

# GravityZone Basics HandBook

Installing and configuring Bitdefender GravityZone  
Platform and Services.

ENDPOINT NETWORK CLOUD

**Bitdefender**<sup>®</sup>

[WWW.BITDEFENDER.COM](http://WWW.BITDEFENDER.COM)

# GravityZone Basics HandBook

GRAVITYZONE™  
THE SECURITY PLATFORM FOR  
END-TO-END BREACH AVOIDANCE

## INDEX

1. [Introduction](#)
2. [Architecture](#)
3. [Endpoint Security \(BEST\)](#)
4. [Policies](#)
5. [System Requirements](#)
6. [GravityZone Appliance Deployment](#)
7. [GravityZone Deployment Scenarios](#)
8. [Control Center Configuration](#)
9. [Control Center Update](#)
10. [Licensing](#)
11. [Dashboard](#)
12. [Network](#)
13. [Packages](#)
14. [Tasks](#)
15. [Incidents](#)
16. [Hyper Detect](#)
17. [Sandbox Analyzer](#)
18. [Application Inventory](#)
19. [Reports](#)
20. [Quarantine](#)
21. [Accounts](#)
22. [Security for Exchange](#)
23. [Full Disk Encryption](#)
24. [Report Builder](#)
25. [Patch Management](#)
26. [Security for Virtual Environments](#)
27. [Security Servers](#)

2

[Back to Index](#)

## Introduction

This handbook provides security administrators with the knowledge, skills and ability to build and run a GravityZone environment. Next pages focuses on the installation and configuration of GravityZone management component called Control Center and security services. You will learn how to install and manage the security solution for physical machines, virtual machines, mobile devices and Exchange mail servers using a unified web console.

3

# GravityZone Basics Handbook

## References

[Back to Index](#)

GravityZone On Premise	
GravityZone Enterprise	<ul style="list-style-type: none"><li>• <a href="#">Installation Guide (en-US)</a></li><li>• <a href="#">Administrator's Guide (en-US)</a></li><li>• <a href="#">Security Analyst's Guide (en-US)</a></li></ul>
GravityZone Elite	<ul style="list-style-type: none"><li>• <a href="#">Installation Guide (en-US)</a></li><li>• <a href="#">Administrator's Guide (en-US)</a></li><li>• <a href="#">Security Analyst's Guide (en-US)</a></li></ul>
GravityZone Cloud	
GravityZone Elite	<ul style="list-style-type: none"><li>• <a href="#">Installation Guide (en-US)</a></li><li>• <a href="#">Administrator's Guide (en-US)</a></li><li>• <a href="#">Security Analyst's Guide (en-US)</a></li></ul>
GravityZone Ultra	<ul style="list-style-type: none"><li>• <a href="#">Installation Guide (en-US)</a></li><li>• <a href="#">Administrator's Guide (en-US)</a></li><li>• <a href="#">Security Analyst's Guide (en-US)</a></li></ul>
Cloud Security for MSP / Bitdefender Partners	<ul style="list-style-type: none"><li>• <a href="#">Installation Guide (en-US)</a></li><li>• <a href="#">Partner's Guide (en-US)</a></li><li>• <a href="#">Administrator's Guide (en-US)</a></li><li>• <a href="#">Security Analyst's Guide (en-US)</a></li></ul>
<b>Bitdefender Business Cybersecurity Solutions Comparison</b>	<a href="https://www.bitdefender.com/business/compare.html">https://www.bitdefender.com/business/compare.html</a>

Bitdefender®

4

[Back to Index](#)

## What is GravityZone?

Bitdefender GravityZone addresses the needs of the most demanding enterprises by providing cross-platform security for physical desktops and servers, virtualized endpoints, mobile devices, Exchange mail servers and using our newest product, Bitdefender Hypervisor Introspection (HVI), is able to protect XenServer hosts against targeted attacks.



Bitdefender®

5

Bitdefender®

# GravityZone Basics HandBook

[Back to Index](#)

## Architecture

GRAVITYZONE™  
THE SECURITY PLATFORM FOR  
END-TO-END BREACH AVOIDANCE

Business

Engineering

Science

## Components

[Back to Index](#)



Bitdefender®

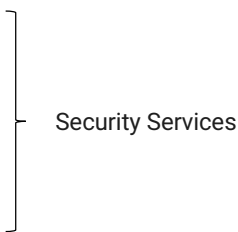
Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## Components

GravityZone Enterprise Security architecture includes 1 management component and 5 Security Services:

- **Control Center**
  - **Security for Endpoints**
  - **Security for Virtualized Environments**
  - **Security for Mobile Devices\***
  - **Security for Exchange\***
  - **Security for HVI\*\***
- 
- Security Services

\*not available on GravityZone Business Security

\*\*only available on GravityZone Elite Security and GravityZone Enterprise Security

Bitdefender®

3

[Back to Index](#)

## CONTROL CENTER GRAVITYZONE APPLIANCE

GravityZone Control Center is delivered as a virtual appliance, available in several different formats compatible with the main virtualization platforms.

➔ **preconfigured virtual machine running a hardened Linux Server distribution (Ubuntu 16.04)**

The GravityZone appliance can run **one**, **several** or **all** of the following roles:

- Database
- Update Server
- Web Server (Web Console)
- Communication Server

A GravityZone deployment requires running at least one instance of each role.

Depending on GravityZone roles distribution, you will run one to multiple GravityZone appliances.

Bitdefender®

3

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER GRAVITYZONE APPLIANCE

Additional GravityZone appliance roles:

- Role Balancer

Allows you to install multiple instances of the Communication Server role or Web Server role.

→ ensure high availability and scalability

The built-in Role Balancer role cannot be installed together with other roles on the same GravityZone appliance.

3<sup>rd</sup> party software or hardware Role Balancers can also be used.

Bitdefender®

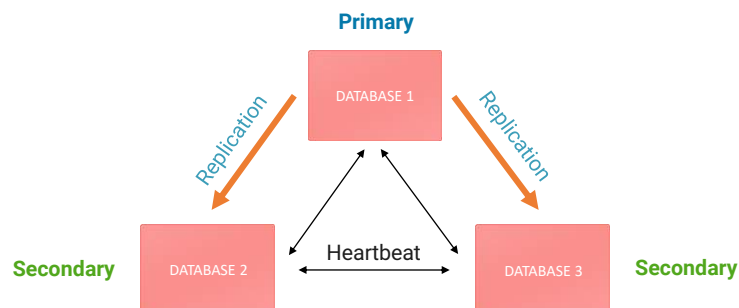
10

[Back to Index](#)

## CONTROL CENTER DATABASE REPLICA SET

This mechanism allows installing multiple database instances across a distributed GravityZone environment.

→ ensure high-availability in the case of a database instance failure



Bitdefender®

11

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER COMPONENTS

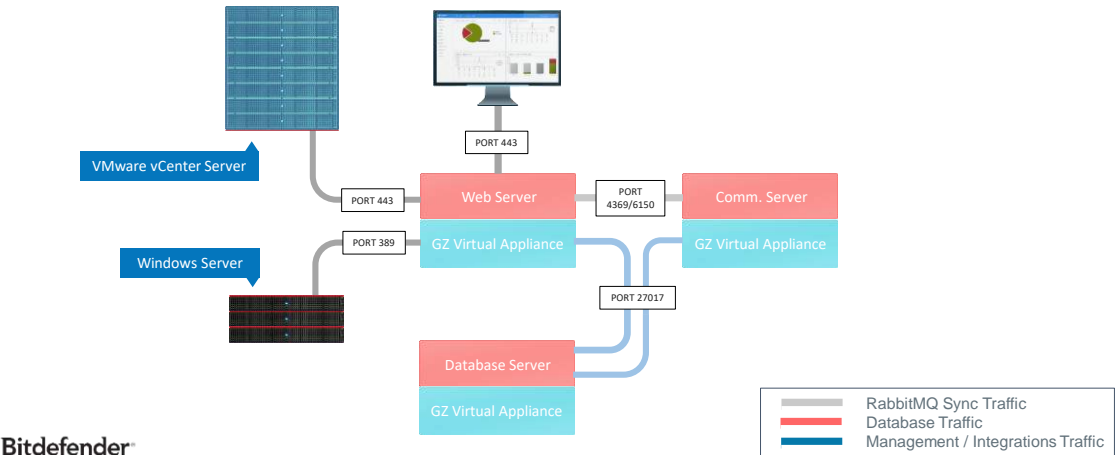
	GravityZone Appliance Roles	Nr. of deployments
Control Center	Database	At least 1, otherwise 3, 5, 7 for Replica Set
	Update Server	No more than 1
	Web Server	At least 1
	Communication Server	At least 1
	Load Balancer	Optional deployment

