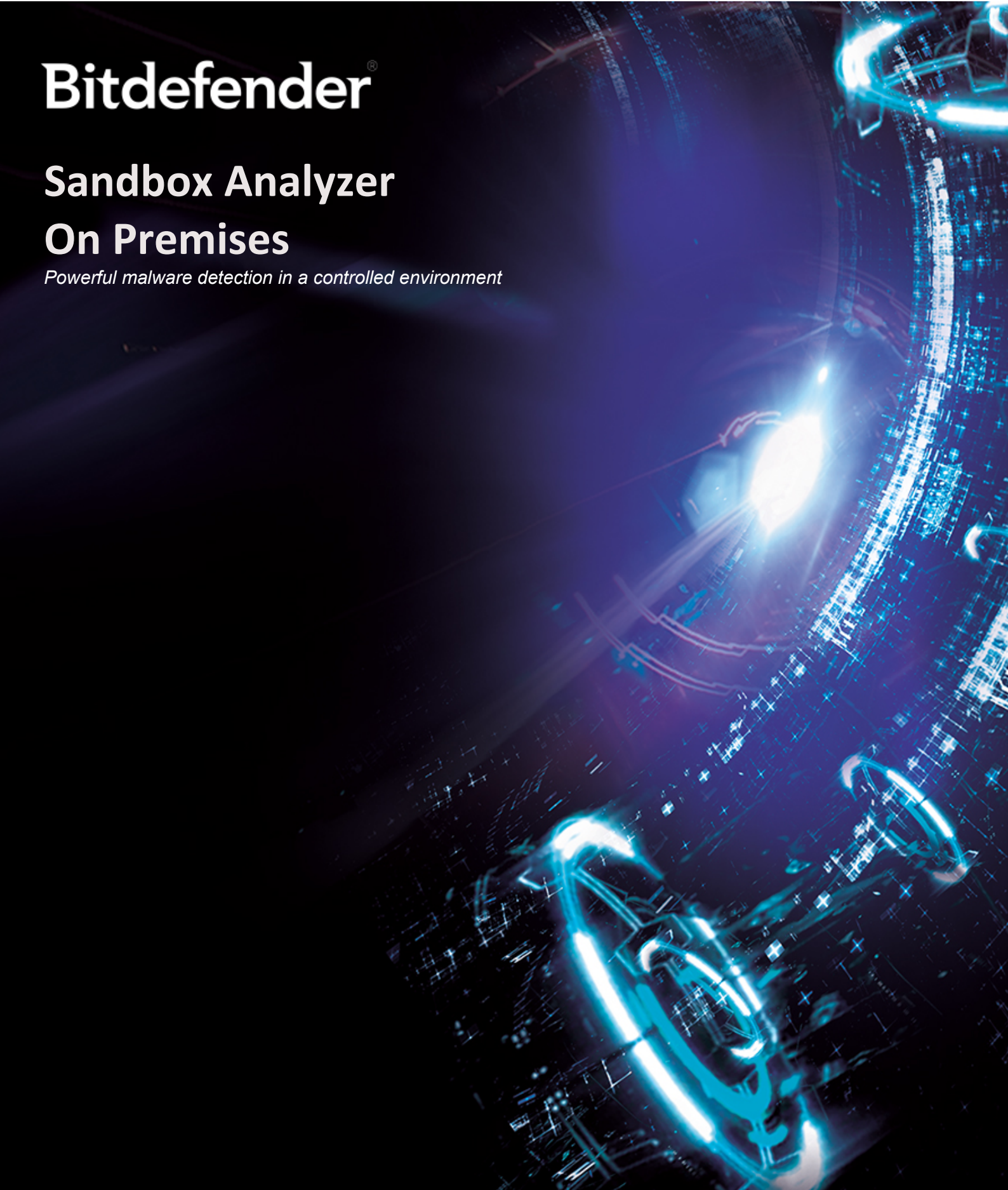
Bitdefender

Sandbox Analyzer On Premises

Powerful malware detection in a controlled environment



EVALUATION GUIDE

Controlled Availability

LEGAL NOTICE

Warning and Disclaimer.

The Bitdefender product and related services and documentation used for evaluation purposes are provided on an “as is” basis, without warranty.

This product is in the Proof of Concept phase and it is believed to contain defects. You are advised to safeguard important data, to use caution and not to rely in any way on the correct functioning or performance of the software and/or accompanying materials. The product should be installed on a lab environment only, Bitdefender not being responsible of any damage to production environments.

Bitdefender does not warrant that the product will meet your requirements. Bitdefender does not guarantee that the software will perform error-free or uninterrupted or that Bitdefender will correct all program errors.

Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This document contains links to third-party websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

To the extent permitted by law, these warranties are exclusive and there are no other express or implied warranties or conditions, including warranties or conditions of merchantability and fitness for a particular purpose.

Trademarks.

Trademark names may appear in this document. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Bitdefender

Table of Contents

1. Technology Description

Proper analysis of modern attacks needs powerful detection technologies. Having all the power in an endpoint is challenging, as the endpoint has primarily to do actual dedicated work. Furthermore, the best analysis requires a controlled environment to figure out all issues the attacks have caused.

This makes Sandbox Analyzer a powerful technology for Bitdefender to fight against the new wave of malware. Sandbox Analyzer also provides a reliable tool for companies to augment their protection and detection against targeted attacks and malware infiltration.

While Bitdefender initially designed Sandbox Analyzer detection of Advanced Persistent Threats (APT), this product currently provides detection on any forms of malware and it can uncover targeted attacks.

The end-user has total control over Sandbox Analyzer with the on-premises packaging, which reduces the total cost of ownership (TCO) for the business and provides a scalable architecture that allows multiple-instance deploying.

1.1. Overview

The Sandbox Analyzer is a standalone advanced malware analysis solution designed to analyze suspicious content. Detonation capabilities include file analysis and URL analysis, covering various file formats that are commonly used in advanced attacks.

Sandbox Analyzer is capturing suspicious data through different sensors deployed in the enterprise network.

Solution administrators can also manually submit samples or URLs for analysis by using Manual Submission.

Benefits

- A single virtual appliance (OVA format) allowing on-premises deployment.
- Scalable architecture supporting installation of multiple Sandbox Analyzer instances and centralized management from the GravityZone console.
- Out-of-the-box integration with a variety of Bitdefender sensors that automatically feed content for detonation in Sandbox Analyzer.

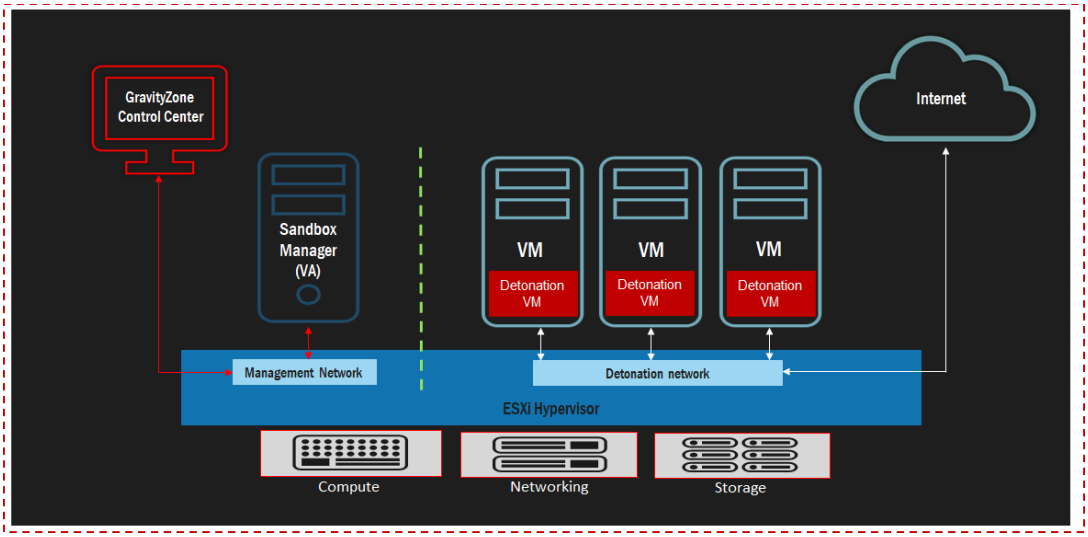
Features

- Fast and easy deployment using a CLI-based graphical installer.
- Centralized console for management, reporting and configuration that takes advantage of the existing GravityZone Control Center.
- Unified reporting interface for viewing detonation reports with filtering capabilities.
- Individual detonation reports using rich HTML interface containing aggregated data about sample behavior.
- Custom image support (GravityZone administrator provides the virtual machine images that are used for content detonation in the sandbox environment). Supported operating systems: Windows 7 and Windows 10 64-bit versions.
- Manual detonation capability file and URL detonation with flexible runtime configurations such as detonation length, command-line arguments and internet connectivity.
- Automatic detonation of malware samples captured on endpoints and reported to the Centralized Quarantine.
- Configurable settings for manual detonations.
- Content detonation from network traffic capture files (.pcap files).
- API support for programmatic interaction with the sandbox environment.

1.2. Sandbox Analyzer Components

Bitdefender Sandbox Analyzer (SBA) comes as a virtual appliance that you can deploy on VMware ESXi. A Sandbox Analyzer instance contains the following components:

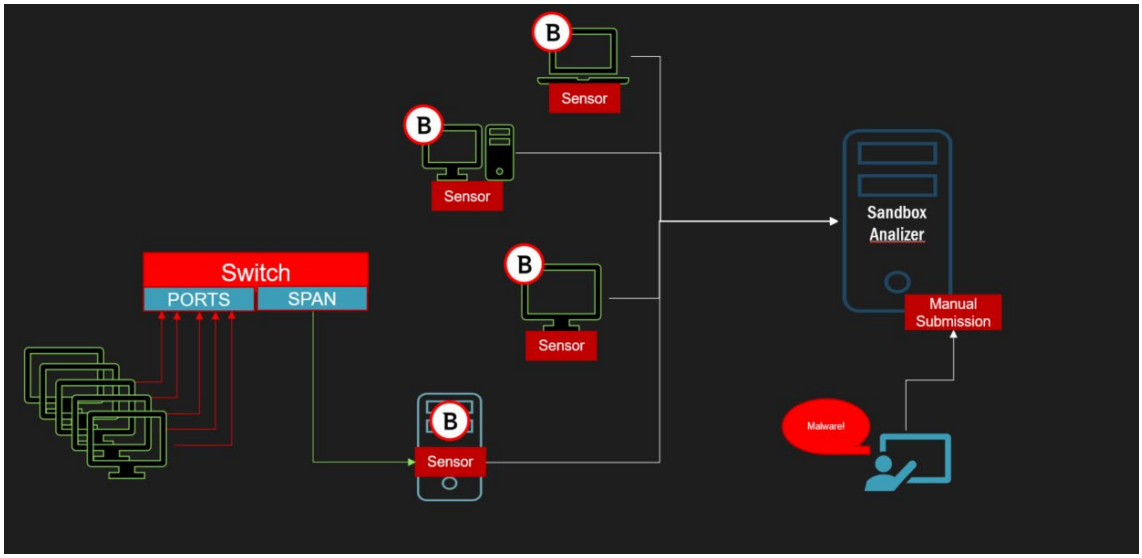
- **Sandbox Manager –** the sandbox orchestrator. This component connects to the ESXi hypervisor via APIs and uses the hardware resources to build and operate the malware analysis environment.
- **Detonation VMs –** virtual machines leveraged by Sandbox Analyzer to detonate suspicious files and analyze behavior. Sandbox Manager is orchestrating the detonation VMs based on a customer provided VM image.



Sandbox Analyzer Sensors

Sandbox Analyzer operates sensors for automatic suspicious sample submission. They include:

- **Network Security Virtual Appliance** (NSVA) - the network sensor, which is a virtual appliance deployable in a virtualized environment (ESXi). It extracts and sends content for detonation to a Sandbox Analyzer.
- **Bitdefender Endpoint Security Tools** (BEST) - the endpoint sensor, which leverages advanced machine learning and neural networks algorithms to determine suspicious content that Sandbox Analyzer needs to analyze.



1.3. Supported File Types

In order for Sandbox Analyzer to detonate a file, two conditions are mandatory:

- The file type is part of supported file types (see the list below).
- The image against the file is detonated comes preinstalled with the application that will open the particular file type. For example, Microsoft Office must be preinstalled for a .doc file sent to Sandbox Analyzer.

