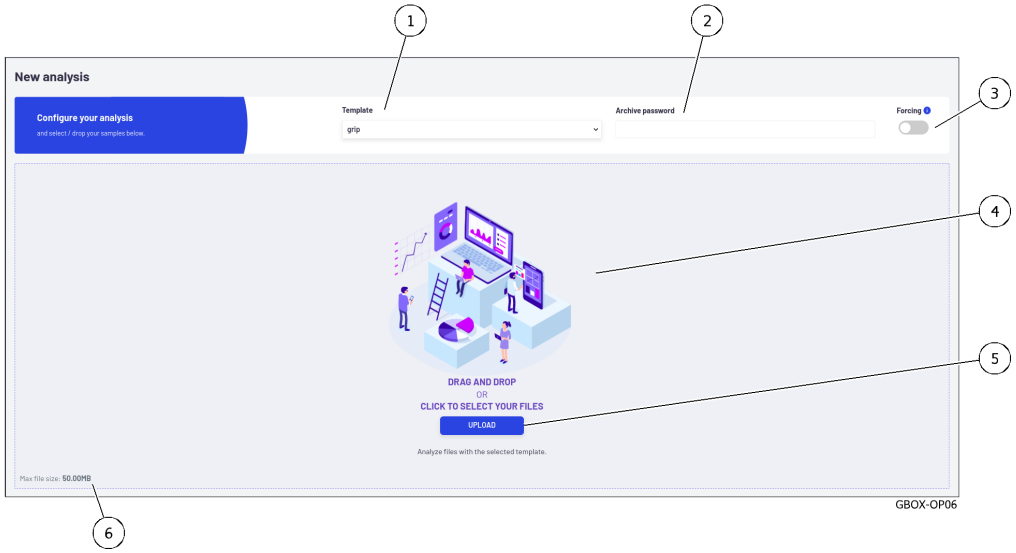
8.2.3.2 Prérequis

- Utilisateur : membre du groupe **Operators**

8.2.3.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

8.2.3.4 Procédure



- Si besoin, sélectionner le moteur à utiliser (1) dans le champ `Template`.
- Pour les fichiers compressés protégés par un mot de passe, saisir le mot de passe (2) dans le champ `Archive password`.
- Si besoin, utiliser le sélecteur (3) `Forcing` pour forcer la réanalyse du fichier s'il a déjà été analysé avec le même modèle sélectionné.
- Suivant le cas :
  - déposer le fichier souhaité dans la zone (4) `DRAG and DROP`

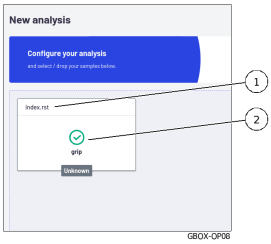
    ou

– cliquer sur le bouton (5) `UPLOAD` puis sélectionner le fichier à charge depuis le pc utilisateur et enfin valider la sélection

Note:

La sélection d'un fichier ainsi que le choix d'un modèle sont obligatoires. Par contre, utiliser le sélecteur (3) `Forcing` est optionnel.
La taille du fichier ne doit pas dépasser 50MO.

L'analyse est automatiquement lancée et le résultat est affichée automatiquement.
Dans le cas ou le fichier a été analysé alors le rapport est de ce type :

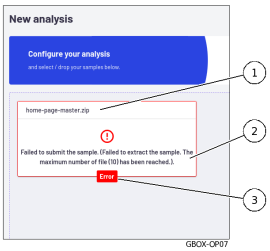


Le rapport affiché indique :

- le nom du fichier analysé (1)
- le résultat de l'analyse (coche = ok) et le nom du moteur utilisé (ici le moteur grip)
- Cliquer sur le rapport (2) :
  – ouvre sa version détaillée
  – supprime le rapport de la fenêtre
  – enregistre le rapport dans la fenêtre rapport
- Analyser les rapports.
  Pour cela, se référer à la *Procédure d'analyse du contenu d'un rapport*

8.2.3.5 Cas d'erreur

En cas d'erreur, un rapport est affiché : par exemple, le cas suivant...



Le rapport affiché indique :

- le nom du fichier analysé (1)
- la présence d'une erreur (3)
- le type de l'erreur (2) : ici le nombre maximum de fichiers inclus dans un fichier compressé a été atteint (10 max)

Note:

Si le fichier est trop grand alors le message est : `File is larger than 50.00MB`.

8.2.4 Procédure d'analyse de la liste des rapports de page `Reports`

8.2.4.1 Introduction

Les résultats des analyses sont représentés sous forme de liste (mis à jour toutes les 30 secondes) dans la zone `` `Analysis analysis` `` de l'écran Quick analysis où chaque ligne correspond à une analyse d'un fichier différent.
Les différents champs affichés sont décrits dans la *Zone `Analysis history`*.

8.2.4.2 Prérequis

- Utilisateur : membre du groupe **Operators**

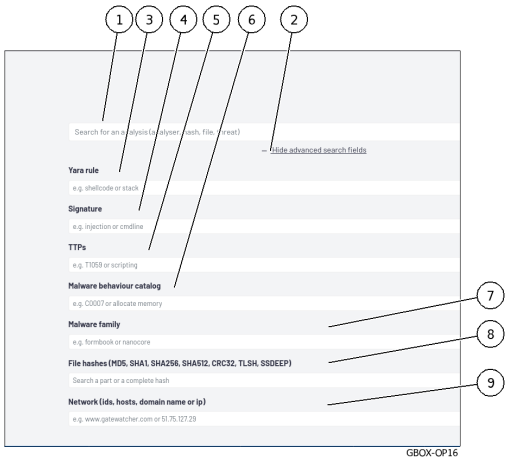
8.2.4.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

8.2.4.4 Procédure de filtration des rapports en utilisant le champ de recherche (1)

Note:

Cette fonction n'est pas présente dans l'écran `` `Home` `` dans la zone `` `Analysis history` ``.



IL y a plusieurs options pour saisir une valeur dans un champ de recherche (1) :

- soit saisir directement la valeur dans le champ de recherche
- soit copier l'information dans la zone d'un rapport (champs `` `FILENAME` ``, `` `FILE HASH (SHA256)` ``, `` `THREAT NAMES` ``) puis coller dans le champ de recherche (1)

La liste des rapports est automatiquement mise à jour.

8.2.4.5 Procédure de filtration des rapports en utilisant les champs de recherche avancés

Cet écran permet de filtrer les rapports à travers de différents choix définis dans la fenêtre *Zone permettant la recherche*.
Ces choix sont complémentaires au champ de recherche (1) et permettent une recherche sur des paramètres très précis.

- Cliquer sur le lien `Hide advanced search fields` (2) pour afficher les champs de recherche avancés.
- Saisir la valeur dans le champ choisi.

8.2.4.6 Procédure d'analyse du contenu d'un rapport

Se reporter à la *Procédure d'analyse du contenu d'un rapport*.

8.2.5 Procédure d'analyse du contenu d'un rapport

8.2.5.1 Introduction

Le rapport détaillé d'analyses donne les informations données par les moteurs d'analyses valides lors de l'analyse.
Les différents champs affichés sont décrits dans le *Rapport détaillé*.
Ce rapport doit être analysé par un analyste.

8.2.5.2 Prérequis

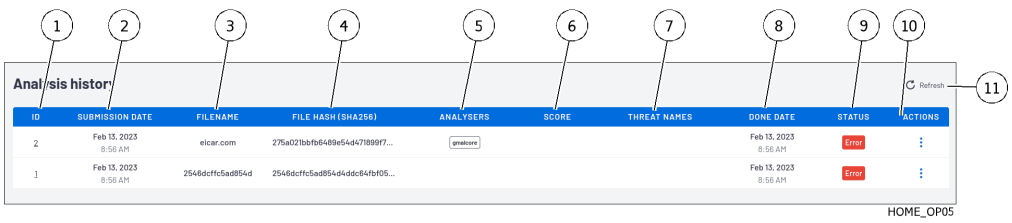
- Utilisateur : membre du groupe **Operators**

8.2.5.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

8.2.5.4 Procédure de sélection du rapport

- Appliquer la *Procédure d'analyse de la liste des rapports de page Reports*.



- Dans la zone des rapports, cliquer sur l'ID du rapport souhaité (1).
- Toutefois, faire attention à l'état (9) du rapport :
  - pour l'état `` `In queue` ``, attendre l'analyse du fichier
  - pour l'état `` `In Progress` ``, attendre la fin de l'analyse du fichier

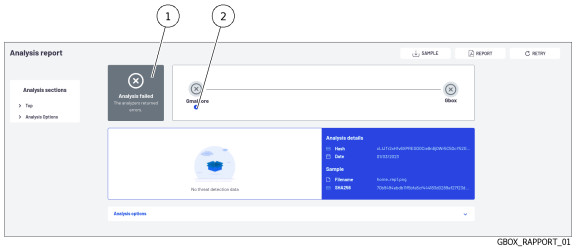
Astuce:

Si l'état `` `In Progress` `` prend du temps, il est possible de cliquer sur l'ID pour avoir le détail du traitement.
Cliquer sur le bouton d'information du moteur pour avoir l'état de son analyse.

  - pour l'état `` `Error` ``, se reporter à la *Procédure d'analyse des rapports avec l'état `Error`*
  - pour l'état `` `Clean` ``, avant de déterminer que le fichier est sain, vérifier que les moteurs actifs soient bien ceux qui sont pertinents...
  - pour l'état `` `Malicious` ``, se reporter à la *Procédure d'analyse des rapports avec l'état `Malicious`*

8.2.5.5 Procédure d'analyse des rapports avec l'état `` `Error` ``

- Cliquer sur l'ID correspondant.
  Une fenêtre s'ouvre donnant le rapport détaillé.



  La zone (1) indique que l'analyse a été défaillante et que les moteurs remontent des erreurs.

- Pour avoir plus d'informations, cliquer sur sur l'icône information (2) pour avoir le détail de l'erreur.
  Exemple : `` `gmalcore: Malcore analysis error for task id ****. Scan result code received: 10` ``
- A partir du code lu sur l'écran, se référer au tableau suivant pour connaître la raison et adopter la solution adéquate.

Table1: Codes résultats de l'analyse

Valeur	Brève description	Longue description
0	Aucune menace détectée	Aucune détection de menace ou le fichier est vide
1	Infecté/connu	Une menace est découverte
2	Suspect	Classé comme une menace possible mais non identifié comme une menace spécifique
3	Échec de la numérisation	L'analyse n'est pas entièrement effectuée (par exemple, fichier non valide ou aucune autorisation de lecture). Si aucun moteur n'est inclus et que l'analyse est activée, ce sera le résultat final.

suite sur la page suivante

Table 1 – suite de la page précédente

Valeur	Brève description	Longue description
5	Inconnu	Signature inconnue. REMARQUE : ceci n'est utilisé que dans la recherche de plusieurs hachages. Pour la recherche de hachage unique, scan_result n'est pas renvoyé comme réponse.
7	Nettoyage ignoré	L'analyse est ignorée car ce type de fichier figure sur la liste d'autorisation
8	Infecté ignoré	L'analyse est ignorée car ce type de fichier figure sur la liste de blocage.
9	Profondeur d'archivage dépassée	La menace est introuvable, mais il existe d'autres niveaux d'archives qui n'ont pas été extraits.
10	Non scanné / Aucun résultat de scan	L'analyse est ignorée par le moteur en raison d'une mise à jour ou d'une autre raison spécifique au moteur. Si l'analyse est désactivée, ce sera le résultat final.
11	Avorté	L'analyse en cours a été arrêtée en raison d'un problème.
12	Crypté	Le fichier/tampon n'est pas analysé car le type de fichier est détecté comme chiffré (protégé par mot de passe).
13	Taille d'archive dépassée	L'archive extraite est trop volumineuse pour être analysée.
14	Numéro de fichier d'archive dépassé	Il y a plus de fichiers dans l'archive qu'il n'en est configuré sur le serveur.
15	Document protégé par mot de passe	Un document protégé par un mot de passe [par exemple, des documents Office ou des fichiers PDF qui nécessitent un mot de passe pour afficher leur contenu]. Si un fichier est un document protégé par un mot de passe, aucune désinfection ne sera appliquée. Les formats de fichiers pris en charge sont : 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	Délai d'archivage dépassé.	Le processus d'archivage a atteint la valeur de délai d'attente donnée (valeur prédéfinie de 30 minutes).
17	Décalage	L'extension du fichier ne correspond pas au type de fichier détecté.
18	Fichier potentiellement vulnérable.	Vulnérabilité possible détectée pour le fichier appliqué.
19	Annulé	L'analyse du fichier a été annulée car elle n'a pas pu être analysée trop de fois.
23	Type de fichier non pris en charge	Le moteur ne prend pas en charge l'analyse de ce type de fichier. Certains moteurs n'analysent que des types de fichiers spécifiques tels que des fichiers exécutables ou des documents.

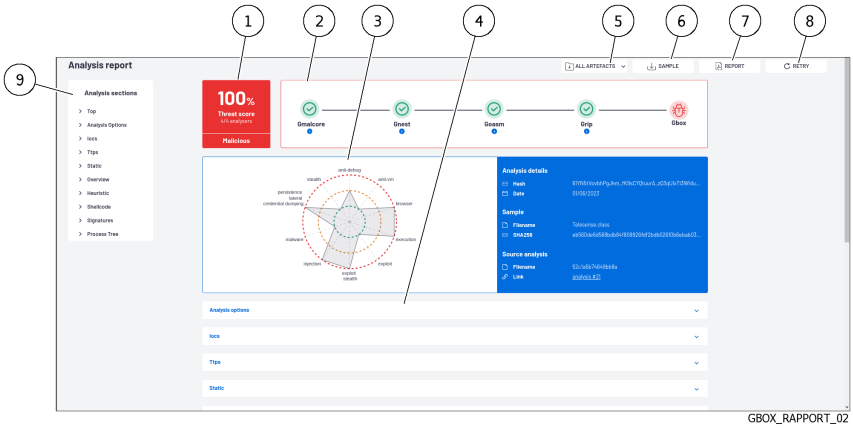
suite sur la page suivante

Table 1 – suite de la page précédente

Valeur	Brève description	Longue description
24	Dans la queue	Le fichier a été ajouté à la file d'attente d'analyse et attend d'être traité.
25	En cours.	La numérisation est en cours.

8.2.5.6 Procédure d'analyse des rapports avec l'état `Malicious`

- Cliquer sur l'ID correspondant.
  Une fenêtre s'ouvre donnant le rapport détaillé.



Les différents champs affichés sont décrits dans la *Procédure d'analyse des rapports avec l'état `Error`*.

- Consulter le résumé des étapes de l'analyse (2).
  Chaque moteur doit avoir une coche pour indiquer que son analyse s'est bien passée.
  Dans le cas contraire, cliquer sur le l'icône `i` pour avoir des informations sur l'état du moteur : résoudre le sujet avant de relancer l'analyse.
  Le cas normal est que tous les moteurs présents sont OK: la couleur de l'icône GBox indique le résultat Clean ou malicieux.
- Consulter le résultat de l'analyse (1) : le score, l'état global.
  Rappels :
  - un score n'est donné que pour les moteurs Gmalcore et Goasm
  - le score n'est affiché que pour les moteurs actifs au moment de l'analyse visibles dans le résumé des étapes de l'analyse(2)

Important:

Le champ SCORE n'a de sens que pour le moteur présélectionné. Il n'indique pas que le fichier analysé est sain mais uniquement qu'il est déclaré comme sain par ce moteur.

- Consulter les informations des zones (3) et des sections d'analyses (4) optionnelles.
  Rappels :
  - Le graphique est disponible uniquement si Gnest fait partie du modèle (les données nécessaires au graphique sont retournées par ce moteur).
  - Ce graphique permet d'avoir un visuel sur la dangerosité du fichier analysé.
  - Les sections d'analyses optionnelles dépendent du ou des moteur(s) actifs dans le modèle utilisé.

- Si besoin, cliquer sur le bouton (5) `ALL ARTEFACTS`.
  Il permet de télécharger les artefacts issus de l'analyse (dump mémoire, capture réseau (pcap), chaînes de caractères détectées).
  Cette section permet également de supprimer les artefacts.
  Ce bouton n'est présent que si le moteur Gnest est actif.
- Si besoin, cliquer sur le bouton `REPORT`.
  Il permet de télécharger le rapport en format pdf.
- Si besoin, cliquer sur le bouton `RETRY`.
  Il permet de rejouer l'analyse de ce fichier (avec ce template ou un autre).
- Si besoin, cliquer sur le bouton `SAMPLE`.
  Il permet de télécharger le fichier analysé.

8.3 Gestion des utilisateurs locaux

Cette rubrique décrit la gestion des utilisateurs locaux sur la GBox.
Pour plus de détails, voir la *Présentation des comptes de l'interface web et de leurs gestions*.

8.3.1 Modification du mot de passe du compte courant

8.3.1.1 Introduction

Cette procédure décrit comment modifier le mot de passe de l'utilisateur courant.
Pour entrer un nouveau mot de passe conforme avec la politique à appliquer, le système propose, de base, six mots de passe.
Le bouton `REGENERATE` permet de créer six nouveaux mots de passe.

Danger:

Noter précautionneusement le mot de passe saisi, surtout si le compte courant est le seul compte du groupe Administrators.

L'interface graphique est décrite dans la présentation de la *Gestion du compte courant, membre du groupe Operators*.

8.3.1.2 Prérequis

- Utilisateur : membre du groupe **Operators**

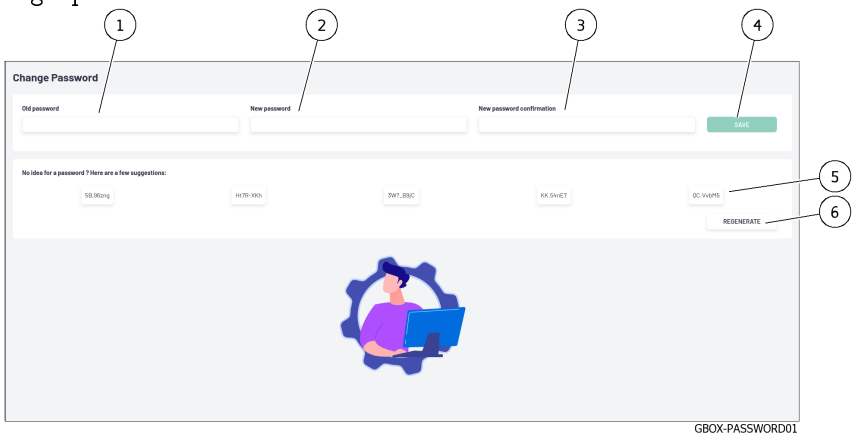
8.3.1.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

8.3.1.4 Procédure

BARRE_TITRE_OPERATOR

- Cliquer sur le bouton du compte courant (4).
- Sélectionner la commande `Change password`.
  La fenêtre `Change password` est affichée.