Bitdefender®

12

[Back to Index](#)

## GRAVITYZONE APPLIANCE INTERNAL NETWORK COMMUNICATION



Bitdefender®

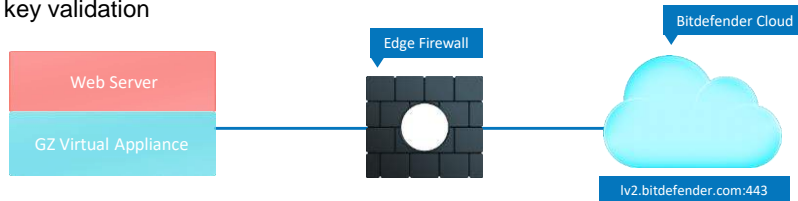
13

# GravityZone Basics Handbook

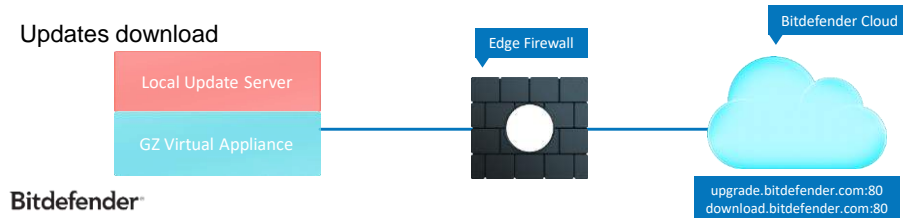
[Back to Index](#)

## GRAVITYZONE APPLIANCE EXTERNAL NETWORK COMMUNICATION

- License key validation



- Updates download

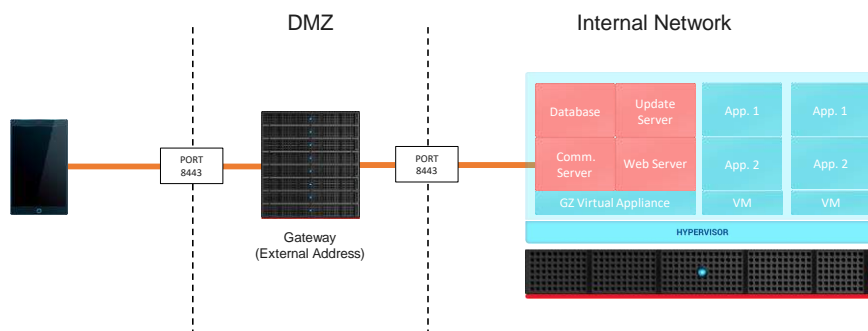


Bitdefender®

14

[Back to Index](#)

## CONTROL CENTER MDM COMMUNICATION SERVER



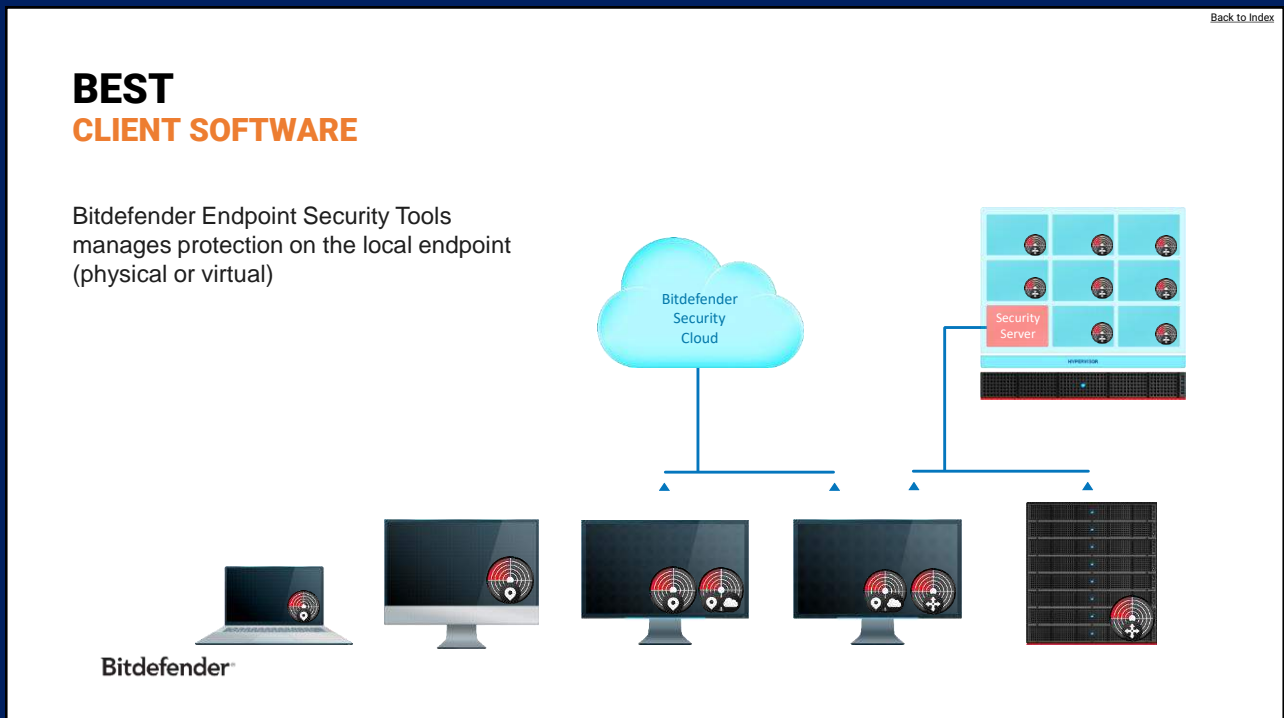
Bitdefender®

15

# GravityZone Basics HandBook



16



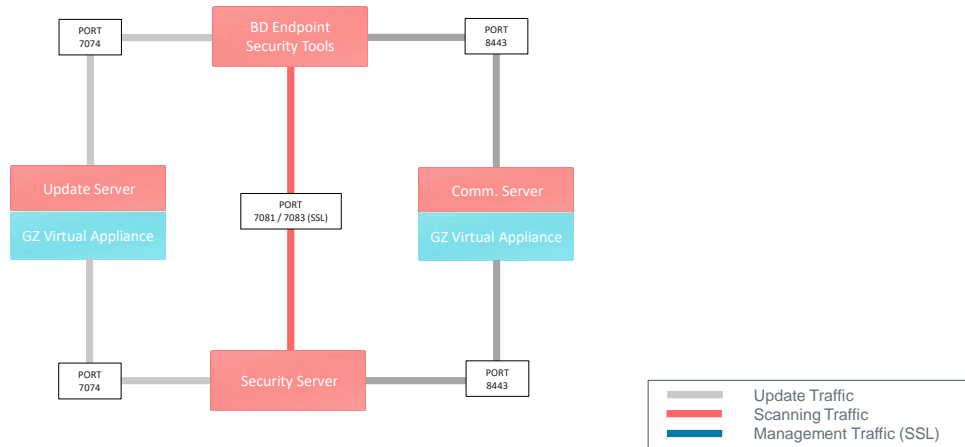
17

# GravityZone Basics Handbook

[Back to Index](#)