Extension	File type
swf	Flash SWF [document]
xls	MS Excel [document]
ppt	MS PowerPoint [document]
doc	MS Word [document]
dot	MS Word [document]
pdf	PDF [document]
rtf	RTF [document]
bat	Batch [script]
cmd	Batch [script]
ws	Windows Script File [script]
wsf	Windows Script File [script]
php	PHP [script]
py	Python [script]
reg	Registry [script]
exe	PE [executable]
dll	PE [executable]
url	URL [binary]
html	HTML [document]
js	JS [script]
vb	VBS [script]
vbs	VBS [script]
pif	PIF [executable]
pyc	Python 2.7 Bytecode [binary]
pyo	Python Optimized Code [binary]

Extension	File type
jse	Generic [binary]
wsc	Generic [binary]
wsh	Generic [binary]
psc1	Generic [binary]
scf	Generic [binary]
lnk	LNK [binary]
docm	MS WordX [document]
docx	MS WordX [document]
dotm	MS WordX [document]
dotx	MS WordX [document]
potm	MS PowerPointX [document]
potx	MS PowerPointX [document]
ppam	MS PowerPointX [document]
ppax	MS PowerPointX [document]
pps	MS PowerPointX [document]
ppsm	MS PowerPointX [document]
ppsx	MS PowerPointX [document]
pptm	MS PowerPointX [document]
pptx	MS PowerPointX [document]
sldm	MS PowerPointX [document]
sldx	MS PowerPointX [document]
xlam	MS ExcelX [document]
xlax	MS ExcelX [document]
xlm	MS ExcelX [document]

Extension	File type
xlsx	MS ExcelX [document]
xltm	MS ExcelX [document]
xltx	MS ExcelX [document]
7z	7z [archive]
bz	BZip [archive]
bz2	BZip2 [archive]
tgz	GZip [archive]
msi	MSI [archive]
rar	RAR [archive]
rev	RAR [archive]
zip	ZIP [archive]
z	Unix Z [archive]
arj	ARJ [archive]
iso	ISO [binary]
lha	LHA [archive]
lhz	LHA [archive]
uu	UUEncoded [binary]
uue	UUEncoded [binary]
xxe	XXEncoded [binary]
lzma	LZMA Compressed Archive [archive]
ace	ACE [archive]
r00	RAR [archive]
eml	Generic [email]

jar	JAR [archive]
com	PE [executable]
chm	Generic [binary]
xlm	Generic [binary]
application	Generic [binary]
gadget	Generic [binary]
msp	Generic [binary]
scr	Generic [binary]
hta	Generic [binary]
cpl	Generic [binary]

xlsm	MS ExcelX [document]

tnef	TNEF [binary]
msc	Generic [binary]
vbe	Generic [binary]

2. The Evaluation Program

This section describes the technical preview program timeline, requirements for participation, quick-start instructions and guidelines for successfully deploying and testing the Sandbox Analyzer software.

2.1. Timeline

The Bitdefender Sandbox Analyzer technical preview program starts in July 2019 and ends in November 2019.

In this timeframe, select Bitdefender customers are invited to evaluate the technical preview release and provide their feedback, including defect discovery and new feature requests, to the Bitdefender product management team.

2.2. Environment Requirements

The Sandbox Analyzer Technical Preview program has a few hardware and software prerequisites. The program assumes the evaluator is willing to dedicate these resources towards building a test environment.

For testing Sandbox Analyzer, evaluators are advised to build a test environment that is network isolated from the rest of their production environments.

In terms of requirements, the following are needed:

- VMware ESXi server running version 6.5 or 6.7
- Minimum 1 TB storage
- 1 dedicated NIC

We recommend 2 physical NICs with the following mapping:

  - 1 NIC will be used for the management interface
  - 1 NIC will be used the detonation network

Note

Sandbox Analyzer is compatible with the trial version of VMware ESXi. You can obtain the trial version of VMware software by registering an account on VMware's website. During the download process, make sure you select VMware ESXi.

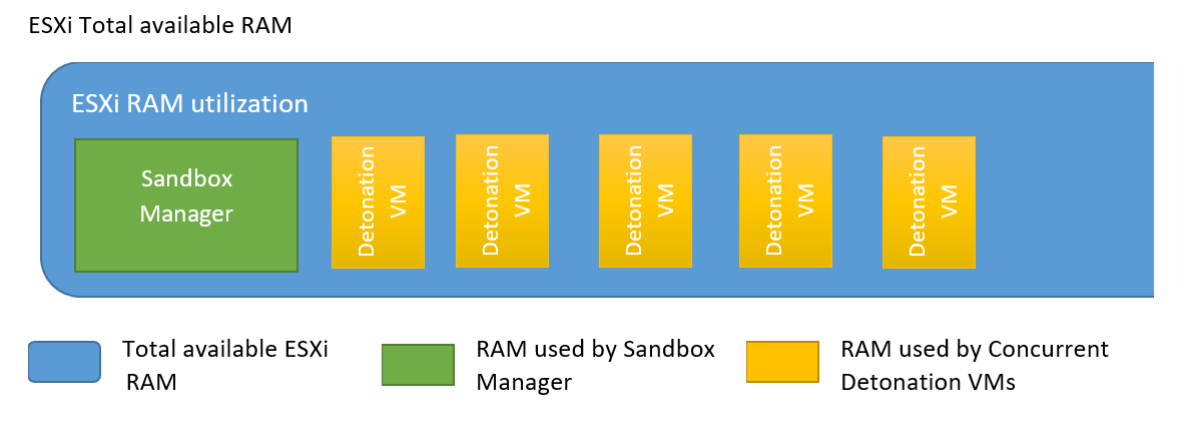
However, given the time limitations on the trial version, production deployments must run on a licensed version of VMware ESXi server.

Sandbox Analyzer Hardware Sizing

The packaging of Sandbox Analyzer in a virtual appliance allows for a deployment, which offers virtually unlimited scalability as long as the underlying hardware resources are available.

You can get a better overview of how the hardware resources are utilized in the graphic below. Please note that although the graphic mentions RAM memory, the same concept applies to CPU allocation.

- The total available RAM will be shared between the dedicated virtual machine used for the orchestration of the concurrent detonation VMs (Sandbox Manager) and the detonation VMs.



In order to determine the resource allocation for the Sandbox Manager and detonations VMs, consult the hardware allocation sizing guideline below. The amount of resources will be determined on the desired number of parallel detonations chosen.

VMware Hardware Allocation Sizing Guidelines

In order to estimate the amount of hardware resources, the following table provides a high-level estimation regarding the amount of resources that should be allocated.

In the Bitdefender testing labs, the barebone server used during the tests had the following specifications:

Supermicro SYS-6028R-WTR-N

2 x Intel® Xeon™ 20-Core E5-2698V4 2.2GHz, 50MB Cache

12 x 32GB DDR4 2400MHz Registered ECC RDIMM

To give a better understanding of the resources required, several scenarios were constructed involving 5, 10, 20 and 40 concurrent detonation VMs.

The **Total** column indicates the amount of resources needed for ESXi server as a whole, while the **Sandbox Manager** column indicates how many will be reserved for the Sandbox Manager component only (and they will be allocated when deploying the virtual appliance).

Note

The peak notation indicates a worst-case scenario, involving malware, which required intensive CPU processing, and memory utilization.

	Sandbox Manager				Total			
No. of parallel detonations	Non-peak		Peak		Non-peak		Peak	
	vCPU	RAM (GB)	vCPU	RAM(GB)	vCPU	RAM(GB)	vCPU	RAM(GB)
5	6	20	10	32	24	36	34	48
10	12	26	16	38	42	56	50	68
20	20	48	30	60	56	108	80	120
40	26	80	28	100	76	200	80	220

Note

Number of vCPUs are calculated based on the number of hardware CPUs, CPU cores and whether different technologies such as Intel Hyper-Threading are present or not.

On average each VM used for detonation consumes 2vCPU, 3 GB RAM and 50GB of disk storage.

Network Sensor Virtual Appliance (NSVA)

During the technology preview program, NSVA is deployed in ESXi environments and configured in tap mode to extract malicious content from network connections. The minimum hardware requirements are:

- 4 vCPUs
- 4 GB of RAM
- 1 TB disk
- 2 dedicated NICs

Software Requirements

The Sandbox Analyzer evaluation environment should contain the following software components:

- GravityZone On-premises management server deployed and licensed with an Elite license key and Sandbox Analyzer key. Sandbox Analyzer is managed through GravityZone.
  - You can download GravityZone On-premises Virtual Appliance (VA) from **here**.
  - The Bitdefender representative will provide you with evaluation keys during the evaluation on-boarding process.
- One Windows 7 x64 or Windows 10 x64 OS image in OVA, OVF or VMDK format. This image will be uploaded and used by Sandbox Analyzer for building detonation VMs.
- One test VM running a Windows Workstation operating system (7, 8.1 or 10). This system will host the Bitdefender Endpoint Security Tools (BEST) with the Sandbox Analyzer sensor enabled.
  - This system can run the same image as the detonation VM template.

Network Communication Requirements

The following ports need to be open for communication:

Component	Direction	Port	Source/Destination	Description
GravityZone On-premises (VA)	Inbound	**443**	Internal Network	Access to the Control Center web console
		8443	Internal Network	Managed systems traffic
	Outbound	**443**	my.bitdefender.com	My Bitdefender account integration
			lv2.bitdefender.com	License key validation
		80	Download.bitdefender.com Upgrade.bitdefender.com	Software updates
ESXi console	Inbound	**22**	Internal network	Access ESXi console by Sandbox Manager
Sandbox Analyzer (VA)	Inbound	**443**	Any	Submitting content from external sensors
	Outbound	**8443**	Communication server	Sandbox configuration, Management traffic
BEST Client Sensor	Inbound	**N/A**	N/A	
	Outbound	**443**	Sandbox Analyzer VA	Sample Submission to Sandbox Analyzer
		8443	GravityZone VA	Management Traffic
Network Sensor (VA) Management NIC	Inbound	**N/A**	N/A	
	Outbound	**443**	Sandbox Analyzer VA	Sample Submission to Sandbox Analyzer
		8443	GravityZone VA	Management traffic
Network Sensor (VA) Capture NIC	Inbound / Outbound	**Any**	Any	Plugged in SPAN port to mirror traffic

Network Diagram Architecture

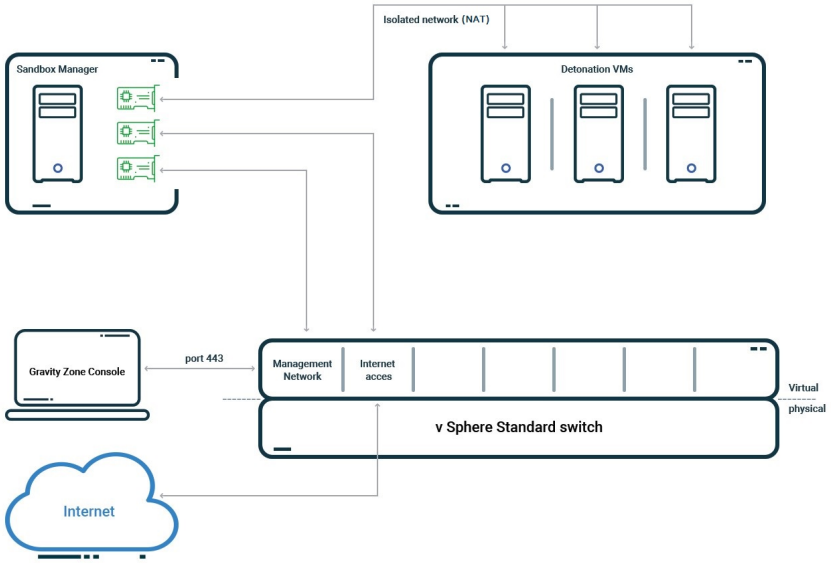
The diagram below depicts the Sandbox Analyzer network architecture.

The Sandbox Manager has three internal virtual NICs, which are allocated as follows:

- 1 NIC will be used for communication with the management console (GravityZone)
- 1 NIC will be used for Internet connectivity
- 1 NIC will be used for internal communication with the detonation machines.

Note

To allow communication with the Sandbox Analyzer, both the ESXi management network and the Sandbox Manager management network NIC must be in the same network.