GBOX-PASSWORD01

- Entrer l'ancien mot de passe dans le champ (1) `Old password`.
- Entrer le nouveau mot de passe dans le champ (2) `New password`.
- Entrer le nouveau mot de passe dans le champ (3) `New password confirmation`.
  Le mot de passe saisi doit correspondre à la *Gestion de la politique des mots de passe*.
  Le système vérifie la concordance du mot de passe avec la politique de vérification.
  Dans le cas de non concordance, un des messages suivants est affiché :
  - `Minimal length 8` : indique un mot de passe trop court (8 caractères minimum)
  - `Uppercase` : indique le manque d'une capitale
  - `Lowercase` : indique le manque d'une minuscule
  - `Symbol` : indique le manque d'un caractère spécial
  - `Digit` : indique le manque d'un digit

> **Note:**
> Pour copier un des mots de passe proposé, cliquer sur le coté droit du mot de passe.
> Une fenêtre est affichée informant que le mot de passe est copié dans le presse papier.
> Pour coller ce mot de passe, cliquer droit puis coller dans chacun des deux champs.
> Surtout, NOTER le mot de passe avant de sauvegarder.

- Cliquer sur le bouton (4) `SAVE`.

> **Note:**
> Si le message suivant est affiché `you used this password recently, please choose a different one.`, saisir un mot de passe qui n'a pas déjà utilisé.

8.3.2 Modification de certaines informations de l'utilisateur courant

8.3.2.1 Introduction

Cette procédure décrit la procédure de certaines informations de l'utilisateur courant :

- l'adresse Email
- le prénom
- le nom

L'interface graphique est décrite dans la présentation de la *Gestion du compte courant, membre du groupe Operators*.

8.3.2.2 Prérequis

- Utilisateur : membre du groupe **Operators**

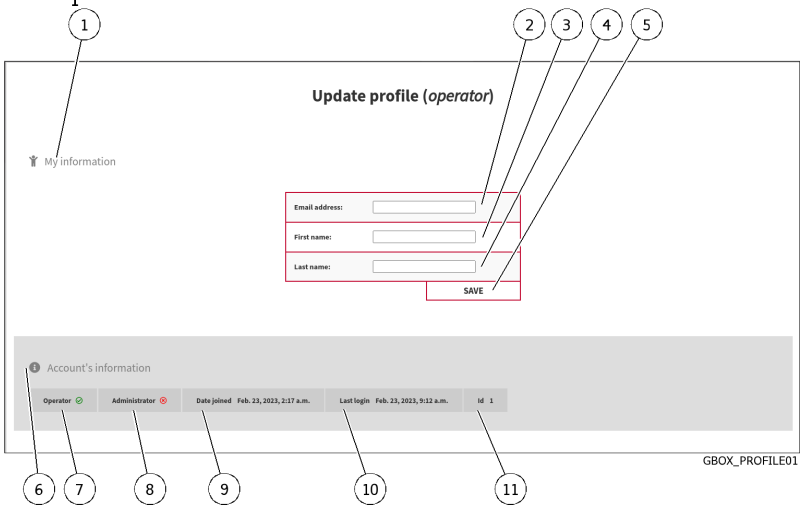
8.3.2.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

8.3.2.4 Procédure

- Dans la barre de navigation, cliquer successivement sur :
- le bouton `Admin`
- le sous menu `Gcenter`
- la commande `Edit profile`

  La fenêtre `Update profile` est affichée.



  La fenêtre indique les informations (6) sur le compte.

- Saisir ou modifier les données présentes dans :

- dans le champ (2) `Email address`
- dans le champ (3) `First name`
- dans le champ (4) `Last name`

- Valider les modifications en utilisant le bouton (5) `Save`.
  Une fenêtre de confirmation affiche le message de réussite `Profile successfully saved!`.

8.4 Déconnexion de l'interface web de la GBox

8.4.1 Introduction

Cette procédure décrit la déconnexion de l'interface Web.

8.4.2 Prérequis

- Utilisateur : tout utilisateur

8.4.3 Opérations préliminaires

- Accéder à l'interface Web depuis son poste de travail (*Connexion à l'interface web via un navigateur internet*).

8.4.4 Procédure

- Dans l'interface Web, cliquer sur le bouton du compte courant (4).
- Sélectionner la commande `Logout`.
  L'interface Web est fermée et l'écran de connexion est affiché.

Chapter 9

Cas d'utilisation niveau administrateur

9.1 Connexion à l'interface Web via un navigateur internet

9.1.1 Introduction

Cette procédure décrit la connexion depuis un ordinateur distant à l'interface Web de la GBox.
Cette connexion est la façon nominale d'accéder à l'interface Web de l'équipement.

9.1.2 Prérequis

- Utilisateur : tout utilisateur

9.1.3 Opérations préliminaires

- Connaître le nom de la GBox ou son adresse IP.

9.1.4 Procédure

Sur le PC distant :

- Ouvrir un navigateur Web
- Entrer l'adresse IP ou le FQDN de la GBox
- Valider
  La fenêtre de connexion est affichée.
- Entrer l'identifiant
- Entrer le mot de passe
- Valider
  L'interface graphique est affichée.

9.2 Gestion des moteurs de détection

9.2.1 Procédure de configuration du moteur Gnest

9.2.1.1 Introduction

9.2.1.1.1 Fonctions du moteur Gnest

Le moteur d'analyse **Gnest** permet une analyse dynamique.
Il exécute le fichier dans une machine virtuelle (sandbox) et analyse son comportement.
Suite à cela, il est possible d'extraire les données générées lors de l'analyse comme un *dump* de la mémoire, les chaînes de caractères extraites, ou une capture des communications réseau (pcap).
Dans le cas d'un fonctionnement connecté au GCenter, ce moteur est utile pour analyser en profondeur un fichier qualifié de *suspicious* ou *malicious*, lors d'une seconde analyse d'un fichier.
Cette analyse est plus lente et requiert un opérateur de niveau confirmé afin d'analyser les résultats produits.

Ces données sont affichées dans le *Rapport détaillé* et plus précisément dans les sections **TOP**, **Iocs**, **Ttps**, **Overview**, **Signatures** et **Process Tree**.

Taille maximum de fichier	50Mo
Timeout d'analyse	1 heure
Type	lent

9.2.1.1.2 Configuration de Gnest

La configuration de Gnest consiste à gérer et configurer des machines virtuelles.
L'interface graphique de la gestion des machines virtuelles est décrite dans l'*Ecran `Gnest configuration`*.

9.2.1.1.3 Procédures décrites

- *Procédure d'accès à la fenêtre `Gnest configuration`*
- *Procédure pour créer une ou des machines virtuelles*
- *Procédure pour afficher l'historique des machines virtuelles*
- *Procédure pour supprimer une machine virtuelle*
- *Procédure pour supprimer plusieurs machines virtuelles par lot*

9.2.1.2 Prérequis

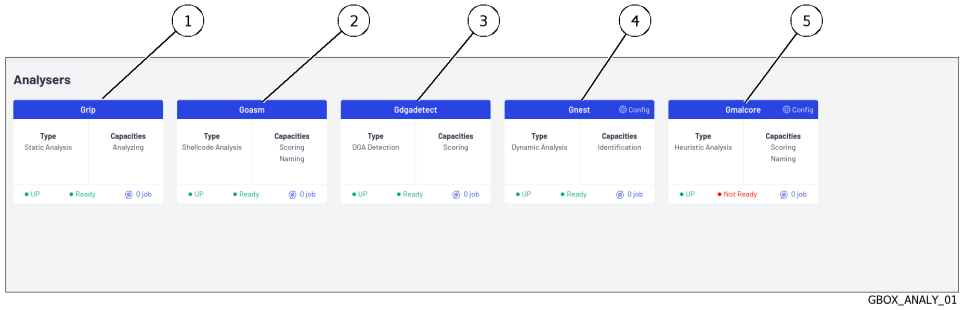
Utilisateur : membre du groupe **Administrators**

9.2.1.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

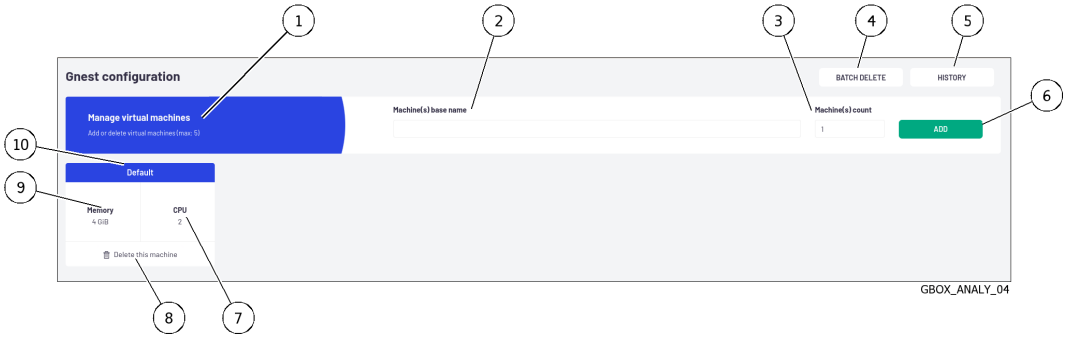
9.2.1.4 Procédure d'accès à la fenêtre `Gnest configuration`

- Dans la barre de navigation, cliquer sur la commande **`Analysers`**.
  L'écran suivant est affiché.



GBOX_ANALY_01

- Cliquer sur le lien **`Config`** du moteur Gnest (4).
  L'écran suivant est affiché.



GBOX_ANALY_04

9.2.1.5 Procédure pour créer une ou des machines virtuelles

Le fait de créer des machines virtuelles permet de multiples analyses en parallèle via l'activation de ces machines virtuelles dans les modèles.
La configuration de **Gnest** consiste en la création de machines virtuelles servant de *sandbox* pour l'analyse.

Note:

Il n'est pas possible d'avoir plus de 5 machines virtuelles.

- Saisir le nom de la machine (ou des machines) à créer dans le champ (2) : par exemple **test_VM**.

Note:

Seuls les lettres, chiffres et le tiret bas sont autorisés.

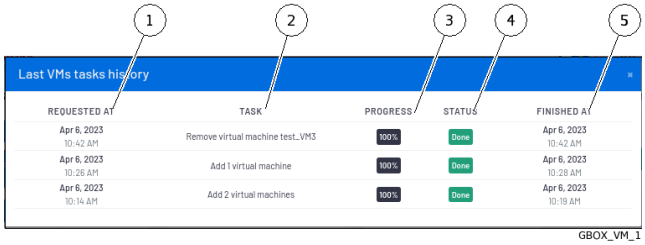
- Saisir dans le champ (2) le nombre de machine(s) à créer.
- Cliquer sur le bouton (6) `ADD`.
  Un message est affiché : `Task in progress: Add 2 virtual machines (x%).`
  Une fois créées, les machines virtuelles sont affichées dans la fenêtre avec les noms **test_VM1** et **test_VM2**.
  Ces machines peuvent être configurées via la création des modèles.

Note:

Les paramètres des moteurs sont indiqués dans le paragraphe *Paramètres de Grip* et dans le paragraphe *Paramètres de Gnest*.
La procédure pour modifier ces paramètres est indiquée dans la *Gestion des modèles d'analyse*.

9.2.1.6 Procédure pour afficher l'historique des machines virtuelles

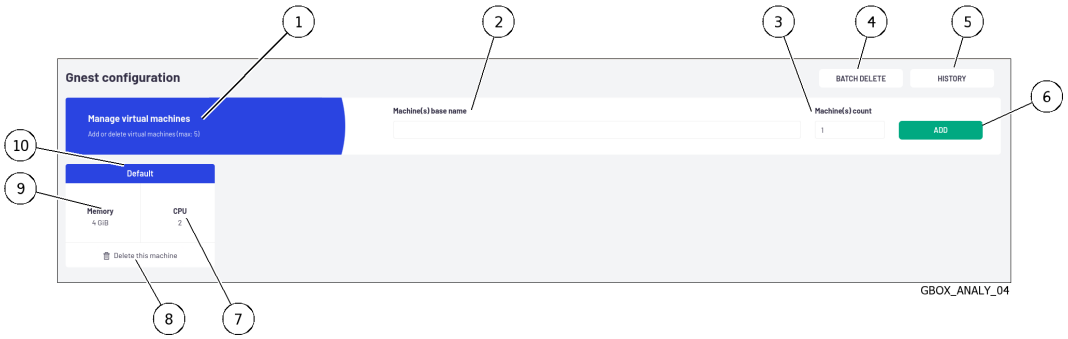
- Cliquer sur le bouton (5) `HISTORY`.
  La fenêtre `Last VMs tasks history` est affichée.



La fenêtre affiche les informations suivantes :

Repère	Nom du champ	Description
1	`REQUESTED AT`	Date et heure du début de la tâche
2	`TASK`	Informations sur la tâche courante
3	`PROGRESS`	Pourcentage d'avancement de la tâche
4	`STATUS`	Etat courant de la tâche
5	`FINISHED AT`	Date et heure de fin de la tâche

9.2.1.7 Procédure pour supprimer une machine virtuelle



- Cliquer sur le lien (8) `Delete this machine` de la machine à supprimer.
  Le message suivant est affiché.

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

- Cliquer sur le bouton `Confirm`.
  Le message informe sur l'action en cours : `Task in progress: Remove virtual machine xxxxx (xx%)`.
  Une fois la tâche terminée, le message est affichée : `Task successful: Remove virtual machine xxxx (100%)`.
  La VM est supprimée du tableau de bord.
  Si la VM était définie dans des modèles, la VM est supprimée.
  Si un modèle n'avait que cette VM définie alors le modèle est conservé et la VM détruite est remplacée par l'ensemble des VM présentes (paramètre any).

9.2.1.8 Procédure pour supprimer plusieurs machines virtuelles par lot

Tout comme la création de plusieurs machines est possible, la suppression par lot l'est également.

- Cliquer sur le bouton (4) `BATCH DELETE`.
  La fenêtre `Delete multiple VMs` est affichée pour sélectionner les machines à supprimer.
- Sélectionner la ou les VM à supprimer.
- Cliquer sur le bouton `Delete`.
  Le message informe sur l'action en cours : `Task in progress: Remove virtual machine xxxxx (xx%)`
  Une fois la tache terminée, le message est affichée : `Task successful: Remove virtual machine xxxx (100%)`
  Les VMs sont supprimées du tableau de bord.
  Si les VMs étaient définies dans des modèles, ces VMs sont supprimées.
  Si un modèle n'avait que cette VM définie, alors le modèle est conservée et la VM détruite est remplacée par l'ensemble des VM présente (paramètre any).

Note:

La suppression est séquentielle, si une erreur survient, le processus est stoppé (et les machines suivantes ne sont pas supprimées).

9.2.2 Procédure de configuration du moteur Gmalcore

9.2.2.1 Introduction

La configuration de Gmalcore consiste à :

- s'assurer que les moteurs ont été démarrés
- s'assurer que les moteurs soient à jour
- s'assurer que les mises à jour des moteurs ont été planifiées

Les fonctions du moteur Gmalcore sont décrites dans le paragraphe *Présentation du moteur Gmalcore*.
L'état des moteurs de Gmalcore est donnée via la fenêtre `Gmalcore configuration`.
L'interface graphique de configuration est décrite dans l'*Ecran `Gmalcore configuration`*.

9.2.2.2 Prérequis

Utilisateur : membre du groupe **Administrators**

9.2.2.3 Opérations préliminaires

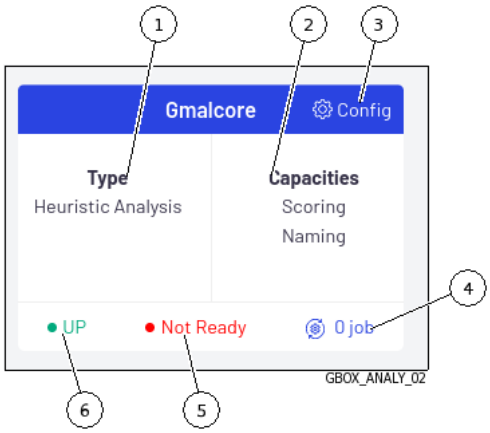
- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.2.2.4 Procédure pour vérifier que les moteurs Gmalcore ont été démarrés

- Dans la barre de navigation, cliquer sur la commande `Analysers`.
  L'écran suivant est affiché.

GBOX_ANALY_01

  Pour le moteur Gmalcore, les informations affichées sont :

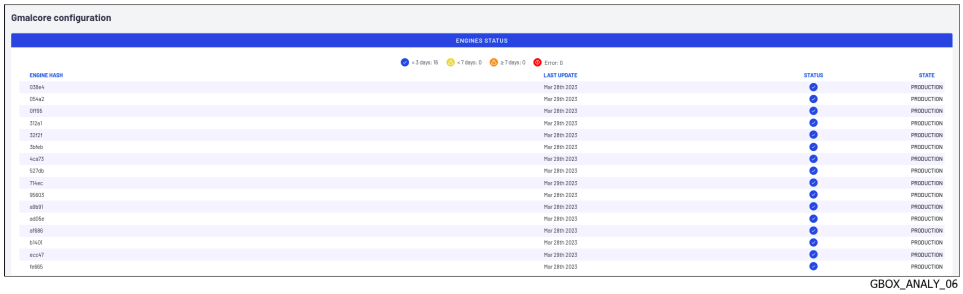


Si l'état (5) est `Ready` alors les moteurs sont prêts.
Si l'état (5) est `Not ready` comme visualisé ci-dessus alors la configuration des moteurs n'est pas faite (les moteurs ne sont pas prêts).

- Cliquer sur le lien (3) `Config` pour le vérifier.