## ENDPOINT PROTECTION

### SECURITY SERVER NETWORK COMMUNICATION



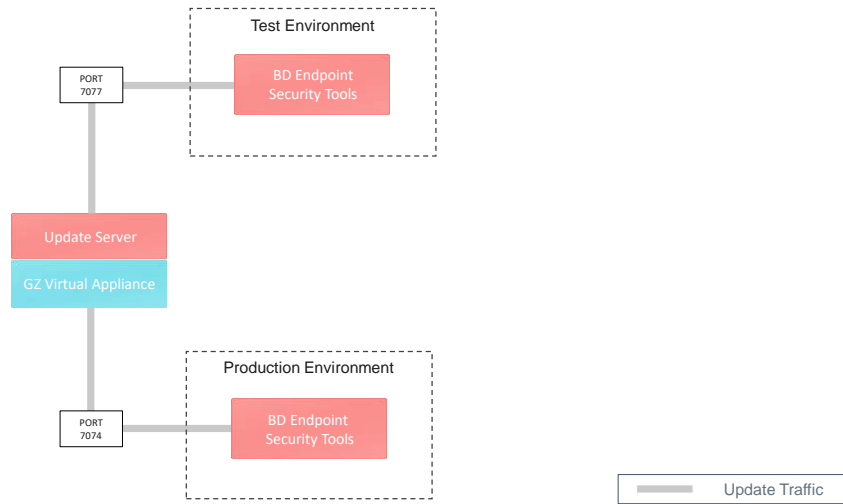
Bitdefender®

18

[Back to Index](#)

## ENDPOINT PROTECTION

### UPDATE STAGING



Bitdefender®

19

# GravityZone Basics HandBook

[Back to Index](#)

## SECURITY FOR ENDPOINTS

### BEST SCANNING ENGINES

The scanning engines are automatically set during Bitdefender Endpoint Security Tools packages creation, letting the endpoint agent detect the machine's configuration and adapt the scanning technology accordingly:



Local Scan



Hybrid Scan



Central Scan

\*Central Scan is not available on GravityZone Business Security

Bitdefender™

20

[Back to Index](#)

## SECURITY FOR ENDPOINTS

### BITDEFENDER ENDPOINT SECURITY TOOLS (BEST)

Protects any number of Windows, Linux and Mac OS X systems.

Includes the following modules and roles:

- Antimalware, Advanced Threat Control, Advanced Anti-Exploit, Hyper Detect (not available on GravityZone Business Security and Advanced Business Security)
- Firewall\*
- Network Protection\* (web access control, application blacklisting, data protection, Network Attack Defense)
- Device Control\*\*
- Application Control (application whitelist)\*\* (available on Elite Security On Premise and Enterprise Security)
- Encryption\*\*\*
- Patch Management \*\*\*
- Power User\*\*
- Exchange Protection (not available on GravityZone Business Security)
- Relay (not available on MAC OS)
- EDR Sensor

\*not available for Linux and Windows Server OS

\*\*not available for Mac and Linux OS

\*\*\*available for certain Windows and MAC OS and requires a separate license Add-on key

Bitdefender™

<https://www.bitdefender.com/support/GravityZone-Protection-Layers-Availability-2399.html>

21

# GravityZone Basics Handbook

[Back to Index](#)

## BEST

### CREATE INSTALLATION PACKAGE

Create under Network → Packages custom installation packages that can be used for remote deployments or manual installations.

Settings that can be configured when creating custom installation packages:

- **Modules:** Antimalware, Advanced Threat Control, Firewall, Content Control, Device Control, Power User, Application Control, Encryption, Patch Management
- **Roles:** Relay, Exchange Protection
- **Scan mode:** Automatic or Custom (local, central or hybrid scan)
- **Settings:** scan before installation, custom installation path, uninstall password
- **Deployer:** specify the package communication settings (GZ Appliance or Relay)

Bitdefender®

22

[Back to Index](#)

## ENDPOINT SECURITY TOOLS

### CREATE INSTALLATION PACKAGE

You can create multiple custom installation packages, that cover the different protection needs of your endpoints and save them all under the Packages Window.

Bitdefender®

New Endpoint Package

General

Name: \*

Description:

Language: English

Modules:

- ☒ Antimalware
- ☒ Advanced Threat Control
- ☒ Advanced Anti-Exploit
- ☒ Firewall
- ☒ Network Protection
- ☒ Content Control
- ☒ Network Attack Defense
- ☒ Device Control
- ☒ Power User
- ☒ Application Control
- ☒ Encryption

Roles:

- ☐ Relay

Additional settings:

- ☒ Remove Competitors

**Warning**

Windows legacy operating systems support only Antimalware and Advanced Threat Control. For more information, check the Installation Requirements in the [Installation Guide](#).

Scan mode

☒ Automatic ☐ Custom

Save Cancel

Network → Packages → New Endpoint Package Window

23

# GravityZone Basics Handbook

[Back to Index](#)

## BEST Manual Installation

Bitdefender®

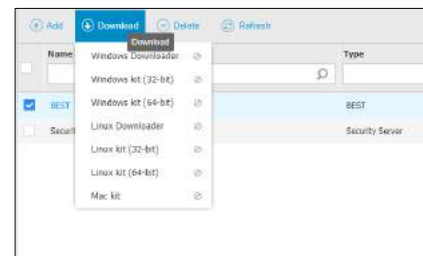
24

[Back to Index](#)

## BEST LOCAL INSTALLATION

Download the installation package from the Control Center web console and run it locally.

- The installation package must be run using administrator privileges or under an administrator account
- Once BEST has been installed, the computer will show up as managed in Control Center (Network page) within a few minutes



Package Download

Bitdefender®

25

# GravityZone Basics HandBook

[Back to Index](#)

## BEST Remote Installation

Bitdefender™

26

[Back to Index](#)

## BEST REMOTE INSTALLATION

Endpoint Security can be installed remotely on Active Directory computers and on other computers detected in the network.

- BEST uses **Microsoft Computer Browser Service** to detect computers that are not in AD:
  - automatic detection for BEST with Relay role
  - manually start *Network Discovery* Task for BEST without Relay role
- Detected computers are displayed as unmanaged computers on the Network page
- Network discovery workflow and requirements:

<http://enterprise.bitdefender.com/support/how-network-discovery-works-990.html>

Bitdefender™

27

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

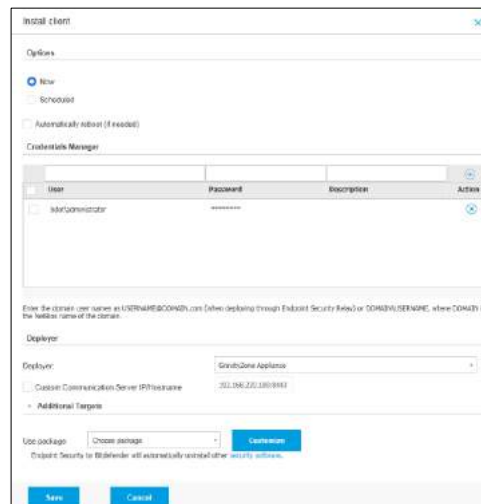
## BEST REMOTE INSTALLATION

Select unmanaged computers under the Network page and assign them *Installation Tasks*.