Sandbox Analyzer internal network diagram

3. Preparing the Test Environment

This section provides a step-by-step installation guide for Sandbox Analyzer and respective sensors. Before proceeding further, make sure that:

- VMware ESXi is installed and configured on hardware dedicated to building this test environment. Additional details are available in VMware vSphere Installation and Setup documentation (section 2 covers step-by-step deployment of ESXi).
- Bitdefender GravityZone On-premises virtual appliance is deployed and configured. Step-by-step details are available in the GravityZone Installation Guide.
- One test VM running Windows workstation OS has been deployed.

3.1. License GravityZone for Sandbox Analyzer

The Sandbox Analyzer license key controls the number of maximum concurrent detonations that can take place. Since each detonation requires an instance of a running virtual machine, the number of concurrent detonations reflect in the number of virtual machines created.

To add the Sandbox Analyzer license key:

1. Log in to GravityZone Control Center.
2. From the left-side menu, go to the **License** page.
3. Select the **Add** button from the top left corner of the page to enter the key.
4. Click **Save** to make the changes.

3.2. Considerations before Installation

Sandbox Analyzer is packaged as an OVA package and certified to run only on the VMWare ESXi hypervisor. The following conditions must be met regarding the ESXi server:

- ESXi minimum version is 6.5
- VMFS data store version is 5.
- SSH is enabled in the Startup policy with “Start and Stop with host” configuration.
- NTP service is active and configured.

3.3. Deploying Sandbox Analyzer Virtual Appliance

To access the OVA package please follow the steps below:

1. Log in to the GravityZone Control Center.
2. Go to the **Network** > **Packages** page.
3. Select **Sandbox Analyzer** check box from table.
4. Click the **Download** button at the upper-left side of the page. Select the **Security Appliance (ESXi standalone)** option.
5. Use your virtualization management tool (for example, vSphere Client) to import the downloaded image into your virtual environment.

Note

When deploying the OVA file, map the networks as follows:

- **Bitdefender Network** – this is the network where other Bitdefender components reside. This is the NIC which is in direct communication with the GravityZone installation.
- **Private Detonation Network** – this network will be used by the Sandbox for internal communication. This network must be isolated from any other network segments.
- **Internet Access Network** – Sandbox Analyzer will use this network for obtaining the latest updates.

3.4. Configuring Sandbox Analyzer

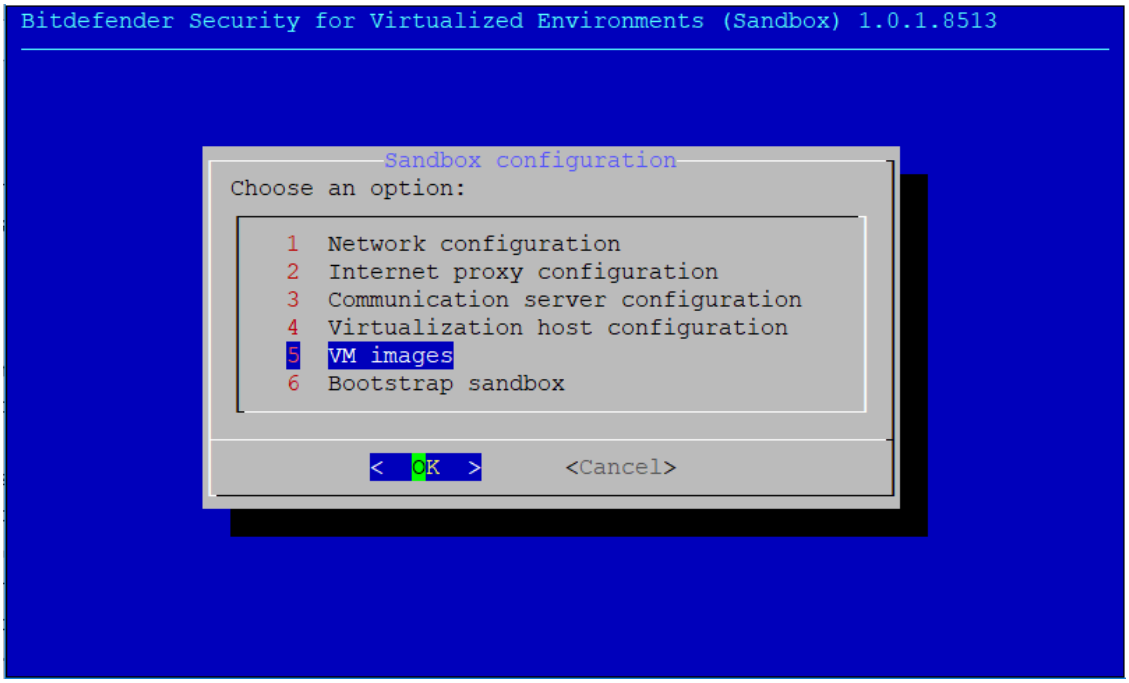
Once you have successfully deployed the virtual appliance into your ESXi environment, connect to its command-line interface (CLI).

1. Console authentication.

   When prompted for credentials, enter **root** for username and **sve** for password.

2. Configuration menu.

   Launch the installer by running the following command:
   `/opt/bitdefender/bin/sandbox-setup`



3. Network configuration.

   Access the **Network configuration** menu to configure the management NIC. Sandbox Analyzer will use this network interface in communication with GravityZone.

   The IP address can be manually specified or automatically through DHCP.

4. Communication server configuration.

   The communication between GravityZone and Sandbox Analyzer is performed through an embedded component inside GravityZone on-premises named Communication server.

   Using the **Communication server configuration** menu option, specify either the IP address of a GravityZone On-premises installation or a Communication server role.

> **Note**
>
> As soon as an IP address/hostname is specified, and configuration is saved, the Sandbox Analyzer instance will become visible in GravityZone Control Center, in the **Sandbox Analyzer** > **Infrastructure** page.

5. Virtualized Host Configuration.

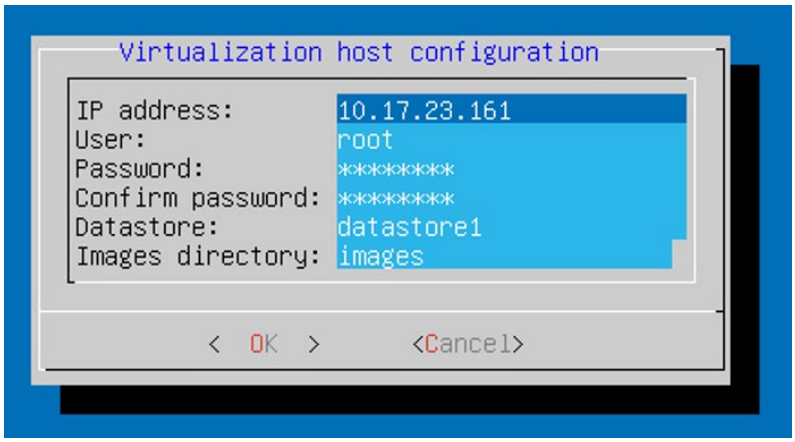
   Sandbox Analyzer is using an ESXi server to provision the malware analysis infrastructure. Using Virtualized Host Configuration, the administrator connects Sandbox Analyzer VA with the ESXi host by providing the following information:

   - The ESXi server IP address
   - Root credentials for accessing the ESXi host

6. Datastore dedicated to Sandbox Analyzer.

   Administrator should type in the datastore name as displayed by ESXi.

   - You need a folder name on the datastore for storing the custom virtual machine images. If this folder does not exist, you must create it on the datastore before proceeding to save the configurations.



7. Bootstrap sandbox

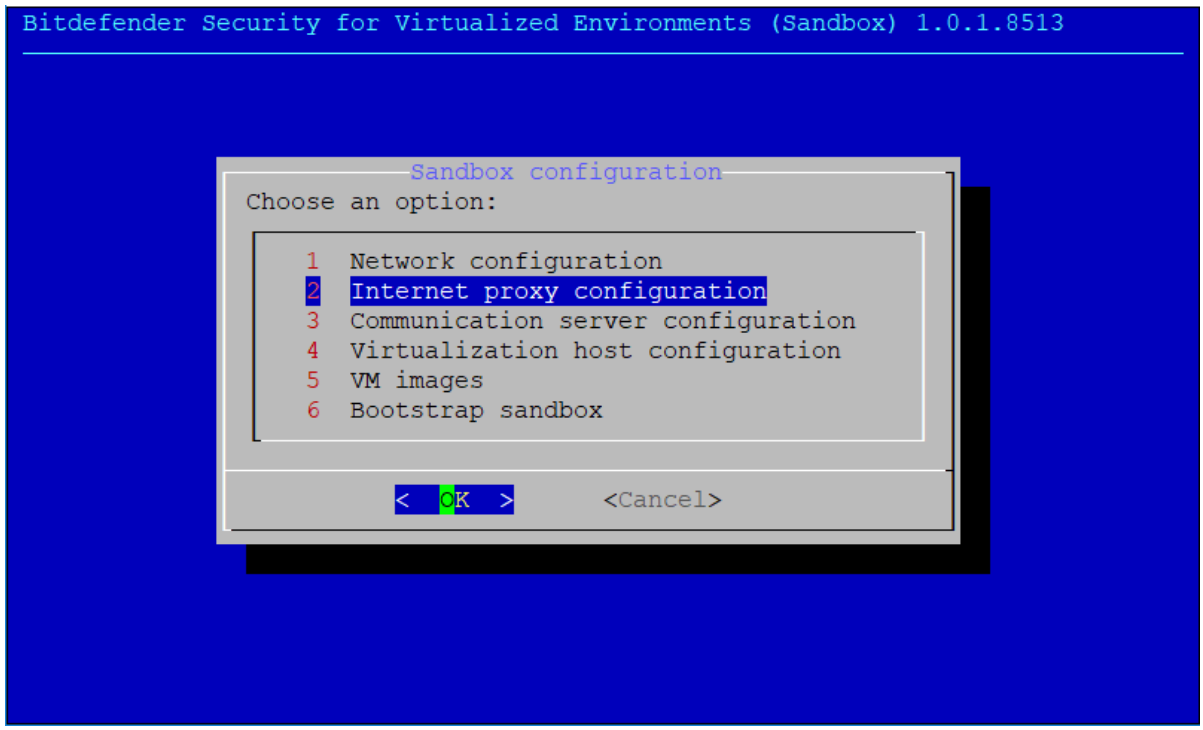
Once you have added the Sandbox Analyzer configuration details, proceed with the installation by selecting the **Bootstrap sandbox** menu option. The status of the installation will be reflected in GravityZone Control Center, under the **Sandbox Analyzer** > **Infrastructure** page.

> **Note**
>
> For a smooth installation process, you need to update your GravityZone solution to version 6.7.1-1 or later.