9.2.2.4.1 Procédure pour l'état `Ready`

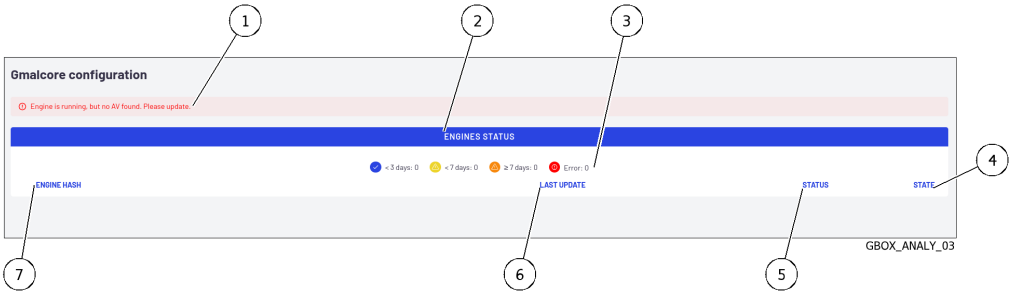
L'écran suivant est affiché.



- Vérifier les éléments suivants :
- les moteurs sont listés (colonne `ENGINE HASH`)
- tous les moteurs ont le statut ok (coche dans la colonne `STATUS`)
- la dernière mise à jour est récente (moins de 3 jours grâce aux couleurs de l'icône de colonne `STATUS`)
- Si les mises à jour sont anciennes alors vérifier le système de mise à jour mis en place dans GUM (online, local...).
- Pour les mises à jour (online ou local), se référer à la *Configuration de la mise à jour automatique via GUM*.
  Si cette configuration ne fonctionne pas, contacter le support de GATEWATCHER.

9.2.2.4.2 Procédure pour l'état `Not Ready`

L'écran suivant est affiché.



Dans l'écran `Gmalcore configuration`, le message suivant (1) est affiché : `Engine is running, but no AV found. Please update.`
Dans ce cas, il n'y a aucun moteur installé.

- Installer impérativement une mise à jour des signatures et des moteurs soit :
  - de façon automatique via GUM (online, local) : voir la *Configuration de la mise à jour automatique via GUM*
  - de façon manuelle alors se référer à la procédure d'*Installation manuelle d'une mise à jour des signatures (update)*

Note:

Si besoin, configurer un proxy (voir la procédure de *Configuration d'un proxy*).

9.2.3 Procédure de surveillance des moteurs d'analyse

9.2.3.1 Introduction

Cette procédure permet d'afficher les états des différents moteurs d'analyse et des actions à entreprendre.
L'interface graphique est décrite dans l'*Ecran `Analysers` de la Web UI*.

9.2.3.2 Prérequis

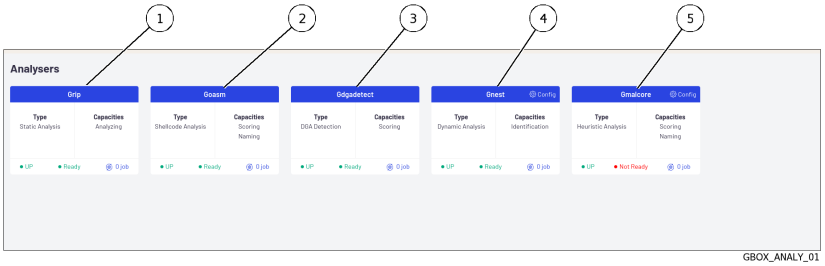
Utilisateur : membre du groupe **Administrators**

9.2.3.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

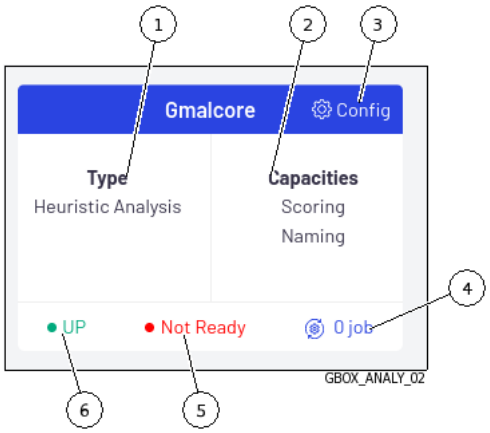
9.2.3.4 Procédure d'accès à l'écran `Analysers`

Après appui sur la commande `Analysers`, l'écran suivant est affiché.



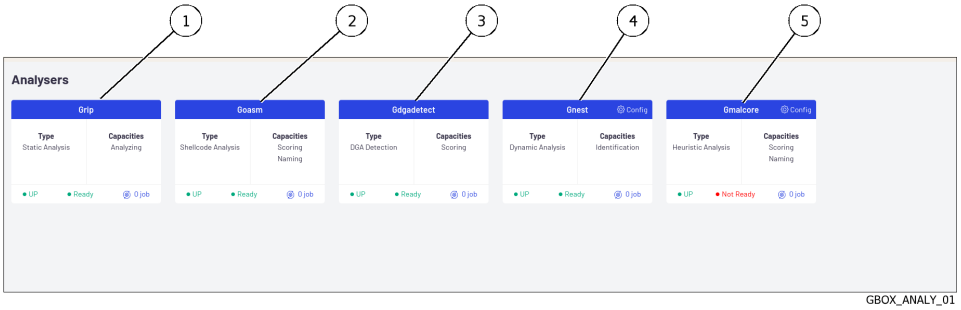
Repère	Moteur	Fonction du moteur
1	*Moteur Grip*	Analyse statique
2	*Moteur Goasm*	Détection des shellcodes
3	*Moteur Gdgadetect*	Détection de noms de domaine
4	*Moteur Gnest*	Analyse dynamique dans une machine virtuelle
5	*Moteur Gmalcore*	Analyse statique et heuristique

Pour chacun des moteurs, les informations suivantes sont affichées :



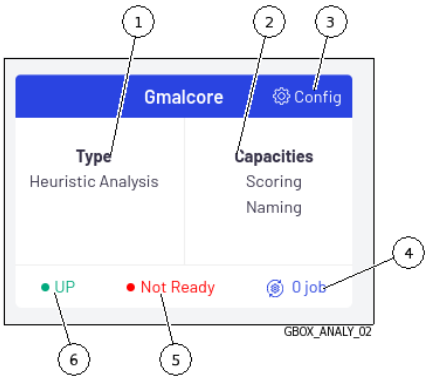
Repère	Nom	Moteur Grip	Moteur Goasm	Moteur Gdgadetect	Moteur Gnest	Moteur Gmalcore
1	Type	Analyse statique	Détection des shellcodes	Détection de noms de domaine générés par des DGA (Domain Generation Algorithm)	Exécute le fichier dans une machine virtuelle et analyse son comportement	Analyse statique et heuristique multi-moteurs
2	Capacités	Analyse	Donne un score de la dangerosité potentielle et nomme le shellcode détecté	Donne un score de compromission	Nomme le problème détecté	Donne un score de la dangerosité potentielle et nomme le problème détecté
3	Config	Non configurable donc ce champ n'est pas affiché			Gestion des machines virtuelles (ajout, suppression, historisation)	Gestion des moteurs de Gmalcore
4	x jobs : nombre de tâches en cours (statut de l'analyse NEW + IN PROGRESS)	Nombre de tâches en attente de traitement				
5	Capacité à effectuer des analyses	Ce moteur n'a pas d'exigences donc toujours à l'état `ready`			Le moteur est à l'état `ready` s'il y a le même nombre de VM dans la GBox et dans CAPE (le moteur d'analyse dynamique)	Le moteur est à l'état `ready` si tous les moteurs sont installés et l'API est up
6	Etat du moteur	UP : l'api du moteur est en écoute : DOWN : l'api du moteur est non actif				

Après appui sur la commande `Analysers`, l'écran suivant est affiché.



Repère	Moteur	Fonction du moteur
1	*Moteur Grip*	Analyse statique
2	*Moteur Goasm*	Détection des shellcodes
3	*Moteur Gdgadetect*	Détection de noms de domaine
4	*Moteur Gnest*	Analyse dynamique dans une machine virtuelle
5	*Moteur Gmalcore*	Analyse statique et heuristique

Pour chacun des moteurs, les informations suivantes sont affichées :



Repère	Nom
1	Type
2	Capacités
3	Config (présent uniquement pour certains moteurs)
4	x jobs
5	Statut
6	Etat du moteur

9.2.3.5 Procédure de vérification du bon état des moteurs

- Vérifier que chaque moteur soit bien dans l'état `` `UP` ``.

> **Astuce:**
>
> Si l'état du moteur (Grip, Goasm, Gdgadetect ou Gnest) est `` `DOWN` ``, attendre un moment.
> Si le moteur reste dans l'état `` `DOWN` ``, contacter le support de Gatewatcher.

- Vérifier que chaque moteur soit bien dans le statut `` `Ready` ``.

> **Astuce:**
>
> Le statut `` `Not Ready` `` pour le moteur **Gmalcore** ne signifie pas forcément que ce dernier n'est pas en capacité d'effectuer des analyses mais indique qu'au moins un des 16 moteurs antivirus n'est pas à jour ou est hors service.

- Vérifier le bon état des moteurs Gmalcore : voir la *Procédure de configuration du moteur Gmalcore*.

9.2.3.6 Procédure de mise à jour des moteurs Gnest et Gmalcore

Les mises à jour de signatures ou **updates** correspondent aux mises à jour des moteurs de détection de la GBox.
Il existe 3 types de paquets de mise à jour :

- les paquets Gmalcore (*latest_malcore*) : ces paquets contiennent uniquement les mises à jour des moteurs et des bases des antivirus utilisés par Malcore
- les paquets sandbox (*latest_sandbox*) : ces paquets contiennent des mises à jour des signatures et des modules utilisés par les sandbox du moteur Gnest
- les paquets complets (*latest_full*) : ces paquets sont une combinaison des 2 précédents paquets

Ces paquets peuvent être installés de façon :

- manuelle.
  Dans ce cas, l'interface graphique à utiliser est décrite dans l'*Ecran `Admin-GUM - Updates` de la legacy Web UI*.
- automatiquement. Cette planification doit être configurée.
  Le principe est décrite dans la *Configuration de GUM*.
  L'interface graphique à utiliser est décrite dans l'*Ecran `Admin-GUM - Config` de la legacy Web UI*.
- Si l'installation doit être manuelle, voir la procédure d'*Installation manuelle d'une mise à jour des signatures (update)*
- Si l'installation doit être automatique, voir la *Configuration de la mise à jour automatique via GUM*.

9.3 Gestion des modèles

9.3.1 Création d'un modèle d'analyse

9.3.1.1 Introduction

Il est indispensable d'avoir au minimum un modèle (template) défini afin que les opérateurs puissent effectuer des analyses.
Cette procédure permet de créer des modèles d'analyse en combinant les différents moteurs d'analyse.
L'interface graphique est décrite dans l'*Ecran `Admin/Templates` de la Web UI*.

9.3.1.2 Prérequis

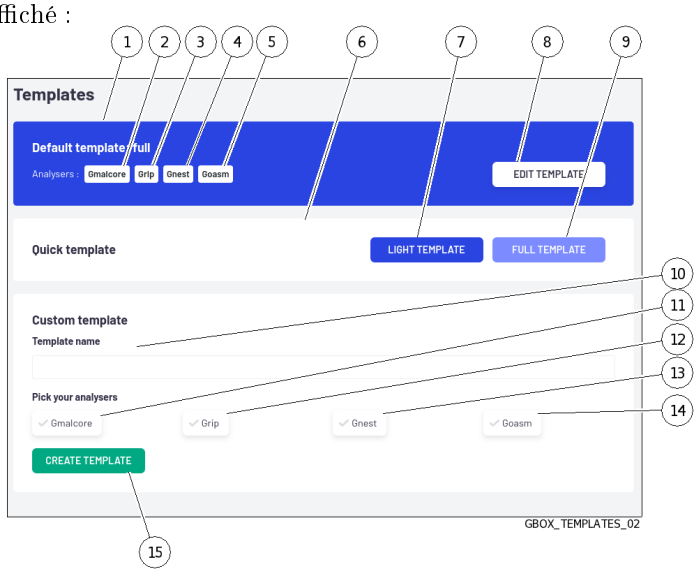
Utilisateur : membre du groupe **Administrators**

9.3.1.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.3.1.4 Procédure d'accès à la fenêtre Ecran `Admin/Templates` pour un compte de type Administrators

- Dans la barre de navigation, cliquer sur la commande `Templates`.
  L'écran suivant est affiché :



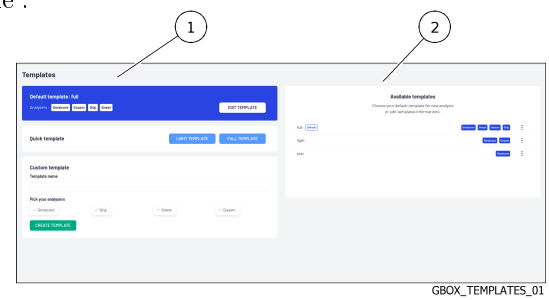
9.3.1.5 Procédure de création rapide d'un modèle

Il est à noter que le premier modèle créé a automatiquement le tag **Default**.

- Pour créer un modèle léger (zone `` `Quick template` ``) :
  - cliquer sur le bouton (7) `` `LIGHT TEMPLATE` ``.
    La fenêtre `` `Create a quick template` `` affiche le message `` `Do you want to create the quick template light ?` ``.
  - cliquer sur le bouton `` `Confirm` ``.
    Le message `` `Success - Template created` `` est affiché.
    Le modèle créé apparaît aussitôt dans la zone (2) `` `Available templates` ``.

> **Note:**
>
> Le modèle `` `full` `` a tous les moteurs actifs avec les paramètres par défaut des moteurs.
> Il ne peut y avoir qu'un seul modèle nommé `` `full` ``.

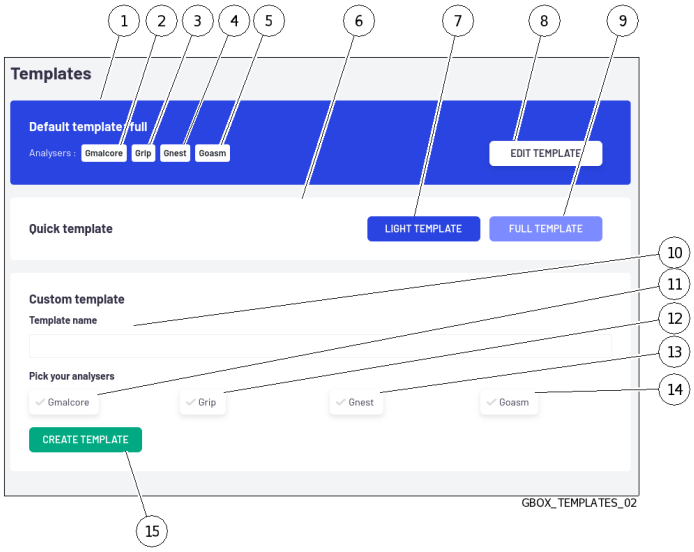
- Pour créer un modèle complet (zone `` `Quick template` ``) :
- cliquer sur le bouton (8) `` `FULL TEMPLATE` ``.
  La fenêtre `` `Create a quick template` `` affiche le message `` `Do you want to create the quick template full ?` ``.
- cliquer sur le bouton `` `Confirm` ``.
  Le message `` `Success - Template created` `` est affiché .
  Le modèle créé apparaît aussitôt dans la zone (2) `` `Available templates` ``.
  L'écran suivant est affiché :



GBOX_TEMPLATES_01

> **Note:**
>
> Le modèle `` `full` `` a tous les moteurs actifs avec les paramètres par défaut des moteurs.
> Il ne peut y avoir qu'un seul modèle nommé `` `full` ``.

9.3.1.6 Procédure de création d'un modèle personnalisé (zone `Custom template`)



- Saisir le nom du modèle dans le champ (10) `Template name`.
- Sélectionner les moteurs (11 à 14) à utiliser dans le modèle.
- Si besoin, modifier les paramètres des moteurs (pour le détail de ces paramètres, se référer aux *Paramètres de Grip* et aux *Paramètres de Gnest*)
- Cliquer sur le bouton (15) `CREATE TEMPLATE`.
  Le message `Success - Template created` est affiché .
  Le modèle créé apparaît aussitôt dans la zone (2) `Available templates`.

9.3.2 Gestion des modèles d'analyse

9.3.2.1 Introduction

Cette procédure permet de gérer (supprimer ou modifier) les modèles existants.
L'interface graphique est décrite dans l'*Ecran `Admin/Templates` de la Web UI*.

9.3.2.2 Prérequis

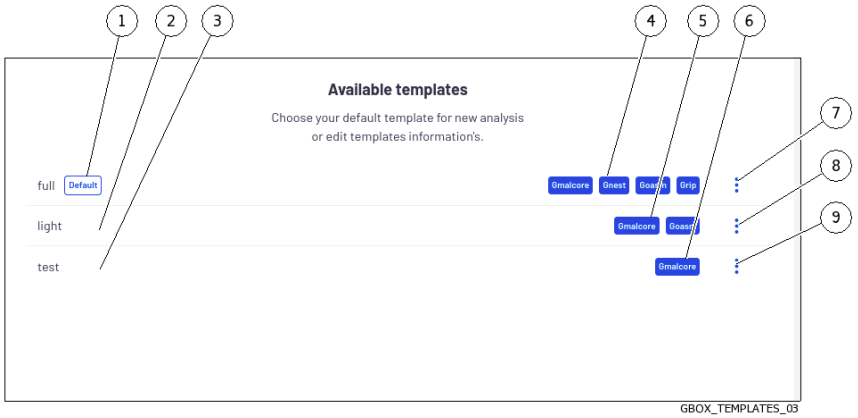
Utilisateur : membre du groupe **Administrators**

9.3.2.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.3.2.4 Procédure d'accès à la fenêtre Ecran `Admin/Templates` pour un compte de type Administrators

- Dans la barre de navigation, cliquer sur la commande `Templates`.
  L'écran suivant est affiché :



9.3.2.5 Procédure de modification d'un modèle existant

Un modèle défini par défaut (1) a uniquement la possibilité de modifier ses paramètres.

- Pour cela, cliquer sur la commande `Edit` du menu (7).
  La fenêtre `Edit template DefaultProfile` est affichée.
- Si besoin, modifier les paramètres des moteurs (pour le détail de ces paramètres, se référer *Paramètres de Grip* et *Paramètres de Gnest*)
- Cliquer sur le bouton `Confirm`.
  Le message `Success - Template updated` est affiché.
  Le modèle modifié est présent dans la zone `Available templates`.
  Les modifications sont aussitôt prises en compte pour les analyses.

9.3.2.6 Procédure de suppression d'un modèle

Un modèle défini par défaut (1) ne peut être supprimé.

- Cliquer sur la commande `Remove` du menu (7).
  La fenêtre `Delete template test` est affichée.
- Cliquer sur le bouton `Confirm`.
  Le message `Success - Template deleted` est affiché.
  Le modèle supprimé n'est plus présent dans la zone `Available templates`.