The installation task allows you to:

- Run the deployment immediately or scheduled
- Provide administrative credentials
- Select Deployer (GZ Appliance or Relay)
- Provide additional targets (IPs or hostnames)
- Select installation package
- Customize installation package

Bitdefender®



Install client task

28

[Back to Index](#)

## BEST MANAGED SYSTEMS

Once Endpoint Security Tools has been installed, the computer will show up as managed in Control Center, Network page → Computers and Virtual Machines, within a few minutes:

Managed computer, no issues

Managed computer, with issues

Managed computer, Relay

Managed virtual machine

Security Server

Managed computer, offline, with issues

Name	OS	IP	Last Seen
CLIENT05	Windows 7 Professional	192.168.230.162	Online
CLIENT06	Windows 7 Professional	192.168.230.163	Online
DC-01	Microsoft Windows Server 2003	192.168.230.161	Online
BDVM-PC	Windows 7 Professional	192.168.230.132	Online
bitdefender-ova	Linux	192.168.230.145	Online
WIN-A3106LEVCP2	Windows Server 2008 R2 Enterprise	192.168.230.131	13 May 2015, 15:08:03

Bitdefender®

Network → Managed Computers

29

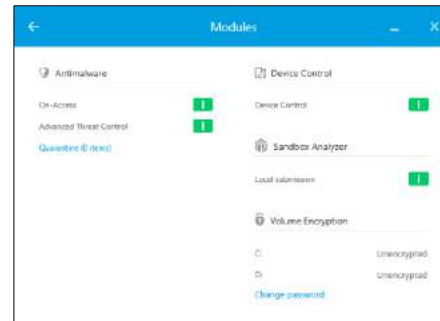
Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## BEST LOCAL

Once installed, BEST can be opened locally from the icon tray



Bitdefender®

30

[Back to Index](#)

## BEST LOCAL

- Filters
- Scan and Update



Bitdefender®

31

Bitdefender®

# GravityZone Basics HandBook

[Back to Index](#)

## BEST Relay

Bitdefender®

32

[Back to Index](#)

## SECURITY FOR ENDPOINTS

### BEST WITH RELAY ROLE

Special role of Bitdefender Endpoint Security Tools which installs an Update Server on the target machine along with BEST client.

Provides the following additional functionalities:

- Communication Proxy for the BEST clients installed in a remote office
- BEST installation package for remote deployments
- Network Discovery
- Local Update Server

Bitdefender®

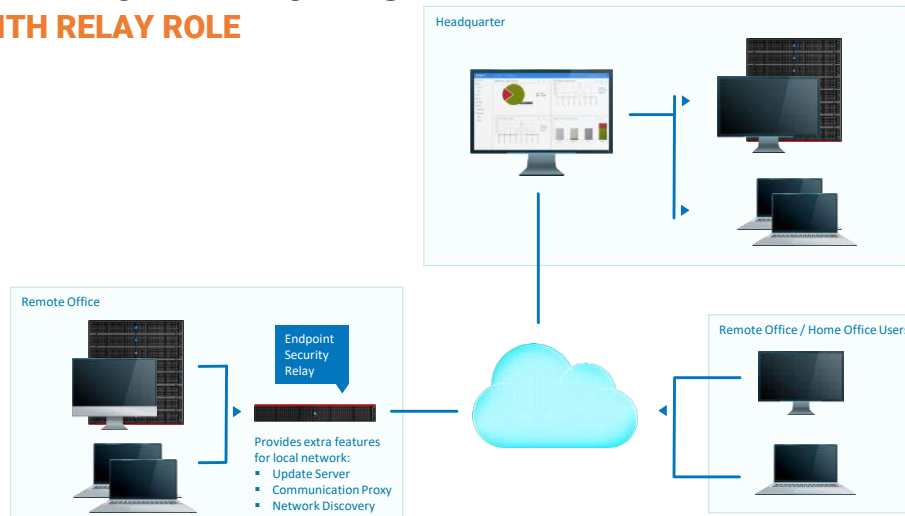
33

# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR ENDPOINTS

### BEST WITH RELAY ROLE



Bitdefender®

34

[Back to Index](#)

## AD Integration using BEST

(cloud console only)

Bitdefender®

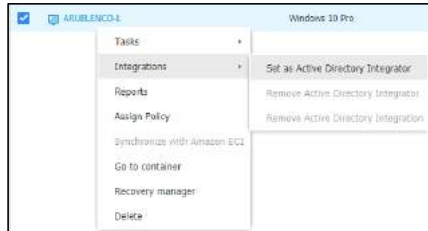
35

# GravityZone Basics Handbook

[Back to Index](#)

## ACTIVE DIRECTORY INTEGRATION CONFIGURATION

The integration allows GravityZone to import the computer inventory from Active Directory (AD). This way, you can easily deploy and manage protection on Active Directory endpoints. Integration is performed through a managed endpoint called Active Directory Integrator.



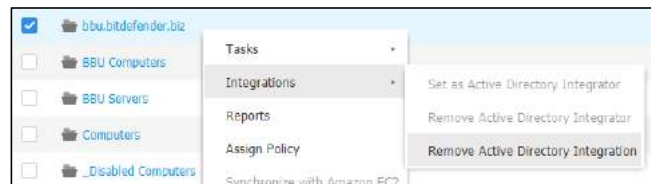
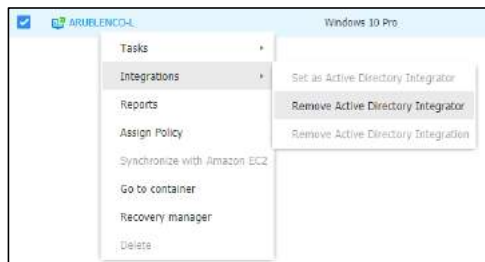
Bitdefender®

35

[Back to Index](#)

## ACTIVE DIRECTORY INTEGRATION CONFIGURATION

Removing the Integrator and Integration.



Bitdefender®

37

# GravityZone Basics HandBook



38

## Policies

Bitdefender protection can be configured and managed from Control Center using security policies.

- A policy specifies the security settings to be applied on target network inventory objects (computers, virtual machines or mobile devices).
- After installation, network inventory objects are assigned the default policy, which is preconfigured with the recommended protection settings.

**You cannot modify or delete the default policy. You can only use it as a template for creating new policies.**

Bitdefender®

39

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## POLICIES

### FEATURES

- Policies can inherit several modules settings from other policies
- You can configure policy assignment to endpoints so that a policy can apply only in certain conditions, based on location or logged-in user. Therefore, an endpoint can have multiple policies assigned to it but only one active policy at one time
- You can assign a policy to individual endpoints or to groups of endpoints
- The policy applies only to the installed protection modules

Bitdefender®

40

[Back to Index](#)

## POLICIES

### ASSIGNMENT

Assignment	Options	Description	Priority
Rule-based	Location	IP, Gateway Address, WINS Server Address, DNS Server Address, DHCP connection DNS suffix, Endpoint can resolve host, Endpoint can connect to GravityZone, Network type, Hostname	1 or 2
	Users	Active Directory Users	1 or 2
Device-based	Directly	Assigned directly to endpoints or groups of endpoints	3

The priority for Rule-based policies can be changed in the Policies → Assignment Rules section

Bitdefender®

41

# GravityZone Basics Handbook

[Back to Index](#)

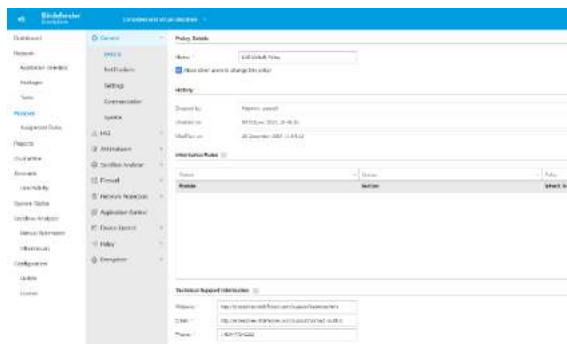
## POLICIES

### COMPUTERS AND VIRTUAL MACHINES

Allow you to configure the **Endpoint Security Tools** settings:

- General (display, update settings and uninstall password)
- Antimalware (ATC, real-time protection and on-demand scan settings and HyperDetect)
- Firewall (IDS settings)
- Network Protection
- Application Control (only Elite and Enterprise)
- Device Control
- Sandbox Analyzer (only Elite, Ultra and Enterprise)
- Relay
- Exchange Protection (not available in BS)
- HVI (only Elite and Enterprise)
- Patch Management (add-on license key)
- Encryption (add-on license key)
- Storage Protection (add-on license key OP)