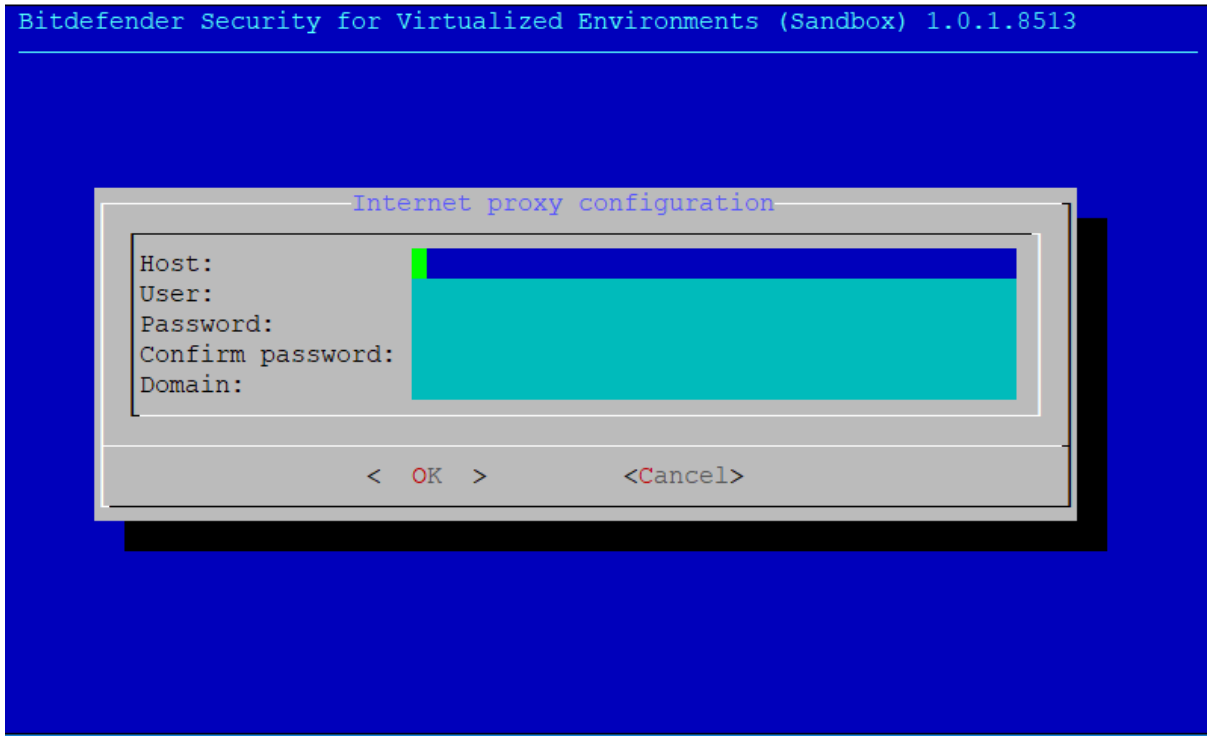
Configuring the Proxy

In order for installation to succeed, Sandbox Analyzer requires an Internet connection. In case a proxy is needed for Internet connectivity, the Sandbox can be configured to use one. Follow the steps below:

1. From the main manu, select **Internet proxy configuration**.



2. Provide the necessary information:
   - **Host** – IP or FQDN of the proxy server, with <IP>:<port> or <FQDN>:<port> format.
   - **User and password** - you need to type in the password twice.
   - **Domain** – the Active Directory domain, if the case.



VM Images for Sandbox Analyzer

Sandbox Analyzer On-premises has support for custom virtual machine (VM) images. This allows for sample detonation in a runtime environment that mimics a realistic production environment.

Guidelines for Creating VM Images

These are the prerequisites for building a VM image that Sandbox Analyzer will use for sample detonation:

- The VM image must be available in a VMware compatible format. Sandbox Analyzer will use the VM disk file format VMDK.

  Note

  The VMDK version supported is 5.

- The VM must be built using a supported operating system:
  - Windows 10 64-bit (any patch level).
  - Windows 7 64-bit (any patch level).
- The VM must be built using a single disk. Multiple disks are not supported.
- The operating system must be installed on the second partition in the partition table and mounted at drive letter C: (default Windows install configurations).
- Local system “Administrator” account must be enabled and have an empty password string (password disable).
- Before exporting the VM image, the administrator must correctly license the operating system and all installed software in the VM image.

Custom Image Software

Sandbox Analyzer supports for detonation a wide range of file formats and types (see the full list in the Supported File Types section, at the beginning of this document).

For conclusive reports, make sure you have installed in the custom image the software that can open a particular file type you want to detonate. The list below specifies the supported file types and the associated software that can open them.

File extension	Application (s)
xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx	Microsoft Office suite
swf	Adobe Flash Player
pdf	Adobe Acrobat Reader
bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif	Windows default
7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue	7zip or Winzip or WinRAR

html, url	Google Chrome, Internet Explorer
py, pyc, pyp	Python
eml	Mozilla Thunderbird or Microsoft Outlook

Note

In terms of application versions or patch level, there are no constraints. Additionally, there are no constraints for enabling or disabling software updates for the image operating system, neither for the installed applications.

However, for the best performance it is recommended to manually disable software updates (operating system and 3rd party applications) in the images being used for detonation.

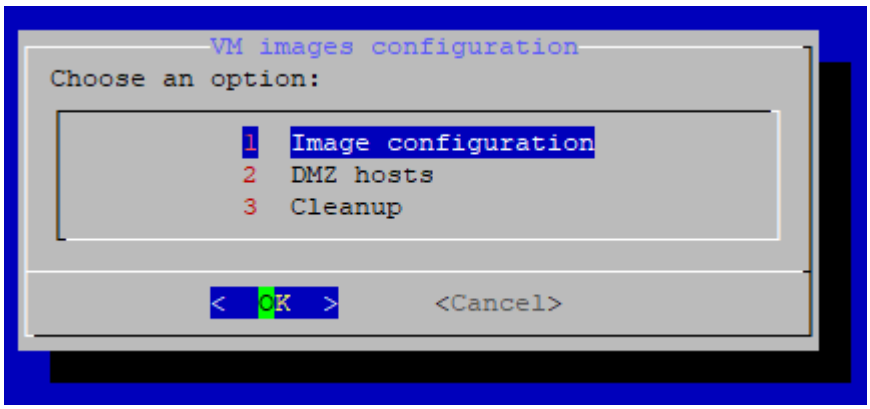
Adding New VM Image

GravityZone administrators can add new VM images to Sandbox Analyzer. Administrators must copy the desired VM image VMDK file in the **Images** directory specified in the **Virtualized Host Configuration** menu.

Note

The folder specified under **Images** configuration item is periodically scanned and new entries are reported to GravityZone. These entries are visible in the GravityZone web interface, under the **Sandbox Analyzer** > **Infrastructure > Image Management** tab.

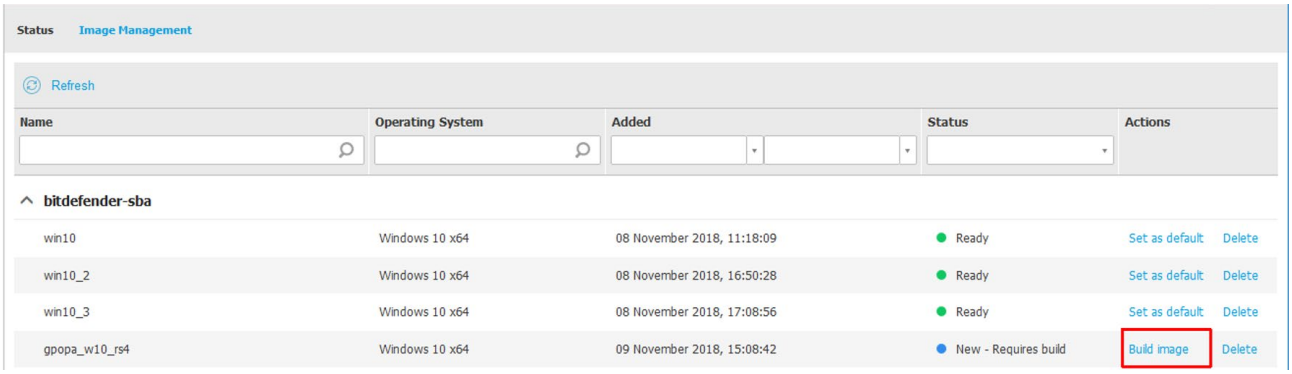
From the **Image Configuration** option specify for each added image:



- Image name (as it will be reported in GravityZone)
- Operating system

Building VM Images

Once all the configuration is done in the CLI console, switch over to GravityZone web interface to the **Sandbox Analyzer** > **Infrastructure**, **Image Management** tab. For each image listed, click the **Build image** option to create an image that will be used as detonation environment.



Note

Building an image typically requires between 15 and 30 minutes depending on its size.

Configuring the Default VM Image

A Sandbox Analyzer instance can have multiple images installed and configured.

In case of automatic submissions, Sandbox Analyzer will use by default the first built image to detonate samples.

To change this behavior and specify a particular image for automatic submissions, you can a default image for each deployed Sandbox Analyzer instance. To do so, click the **Set as default** option corresponding to a specific VM in the images table.

Note

The **Set as default** option is available only for images with the **Ready** status.

Specifying DMZ Servers

During the image building process, a virtual infrastructure will be created to facilitate communication between the Sandbox Manager and the virtual machines. From the network perspective, this translates into an isolated network environment that will contain all the potential communication that a detonated sample might create.

The **DMZ servers** menu allows to whitelist hostnames that 3rd party services and components embedded in the virtual machines require to communicate with, in order to function properly.

An example for this situation would be the KMS licensing servers used by Windows licensing, if a Volume license is applied on the supplied virtual machines.

Anti-fingerprinting Techniques

By default, during the image build process, Sandbox Analyzer will enable various anti-fingerprinting techniques. Certain types of malware are capable to determine whether they are running themselves in a sandbox environment and, if so, they will not activate their malicious routines.

The purpose of the anti-fingerprinting techniques is to simulate various conditions with the purpose of mimicking a real world environment. Due to a virtual eliminated combination of deployed software and environment configuration, a combination that cannot be foreseen in advance or controlled, it is possible that certain techniques will not be compatible with the software installed in the golden image. You can recognize such rare situations by the following symptoms:

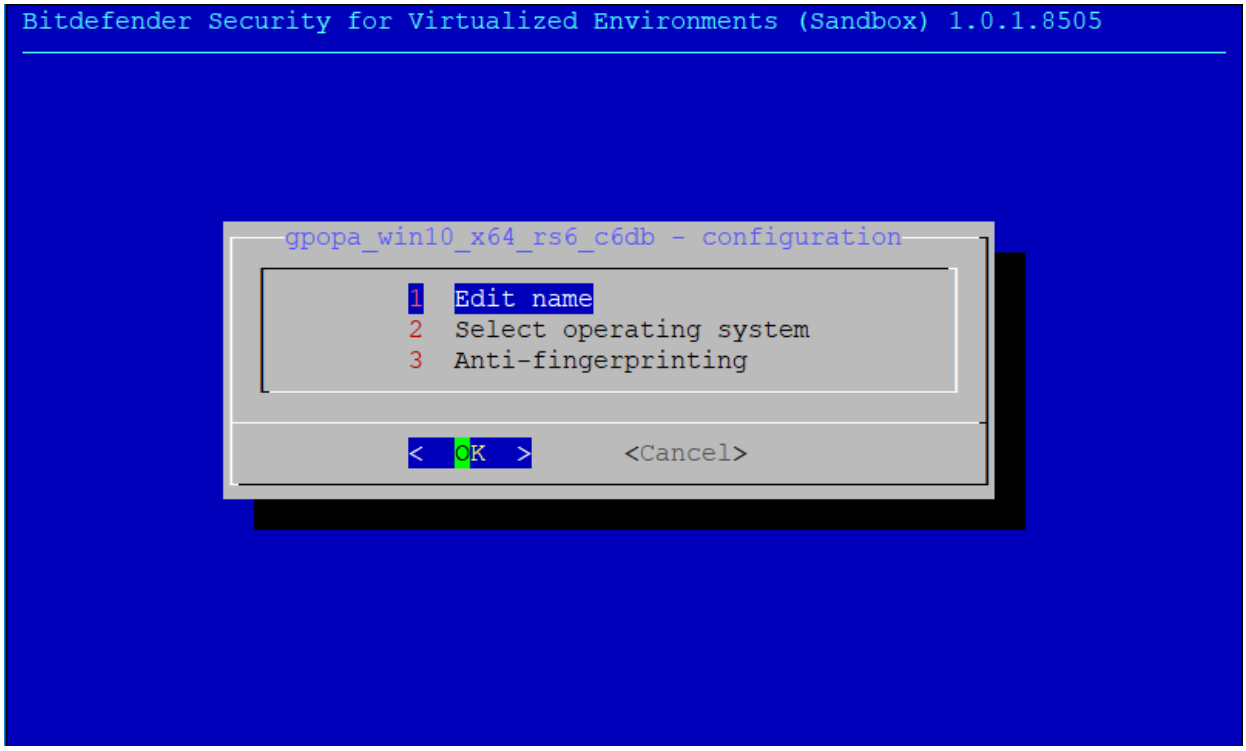
- Errors during the image build process.
- Errors when trying to run the software inside the image.
- Failure messages returned when detonating samples.
- Licensed software no longer working due to invalid license keys.

While constant effort is being put into addressing such issues, a quick remedy to such rare occurrences consists in rebuilding the image with the anti-fingerprinting techniques disabled. To do so, follow the steps below:

1. Log-on to Gravity Zone console and delete the image.
2. Log-in to the Sandbox Analyzer appliance and launch the Sandbox Analyzer installer:

   ```
   /opt/bitdefender/bin/nsva-setup
   ```

3. Go to **VM Images > Image Configuration**.
4. Select the image that is causing problems.
5. Go to **Anti-fingerprinting** option.