9.3.2.7 Procédure de suppression d'un modèle défini par défaut

Un modèle défini par défaut (1) ne peut être supprimé, donc il est nécessaire de définir un autre module comme étant par défaut pour pouvoir après supprimer le modéle voulu.

- Pour changer le modèle par défaut, sélectionner le nouveau modèle puis cliquer sur la commande `` `Set as default` `` de son menu.
  La fenêtre `` `Set template as default` `` est affichée.
- Cliquer sur le bouton `` `Confirm` ``.
  Le message `` `Success - Default template updated.` `` est affiché.
  Le nouveau modèle par défaut est pris en compte et est affiché dans la zone `` `Available templates` ``.

9.4 Gestion du logiciel GBox

9.4.1 Configuration de la mise à jour automatique via GUM

9.4.1.1 Introduction

GUM (Gatewatcher Update Manager) est un outil qui permet la gestion des mises à jour (updates) de la **GBox**.

Cet écran permet de configurer la planification automatique des mises à jour.
Ces mises à jour peuvent être faites :

- par le mode Online
  Si besoin, configurer un proxy (voir la procédure de *Configuration d'un proxy*)
  Le mode online permet de faire les mises à jour de manière automatique (à partir d'Internet).
  Le champ URL sera automatiquement renseigné. Les packages de mise à jour sont récupérés depuis les serveurs Gatewatcher https://update.GATEWATCHER.com/update/.
- par le mode Local
  Si besoin, configurer un proxy (voir la procédure de *Configuration d'un proxy*)
  Le mode Local permet de faire les mises à jour à partir d'un dépôt local préalablement configuré pour télécharger les paquets depuis les serveurs Gatewatcher
  https://update.GATEWATCHER.com/update/.
  Ce dépôt local est défini dans l'*Ecran `Admin-GUM - Config` de la legacy Web UI*.

Un compte intelligence sera nécessaire pour que le téléchargement du package de mise à jour puisse se faire depuis le site.
Dans le cas du mode `` `online` ``, ce couple utilisateur et mot de passe doivent être renseignés dans les champs `` `Username` `` et `` `Password` `` situés sous l'adresse.

Cette procédure décrit le configuration de la mise à jour automatique à partir :

- soit d'un serveur sur le réseau local (choix `` `local` ``)
- soit d'un serveur sur Internet (choix `` `online` ``)

L'interface graphique est décrite dans l'*Ecran `Admin-GUM - Config` de la legacy Web UI*.

Note:

Si besoin, configurer un proxy (voir la *Configuration d'un proxy*).

9.4.1.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

9.4.1.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).
- Dans le cas du mode local, effectuer les prérequis de configuration du dépôt local :

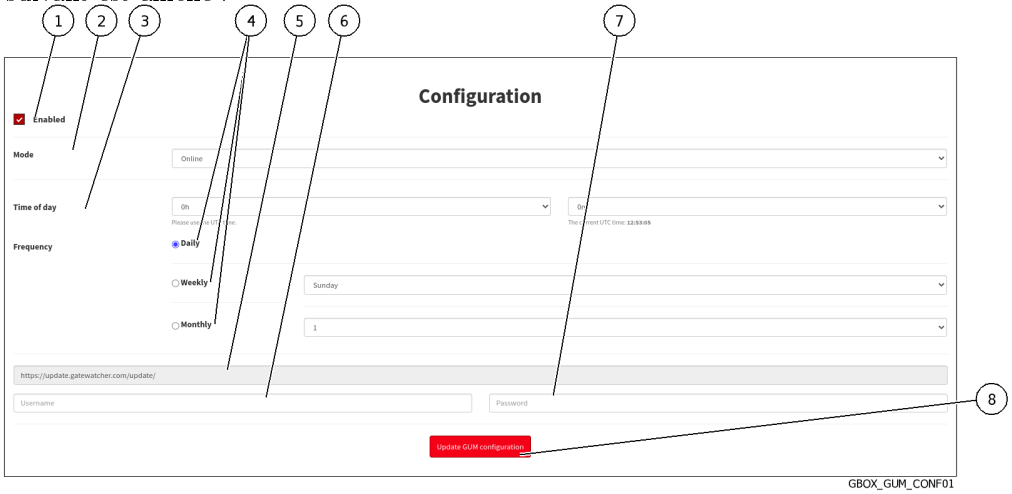
- Le serveur doit être joignable en HTTP sur le port 80
- Créer l'arborescence suivante: "2.5.3.10X/GBox" selon la version du GBox (2.5.3.100 ou 2.5.3.101)
- Récupérer les fichiers gwp nécessaires (latest_full.gwp pour une GBox V100, latest_full_v3.gwp pour une 2.5.3.101) sur *https://update.gatewatcher.com/update/<version_gbox>/gbox/*
- Dans "2.5.3.10X/gbox", mettre le fichier gwp récupéré précédemment
- Dans "2.5.3.10X/gbox", mettre un fichier sha256sum.txt qui contient une entrée "sha256sum NomDuFichier"

Note:

Le dossier 2.5.3.10X doit obligatoirement se trouver à la racine du serveur HTTP lancé précédemment pour que le mode local fonctionne.

9.4.1.4 Procédure d'accès à la fenêtre Ecran `Configuration`

- Dans la barre de navigation, cliquer sur la commande `Config` du menu `GUM`.
  L'écran suivant est affiché :



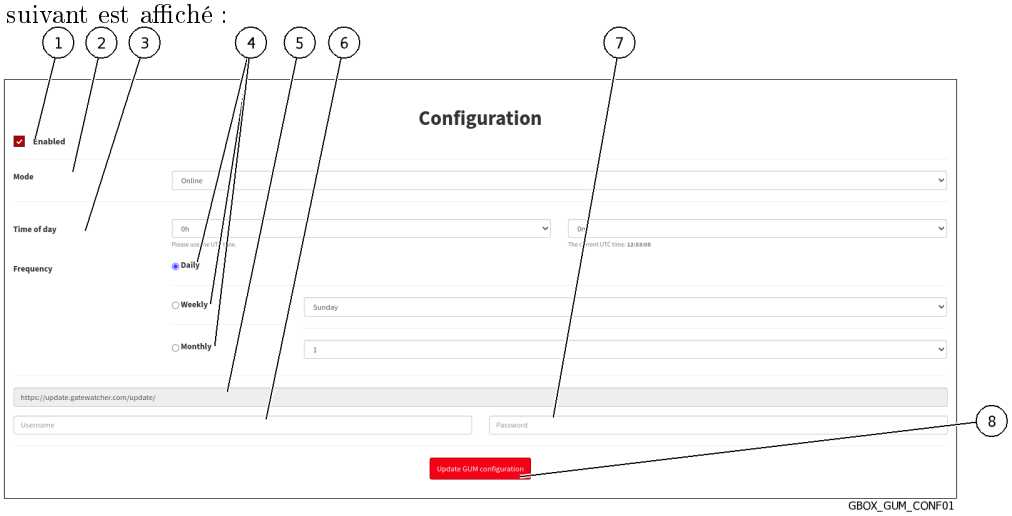
GBOX_GUM_CONF01

- Effectuer la *Procédure pour configurer le mode en ligne*

ou
Effectuer la *Procédure pour configurer le mode local*

9.4.1.5 Procédure pour configurer le mode en ligne

- Dans la barre de navigation, cliquer sur la commande `Config` du menu `GUM`.
  L'écran suivant est affiché :



- Cocher le choix (1) `Enabled`.
- Dans le champ (2) `Mode`, sélectionner le choix `Online`.
- Sélectionner l'heure (champ (3) `Time of day`) de la mise à jour.
- Configurer la fréquence des mises à jour :
  - Sélectionner la fréquence (choix à l'aide des boutons (4) `Daily`, `Weekly`, `Monthly`)
  - Dans le cas du choix `Weekly`, sélectionner le jour
  - Dans le cas du choix `Monthly`, sélectionner le mois

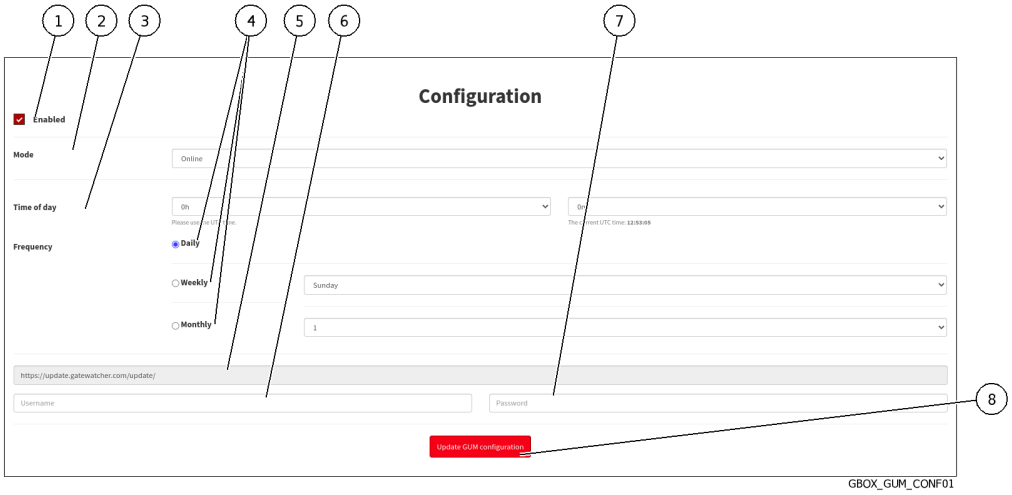
Note:

Le champ source des mises à jour (5) est automatiquement renseigné.

- Renseigner le login pour se connecter à update.gatewatcher.com :
- `Username` : champ (6)
- `Password` : champ (7)
- Cliquer sur le bouton `Update GUM configuration` (8).

9.4.1.6 Procédure pour configurer le mode local

- Dans la barre de navigation, cliquer sur la commande `Config` du menu `GUM`.
  L'écran suivant est affiché :



- Cocher le choix (1) `Enabled`.
- Dans le champ (2) `Mode`, sélectionner le choix `local`.
- Configurer la fréquence de mises à jour :
  - Sélectionner la fréquence (choix à l'aide des boutons (4) `Daily`, `Weekly`, `Monthly`)
  - Dans le cas du choix `Weekly`, sélectionner le jour
  - Dans le cas du choix `Monthly`, sélectionner le mois
- Renseigner l'URL du dépôt local (5).
- Renseigner le login d'accéder au dépôt local (optionnel) :
  - `Username` : champ (6)
  - `Password` : champ (7)
- Cliquer sur le bouton `Update GUM configuration` (8).

9.4.2 Installation manuelle d'une mise à jour des signatures (update)

9.4.2.1 Introduction

Cette procédure décrit les différentes possibilités pour mettre à jour les fichiers de signatures des moteurs de détection de la solution.
Le déclenchement des mis à jour peut être :

- soit planifié .

  Cette planification est programmée dans la configuration de GUM (voir l'*Ecran `Admin-GUM - Config` de la legacy Web UI*).

  Dans ce cas, l'écran `Updates` donne les informations sur la dernière installation planifiée.
- soit manuelle.

  Dans ce cas, il est nécessaire de charge un package depuis le PC distant sur la GBox puis déclencher l'installation de ce paquet.

  Dans ce cas, l'écran `Updates` donne les informations sur cette installation.

Important:

Il n'est pas possible de faire une mise à jour en mode manuel si le mode online est configuré.

Note:

Voir la présentation décrite dans la *Mise à jour des signatures de détection et/ou des moteurs anti-viraux (updates)*.
L'interface graphique est décrite dans le paragraphe de l'*Ecran `Admin-GUM - Updates` de la legacy Web UI*.

Note:

Si besoin, configurer un proxy (voir la *Configuration d'un proxy*).

9.4.2.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

9.4.2.3 Opérations préliminaires

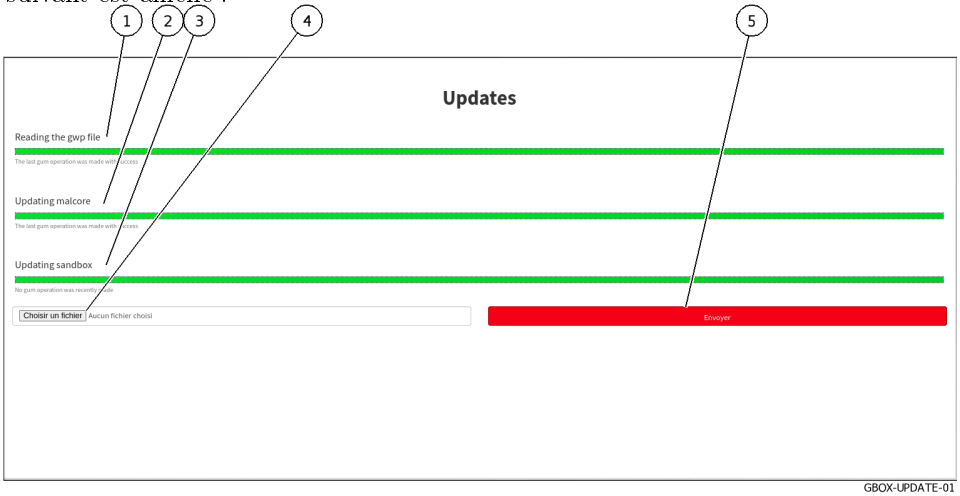
- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).
- Télecharger un fichier *.gwp* sur *https://update.gatewatcher.com/update/<version_gbox>/gbox/*

Note:

Les fichiers dont les noms se terminent par "v3.gwp" comme latest_malcore_v3.gwp ou latest_full_v3.gwp concernent la V101.
Les autres fichiers (latest_full.gwp, latest_malcore.gwp, ...) concernent la version 100 de la GBox

9.4.2.4 Procédure d'accès à la fenêtre Ecran `Admin/GUM/Updates`

- Dans la barre de navigation, cliquer sur la commande `Updates` du menu `GUM`.
  L'écran suivant est affiché :



9.4.2.5 Procédure de mise à jour des fichiers de signatures en mode manuel

- Cliquer sur le bouton `Parcourir` (4) et sélectionner le package préalablement téléchargé
- Valider le choix.

  Le bouton affiche `Please wait...`.

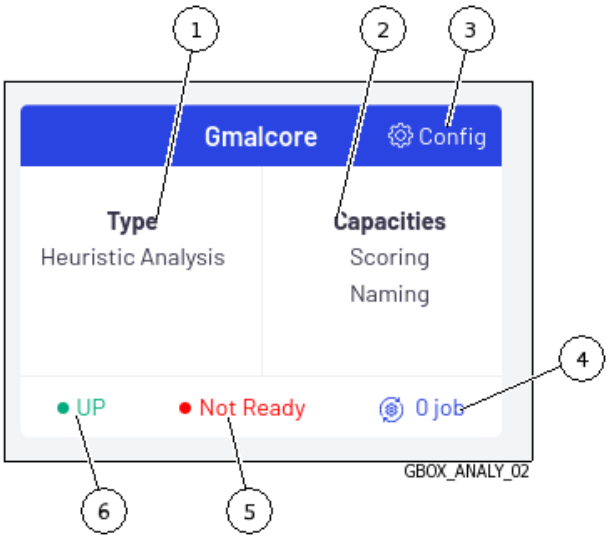
  La barre de progression du champ `Reading the gwp file` commence sa progression : ceci signifie que le fichier a été téléchargé et le système contrôle son intégrité.
- Attendre l'affichage du message `The last gum operation was made with success`.

  La barre de progression du champ `Updating malcore` commence sa progression : ceci correspond au traitement des fichiers du moteur Malcore.
- Attendre l'affichage du message `The last gum operation was made with success`.

  La barre de progression du champ `Updating sandbox` commence sa progression : ceci correspond au traitement des mises à jour des signatures et des modules utilisés par la sandbox.
- Attendre l'affichage du message `The last gum operation was made with success`.

9.4.2.6 Procédure de vérification du bon état des moteurs Gmalcore

- Dans la barre de navigation, cliquer sur la commande `Analysers`.



- Cliquer sur la commande (3) `Config`.

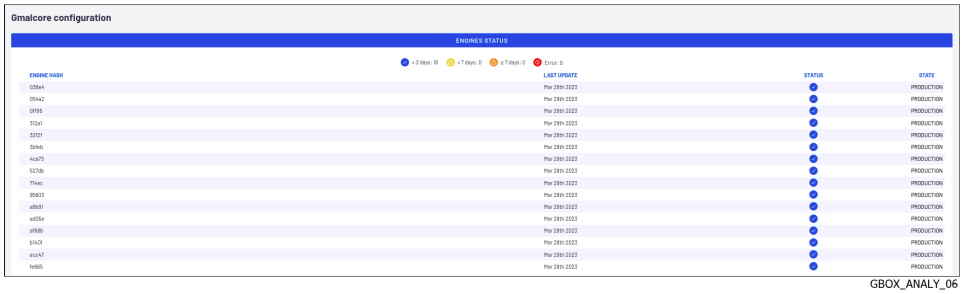
  L'écran suivant est affiché.

- Regarder la présence d'un message dans la zone (1).
- Dans le cas d'un message de type `x engine(s) have failed to update`, vérifier l'état des moteurs installés (colonne (2)).

  Les moteurs dont l'état est rouge dans la colonne (2) ne sont pas dans l'état PRODUCTION.

Certains moteurs prennent du temps pour se mettre à jour et sont toujours dans l'état DOWNLOADED.

- Attendre que la mise à jour se termine et que tous les moteurs soient OK (état PRODUCTION).



GBOX_ANALY_06

- Si l'un des moteurs n'est toujours pas OK alors il est nécessaire de redémarrer les services de Gmalcore.
  Pour cela, voir la *Procédure d'accès au service du moteur Malcore*.
- Si cela ne corrige pas le problème alors réinstaller les services de Gmalcore.
  Pour cela, voir la *Procédure d'accès au service du moteur Malcore*.

9.4.3 Installation d'un correctif (Hotfix)

9.4.3.1 Introduction

Un correctif permet d'appliquer une correction ou une modification donnée sans avoir à procéder à un mise à niveau complète de la solution ni à redémarrer la GBox.
À la différence des mises à jour, les correctifs ne sont pas automatisables et doivent être réalisés par un administrateur après avoir pris connaissance des notes de version.
Tous les paquets des correctifs sont téléchargeables via la plate-forme de téléchargement : https://update.gatewatcher.com/hotfix
Cette procédure décrit le déroulement de l'application d'un correctif.