Bitdefender®



Policies – New Policy Template

42

[Back to Index](#)

## POLICIES

### COMPUTERS AND VIRTUAL MACHINES

Policy Section	Settings
General Settings	Inheritance rules
	Pop-up notifications, status alerts
	Uninstall password, Power User password, Proxy Configuration
	Endpoint communication assignment
	Update settings
Antimalware	On-access scan, Advanced Threat Control, On-Demand scan
	Device scanning, Hyper Detect, Advanced Anti Exploit
	Quarantine, Exclusions
	Security Server assignment
Firewall	Block Port Scans, ICS, IDS
	Networks, Adapters
	Firewall Rules

Bitdefender®

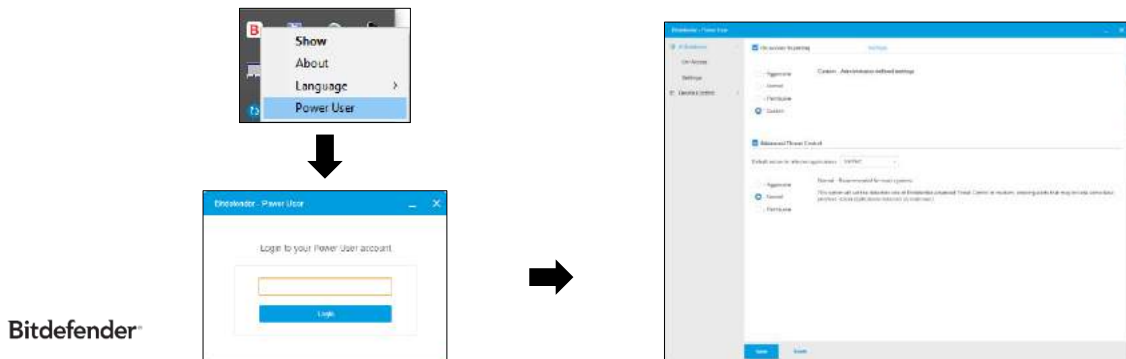
43

# GravityZone Basics Handbook

[Back to Index](#)

## BEST POWER USER

- Control Center administrators can grant Power User rights to endpoint users via policy settings
- The Power User module enables administration rights at user level, allowing the endpoint user to access and modify security settings via a local console.
- Control Center is being notified when an endpoint is in Power User mode and the Control Center administrator can always overwrite local security settings.



44

[Back to Index](#)

## POLICIES COMPUTERS AND VIRTUAL MACHINES

Policy Section	Settings
Network Protection	Traffic Scan Settings
	Web access control and Applications Blacklisting
	Data protection, Network Attack Defense
Application Control	Scans for applications installed on the machines
	Blacklists / Whitelists applications
Device Control	Applies blocking rules and exceptions via policy to a vast range of device types
	Can block devices such as USB Flash Drives, Bluetooth Devices, CD/DVD-Players, Storage Devices, etc.
Relay	Communication between Relays, Cloud Services and GravityZone
	Update Settings
Exchange Protection	User groups
	Antimalware filtering rules, Exclusions for Antimalware rules, On-demand scan tasks
	Antispam filtering rules
	Content Control filtering rules
	Attachment filtering rules

Bitdefender®

45

# GravityZone Basics Handbook

[Back to Index](#)

## POLICIES

### COMPUTERS AND VIRTUAL MACHINES

Policy Section	Settings
Patch Management	Patch Download Settings Automatic patch scan
Encryption	Encryption Management
EDR Sensor	Enable / Disable the EDR Sensor
Storage Protection	ICAP / Exclusions

Bitdefender®

46

[Back to Index](#)

## POLICIES

### HYPERDETECT CONFIGURATION

Hyper Detect is a feature available in the GravityZone Elite / Ultra / Enterprise, which uses specialized local machine models, behavior analysis techniques trained to spot hacking tools, exploits and malware obfuscation techniques, in the pre-execution stage:

- Targeted attack
- Suspicious file and network traffic
- Exploits
- Ransomware
- Grayware

Bitdefender®

☒ HyperDetect

This feature is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. It can be customized to suit your organization's security requirements.

Protection Level

☐ Permissive ☒ Normal ☐ Aggressive

<input checked="" type="checkbox"/> Targeted Attack	<input type="radio"/> Permissive <input checked="" type="radio"/> Normal <input type="radio"/> Aggressive
<input checked="" type="checkbox"/> Suspicious files and network traffic	<input type="radio"/> Permissive <input checked="" type="radio"/> Normal <input type="radio"/> Aggressive
<input checked="" type="checkbox"/> Exploits	<input type="radio"/> Permissive <input checked="" type="radio"/> Normal <input type="radio"/> Aggressive
<input checked="" type="checkbox"/> Ransomware	<input type="radio"/> Permissive <input checked="" type="radio"/> Normal <input type="radio"/> Aggressive
<input checked="" type="checkbox"/> Grayware	<input type="radio"/> Permissive <input checked="" type="radio"/> Normal <input type="radio"/> Aggressive

Actions ⓘ

Files:  ☐ Extend reporting on higher levels

Network traffic:  ☐ Extend reporting on higher levels

[Reset to default](#)

47

Bitdefender®

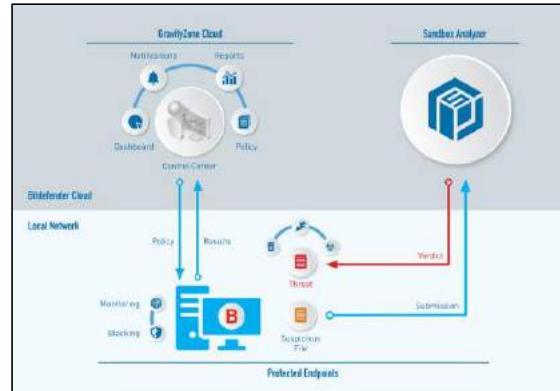
# GravityZone Basics Handbook

[Back to Index](#)

## POLICIES

### SANDBOX ANALYZER CONFIGURATION

Sandbox Analyzer provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not yet signed by Bitdefender antimalware engines.



Bitdefender®

43

[Back to Index](#)

## POLICIES

### ENCRYPTION CONFIGURATION

The Volume Encryption module allows you to provide full disk encryption by managing BitLocker on Windows machines.



Bitdefender®

44

# GravityZone Basics Handbook

[Back to Index](#)

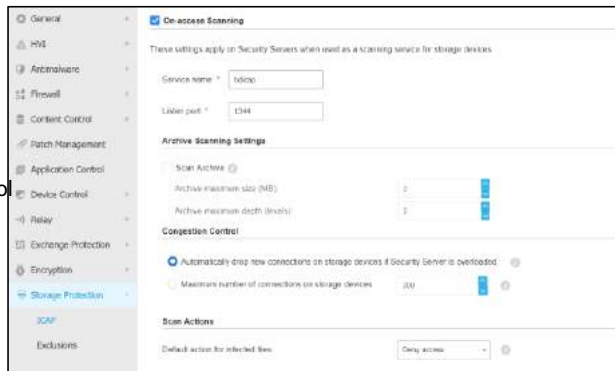
## POLICIES

### STORAGE PROTECTION

Security Servers can be configured as scanning service for network-attached storage (NAS) devices and file-sharing solutions compliant with Internet Content Adaptation Protocol (ICAP).

Exclusions can be defined:

- By hash – you identify the excluded file by SHA-256 hash.
- By wildcard – you identify the excluded file by path.