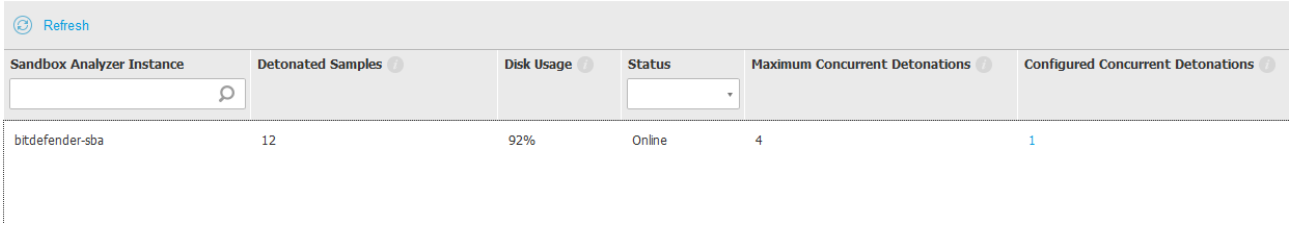


6. Deselect the checkbox to disable anti-fingerprinting techniques.

Sandbox Analyzer Configuration and Validation

Check Deployment Status

Once the Sandbox Analyzer installation is complete, navigate to the **Sandbox Analyzer** > **Infrastructure** section and check the status. If the deployment operations are completed correctly, the Sandbox Analyzer instance is displaying the **Online** status as shown below:



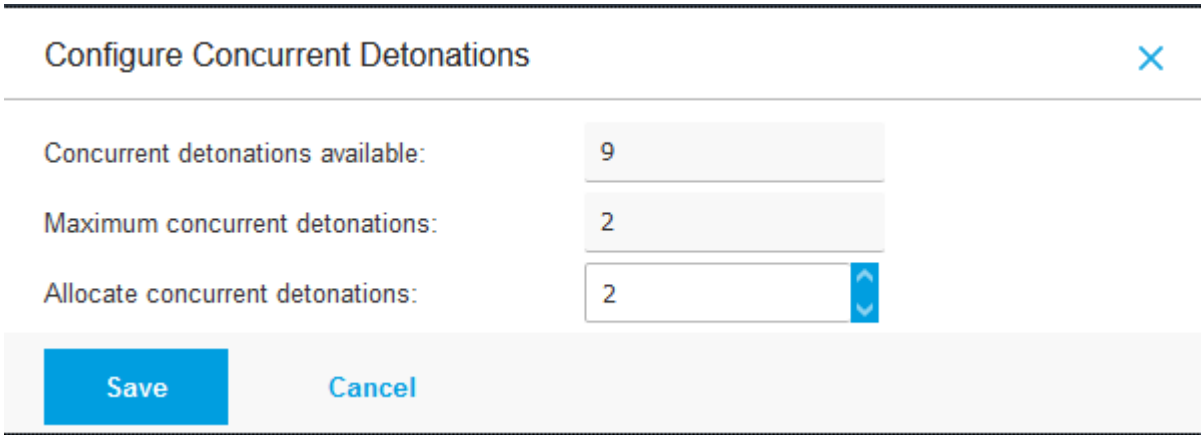
Configure Detonation Slots

Sandbox Analyzer calculates the maximum number of concurrent detonations through a series of automatic benchmarks executed on the dedicated hardware. The **Maximum Concurrent Detonations** column from the **Infrastructure** table displays the estimated number of concurrent detonations**.**

The number of the detonation VMs that you can power on concurrently, on each instance of Sandbox Analyzer, is configurable. However, the number of concurrent detonations depend on the available license slots and how the administrator decides to distribute the slots across multiple instances of Sandbox Analyzer.

To specify the number of samples that Sandbox Analyzer can concurrently detonate:

1. Click the number in the **Configured Concurrent Detonations** column.
2. Enter a number in the **Allocate concurrent detonations** text field of the popup window.
3. Click the **Save** button.



3.5. Endpoint Sandbox Sensor Deployment

Installation

1. Go to **Network > Packages** and create a Bitdefender Security Tools installation package.
2. Choose the client installation method that best suits your needs:
   - Use the **Downloader for Windows** from the **Network** > **Packages** page and install it manually.
   - Deploy the client via a Bitdefender Security Tools Relay previously installed on a station in your **network**, which automatically performs a network discovery. As soon as all computers existing in the network are visible in Control Center, proceed as follows:
     a. Select the endpoints that you want (chose a Windows endpoint) in the **Network** page and choose **Install** from the **Tasks** menu.
     b. In the **Connection** tab of the installation wizard, select the Bitdefender Endpoint Security Tools Relay role.
   - If you have an Active Directory integration:
     - Start the deployment in your network by going to the **Network** page and sending the **Install** task to the selected targets.
     - In the installation wizard, choose the package role that you would like to install on the selected target.

Check if the installed clients are properly displayed in the **Network** page. You can see your endpoints using the following views:

- The **Network** page**:**
  - You should see Active Directory physical machines in the **Active Directory** container.
  - You should see non-Active Directory physical endpoints in the **Custom Groups** container.

- The **Computer Details** window:

1. In the **Network** page, click the endpoint name that you are interested in.
2. You can view the client installation and configuration details for each managed computer in its details page. Verify that the information is correct.

Configuration

You can configure the endpoint sensor to automatically send suspicious content to a Sandbox Analyzer instance.

To do so, create a security policy and apply it to a list of endpoints from your Network inventory:

1. In GravityZone Control Center, go to the **Policies** page**.**
2. Click the **Add** button to create a new policy.
3. Go to the **Sandbox Analyzer > Endpoint sensor** page.
4. Select the **Automatic sample submission from managed endpoints** check box.
5. Enter a hostname representing the Sandbox Analyzer instance used for sample submission.

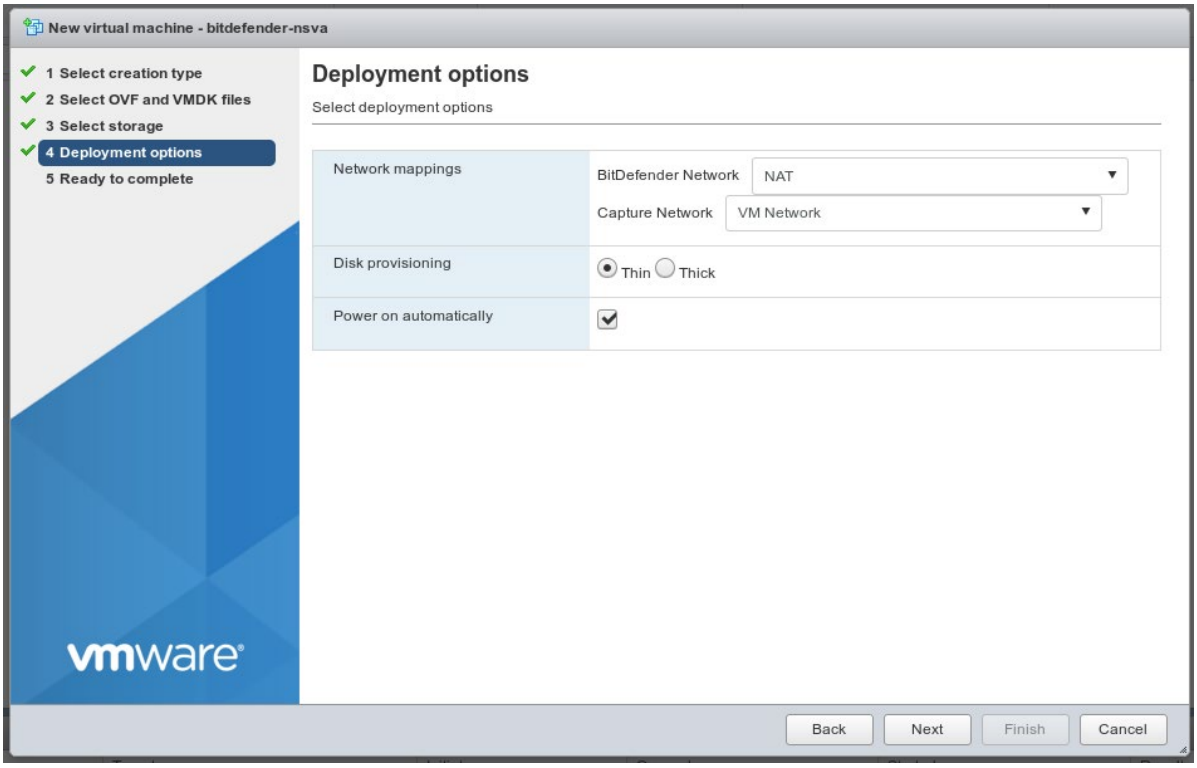
3.6. Network Sensor Deployment

Network Security Virtual Appliance (NSVA) is a network sensor designed to capture, pre-filter and send content from traffic streams to a Sandbox Analyzer instance for detonation.

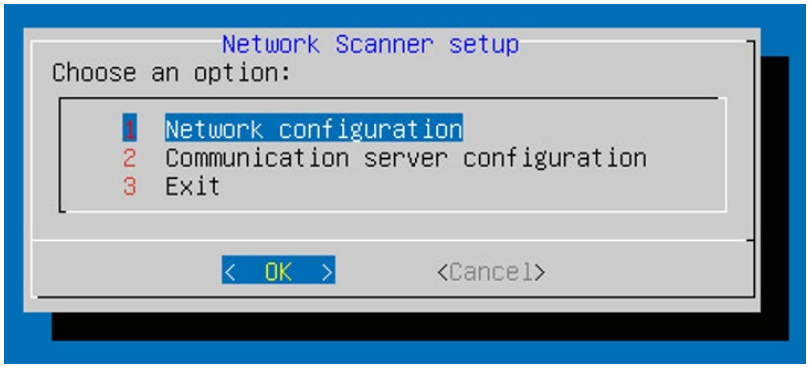
Installation

The NSVA appliance is available as an OVA package. To access the package:

1. Log in to the GravityZone Control Center.
2. Go to the **Network** > **Packages** page.
3. Select the **Network Security Virtual Appliance** check box from the table.
4. Click the **Download** button at the upper-left side of the page and select the **Security Appliance (VMware OVA)** option.
5. Use your virtualization management tool (for example, vSphere Client) to import the downloaded image into your virtual environment.
6. In the deployment wizard, select the Network Interface card (NIC) used for communication with GravityZone and the NIC used for capturing traffic.



7. Once the deployment is complete, connect to the command-line interface (CLI) of the newly deployed appliance. By default, the new appliance will be listed using the **GravityZone SVE SVA Network Security VA** name).
8. Log in to the appliance by supplying the **root/sve** credentials.
9. Start the installation by running the following command: `/opt/bitdefender/bin/nsva-setup`



10. Go to **Communication server configuration** menu option.
11. Specify the IP address and port of an installed GravityZone Communication server component or GravityZone On-premises.

Note

Accepted format is *<IP address>:<port>.*

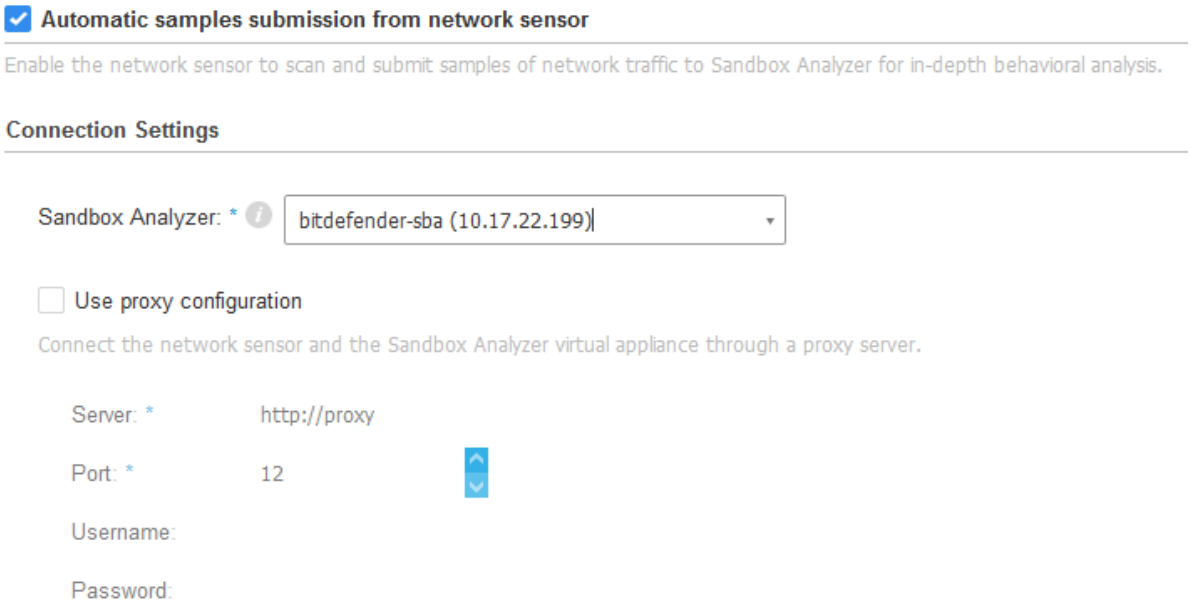
Default port is *8443.*

12. Save the configuration. The NSVA appliance will now be available for use from the GravityZone interface.

Configuration

To configure an NSVA appliance:

1. In an existing or new policy, go to the **Sandbox Analyzer** > **Network Sensor** section.
2. Check the **Automatic samples submission from network sensor** check box.
3. Choose a Sandbox Analyzer instance from the drop-down list where NSVA will send the extracted content.