Note:

Voir la présentation décrite dans l'*Application d'un correctif (Hotfix)*.
L'interface graphique est décrite dans l'*Ecran `Admin-GUM - Hotfix` de la legacy Web UI*.

9.4.3.2 Prérequis

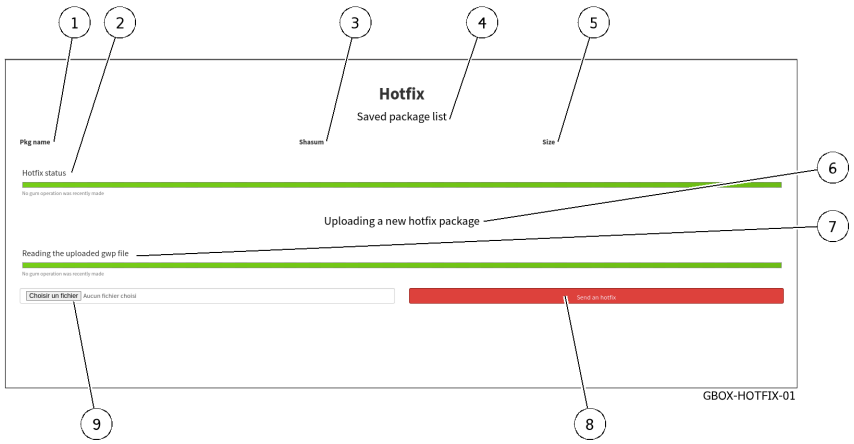
- Utilisateur : membre du groupe **Administrators**

9.4.3.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).
- Lire la note de version de la version souhaitée pour savoir si d'autres prérequis inhérents à cette dernière sont nécessaires.
- Récupérer un fichier *.gwp* sur https://update.gatewatcher.com/update/<version_gbox>/gbox/

9.4.3.4 Procédure d'accès à la fenêtre Ecran `Admin/GUM/Hotfix`

Dans la barre de navigation, cliquer sur la commande `Hotfix` du menu `GUM`.
L'écran suivant est affiché :



9.4.3.5 Procédure d'application d'un correctif

- Cliquer sur le bouton (9) `Choisir un fichier` et sélectionner le package préalablement téléchargé.
- Cliquer sur le bouton (8) `Send a hotfix`.
- Une fois le package présent dans la zone (1) `Saved package list`, cliquer sur le bouton `Apply`.
- Attendre que la barre de progression indique que l'opération a été complétée avec succès.
  Le correctif a été appliqué et les corrections sont effectuées sur l'équipement.

> **Note:**
>
> Dans certains cas, l'application d'un correctif peut engendrer un redémarrage du serveur Web et rendre indisponible l'interface Web quelques minutes (précisé dans la note de version).

9.4.4 Installation d'une mise à niveau (upgrade)

9.4.4.1 Introduction

Une mise à niveau permet de réaliser une montée de version majeure et implique un redémarrage de l'appliance concernée.
À la différence des mises à jour, les mises à niveau ne sont pas automatisables et doivent être réalisées par un administrateur après avoir pris connaissance des notes de version et des notes de mise à jour.
Cette procédure décrit le déroulement de l'application d'un mise à niveau.

Note:

Voir la présentation décrite dans le paragraphe *Mise à niveau (Upgrade)*.
L'interface graphique est décrite dans le paragraphe *Ecran `Admin-GUM - Upgrade` de la legacy Web UI*.

9.4.4.2 Prérequis

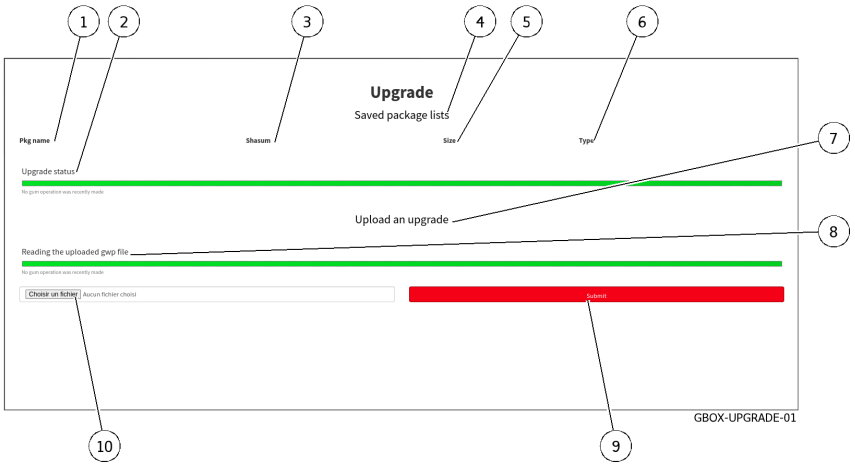
Utilisateur : membre du groupe **Administrators**

9.4.4.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).
- Lire la note de version de la version souhaitée pour savoir si d'autres prérequis inhérent à cette dernière sont nécessaires.
- Télécharger le paquet de mise à niveau de la version souhaitée sur le site (https://update.gatewatcher.com/upgrade).

9.4.4.4 Procédure d'accès à la fenêtre Ecran `Admin/GUM/Updates`

- Dans la barre de navigation, cliquer sur la commande `Updates` du menu `GUM`.
  L'écran suivant est affiché :



9.4.4.5 Procédure d'application d'une mise à niveau

- Cliquer sur le bouton (10) `Choisir un fichier` et sélectionner le package préalablement téléchargé.
- Cliquer sur le bouton (9) `Submit`.
- Une fois le package présent dans la zone (1) `Saved package list`, cliquer sur le bouton `Apply`.
- Attendre que la barre de progression indique que l'opération a été complétée avec succès.
- Redémarrer la GBox (voir l'utilisation de la *Commande `Restart`*).

  Après redémarrage, la GBox a pris en compte la version téléchargée.

9.5 Configuration de la GBox

9.5.1 Configuration de la GBox lors de la première connexion

9.5.1.1 Introduction

Bien qu'une grande partie de la solution soit déjà configurée par les équipes Gatewatcher, il est nécessaire d'effectuer, à minima, la configuration réseau de la GBox afin de pouvoir accéder à la Web UI.
Lors de la première connexion, il est nécessaire d'accéder à la **GBox** par l'interface iDRAC ou un terminal afin d'effectuer la configuration réseau.
L'utilisateur recommandé est **setup**, par défaut le mot de passe de cet utilisateur est : **default**.

Important:

Il est important de changer ce mot de passe dès que possible.

9.5.1.2 Prérequis

- Utilisateur : setup
- Utilisateur : membre du groupe **Administrators**
- Brancher le port réseau GBx0 pour l'interface de management (pour plus d'information, voir la présentation de l'*Interface réseau `Gbx0`*).
- Si besoin, brancher le port réseau l'interface GBx1 pour la connection des machines virtuelles de Gnest à Internet (pour plus d'information, voir la présentation de l'*Interface réseau `Gbx1`*).

9.5.1.3 Opérations préliminaires

- Vérifier que la clé LUKS soit bien connectée sur l'équipement.

Note:

Au démmarrage, s'il n y a pas de clé LUKS ou si ce n'est pas la bonne, le système d'exploitation ne pourra pas accéder au contenu des disques durs.
En cas de problèmes, vérifier :

- la clé : elle doit être la bonne (et non celle d'une autre appliance...)
- le bon fonctionnement du port USB : si besoin, changer de port USB

Suivant le cas :

- soit utiliser la *Connexion directe au menu de configuration avec clavier et écran*
- soit utiliser l'*Accès au menu de configuration en HTTP via l'iDRAC (serveur DELL)*
- soit utiliser l'*Accès au menu de configuration en SSH via l'interface iDRAC en mode redirection du port série*

Note:

Faire attention à la configuration du clavier (version fr ou us).

Le menu de configuration est affiché.

- Si nécessaire, sélectionner la langue utilisée pour le clavier (voir la *Commande `Keymap`*).

9.5.1.4 Procédure de configuration des paramètres généraux de la GBox

Note:

Les paramètres généraux sont :
- le nom (hostname)
- le nom du domaine (domain name)
- les serveurs DNS (primaire et secondaire)
- les serveurs NTP (primaire et secondaire)

- Accéder au menu de visualisation et de configuration réseau (voir la *Commande `Network`*).
- Visualiser la configuration courante (voir la *Procédure de visualisation de la configuration courante*).
- Modifier les paramètres généraux si nécessaire (voir la *Procédure de modification des paramètres généraux de la GBox*).
- Appliquer la procédure de prise en compte des modifications si besoin (voir la *Procédure de prise en compte des modifications*).

9.5.1.5 Procédure de configuration des paramètres de l'interface réseau de management GBx0

- Visualiser la configuration de chaque interface réseau (voir la *Procédure de visualisation de l'état des interfaces réseau*).
- Modifier les paramètres si nécessaire (voir la *Procédure de modification des paramètres des interfaces réseaux*).
- Appliquer la *Procédure de prise en compte des modifications* pour l'interface GBx1.

Note:

Une fois cette première configuration effectuée, il est possible de se connecter à l'interface de la GBox par un navigateur Web en HTTPS à l'adresse configurée.
Les utilisateurs par défaut sont les suivants :

- admin
- administrator
- operator

Pour connaître les droits et fonctions autorisés à chacun des comptes / groupe, voir la *Présentation des comptes*.
Pour connaître les différentes fonctions de l'interface graphique administrateur ou opérateur, voir la *Présentation des interfaces graphiques*.

9.5.1.6 Procédure de configuration des paramètres de l'interface réseau GBx1 (des machines virtuelles de Gnest) à Internet

- Appliquer la *Procédure de modification des paramètres des interfaces réseaux* pour l'interface GBx1
- Appliquer la *Procédure d'accès au menu `Services`*
- Appliquer la *Procédure d'accès aux services Sandbox du moteur Gnest*
- Appliquer la *Procédure d'activation de la connexion internet*

9.5.1.7 Procédure de saisie de la licence

- Appliquer la procédure de saisie de la *Mise en place d'un certificat SSL*.
  Une fois la licence validée et activée, le contenu de la page se met à jour et affiche le détail du contenu de la licence.
  En cas de licence absente ou expirée, l'interface redirige automatiquement vers cette page afin de résoudre la situation.

9.5.1.8 Procédure de configurer le certificat SSL

Le certificat SSL atteste de l'identité de la GBox et permettra de chiffrer les données échangées.

- Appliquer la procédure de saisie de la *Mise en place d'un certificat SSL*.

9.5.1.9 Procédures post liminaires

- Mettre en exploitation la GBox : voir la *Mise en exploitation d'une GBox*.

9.5.2 Mise en exploitation d'une GBox

9.5.2.1 Introduction

Après avoir configurée la GBox, cette procédure indique comment la mettre en exploitation.

9.5.2.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

9.5.2.3 Opérations préliminaires

- Effectuer la *Configuration de la GBox lors de la première connexion*

9.5.2.4 Procédure de gestion des utilisateurs

Les comptes étant par défaut, il peut être nécessaire de modifier les comptes par défaut ou en ajouter des nouveaux.

- *Création d'un utilisateur local*
- *Modification de certaines informations d'un utilisateur local*

9.5.2.5 Gérer les moteurs d'analyse

- Si besoin, modifier le nombre de machines virtuelles du moteur Gnest :
  - pour cela, voir la procédure pour créer une ou des machines virtuelles (*Procédure de configuration du moteur Gnest*)
  - prendre en compte cette nouvelle configuration en créant ou modifiant les modèles d'analyse (voir la *Gestion des modèles*)
- Appliquer la procédure de vérification du bon état des moteurs d'analyse et des mises à jour (voir la *Procédure de surveillance des moteurs d'analyse*)

9.5.2.6 Procédure de gestion des modèles d'analyse

- Créer des modèles d'analyse (voir la procédure de *Création d'un modèle d'analyse*).
- Gérer les modèles d'analyse (voir la procédure de *Gestion des modèles d'analyse*).

Astuce:

Créer un modèle en utilisant les moteurs Gmalcore et Gnest préalablement configurés et le définir par défaut.

Avec un compte du groupe Operators, sélectionner un fichier et effectuer une analyse rapide.

Vérifier que l'analyse s'effectue correctement.

9.5.2.7 Procédure d'association avec le GCenter

- Créer un token API et le copier.
- Se connecter au GCenter et effectuer l'association avec la GBox (se référer à la documentation du GCenter).
- Coller le token durant la procédure d'association.
- Mettre en exploitation le GCenter.
- En cas d'envoi automatique des fichiers à analyser, vérifier que les analyses soient bien effectuées : de nouveaux rapports sont crées...
- Envoyer manuellement un fichier à analyser depuis le GCenter puis télécharger le rapport correspondant : ces opérations se font sur le GCenter.

9.5.3 Modification de la licence

9.5.3.1 Introduction

La licence peut avoir une fin de validité.

Il est possible de renseigner une nouvelle licence, et également de régler la notification dans l'interface d'une date d'expiration proche en renseignant le nombre de jour avant l'expiration.

Pour obtenir une licence GCenter, merci de vous rapprocher de votre ingénieur d'affaires GATEWATCHER ou contacter le à l'adresse commerciaux@GATEWATCHER.com.

Une fois la licence validée et activée, le contenu de la page se met à jour et affiche le détail du contenu de la licence.

En cas de licence absente ou expirée, l'interface redirige automatiquement vers cette page afin de résoudre la situation.

L'interface graphique est décrite dans l'*Ecran `Licence configuration`*.

9.5.3.2 Prérequis

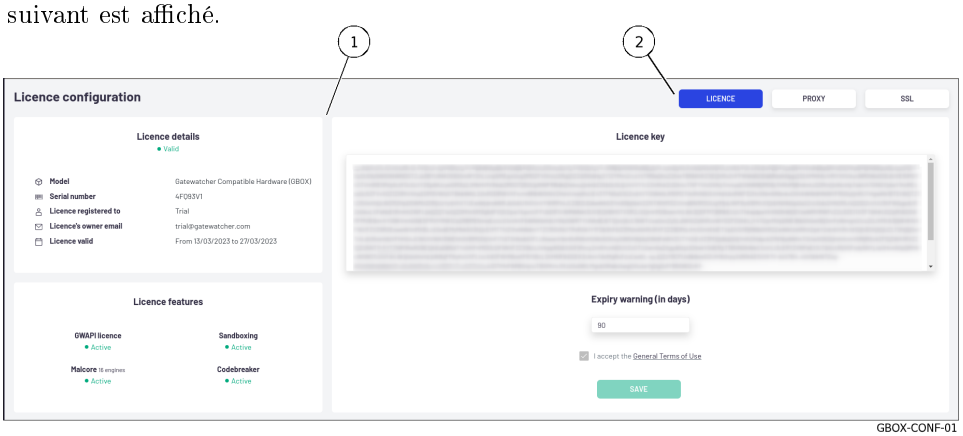
- Utilisateur : membre du groupe **Administrators**

9.5.3.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

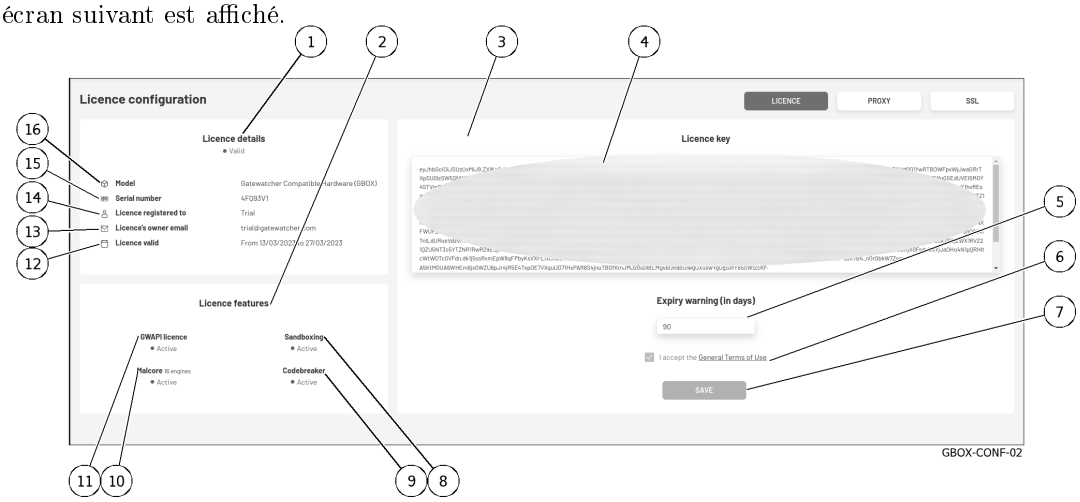
9.5.3.4 Procédure d'accès à la fenêtre Ecran `LICENCE`

- Cliquer sur la commande `Configuration` du menu `Admin-GBox`.
  L'écran suivant est affiché.



GBOX-CONF-01

- Cliquer sur sur le bouton `LICENCE`.
  L'écran suivant est affiché.



GBOX-CONF-02

9.5.3.5 Procédure de mise à jour de la licence

Important:

Pour obtenir une licence GCenter merci de vous rapprocher de votre ingénieur d'affaire GATEWATCHER ou contacter le à l'adresse commerciaux@GATEWATCHER.com

- Coller la licence dans le champ (4) `License key`.
- Saisir le nombre de jours avant l'expiration.de la licence.
- Cocher le champ (6) `I accept the General Terms of Use`.
- Cliquer sur le bouton (7) `SAVE`.
  Une fois la licence validée et activée, le contenu de la page se met à jour et affiche le détail du contenu de la licence.

9.5.4 Configuration d'un proxy

9.5.4.1 Introduction

La GBox offre la possibilité de configurer un serveur mandataire (ou proxy) afin de récupérer les updates (mise à jour de signatures) via celui-ci.

Cet écran permet de définir un proxy pour les mises à jour via GUM.
L'interface graphique est décrite dans l'*Ecran `Proxy settings`*.