Bitdefender®

50

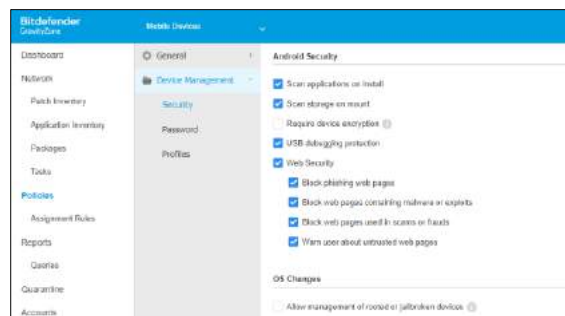
## POLICIES

### MOBILE DEVICES (ON PREMISE ONLY - NOT AVAILABLE ON BUSINESS SECURITY)

Allows you to configure the **Security for Mobile Devices** settings:

- Scan settings, storage encryption (only for Android devices)
- Compliance settings
- Password settings
- Configure Profiles
  - Push Wi-Fi and VPN settings to mobile devices
  - Enforce web access control

\*Web Security is available only for Android 5 and below.



Bitdefender®

Policies – New Policy Template

51

# GravityZone Basics Handbook

[Back to Index](#)

## POLICIES

### MOBILE DEVICES

A mobile device is declared non-compliant in the following situations:

Android devices	iOS devices
Device is rooted	Device is jailbroken
Mobile Client is uninstalled from the device	Mobile Client is uninstalled from the device
Mobile Client is not "Device Admin"	The Mobile Client profiles are removed from the device
USB Debugging is enabled	Policy not satisfied*
No location service is enabled on the device	
Malware is not removed within 24h after detection	
Policy not satisfied*	

- \* - The user does not set the lock screen password within 24h after the first notification
- The user does not change the lock screen password at the specified time
- Storage encryption required but disabled in the device (Android only)

Bitdefender®

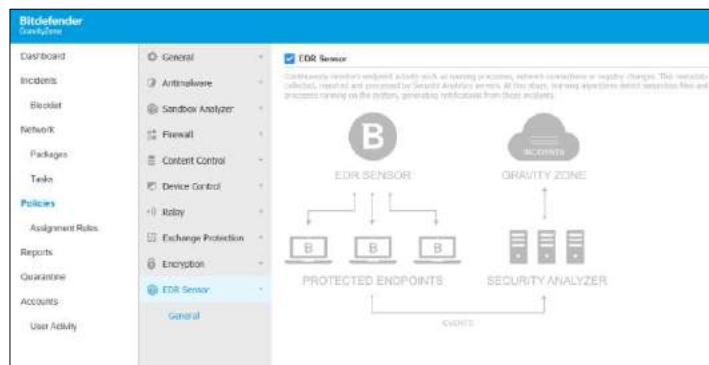
52

[Back to Index](#)

## POLICIES

### EDR SENSOR (ONLY AVAILABLE ON ULTRA SECURITY)

Allows you to enable or disable the EDR Sensor



Bitdefender®

53

# GravityZone Basics HandBook



54

Back to Index

## GravityZone Appliance (On Premise)

Delivered as a virtual appliance in the following formats:

Environment	Format
VMware vSphere, View, VMware Player	OVA
Citrix XenServer, XenDesktop, VDI-in-a-Box	XVA
Microsoft Hyper-V	VHD
Red Hat Enterprise Virtualization	OVF
Oracle VM	OVF
Kernel-based Virtual Machine or KVM	RAW

Bitdefender®

55

# GravityZone Basics Handbook

[Back to Index](#)

## GRAVITYZONE APPLIANCE

### HARDWARE REQUIREMENTS

The hardware requirements of GravityZone virtual appliance vary with the size of your network and with the deployment architecture you choose. For networks up to 3000 endpoints, you can choose to install all GravityZone roles on a single appliance, while for bigger networks, you need to consider distributing the roles among several appliances. The resources required by the appliance depend on the roles you install on it and whether or not you use Replica Set

#### Note

Replica Set is a MongoDB feature that maintains replication of the database, and ensures redundancy and high availability of the stored data.

For more details, refer to [MongoDB documentation](#) and "Managing the GravityZone Appliance" chapter of the Installation Guide (p. 98).

#### Important

The measurements are a result of Bitdefender internal tests on a basic GravityZone configuration and regular usage. Results may vary upon the network configuration, installed software, number of generated events, etc.

For custom scalability metrics, please contact Bitdefender.

Bitdefender®

56

[Back to Index](#)

## GRAVITYZONE APPLIANCE

### HARDWARE REQUIREMENTS

#### vCPU

The following table informs you of the number of vCPU each role of the virtual appliance requests. Each vCPU must be of minimum 2GHz

Component	Number of Endpoints (up to)							
	250	500	1000	3000	5000	10000	25000	50000
<b>GravityZone basic features</b>								
Update Server*	8	4	4	4	4	4	6	8
Web Console**		6	8	8	10	10	12	12
Communication Server		6	8	8	10	10	16	20
Database***		6	6	6	6	6	9	12
Total	8	22	26	26	30	30	43	52

\* Recommended when no Relays are deployed.

\*\* For each active integration, add one vCPU on the virtual appliance with Web Console role.

\*\*\* In case of distributed installation of roles, along with Replica Set: for each additional Database instance, add the specified number to the total amount.

#### Required RAM (GB)

Component	Number of Endpoints (up to)							
	250	500	1000	3000	5000	10000	25000	50000
<b>GravityZone basic features</b>								
Update Server	16	2	2	2	2	2	3	3
Web Console*		8	10	10	10	10	12	16
Communication Server		8	10	10	12	12	16	20
Database**		8	8	8	8	12	12	12
Total	16	26	30	30	32	36	43	51

\* For each active integration, add one GB RAM on the virtual appliance with Web Console role.

\*\* In case of distributed installation of roles, along with Replica Set: for each additional Database instance, add the specified number to the total amount.

Bitdefender®

57

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## GRAVITYZONE APPLIANCE EXTERNAL NETWORK COMMUNICATION

Component	Direction	Port	Destination	Description
Web Server	Outbound	443	lv2.bitdefender.com	License Validation
Update Server	Outbound	80	upgrade.bitdefender.com download.bitdefender.com	Update download

A full list of ports can be found in the below link:

<https://www.bitdefender.com/support/gravityzone-communication-ports-1132.html>

Bitdefender®

53

[Back to Index](#)

## GRAVITYZONE APPLIANCE INTERNAL NETWORK COMMUNICATION

Component	Direction	Port	Source / Destination	Description
Web Console Server	Inbound	443	Any	Admin Web Console
		4369, 6150	Communication Server	RabbitMQ Messaging
		27017	Database Server	Database Access
	Outbound	389	Domain Controller	AD Integration
		443	vCenter Server	vCenter Integration
		4369, 6150	Communication Server	RabbitMQ Messaging
Communication Server	Inbound	8443	Any	Agent Management Traffic
		4369, 6150	Web Server	RabbitMQ Messaging
	Outbound	27017	Database Server	Database Access
		4369, 6150	Web Server	RabbitMQ Messaging
Database Server	Inbound	27017	Any	Database Access
	Outbound	N/A	N/A	N/A

Bitdefender®

59

# GravityZone Basics HandBook

[Back to Index](#)

## CONTROL CENTER

### WEB CONSOLE

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Recommended screen resolution: 1280x800 or higher
- Network connectivity to the GravityZone appliance with the Web Server role installed

Bitdefender™

60

[Back to Index](#)

## ENDPOINT PROTECTION

### PHYSICAL AND VIRTUAL ENDPOINTS

Windows Operating Systems:

Workstation OS	Server OS	Tablet & Embedded OS*
Windows 10 Anniversary Update and Above	Windows Server 2016 and 2019 / Core	Windows Embedded 8.1 Industry
Windows 10 TH2	Windows Server 2012 R2	Windows Embedded 8 Standard
Windows 10	Windows Server 2012	Windows Embedded Standard 7
Windows 8.1	Windows SBS 2011	Windows Embedded Compact 7
Windows 8	Windows SBS 2008	Windows Embedded POSReady 7
Windows 7	Windows Server 2008, 2008 R2	Windows Embedded Enterprise 7
Windows Vista SP1* (EOS)*	Windows SBS 2003 (EOS)*	Windows Embedded POSReady 2009*
Windows XP SP3 (EOS)*	Windows Server 2003 R2 (EOS)*	Windows Embedded Standard 2009*
Windows XP SP2 64 bit (EOS)*	Windows Server 2003 SP1 (EOS)*	Windows XP Embedded SP2 (EOS)*
	Windows Home Server*	Windows XP Tablet PC Edition (EOS)*

\*Limited Support

Bitdefender™

61

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## ENDPOINT PROTECTION PHYSICAL AND VIRTUAL ENDPOINTS

Mac and Linux Operating Systems:

Mac OS	Linux OS
macOS Mojave (10.14.x)	Red Hat Enterprise Linux / CentOS 6.0 or higher
macOS High Sierra (10.13.x)	Ubuntu 12.04 or higher
macOS Sierra (10.12.x)	SUSE Linux Enterprise Server 11 or higher
OS X El Capitan (10.11.x)	OpenSUSE 11 or higher
OS X Yosemite (10.10.5)	Fedora 16 or higher
OS X Mavericks (10.9.5)	Debian 7.0 or higher
OS X Mountain Lion (10.8.5)	Oracle Linux 6.3 or higher

Bitdefender®

62

[Back to Index](#)

## ENDPOINT PROTECTION PHYSICAL AND VIRTUAL ENDPOINTS

On Linux systems, on-access scanning has limitations:

Kernel Version	Linux Distribution	On-access scanning support
2.6.38 or higher	All supported	On-access scanning monitors mounted network shares only under these conditions: <ul style="list-style-type: none"><li>Fanotify is enabled on both remote and local systems</li><li>The share is based on the CIFS and NFS file systems.</li></ul>
All kernels	All supported systems	On-access scanning is not supported on systems with DazukoFS for network shares mounted on paths already protected by the On-access module.
3.2 - 3.10	Ubuntu 12.04	On-access scanning is not supported.

Fanotify and DazukoFS enable third-party applications to control file access on Linux systems.

For any other distribution or kernel version you need to manually compile the DazukoFS module.

Bitdefender®

63

Bitdefender®

# GravityZone Basics HandBook

[Back to Index](#)

## ENDPOINT PROTECTION

### SUPPORTED BROWSERS

Endpoint browser security is compatible with the following browsers:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

Bitdefender™

64

[Back to Index](#)

## ENDPOINT PROTECTION

### HARDWARE REQUIREMENTS

Intel® Pentium compatible processor:

Workstation Operating Systems

- 1 GHz or faster for Microsoft Windows XP SP3, Windows XP SP2 64 bit and Windows 7 Enterprise (32 and 64 bit)
- 2 GHz or faster for Microsoft Windows Vista SP1 or higher (32 and 64 bit), Microsoft Windows 7 (32 and 64 bit), Microsoft Windows 7 SP1 (32 and 64bit), Windows 8/8.1, Windows 10
- 800 MHZ or faster for tablet & embedded OSes

Server Operating Systems

- Minimum: 2.4 GHz single-core CPU
- Recommended: 1.86 GHz or faster Intel Xeon multi-core CPU

Bitdefender™

65

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## ENDPOINT PROTECTION HARDWARE REQUIREMENTS

RAM Memory Required at Installation (MB):

OS	SINGLE ENGINE					
	Local Scanning		Hybrid Scanning		Central Scanning	
	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
Mac	1024	1024	n/a	n/a	n/a	n/a

Bitdefender®

65

[Back to Index](#)

## ENDPOINT PROTECTION HARDWARE REQUIREMENTS

RAM Memory for Daily Usage (MB):

OS	Antivirus (Single Engine)			Protection Modules				
	Local	Hybrid	Centralized	Behavioral Scan	Firewall	Content Control	Power User	Update Server
Windows	75	55	30	+13	+17	+41	+29	+76
Linux	200	180	90	-	-	-	-	-
Mac	300	-	-	-	-	-	-	-

Bitdefender®

67

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## ENDPOINT PROTECTION

### HARDWARE REQUIREMENTS

Free HDD Space:

OS	SINGLE ENGINE						DUAL ENGINE			
	Local Scanning		Hybrid Scanning		Central Scanning		Centralized + Local Scanning		Centralized + Hybrid Scanning	
	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1024	1024	400	400	250	250	1024	1024	400	400
Mac	1024	1024	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

At least 10 GB free disk space is required for entities with Bitdefender Endpoint Security Tools Relay role, as they will store all updates and installation packages locally.

At least 100 GB needed for patch management cache server.

Bitdefender®

63

[Back to Index](#)

## ENDPOINT PROTECTION

### VMWARE ENVIRONMENTS WITH VSHIELD AND NSX

Platform	RAM	Disk Space
Windows	6-16 MB (~10 MB for GUI)*	24 MB
Linux	9-10 MB	10-11 MB

\*When Silent Mode is enabled, Bitdefender Endpoint Security Tools graphical user interface (GUI) is not loaded automatically at system startup, freeing up associated resources.

Bitdefender®

64

# GravityZone Basics HandBook

[Back to Index](#)

## ENDPOINT PROTECTION

### SUPPORTED VIRTUALIZATION PLATFORMS

- VMware vSphere 6.5, 6.0, 5.5, 5.1, 5.0, 4.1 with VMware vCenter Server 6.5, 6.0, 5.5, 5.1, 5.0 or 4.1
- VMware Horizon/View 7.1\*, 6.x, 5x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 7.0, 6.5, 6.2, 6.0, 5.6 or 5.5 (including Xen Hypervisor)
- Citrix XenDesktop 7.9, 7.8, 7.7, 7.6, 7.5, 7.1, 7, 5.6, 5.5, 5.0
- Citrix XenApp 7.9, 7.8, 7.6, 7.5, 6.5
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 or Windows Server 2008 R2, 2012, 2012 R2 (including Hyper-V Hypervisor)
- Oracle VM 3.0
- **Oracle VM VirtualBox 5.2, 5.1**
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)

Bitdefender®

70

[Back to Index](#)

## ENDPOINT PROTECTION

### INTEGRATION WITH VMWARE VSHIELD ENDPOINT

- ESXi 6.0, 5.5, 5.1, 5.0 (build 474610 or higher), 4.1 (build 433742 or higher)
- vCenter Server 6.0, 5.5, 5.1, 5.0, 4.1
- vShield Manager 5.5.4-3953973 or higher
- vShield Endpoint installed by vShield Manager on the host/hosts protected by Security for Virtualized Environments
- VMware Tools 8.6.0 build 446312 or higher installed on the protected virtual machines in the complete mode or with the vShield Endpoint driver selected under VMCI in custom mode.

Bitdefender®

71

# GravityZone Basics Handbook

[Back to Index](#)

## ENDPOINT PROTECTION INTEGRATION WITH VMWARE NSX

- ESXi 5.5+ for each server
- vCenter Server 5.5+
- NSX Manager 6.2.4+
- VMware Tools 9.1.0+

Bitdefender®

72

[Back to Index](#)

## ENDPOINT PROTECTION NETWORK COMMUNICATION

Component	Direction	Port	Source / Destination	Description
BD Endpoint Security Tools	Outbound	7081	Security Server	Scanning Traffic
		7083	Security Server	Scanning Traffic over SSL
		8443	Communication Server	Management Traffic
		7074	Update Server	Update Download
		7077	Staging / Update Server	Update Download for the Staging Environment
		443	Web Server	Package Download During Install Operation
Security Server	Outbound	7074	Update Server	Update download
		8443	Communication Server	Management Traffic
	Inbound	7081	Any	Scanning Traffic
		7083	Any	Scanning Traffic over SSL

Bitdefender®

73

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR MOBILE DEVICES

### SUPPORTED PLATFORMS

Supports the following types of mobile devices and OS:

- Apple iPhone and iPad tablets (iOS 8.1+)
- Google Android smartphones and tablets (2.3+)

Mobile devices must have an active cellular data or Wi-Fi connection and connectivity with the Communication Server.