Detonating Content from .pcap Files

The NSVA sensor can extract content from network capture files (*.pcap) and automatically send it for detonation to the Sandbox Analyzer instance configured to work with.

To detonate content from .pcap files:

1. Log in to a deployed NSVA appliance using the **root**/**sve** credentials.
2. Run the following command:

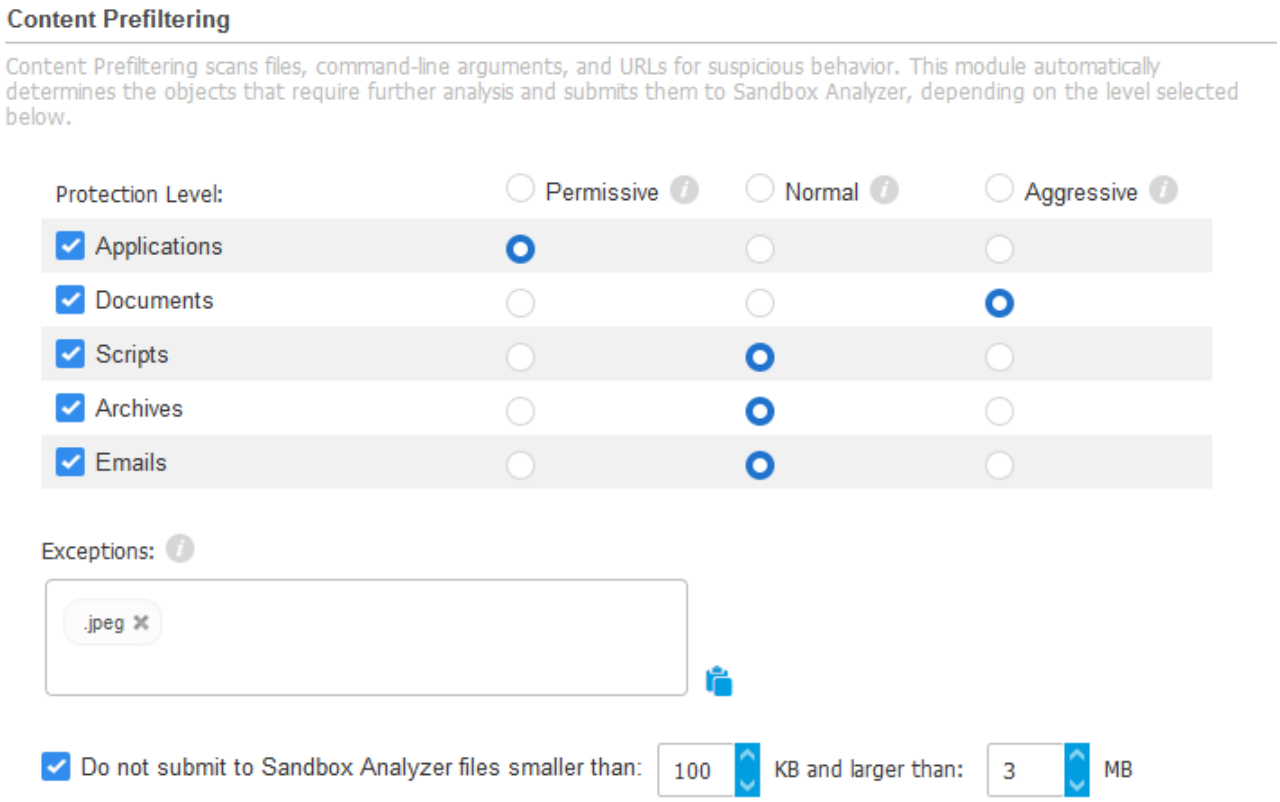
```
/opt/bitdefender/bin/scan-pcap <local pcap path>
```

where `<local pcap path>` represents the location where the .pcap file is uploaded on the NSVA appliance.

3.7. Content Filtering Settings

Content filtering is a technology module embedded in each Sandbox Analyzer sensor that analyzes the object detected by the sensor and based on the configuration set by the end-user determines whether the object should be sent to a Sandbox Analyzer for further forensic analysis.

Content filtering will identify by content analysis and support the following object types: applications, documents, scripts and archives.



Each Sandbox Analyzer sensor has a special section in its Policy settings, that allows the user to configure the **Content filtering** by specifying the following:

- **Protection level** (configurable individually for each object type)**:**
  - *Permissive* – the sensor automatically submits to Sandbox Analyzer only the objects with the highest probability of being malicious and ignores the rest of the objects.
  - *Normal* – the endpoint sensor finds a balance between the submitted and ignored objects and sends to Sandbox Analyzer both objects with a higher and with a lower probability of being malicious.
  - *Aggressive* – the endpoint sensor submits to Sandbox Analyzer almost all objects, regardless of their potential risk.
- **Exceptions:**

  Specify a list of file exceptions that will be ignored.

- **File size limits:**

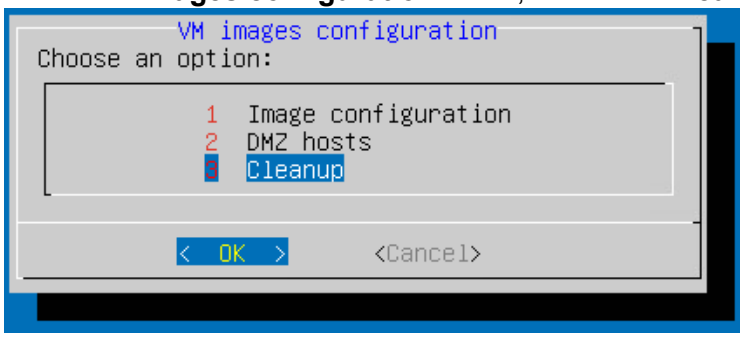
  Allows specifying file size range for submitted objects.

3.8. Uninstalling Sandbox Analyzer

To uninstall Sandbox Analyzer from your infrastructure, you need to perform these operations:

1. Remove the VM images by using the Sandbox Analyzer command-line interface (CLI):
   a. In the **Sandbox configuration** menu, select the **VM images** option.

b. In the **VM images configuration** menu, select the **Cleanup** option.



c. Confirm that you want to remove all installed VM images.
Wait for the VM images to be deleted. During this action, data associated with the VM images will also be deleted.

2. Delete the Sandbox Analyzer Virtual Appliance:
   a. Power off the Sandbox Analyzer Virtual Appliance.
   b. Delete the appliance from the ESXi inventory.

4. Testing Guidelines

4.1. Test Environment

For the testing environment, make sure you have prepared the following:

- A host running any version of Windows operating system. The host will require direct communication with the GravityZone installation.
- A deployment of a Sandbox Analyzer instance with at least one VM image installed.

4.2. Manual File Detonation (Ransomware Scenario)

In this scenario, you will detonate a ransomware sample to test the Sandbox Analyzer capabilities and observe the resulting report.

Detonating the Sample

1. On your test environment, download the sample from **here**.

> **Note**
> The password for the zip archive is **infected.**

2. In GravityZone Control Center, go to the **Sandbox Analyzer** > **Manual submission** page.
3. Use **Browse** button to upload the sample.
4. Select a Sandbox Analyzer instance from the **Local Sandbox Analyzer** list.
5. Select a virtual machine from the **Image** list.
6. Click the **Submit** button.

Observing the Results

To view the detonation report:

1. Go to the **Sandbox Analyzer** page on the left side menu.
2. In the submissions list, find the one you are interested in.
3. Click the **View** button. A new page in the browser will display the report.

4.3. Automatic Detonation from Endpoint Sensor

The Endpoint Sensor (the Bitdefender Endpoint Security Tools agent installed on the machines from network) will determine if the file is suspicious enough to be detonated in the Sandbox Analyzer. The Endpoint Sensor will also allow the user to specify what kind of action to be taken if the file is determined as malicious.

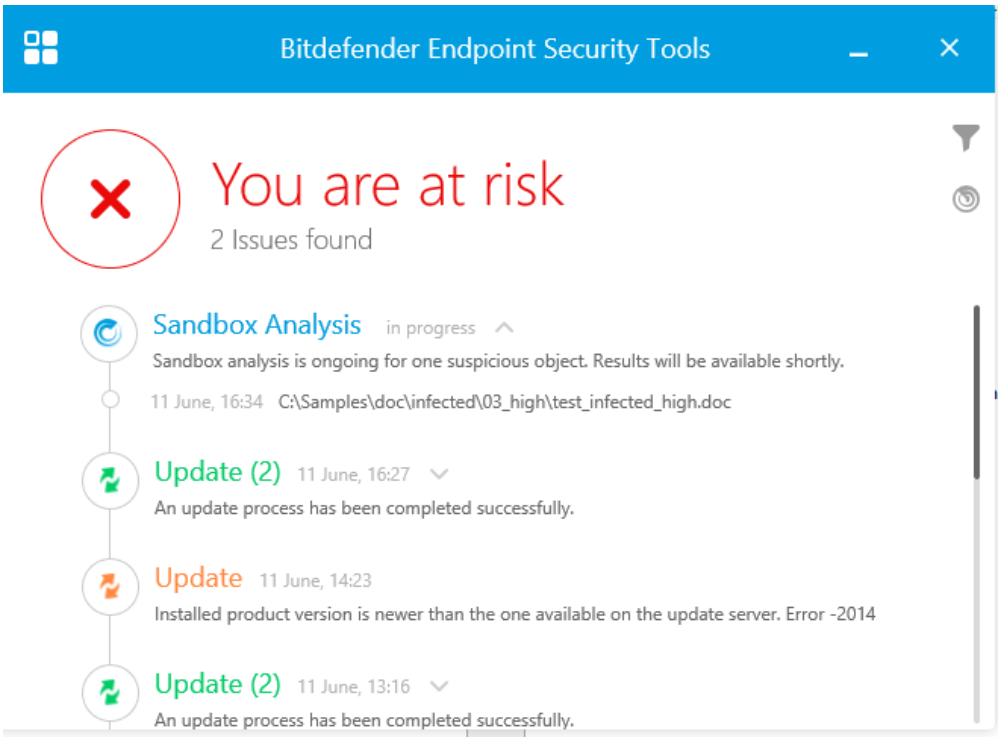
Through a GravityZone security policy, you can configure BEST to do either of these:

- Allows normal file execution while the detonation occurs

- Keeps the file blocked by denying any file access until receiving an answer from the Sandbox Analyzer (it continues to block if infected, it allows execution if clean).