9.5.4.2 Prérequis

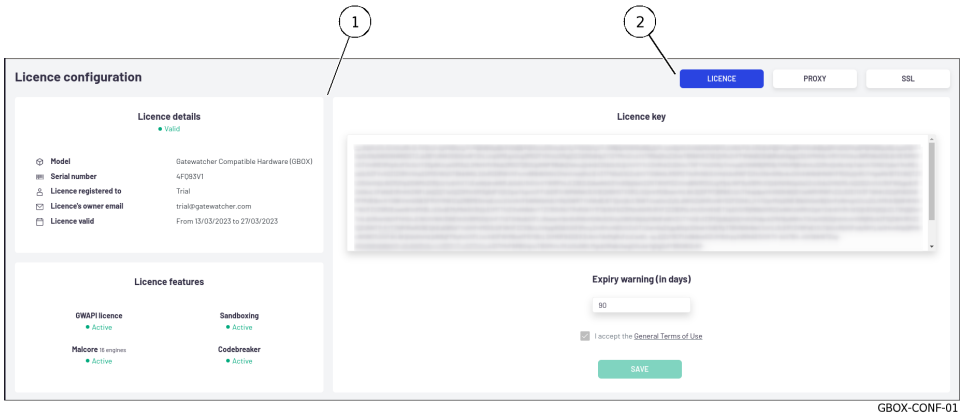
Utilisateur : membre du groupe **Administrators**

9.5.4.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

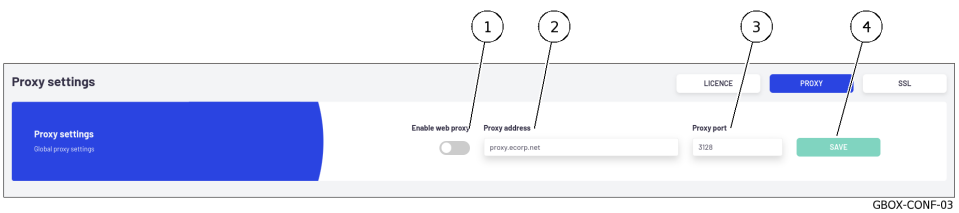
9.5.4.4 Procédure d'accès à la fenêtre Ecran `PROXY`

- Cliquer sur la commande `Configuration` du menu `Admin-GBox`.
  L'écran suivant est affiché.



GBOX-CONF-01

- Cliquer sur sur le bouton `PROXY`.
  L'écran suivant est affiché.



GBOX-CONF-03

9.5.4.5 Procédure de configuration d'un proxy

- Activer l'utilisation du proxy en utilisant le sélecteur (1) `` `Enable Web Proxy` ``.
- Définir l'adresse du serveur mandataire sous forme d'adresse IP ou de FQDN dans le champ (2) `` `Proxy address` ``.
- Sélectionner le port d'écoute du proxy (1-65535) à l'aide du champ (3) `` `Proxy port` ``.
- Cliquer sur le bouton (4) `` `SAVE` ``.
  Si le message suivant est affiché `` `Failed to resolve proxy address` ``, vérifier les paramètres saisis.

9.5.5 Mise en place d'un certificat SSL

9.5.5.1 Introduction

Il est possible d'utiliser un certificat personnalisé de la GBox.
Le certificat généré atteste de l'identité de la GBox et permet de chiffrer les données échangées.

L'interface graphique est décrite dans l'*Ecran `SSL settings`*.

9.5.5.2 Prérequis

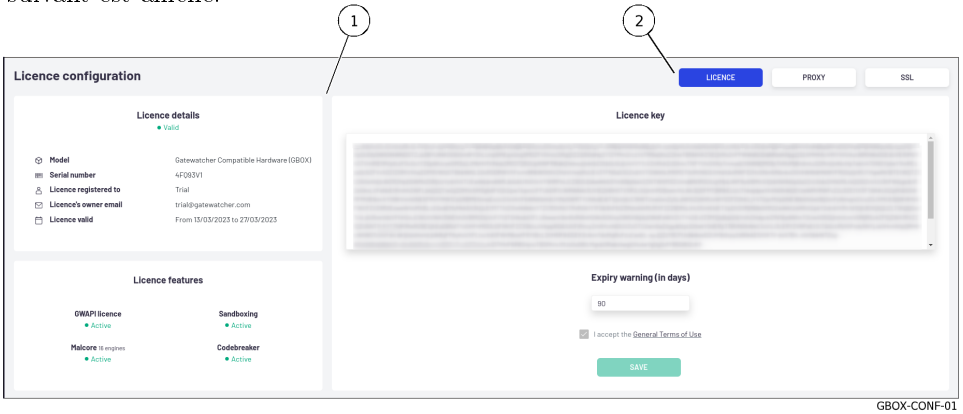
Utilisateur : membre du groupe **Administrators**

9.5.5.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.5.5.4 Procédure d'accès à la fenêtre Ecran `SSL`

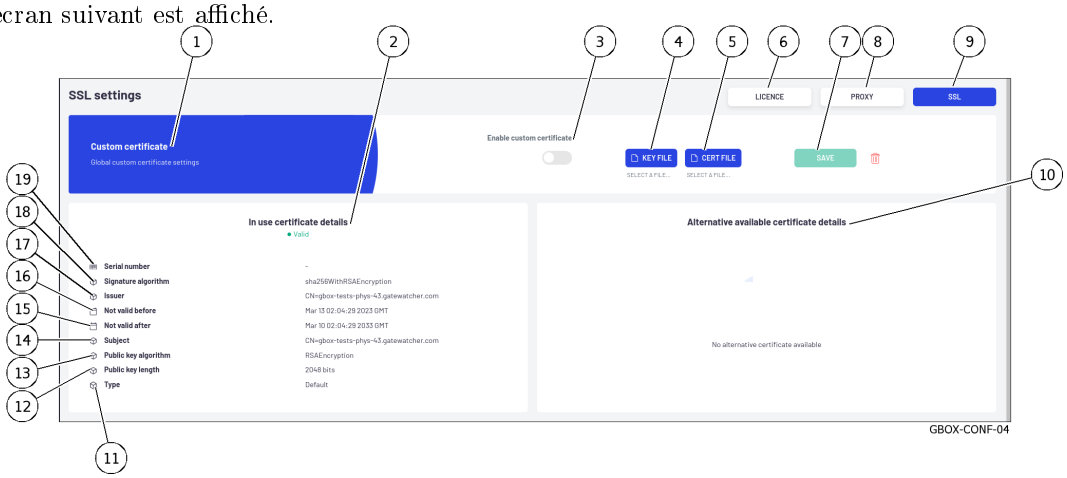
- Cliquer sur la commande `` `Configuration` `` du menu `` `Admin-GBox` ``.
  L'écran suivant est affiché.



GBOX-CONF-01

- Cliquer sur sur le bouton `` `SSL` ``.

L'écran suivant est affiché.



9.5.5.5 Procédure de configuration d'un certificat personnalisé

Dans la zone (1) `Custom Certificate` :

- Sélectionner `Enable Custom Certificate` (3).
- Utiliser le bouton (4) `KEY FILE` pour sélectionner la clé privée à utiliser.
  La fenêtre de selection du fichier (extension .key) s'ouvre pour sélection du fichier.
- Valider le choix.
- Utiliser le bouton (5) `CERT FILE` pour sélectionner le certificat associé à la clé privée.
  La fenêtre de sélection du fichier s'ouvre pour sélection du fichier.
- Valider le choix.
- Cliquer sur le bouton (7) `SAVE`.

9.6 Administration de la GBox

9.6.1 Génération et téléchargement des fichiers pour le diagnostic

9.6.1.1 Introduction

Cette procédure permet de générer et de télécharger un fichier de diagnostic compressé comprenant les fichiers de logs, les tables d'informations des moteurs d'analyse et des échanges syslogs sur une période donnée.

Important:

Le fichier d'export de log peut être protégé par un mot de passe (uniquement connu par le support de GATEWATCHER).

Note:

Voir la présentation des données pour le diagnostic dans le paragraphe *Utilisation des données*.
L'interface graphique de la fonction diagnostic est décrite dans l'*Ecran `Admin-GBox - Diagnostics` de la Web UI*.

9.6.1.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

9.6.1.3 Opérations préliminaires

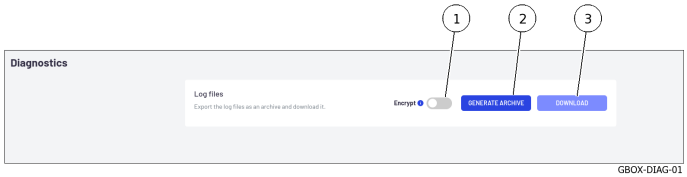
- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.6.1.4 Procédure d'accès à la fenêtre `Diagnostics`

- Dans la barre de navigation, cliquer successivement sur :
  - le bouton `Admin`
  - le sous menu `GBox`
  - la commande `Diagnostics`

  La fenêtre `Diagnostics` est affichée.

9.6.1.5 Procédure de génération et de téléchargement des fichiers de diagnostic



GBOX-DIAG-01

- Utiliser le sélecteur (1) `Encrypt` si le fichier de diagnostic doit être envoyé au support de GATEWATCHER.
- Appuyer sur le bouton (2) `GENERATE ARCHIVE`.

  Un message est affiché pour indiquer le résultat de la génération :

```
Success
Log export in progress.
```

- Appuyer sur le bouton (3) `Download`.

  Une fenêtre s'ouvre qui affiche le téléchargement des fichiers.

  Le fichier de diagnostic est donc présent dans le répertoire local du PC.

  Le fichier de diagnostic téléchargé est nommé :
  - si le fichier est chiffré : **hostname-time-logs.gwl**
  - si le fichier ne l'est pas : **hostname-time-logs.tar.bz2**

  Important:

  Si l'option `Encrypt` est activée, seul le support de GATEWATCHER sera en mesure de déchiffrer le fichier de diagnostic chiffré.

- Envoyer le fichier de diagnostic chiffré au support de GATEWATCHER pour effectuer l'analyse.

9.6.2 Utilisation d'un endpoint API

9.6.2.1 Introduction

Cette procédure indique comment :

- exécuter un endpoint localement
- récupérer la réponse
- avoir le .json correspondant
- connaître le modèle de la réponse et d'avoir un exemple de celle-ci

En cliquant sur le bouton `Try it out`, il est possible de tester la requête sélectionnée et l'outil génère la requête à utiliser avec curl.
La *Procédure d'exécution d'un endpoint* indique comment utiliser l'interface graphique swagger pour sélectionner un API, exécuter la requête, récupérer la réponse et le curl de la requête.
Toutefois cette requête hérite des droits (et donc du token) du créateur de la requête.
Pour effectuer une requête avec des droits différents, se référer à la *Procédure pour modifier le token associé à la requête*.

9.6.2.2 Prérequis

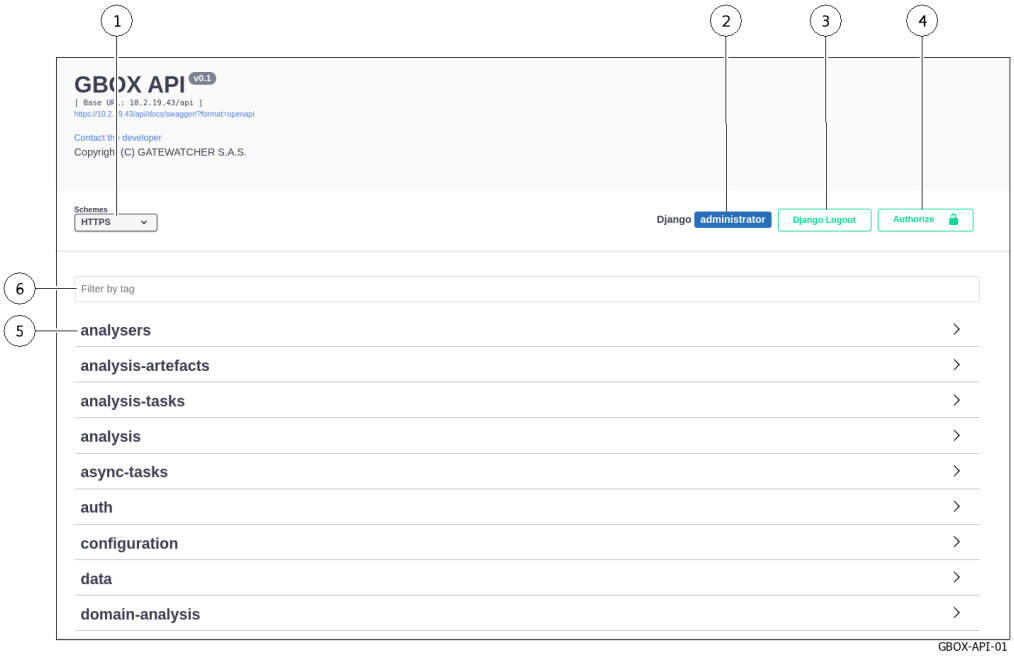
Utilisateur : membre du groupe **Administrators**

9.6.2.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.6.2.4 Procédure d'accès à l'API GBox

- Cliquer sur le bouton (3) `API` de la barre de titre.
  L'écran suivant est affiché.

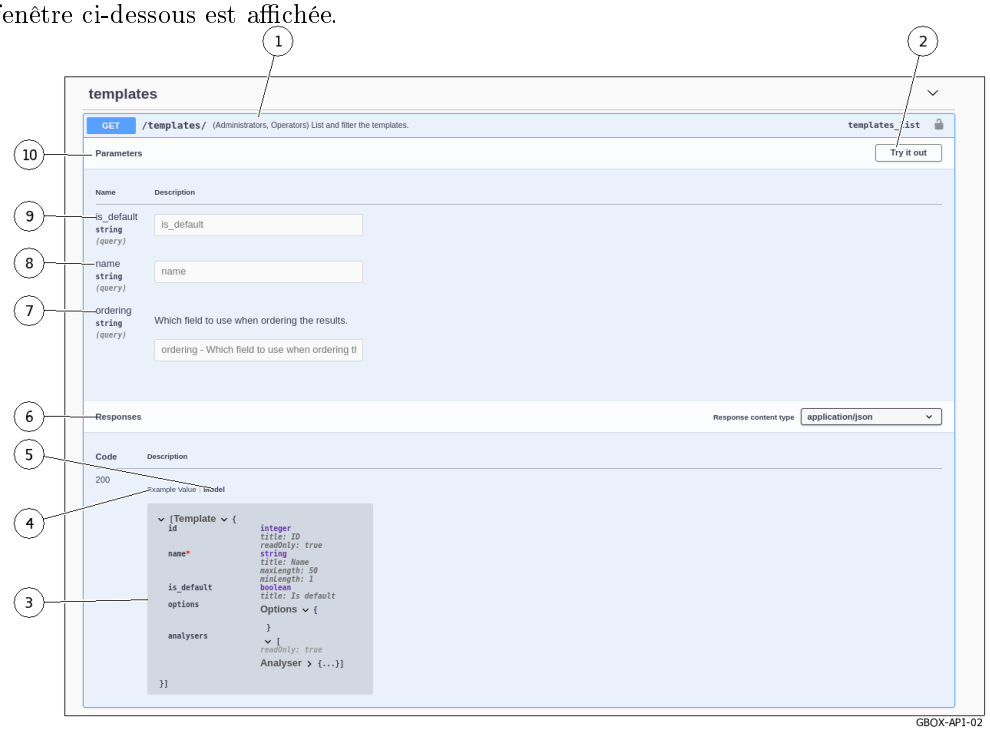


9.6.2.5 Procédure d'exécution d'un endpoint

Pour illustrer cet exemple, l'API choisi est celui qui permet de lister les modèles d'analyse.

- Sélectionner le thème `templates` dans la liste des thèmes existants (5).
- Cliquer sur l'API `GET/templates/ (Operators, Administrators) List and filter the templates`.

  La fenêtre ci-dessous est affichée.



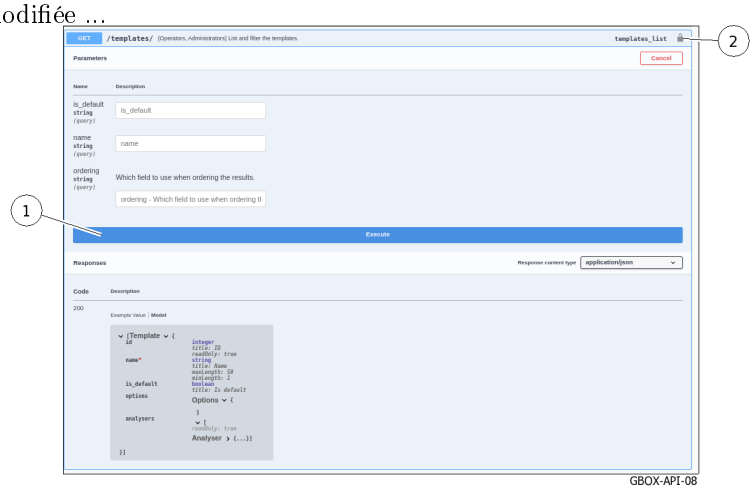
Note:

Pour l'exemple c'est l'endpoint `/templates` qui a été choisi.
Pour rappel : l'objet est de lister et filtrer les modèles existants.

Astuce:

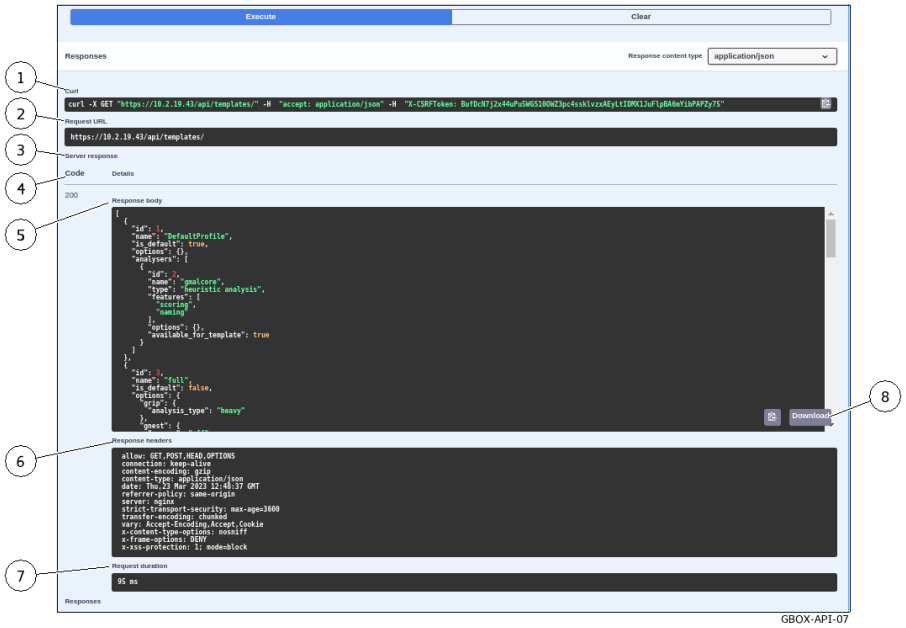
Pour certains endpoints, il est obligatoire se saisir des paramètres avant de pouvoir l'exécuter.