To test Endpoint Sensor submission to a Sandbox Analyzer, following these steps:

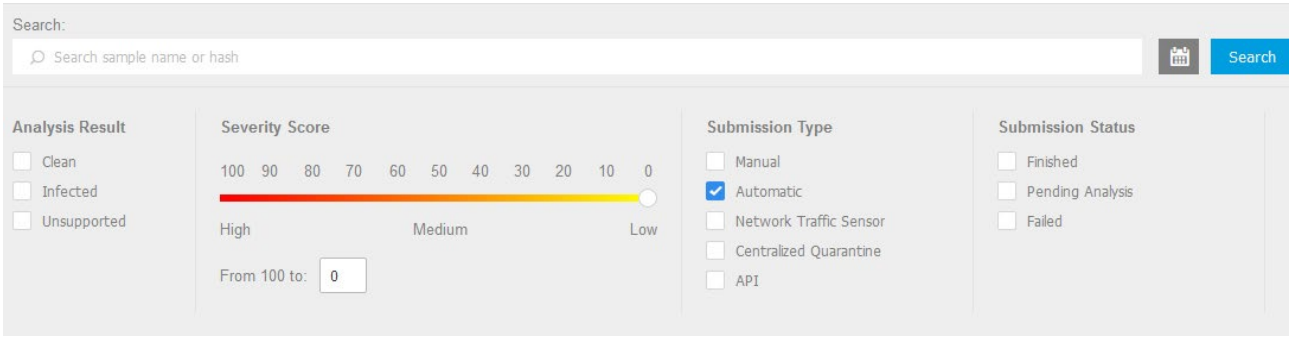
1. Deploy on the endpoint sensor a policy where the submission to Sandbox Analyzer is enabled. You can do this by selecting **Automatic sample submission from managed endpoints** in the policy settings, **Sandbox Analyzer > Endpoint Sensor** section.
2. Under **Content prefiltering,** ensure that the **Documents** object type is selected (a document sample will be used).
3. Copy a document on the machine where the BEST agent is installed.
4. Observe that BEST detects the malware sample and submits it to Sandbox Analyzer.



Observing the Results

To view the detonation report:

1. In GravityZone Control Center left-side menu, click the **Sandbox Analyzer** section.
2. Click **Show filters** in the upper-right corner of the **Sandbox Analyzer** page.
3. Filter the result by selecting **Automatic** in the **Submission Type** column**.**



4.4. Automatic Detonation from NSVA (Network Sensor)

Using the Network Security Virtual Appliance (NSVA), you can extract content from network streams and automatically submit to Sandbox Analyzer. To test this functionality, follow the steps below:

1. Ensure that the NSVA is deployed and configured.
2. Copy a sample from this **location** and save it on the host located in the same network that the NSVA is configured to capture traffic from.
3. On the host where the sample has been copied, share the folder containing the copied malware.
4. From a different host, connect to the shared folder and copy the sample.

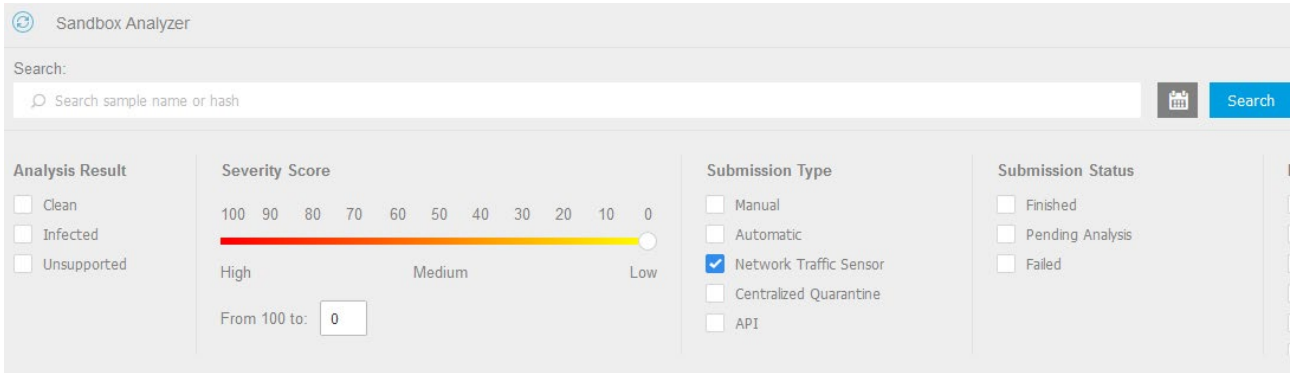
Note

NSVA supports extracting content from the following non-encrypted protocols: SMB, HTTP, FTP, POP3. For testing purposes, SMB will be used. However, any of the protocols previously enumerated can be used.

Observing the Results

The NSVA network sensor will intercept the sample and Sandbox Analyzer will create a report that will be accessible from the GravityZone Control Center.

1. In GravityZone Control Center left-side menu, click the **Sandbox Analyzer** section.
2. Click **Show filters** in the upper-right corner of the **Sandbox Analyzer** page.
3. Filter the result by selecting **Network Traffic Sensor** in the **Submission Type** column.



4.5. Automatic Detonation from GravityZone Centralized Quarantine

You can configure GravityZone with a Centralized Quarantine. In this case, all malware detected by the Endpoint Sensor (BEST) on any protected endpoint is quarantined and a copy is submitted in a centralized CIFS network share. The main objective is for the administrator to get more forensics details about malware behavior.

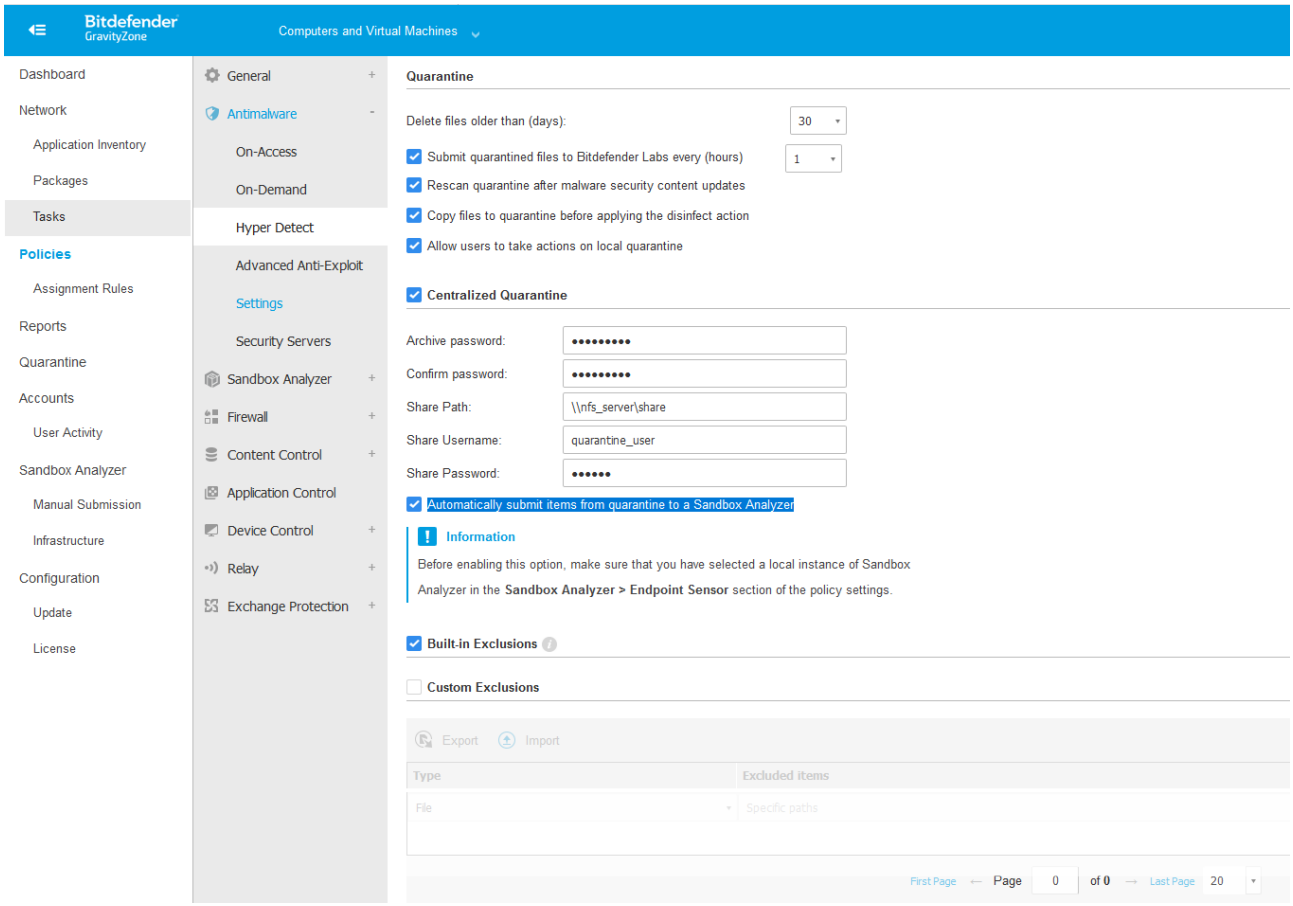
You can configure the BEST agent to automatically submit a quarantined sample to Sandbox Analyzer. After doing so, Sandbox Analyzer will generate a report that will be accesible from **Sandbox Analyzer** unified reporting interface, in GravityZone Control Center.

Note

Before proceeding, follow the instructions from the GravityZone Administrator's Guide on how to configure a centralized quarantine.

Enabling Automatic Submission from Centralized Quarantine

Once you have configured a centralized quarantine, apply a GravityZone policy on your endpoints where the option **Automatically submit items from quarantine to a Sandbox Analyzer** is enabled. To do this, go to the policy settings, **Antimalware > Settings** section, and select the corresponding check box.



Note

The samples will be submitted to the Sandbox Analyzer as defined in the **Endpoint sensor** section of the policy.

Testing the Automatic Submission

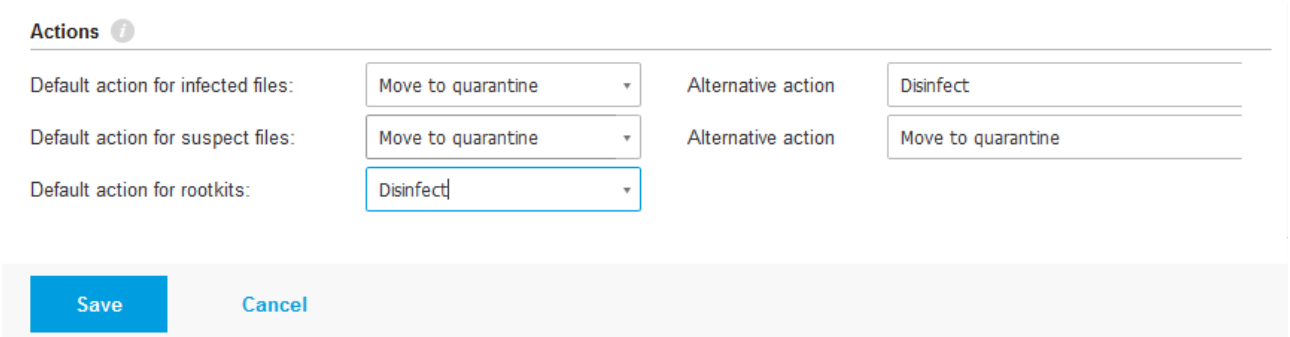
To manually test the automatic submission, you can trigger a custom scan task from GravityZone Control Center, with the specified action **Move to quarantine.** This will cause any infected files to

be moved to the configured Centralized Quarantine, which in turn will cause automatic submission to the Sandbox Analyzer.

Note

Before triggering the task, ensure some samples are copied on your endpoints. The samples can be downloaded from here (the ZIP file password is “infected”).

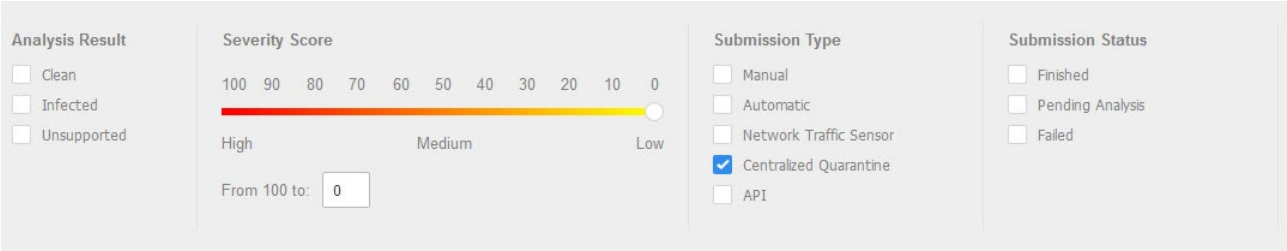
1. Go to **Network** section.
2. Select the groups or endpoints you wish the Scan task to run against.
3. From the **Tasks** menu, select **Scan.**
4. In the **General** tab, select **Custom Scan.**
5. Switch to **Options** tab and expand the **Settings** section.
6. Scroll down to **Actions** and configure as in the screenshot below:



Observing the Results

After running the task, view the reports resulted from samples originating from the Centralized Quarantine.

1. In GravityZone Control Center left-side menu, click the **Sandbox Analyzer** section.
2. Click **Show filters** in the upper-right corner of the **Sandbox Analyzer** page.
3. Filter the result by selecting **Centralized Quarantine** in the **Submission Type** column.



5. Programmatic Interaction with Sandbox Analyzer

Programmatic interaction with the Sandbox Analyzer is possible with the help of its management console, GravityZone Control Center.

GravityZone exposes several methods which allows retrieving the deployed infrastructure of Sandbox Analyzer instances, information about the instances as well as detonation results.

Note

The information below is available also in the GravityZone API Guide.

The URL for invoking the API is:

- https://<GravityZone_IP>/api/v1.0/jsonrpc/sandbox

The following methods are exposed:

- getSandboxAnalyzerInstancesList : lists Sandbox Analyzer instances.
- getImagesList : lists images for a Sandbox Analyzer instance.
- getSubmissionStatus : Returns the status of a submission.
- getDetonationDetails : Returns the details of a submission

5.1. getSandboxAnalyzerInstancesList

This method lists the Sandbox Analyzer instances, which can be found in the Infrastructure menu.

Parameters

Parameter	Type	Optional	Description
page	Number	Yes	The results page number. The default value is 1
perPage	Number	Yes	The number of items displayed in a page. The upper limit is 100 items per page. Default value: 30 items per page.

Return value

This method returns an Object containing information regarding the

- `page` - the current page displayed
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `items` - the list of Sandbox Analyzer instances. Each entry in the list has the following fields:

- `sandboxId`, the ID of the Sandbox Analyzer instance.
- `name`, the name of the Sandbox Analyzer instance.
- `ip`, the IP address of the Sandbox Analyzer instance.
- `macs`, the MAC addresses of the Sandbox Analyzer instance.
- `ssid`, the SSID (Active Directory SID) of the Sandbox Analyzer instance.
- `detonatedSamples`, the number of samples analyzed since first licensing the Sandbox Analyzer instance.
- `diskUsage`, the percentage of space consumed by the Sandbox Analyzer instance in datastore.
- `installationStatus`, The installation status of the Sandbox Analyzer instance. It can have one of the following values:
  - `0` - Not installed
  - `1` - Installed
  - `2` - Installing
  - `3` - Installation failed
- `lastSeen`, the date of the last synchronization with Control Center.
- `configuredConcurrentDetonations`, the number of virtual machines that you have allocated according to your license to detonate samples.
- `maximumConcurrentDetonations`, the maximum number of virtual machines that the Sandbox Analyzer instance can create to detonate samples.
- `submissionUrl`, the url which can be used to submit a file to analysis.

- `total` - the total number of items

Example

Request

```
{
   "method": "getSandboxAnalyzerInstancesList",
   "params": {
      "page": 1,
      "perPage": 20
   },
   "jsonrpc": "2.0",
   "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7"
}
```

Response

```
{
   "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7",
   "jsonrpc": "2.0",
   "result": {
      "page": 1,
      "pagesCount": 1,
      "perPage": 20,
      "total": 1,
      "items": [
         {
             "sandboxId": "5c419e6e26df3d367c49de18",
             "name": "sandbox1",
             "ip": "10.10.20.1",
             "macs": [
                 "00-14-22-01-23-45"
```

```
                ],
                "ssid": "",
                "detonatedSamples": 0,
                "diskUsage": 250,
                "installationStatus": 1,
                "lastSeen": "2019-01-18T11:37:50",
                "configuredConcurrentDetonations": 0,
                "maximumConcurrentDetonations": 10, "submissionUrl":
"https://10.10.20.1:443/api/v1/upload"
            }
        ]
    }
}
```


5.2. getImagesList

This method lists the Sandbox Analyzer images associated with a Sandbox Analyzer instance.

Parameters

Parameter	Type	Optional	Description
`sandboxId`	Number	Yes	The ID of the Sandbox Analyzer instance for which the images list will be returned.
`page`	Number	Yes	The results page number. The default value is 1.
`perPage`	Number	Yes	The number of items displayed in a page. The upper limit is 100 items per page. Default value: 30 items per page.

Return Value

This method returns an Object containing information regarding the images. The returned object contains:

- `page` - the current page displayed
- `pagesCount` - the total number of available pages
- `perPage` - the total number of returned items per page
- `items` - the list of images. Each entry in the list has the following fields:
  - `id`, the ID of the image.
  - `name`, the name of the image.
  - `status`, the status of the image. It can have one of the following values:
    - `1` – New
    - `2` – Failed
    - `3` – Ready
  - `operatingSystem`, the operating system of the image.
  - `dateAdded`, the date on which the image was added.
  - `isDefault`, boolean `True`, if this image is set as default.
  - `actionInProgress`, boolean `True`, if there is an action in progress for this image.
- `total` - the total number of items

Example

Request

```
{
   "method": "getImagesList",
   "params": {
      "sandboxId": "5c419e6e26df3d367c49de18",
      "page": 1,
      "perPage": 20
   },
   "jsonrpc": "2.0",
   "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7"
}
```

Response

```
{
   "id": "91d6430d-bfd4-494f-8d4d-4947406d21a7",
   "jsonrpc": "2.0",
   "result": {
      "page": 1,
      "pagesCount": 1,
      "perPage": 20,
      "total": 1,
      "items": [
         {
             "id": "924cca0d49cc7e350a44502b0bb9026a",
             "name": "image1",
             "status": 1,
             "operatingSystem": "Windows 10",
             "dateAdded": "2019-01-18T09:20:50",
             "isDefault": true,
             "actionInProgress": false
         }
      ]
   }
```

5.3. getSubmissionStatus

Returns a compound status of a submission by combining the "status" and "verdict" properties of a DetonationResult.

Parameters

Parameter	Type	Optional	Description
`submissionId`	String	No	The ID of the submission for which the status should be retrieved.

Return Value

This method returns an Object containing with the following structure:

- `status` - integer with the following possibilities
  - `1` COMPLETED
  - `2` PENDING

- 3 FAILED
- 4 NOT SUPPORTED

Example

Request

```
{
   "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
   "jsonrpc": "2.0",
   "method": "getSubmissionStatus",
   "params": {
      "submissionId": "sp02_1547807011_936_e5"
   }
}
```

Response

```
{
  "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
  "jsonrpc": "2.0",
  "result": {
    "status": 1
  }
}
```

5.4. getDetonationDetails

Returns the details of a submission, included a url pointing to the HTML report.

Parameters

Parameter	Type	Optional	Description
submissionId	String	No	The ID of the submission for which the detonation details should be retrieved

Return Value

This method returns an Object containing containing the details of a completed detonation. It will contain the following keys:

- detailsReportUrl - The url from which the HTML report can be downloaded
- score - integer in the range of 0-100 (the severity of the threat, if any)
- verdict - integer with values: 0 if CLEAN, 1 if INFECTED, 2 if UNSUPPORTED
- mitreTags - array of objects with the following structure:
- - category a string holding the MITRE category.
  - techniques an array of strings holding the MITRE techniques.

Example

Request

```
{
   "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
   "jsonrpc": "2.0",
   "method": "getDetonationDetails",
   "params": {
      "submissionId": "sp02_1547807011_936_e5"
   }
}
```

Response

```
{
   "id": "787b5e36-89a8-4353-88b9-6b7a32e9c87f",
   "jsonrpc": "2.0",
   "result": {
      "detailsReportUrl":
          "https://10.10.20.1:443/api/v1/report?report_id=asd",
      "score": 30,
      "verdict": 0,
      "mitreTags": [
         {
             "category": "Defense Evasion",
             "techniques": [
                "Modify Registry",
             ]
         },
         {
             "category": "Persistence",
             "techniques": [
                ".bash_profile and .bashrc",
                "Account Manipulation",
             ]
         },
      ]
   }
}
```

5.5. Uploading a Sample

To upload a sample for detonation, an API call must be made directly at the Sandbox Analyzer instance you wish to use.

The API URL is: https://SANDBOX_IP/api/v1/upload

Note

The list of available Sandbox Analyzer instances can be retrieved by invoking the getSandboxAnalyzerInstancesList method on GravityZone Endpoint URL

Parameters

Parameter	Type	Optional	Description
`imageId`	String	No	The ID of the submission for which the detonation details should be retrieved
`Detonation`	Object	Yes	**type** - a String representing the submitted information's type. Possible values are • **file** to submit a binary file or url when submitting using a URL • **url** - (optional, String) the URL to be analyzed. • **fileName** - (optional, String) the filename which will be shown in the UI. If missing, the Sandbox will generate a filename. • **archivePassword** - (optional, String) password used for decrypting archives.
`detonationOptions`	Object	Yes	An Object containing detonation options. You can find a list of detonation options in the table below

Detonation Options

All options are optional. If an option is omitted, Sandbox Analyzer uses the default value.

Parameter	Type	Default	Description
`commandLineArguments`	String	No arguments provided	The list of command line arguments that Sandbox Analyzer uses when detonating the sample. This option is available only for file submissions.
`timeLimit`	Number	6 minutes	The maximum number of minutes that a detonation can last.
`numberOfReruns`	Number	2 reruns	The number of detonation attempts, in case of failure.
`preFiltering`	Boolean	True	Specifies whether Sandbox Analyzer caches previously analyzed samples (`True`) or not.
`internetAccess`	Boolean	True	Sets the internet access of the VM. If `True`, the VM can access the internet.

For example, the JSON for a sample with an encrypted archive, to be detonated with command lines arguments, on a VM without internet access, should look like this:

```
{
```

```
    "imageId": "1787b5e3689a8435388b96b7a32e9c87f", "detonation":
    {
        "type":  "file", "fileName: "infected.zip",
        "archivePassword": "123infected"
    },
    "detonationOptions":
      { "commandLineArguments": "--extraParam 41",
        "internetAccess": false
    }
}
```

5.6. Examples

Below is a script written in Python that demonstrates how to interact programmatically with the Sandbox Analyzer.

```
import base64 import pyjsonrpc
import requests import simplejson


# Generate Authorization header from API key

apiKey = "UjlMS+0m1l9IUZjpjWyJG8gbnv2Mta4T"
encodedUserPassSequence = base64.b64encode(apiKey + ":")
authorizationHeader = "Basic " + encodedUserPassSequence


json = pyjsonrpc.create_request_json("getPackagesList")
result = requests.post(
  "https://{domain}/api/v1.0/jsonrpc/packages", json,
  verify=False, headers = {
    "Content-Type": "application/json", "Authorization":
    authorizationHeader
  })


jsonResult = simplejson.loads(result.content)

print jsonResult
```

6. Known Issues

- GravityZone does not display HTML reports for all detonated objects. This behavior is expected when the object is detonated on the Cloud Sandbox Analyzer. Currently, Cloud Sandbox Analyzer does not support HTML reports.
    - **Workaround:** no workaround available. GravityZone will include HTML reports in a future release.
- Subsequent detonations of the same sample but with different values for **Time limit for sample detonation** can produce inconsistent results.
    - **Workaround:** Ensure that the values set for **Time limit for sample detonation** are not below the default ones. Bitdefender will address this issue in a future release (reference).
- Sandbox Analyzer drops from its queue files that exceeded 2 hours.

  Workaround: Increase the number of concurrent virtual machines (VMs) available for detonation to avoid queueing samples (reference).

7. Submitting Feedback

After testing the features described in the Testing Guidelines chapter, please take a few seconds to fill-in the **Feedback Form**. Select your answer regarding the completion status for each feature (**Yes** or **No**). Please enter any encountered issue, comment or any suggestion you may have for the corresponding feature.

We encourage you to send us your feedback by using the feedback feature available in Control Center or by email to enterprise-beta@bitdefender.com.

Thank you for your participation in the Sandbox Analyzer technology preview program!

FEEDBACK FORM				
Features and functionalities		Verdict		Observations
		👍	👎	
Deployment	Sandbox Analyzer installation from CLI	○	○	
Installation	Sandbox Analyzer is fully functional and configurable	○	○	
GravityZone management	Product is manageable. Configuration settings are applied	○	○	
Detonation results		○	○	
Report data		○	○	
Analysis time		○	○	
Documentation		○	○	
NSVA (network sensor) detonation		○	○	