- Cliquer sur le bouton (2) `Try it out`.
  La fenêtre est modifiée ...



GBOX-API-08

- Cliquer sur le bouton (1) `Execute`.
  La requête est lancée et la fenêtre suivante est affichée.

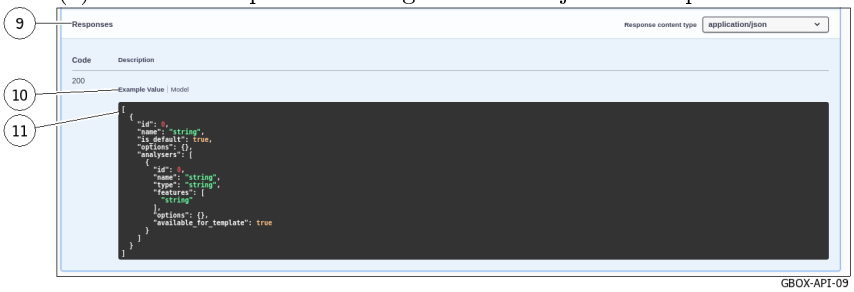


GBOX-API-07

Cette fenêtre comprend plusieurs parties :

- la zone d'affichage (1) `Curl` pour la requête Curl
- la zone d'affichage (2) `URL` pour la requête URL
- la zone (3) `Server response` :
  - le `Code` (4) de retour :
    - Si le code a pour valeur `200` alors l'exécution s'est correctement effectuée.
    - Si le message `code 400 Undocumented Error Bad Request` est affiché, vérifier que les paramètres obligatoires soient bien saisis.
  - le corps de la réponse (5) : se référer à la présentation de l'*Présentation de l'interface API GBOX*
  - la zone détaillant l'entête de la réponse (6)
  - la valeur en ms de la durée de la requête (7)

* le bouton (8) `Download` pour télécharger le fichier .json correspondant



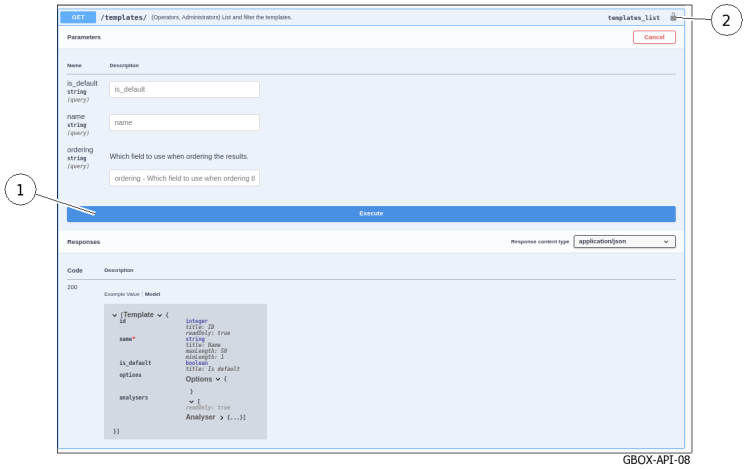
GBOX-API-09

– la zone (9) `Responses`
  Cette zone affiche des informations différentes suivant l'utilisation du lien (10) `Model` ou `Example Value`.
– soit le modèle de sortie (`Model`) dans le champ (11) : se référer à la présentation *Présentation de l'interface API GBOX*
– soit un exemple de la réponse dans le champ (11) attendue avec des valeurs pour exemple (`Example Value`) : se référer à la présentation *Présentation de l'interface API GBOX*
  Les valeurs sont :
  * pour le type integer (valeur 0)
  * pour le type string (valeur = string)
  * pour le type boolean (valeur = true)

Note:

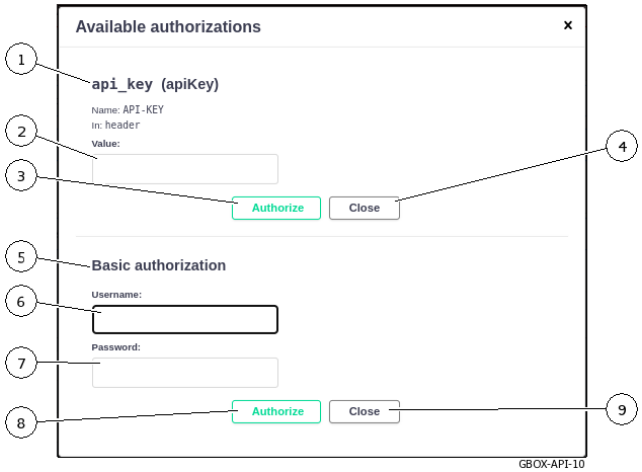
La copie d'écran est un exemple.

9.6.2.6 Procédure pour modifier le token associé à la requête



GBOX-API-08

- Cliquer sur le bouton (2).
  La fenêtre `Available authorizations` est affichée :



Deux options sont possibles :
  - soit l'utilisation d'un apikey (token préalablement créé)
  - soit l'utilisation d'une autorisation par nom et mot de passe d'un compte préalablement créé
- Pour utiliser un apikey (1) (token préalablement créé) :
  - coller le token dans le champ (2) `value`
  - valider en cliquant sur le bouton (3) `Authorize`
  - fermer la fenêtre avec le bouton (4) `Close`

Note:

Le token peut avoir une durée de vie limitée : voir la *Partie `API tokens` du sous menu `Accounts`*.

- Pour utiliser une autorisation (5) :
  - cliquer dans le champ (6) `Username`
    La liste des comptes existants est affichée.
  - entrer le mot de passe du compte (7)
  - valider en cliquant sur le bouton (8) `Authorize`
  - fermer la fenêtre avec le bouton (9) `Close`

9.7 Gestion des comptes utilisateur

9.7.1 Création d'un utilisateur local

9.7.1.1 Introduction

Cette procédure décrit la création d'un nouvel utilisateur.
Pour cela, il est demandé de saisir :

- des informations obligatoires (nom d'utilisateur et mot de passe)
- des informations optionnelles (adresse Email, prénom et nom)
- de sélectionner l'appartenance aux groupes existants (Operators, Administrators)
- d'activer ou non ce nouvel utilisateur

Note:

Voir la présentation des comptes et des groupes décrites dans la *Présentation des comptes de l'interface web et de leurs gestions*.
L'interface graphique est décrite dans l'*Ecran `Admin-GBox- Users management` de la Web UI*.

9.7.1.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

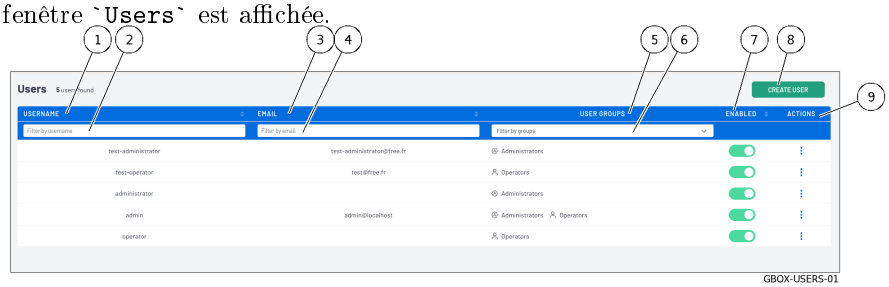
9.7.1.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

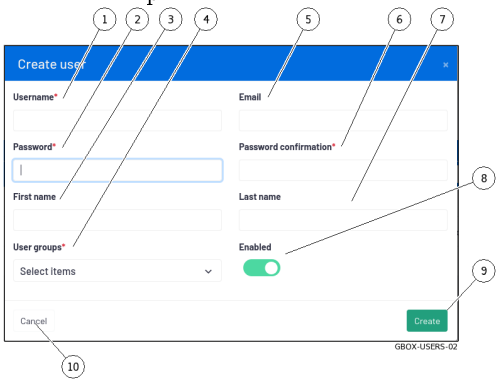
9.7.1.4 Procédure d'accès à la fenêtre `Users management`

- Dans la barre de navigation, cliquer successivement sur :
  - le bouton `Admin`
  - le sous menu `GBox`
  - la commande `Users management`

  La fenêtre `Users` est affichée.



- Cliquer sur le bouton (8) `CREATE USER`.
  La fenêtre `Create user` est affichée et permet la création d'utilisateur.



9.7.1.5 Procédure de création d'un utilisateur

- Entrer les information suivantes :
- le nom complet du nouvel utilisateur dans le champ (1) `Username`
  Ne peut contenir que des lettres, des chiffres et des caractères [@/./+/-/-/_.]
- dans le champ (5) `Email address`, l'adresse mail : champ optionnel
- dans le champ (3) `First name`, le prénom de l'utilisateur : champ optionnel
- dans le champ (7) `Last name`, le nom de l'utilisateur : champ optionnel
- Choisir les droits donc l'appartenance à ou aux groupes :
- `Operators` et / ou `Administrators` avec le sélecteur (4)
- Entrer le mot de passe. Pour cela :
- le saisir dans le champ (2) `Password`
- le saisir à nouveau dans le champ (6) `Password confirmation`
  Si les deux mots de passe ne correspondent pas, le message suivant est affiché : `The two password fields do not match.`
- Activer le compte avec le sélecteur (8) `Enabled`.
- Valider la saisie avec le bouton (9) `Create`.
  Après validation, le nouvel utilisateur apparaît dans l'écran `Users`.

9.7.2 Modification du mot de passe du compte courant

9.7.2.1 Introduction

Cette procédure décrit comment modifier le mot de passe de l'utilisateur courant.
Pour entrer un nouveau mot de passe conforme avec la politique à appliquer, le système propose, de base, six mots de passe.
Le bouton `REGENERATE` permet de créer six nouveaux mots de passe.

Danger:

Noter précautionneusement le mot de passe saisi, surtout si le compte courant est le seul compte du groupe Administrators.

L'interface graphique est décrite dans la présentation de la *Gestion du compte courant, membre du groupe Operators*.

9.7.2.2 Prérequis

- Utilisateur : membre du groupe **Operators**

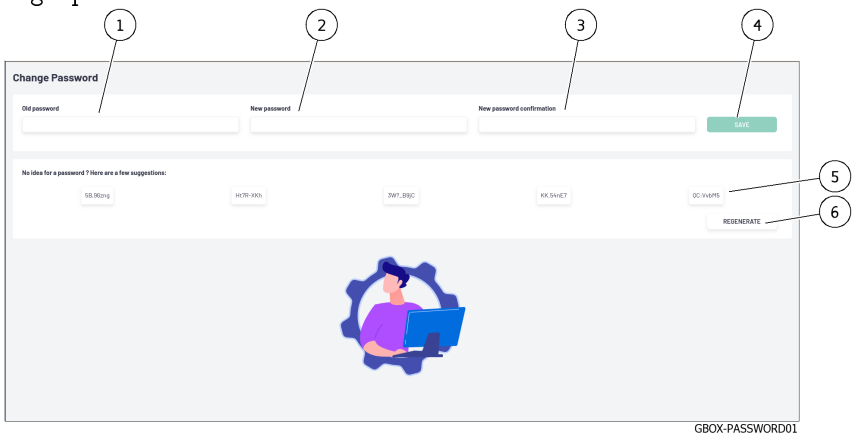
9.7.2.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.2.4 Procédure

BARRE_TITRE_OPERATOR

- Cliquer sur le bouton du compte courant (4).
- Sélectionner la commande `Change password`.
  La fenêtre `Change password` est affichée.



GBOX-PASSWORD01

- Entrer l'ancien mot de passe dans le champ (1) `Old password`.
- Entrer le nouveau mot de passe dans le champ (2) `New password`.
- Entrer le nouveau mot de passe dans le champ (3) `New password confirmation`.
  Le mot de passe saisi doit correspondre à la *Gestion de la politique des mots de passe*.
  Le système vérifie la concordance du mot de passe avec la politique de vérification.
  Dans le cas de non concordance, un des messages suivants est affiché :
  - `Minimal length 8` : indique un mot de passe trop court (8 caractères minimum)
  - `Uppercase` : indique le manque d'une capitale
  - `Lowercase` : indique le manque d'une minuscule
  - `Symbol` : indique le manque d'un caractère spécial
  - `Digit` : indique le manque d'un digit

> **Note:**
> Pour copier un des mots de passe proposé, cliquer sur le coté droit du mot de passe.
> Une fenêtre est affichée informant que le mot de passe est copié dans le presse papier.
> Pour coller ce mot de passe, cliquer droit puis coller dans chacun des deux champs.
> Surtout, NOTER le mot de passe avant de sauvegarder.

- Cliquer sur le bouton (4) `SAVE`.

> **Note:**
> Si le message suivant est affiché `you used this password recently, please choose a different one.`, saisir un mot de passe qui n'a pas déjà utilisé.

9.7.3 Modification de certaines informations d'un utilisateur local

9.7.3.1 Introduction

Cette procédure décrit la procédure de modification d'utilisateurs locaux :

- l'adresse Email
- le prénom
- le nom
- l'appartenance aux groupes `Operator` ou / et `Administrator`
- l'activation du compte

Note:

Voir la présentation des comptes et des groupes décrites dans le paragraphe *Présentation des comptes de l'interface web et de leurs gestions*.
L'interface graphique est décrite dans la *Fenêtre `Edit user`*.

9.7.3.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

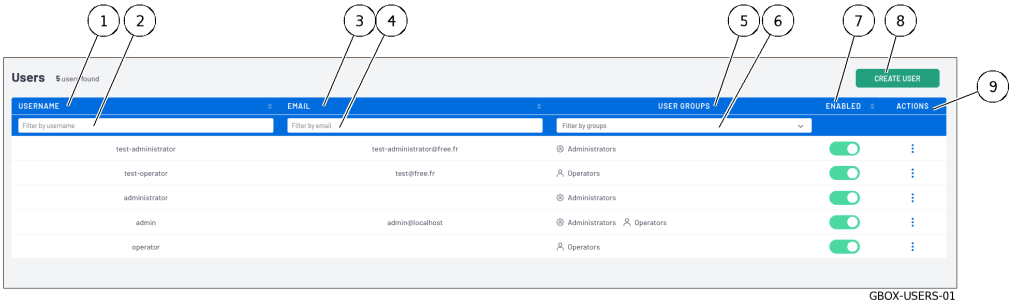
9.7.3.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.3.4 Procédure d'accès à la fenêtre `Users management`

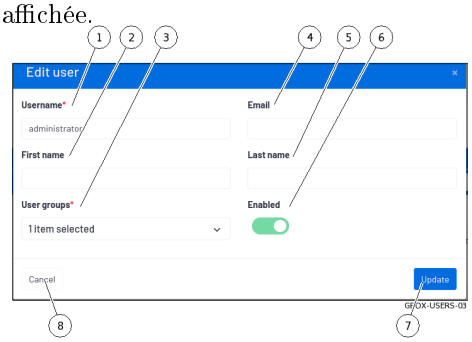
- Dans la barre de navigation, cliquer successivement sur :
  - le bouton `Admin`
  - le sous menu `GBox`
  - la commande `Users management`

  La fenêtre `Users` est affichée.



GBOX-USERS-01

- Cliquer sur la commande `Edit` de la partie (9) `ACTIONS` de l'utilisateur dont il faut modifier les paramètres.
  La fenêtre `Edit user` est affichée.



9.7.3.5 Procédure de modification de certaines informations d'un utilisateur

- Saisir ou modifier les données présentes dans :
- dans le champ (1) `Username`
- dans le champ (4) `Email`
- dans le champ (2) `First name`
- dans le champ (5) `Last name`
- Modifier si besoin les droits avec le choix sélectionné dans le champ (3) `User groups` (`Operators` et / ou `Administrators`).
- Modifier si besoin l'état du compte avec le sélecteur (6) `Enabled`.
- Valider les modifications en utilisant le bouton (7) `Update`.
  Le système affiche le message `Success User updated`.

9.7.4 Réinitialisation du mot de passe d'un utilisateur

9.7.4.1 Introduction

Cette procédure décrit la procédure de réinitialisation du mot de passe d'un utilisateur.

Note:

Voir la présentation des comptes et des groupes décrite dans la *Présentation des comptes de l'interface web et de leurs gestions*.

Note:

Cette procédure permet de régénérer le mot de passe associé au compte utilisateur en cas de perte ou d'oubli.
Le système proposer un nouveau mot de passe.

Danger:

Il est possible de sélectionner son propre compte!
Si c'est volontaire, noter précautionneusement le mot de passe affiché.

9.7.4.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

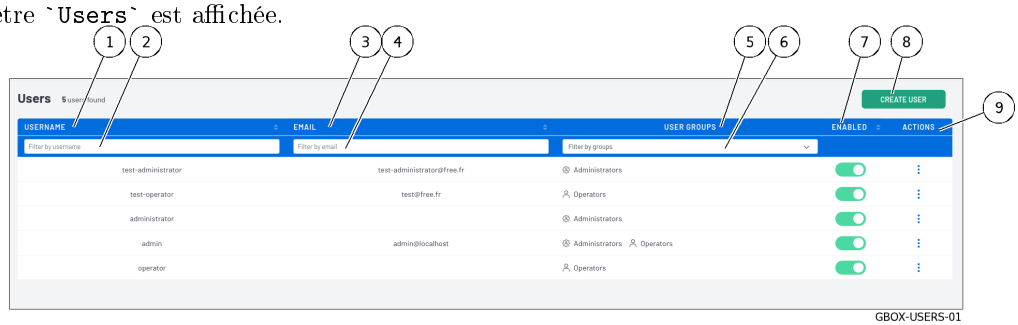
9.7.4.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.4.4 Procédure d'accès à la fenêtre `Users management`

- Dans la barre de navigation, cliquer successivement sur :
- le bouton `Admin`
- le sous menu `GBox`
- la commande `Users management`

  La fenêtre `Users` est affichée.



9.7.4.5 Procédure de réinitialisation du mot de passe d'un utilisateur

Note:

Cette procédure permet de régénérer le mot de passe associé au compte utilisateur en cas de perte ou d'oubli.

Le système propose un nouveau mot de passe.

- Sélectionner le compte de l'utilisateur.
- Cliquer sur la commande `Reset password` de la partie `ACTIONS` (9) de l'utilisateur dont il faut modifier le mot de passe.

  Le message suivant est affiché :

```
Reset user password.
Do you want to reset the following user password ?
test-administrator
The new password will be displayed in this modal.
```

- Cliquer sur le bouton `Confirm`.

  La fenêtre `Reset user password` est affichée.

  Le système propose un nouveau mot de passe pour cet utilisateur.
- Noter le mot de passe de l'utilisateur et le contacter pour indiquer son nouveau mot de passe.

- Cliquer sur le bouton `Close`.
  Le système affiche le message `User password reset successful`.
- Lui demander de le changer lors de sa prochaine connexion.

9.7.5 Suppression d'un utilisateur

9.7.5.1 Introduction

Cette procédure décrit la procédure de suppression d'un utilisateur local.

Note:

Voir la présentation des comptes et des groupes décrites dans la *Présentation des comptes de l'interface web et de leurs gestions*.

9.7.5.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

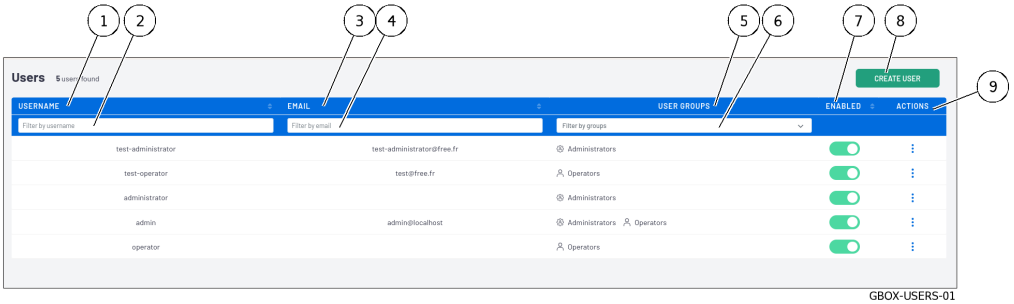
9.7.5.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.5.4 Procédure d'accès à la fenêtre `Users management`

- Dans la barre de navigation, cliquer successivement sur :

- le bouton `Admin`
- le sous menu `GBox`
- la commande `Users management`
  La fenêtre `Users` est affichée.



GBOX-USERS-01

9.7.5.5 Procédure de suppression d'un utilisateur

Danger:

Il est possible de sélectionner son propre compte!
Si cela est volontaire, noter précautionneusement le mot de passe affiché.

- Sélectionner le compte de l'utilisateur.
- Cliquer sur la commande `Remove` de la partie `ACTIONS` (9) de l'utilisateur à supprimer.
  Le message suivant est affiché :

```
Remove user account
Do you want to remove the user account test-operator ?
```

- Cliquer sur le bouton `Confirm`.
  Le système affiche le message `User removed`.
  La liste des comptes est remise à jour.

9.7.6 Visualisation de l'historique des authentifications

9.7.6.1 Introduction

Cette procédure permet de visualiser affiche l'historique de toutes les authentifications sur le GCenter.

Note:

L'interface graphique est décrite dans la *Partie `Authentications history` du sous menu `Accounts`*.

9.7.6.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

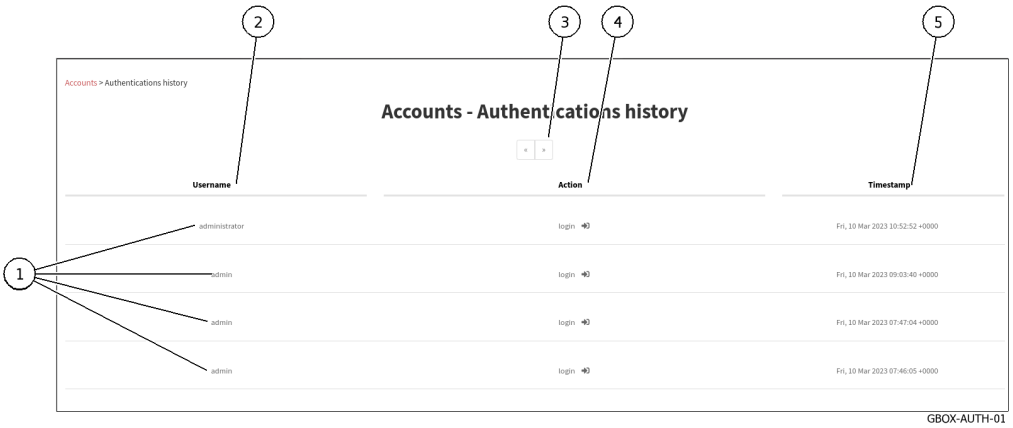
9.7.6.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.6.4 Procédure d'accès à la fenêtre `Users management`

- Dans la barre de navigation, cliquer successivement sur :
- le bouton `Admin`
- le sous menu `GBox`
- la commande `Accounts`
  La fenêtre `Accounts management` est affichée.
- Cliquer sur `Authentications history`.
  La fenêtre `Accounts - Authentications history` est affichée.

9.7.6.5 Procédure



Cette fenêtre affiche les connexions (1) dans l'ordre du plus récent au plus ancien.
Pour chaque connexion, les informations suivantes sont affichées :

- champ (2) `Username` : nom de la personne qui s'est authentifié
- champ (3) `Action` : login ou logout
- champ (4) `timestamp` : date et heure des connexions / déconnexions au format (**jj** , **mm aaaa hh** : **mm** : **ss**)
- Pour changer les pages, utiliser les flèches (4).

9.7.7 Visualisation de l'historique des créations ou suppressions des utilisateurs

9.7.7.1 Introduction

Cette procédure permet de visualiser affiche l'historique de :

- chaque création d'un compte utilisateur
- chaque suppression d'un compte utilisateur

Note:

L'interface graphique est décrite dans la *Partie `Creations/Deletions history` du sous menu `Accounts`*.

9.7.7.2 Prérequis

Utilisateur : membre du groupe **Administrators**

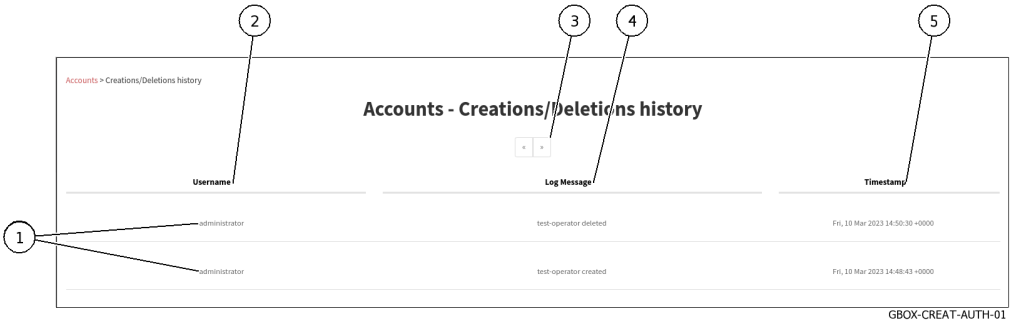
9.7.7.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.7.4 Procédure d'accès à la fenêtre `Creations/Deletions history`

- Dans la barre de navigation, cliquer successivement sur :
- le bouton `Admin`
- le sous menu `Gcenter`
- la commande `Accounts`
  La fenêtre `Accounts` est affichée.
- Cliquer sur la rubrique `Creations/Deletions history`.
  La fenêtre `Creations/Deletions history` est affichée.

9.7.7.5 Procédure



La fenêtre `Creations/Deletions history` affiche historique de toutes les créations ou suppressions des utilisateurs du GCenter.
Cette fenêtre affiche les créations ou suppressions (1) dans l'ordre du plus récent au plus ancien.
Pour chaque connexion, les informations suivantes sont affichées :

- champ `Username` (2) : nom de l'administrateur responsable de l'ajout ou la suppression de l'utilisateur
- champ `Log Message` (4) : comporte plusieurs informations comme le nom de l'utilisateur et son action associée au compte (**created_** ou _deleted_).
- champ `timestamp` (5) : date et heure de la modification au format (**jj** , **mm aaaa hh** : **mm** : **ss**)
- Pour changer les pages, utiliser les flèches (3).

9.7.8 Visualisation de l'historique de toutes les modifications des droits des utilisateurs

9.7.8.1 Introduction

Cette procédure permet de visualiser affiche l'historique de toutes les modifications des droits des utilisateurs.
Ceci se traduit par la modification de l'appartenance au groupe Operators ou Administrators.

Note:

L'interface graphique est décrite dans la *Partie `Permissions history` du sous menu `Accounts`*.

9.7.8.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

9.7.8.3 Opérations préliminaires

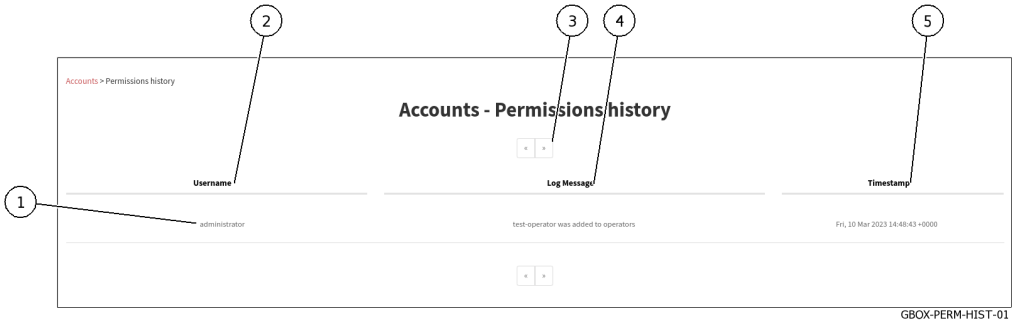
- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.8.4 Procédure d'accès à la fenêtre `Creations/Deletions history`

- Dans la barre de navigation, cliquer successivement sur :
- le bouton `Admin`
- le sous menu `Gcenter`
- la commande `Accounts`
  La fenêtre `Accounts` est affichée.
- Cliquer sur la rubrique `Permissions history`.
  La fenêtre `Permissions history` est affichée.

9.7.8.5 Procédure

La fenêtre `Creations/Deletions history` affiche l'historique de toutes les modifications des droits des utilisateurs.



Cette fenêtre affiche les modifications des droits (1) dans l'ordre du plus récent au plus ancien.
Les flèches (3) permettent de charger la page suivante.
Pour chaque connexion, les informations suivantes sont affichées :

- champ `Username` (2) : le nom de l'administrateur qui a modifié les droits du compte
- champ `Log Message` (4) : le nom du compte dont les droits ont été modifié et la modification faite.
- champ `timestamp` (5) : date et heure de la modification au format (**jj** , **mm aaaa hh** : **mm** : **ss**)
- Pour changer les pages, utiliser les flèches (3).

9.7.9 Création ou suppression d'un token d'accès d'un API

9.7.9.1 Introduction

L'authentification sur l'API de la GBox peut se faire de deux manières :

- en utilisant d'un couple login / mot de passe
- en utilisant d'un token d'api

Les paramètres d'un *token* sont les suivants :

- nom **(requis)** : nom permettant d'identifier le possesseur ou l'utilisation faite du token
- permissions **(requis)** : niveau d'accès du *token* parmi **Operators**, **Administrators** ou **Super Administrator**
- une date d'expiration : permet de désactiver le *token* à la date et l'heure indiquée.
  Si ce champ n'est pas rempli, le *token* n'expire pas.

Cette procédure décrit :

- l'ajout d'un token d'accès d'un API
- la création de ce token d'accès
- la suppression éventuelle d'un token existant

Note:

L'interface graphique est décrite dans la *Partie `API tokens` du sous menu `Accounts`*.

9.7.9.2 Prérequis

- Utilisateur : membre du groupe **Administrators**

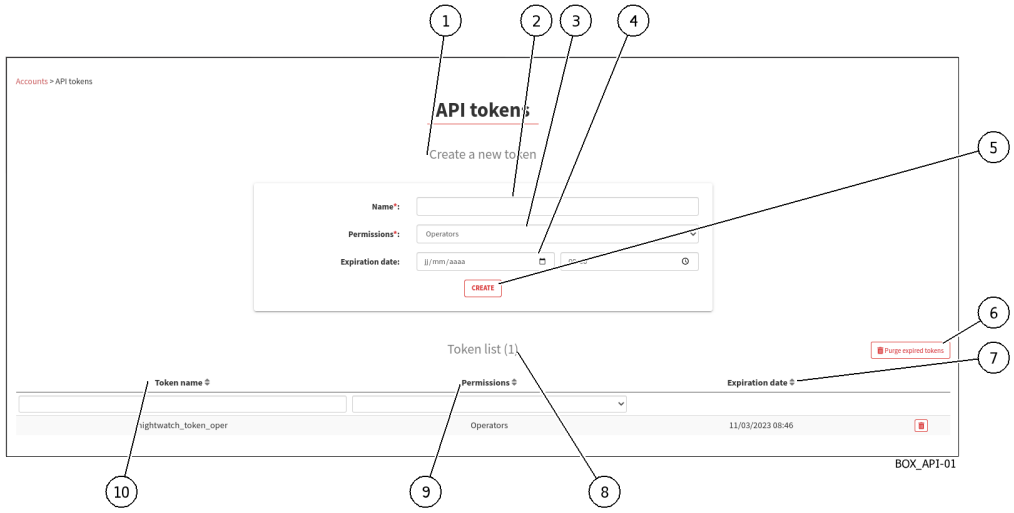
9.7.9.3 Opérations préliminaires

- Se connecter à la GBox via un navigateur (voir la *Connexion à l'interface web via un navigateur internet*).

9.7.9.4 Procédure d'accès à la fenêtre `Permissions history`

- Dans la barre de navigation, cliquer successivement sur :
- le bouton `Admin`
- le sous menu `Gcenter`
- la commande `Accounts`
  La fenêtre `Accounts` est affichée.
- Cliquer sur la rubrique `Api tokens`.
  La fenêtre `Api tokens` est affichée.

9.7.9.5 Procédure de création d'un nouveau token



- Saisir un nom explicite de token dans le champ (2) `Name` de la zone (1) `Create a new token`.
- Sélectionner le compte voulu (et donc les droits) à l'aide du champ (3) `Permissions`.
- Si besoin, sélectionner la date d'expiration en cliquant dans le champ (4) `Expiration date` : utiliser le calendrier affiché.
- Appuyer sur le bouton (5) `Create`.
  Après l'ajout :
  - un message de création du token est affiché
  - le token créé est affiché

```
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.
```

- Utiliser le token affiché.
  La liste de la zone (8) `Token list` est mise à jour.
- Si besoin, supprimer les tokens expirés avec le bouton (6).

9.7.9.6 Procédure pour supprimer un token

- Utiliser , si besoin, les champs `Name` (10) , `Permission` (9), `Expiration` (7) pour filtrer la liste.
- Supprimer un token existant à l'aide du bouton corbeille.
  Une fenêtre de confirmation est affichée avec le message suivant

```
Confirm deletion
Do you confirm the deletion of the API token nightwatch_token_oper ?
```

- Appuyer sur le bouton `Confirm` pour confirmer la suppression.
- Si besoin, supprimer les tokens expirés avec le bouton (6) `Purge expired tokens` ou via l'API */auth/tokens/purge-tokens/*.

> **Note:**
>
> La documentation de l'API de la GBox est disponible via Swagger en cliquant sur le lien présent dans le menu **Administrators** > **GBOX** > **API**.

9.8 Déconnexion de l'interface Web de la GBox

Cette procédure décrit la déconnexion de l'interface Web.

9.8.1 Prérequis

- Utilisateur : tout utilisateur

```

9.8.2 Opérations préliminaires

- Accéder à l'interface Web depuis son poste de travail (*Connexion à l'interface Web via un navigateur internet*).

9.8.3 Procédure

- Dans l'interface Web, cliquer sur le bouton du compte courant (4).
- Sélectionner la commande `Logout`.
  L'interface Web est fermée et l'écran de connexion est affiché.

Chapter 10

Glossaire

API
: L'API (Application Programming Interface) est l'ensemble des endpoints (appelés aussi ressources ou fin d'URL).

DGA
: Les algorithmes de génération de domaine (DGA) sont des algorithmes présents dans diverses familles de logiciels malveillants qui sont utilisés pour générer périodiquement un grand nombre de noms de domaine pouvant être utilisés comme points de rendez-vous avec leurs serveurs de commande et de contrôle .

Engine hash
: Nom des 16 moteurs antivirus de MALCORE

FQDN
: Le FQDN (Fully Qualified Domain Name) correspond au nom hôte.domaine.

GBox
: La GBox est l'équipement qui permet d'analyser automatiquement des fichiers suspicieux provenant du Gcenter et donc nécessitant une analyse approfondie des malwares sans avoir recours à un service externe.

GCap
: Le GCap est la sonde de détection de la solution Trackwatch/Aioniq. Elle récupère le flux réseau du TAP et reconstitue les fichiers qu'elle envoie au GCenter.

GCenter
: Le GCenter est le composant qui administre le GCap et effectue l'analyse des fichiers envoyés par le GCap.

Ggdadetect
: Moteur capable de détecter des noms de domaines ayant été générés par des DGA (Domain Generation Algorithm).

Gmalcore
: Moteur de détection permettant la détection et l'analyse des malwares par une analyse statique et heuristique multi-moteurs

Gnest
: Moteur d'analyse permettant une analyse dynamique en exécutabnt le fichier dans une machine virtuelle (sandbox) et analyse son comportement.

Goasm
: Moteur d'analyse permettant la détection de shellcodes et de powershells malveillants.

Grip
: Moteur permettant une analyse statique et indique des caractéristiques du fichier.

GUM
: Le GUM (Gatewatcher Update Manager) est le service de gestion des mises à jour des bases de données de détection, de l'application des hotfix et des mises à jour système

IDS
: Un système de détection d'intrusion (ou IDS : Intrusion detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte).

LDAP

Le LDAP (Lightweight Directory Access Protocol) est un protocole permettant l'interrogation et la modification des services d'annuaire (Active Directory par exemple)

MTU

La MTU (Maximum Transfert Unit) est la taille maximale d'un paquet pouvant être transmis en une seule fois (sans fragmentation) sur une interface réseau.

OTP

L'OTP (One Time Password) est un mot de passe à usage unique défini sur le GCenter.

setup

Nom du compte destiné à un administrateur système d'accès au menu de configuration

Shellcode

Un shellcode est une chaîne de caractères qui représente un code binaire exécutable. À l'origine destiné à lancer un shell, le mot a évolué pour désigner tout code malveillant qui détourne un programme de son exécution normale.

SIEM

Le SIEM (Security Information and Event Management) est un système centralisé d'événements de sécurité qui offre une visibilité totale sur l'activité d'un réseau et permet ainsi de réagir aux menaces en temps réel.

TAP

Le TAP (Test Access Point) est un dispositif passif qui duplique un flux réseau.

Index

A

C

D

E

F

G

H

I

L

M

O

Q

S

T

U