Bitdefender®

74

[Back to Index](#)

## SECURITY FOR MOBILE DEVICES

### NETWORK COMMUNICATION

Port	Usage
8443	HTTPS port used by the client to connect to GravityZone
2195, 2196, 5223	Apple Push Notification service (APNs) ports. Ports 2195 and 2196 are used by the Communication Server to communicate with the APNs servers. Port 5223 is used by managed iOS devices to communicate with the APNs servers over Wi-Fi in specific conditions.
5228, 5229, 5230	Google Cloud Messaging (GCM) ports. The Communication Server uses GCM to send push notifications to managed Android devices.

Bitdefender®

75

# GravityZone Basics Handbook

[Back to Index](#)

## Report Builder

(Only available on Enterprise Security)

Delivered as a virtual appliance in the following formats:

Environment	Format
VMware vSphere, View, VMware Player	OVA
Citrix XenServer, XenDesktop, VDI-in-a-Box	XVA
Microsoft Hyper-V	VHD
Red Hat Enterprise Virtualization	OVF
Oracle VM	OVF
Kernel-based Virtual Machine or KVM	RAW

Report Builder requires running two instances of the Report Builder Virtual Appliance, one for each role.

Bitdefender™

76

[Back to Index](#)

## REPORT BUILDER HARDWARE REQUIREMENTS

Required CPU:

Virtual Appliance	Number of Endpoints					
	250	1000	5000	10000	25000	50000
Database	4	4	4	4	6	8
Processors	6	6	6	6	6	6

Required RAM (GB):

Virtual Appliance	Number of Endpoints					
	250	1000	5000	10000	25000	50000
Database	8	8	8	8	16	16
Processors	8	8	8	8	8	8

Bitdefender™

77

# GravityZone Basics Handbook

[Back to Index](#)

## REPORT BUILDER

### HARDWARE REQUIREMENTS

Required HDD Space (GB):

Virtual Appliance	Number of Endpoints					
	250	1000	5000	10000	25000	50000
Database*	15	20	50	90	210	400
Processors**	50	200	1000	1950	4800	9500

\*disk usage is provided for events stored for one year

\*\*disk usage is provided considering 10 reports / month on average, with a subset of 15 columns each

Bitdefender®

78

## SECURITY FOR MOBILE DEVICES

### NETWORK COMMUNICATION

[Back to Index](#)

Port	Usage
8443	HTTPS port used by the client to connect to GravityZone
2195, 2196, 5223	Apple Push Notification service (APNs) ports. Ports 2195 and 2196 are used by the Communication Server to communicate with the APNs servers. Port 5223 is used by managed iOS devices to communicate with the APNs servers over Wi-Fi in specific conditions.
5228, 5229, 5230	Google Cloud Messaging (GCM) ports. The Communication Server uses GCM to send push notifications to managed Android devices.

Bitdefender®

79

# GravityZone Basics HandBook

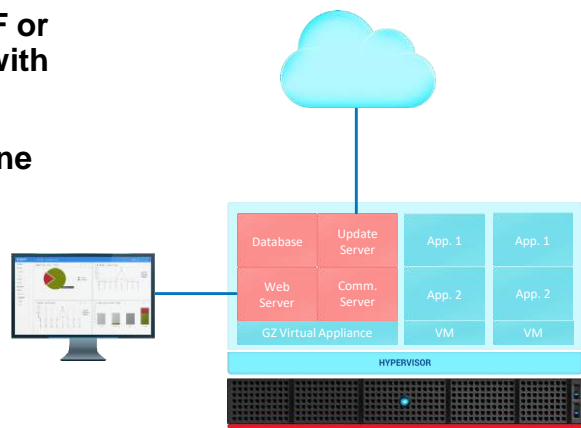
# GravityZone Appliance Deployment

[Back to Index](#)

**GRAVITYZONE™**  
THE SECURITY PLATFORM FOR  
END-TO-END BREACH AVOIDANCE

## Required Components

- **GravityZone virtual appliance**
  - available as OVA, XVA, VHD, OVF or RAW template for compatibility with the main virtualization platforms
- **Other components of the GravityZone security solutions can be remotely installed or downloaded from the Control Center**



Bitdefender®

[Back to Index](#)

# Bitdefender®

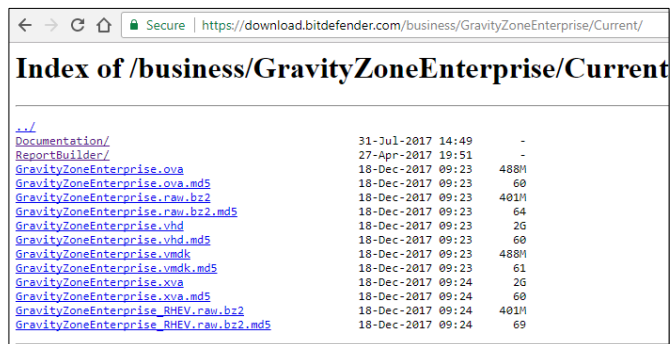
# GravityZone Basics HandBook

[Back to Index](#)

## Appliance Deployment

1. Download the GravityZone Appliance compatible with your virtualization platform:

<https://download.bitdefender.com/business/GravityZoneEnterprise/Current/>



The screenshot shows a web browser window with the address bar displaying "Secure | https://download.bitdefender.com/business/GravityZoneEnterprise/Current/". The page title is "Index of /business/GravityZoneEnterprise/Current". The main content is a table listing various download files with their sizes and dates.

File Name	Size	Date
<a href="#">./</a>	-	31-Jul-2017 14:49
<a href="#">Documentation/</a>	-	27-Apr-2017 19:51
<a href="#">ReportBuilder/</a>	-	27-Apr-2017 19:51
<a href="#">GravityZoneEnterprise.ova</a>	488M	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.ova.md5</a>	60	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.raw.bz2</a>	483M	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.raw.bz2.md5</a>	64	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.vhd</a>	26	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.vhd.md5</a>	60	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.vmdk</a>	488M	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.vmdk.md5</a>	61	18-Dec-2017 09:23
<a href="#">GravityZoneEnterprise.xva</a>	26	18-Dec-2017 09:24
<a href="#">GravityZoneEnterprise.xva.md5</a>	60	18-Dec-2017 09:24
<a href="#">GravityZoneEnterprise_RHEV.raw.bz2</a>	483M	18-Dec-2017 09:24
<a href="#">GravityZoneEnterprise_RHEV.raw.bz2.md5</a>	69	18-Dec-2017 09:24

Bitdefender®

32

[Back to Index](#)

## Appliance Deployment

2. Deploy the GravityZone virtual appliance image in your virtualized environment
  - Depending on how you prefer to distribute Control Center server roles, you will need to deploy at least one GravityZone appliance
  - Make sure this VM is configured so that it has access to the internet
  - The GravityZone VM is configured by default to get IP addresses using DHCP. Configure the DHCP Server to allocate same IP address or use static IP addresses for this VM

Bitdefender®

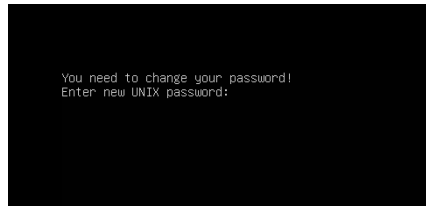
33

# GravityZone Basics HandBook

[Back to Index](#)

## Appliance Deployment

3. Power on the appliance
4. From your virtualization management tool, access the interface of the GravityZone appliance
5. Configure the password for the built-in `bdadmin` system administrator (UNIX = `bdadmin`)



GravityZone Appliance Terminal

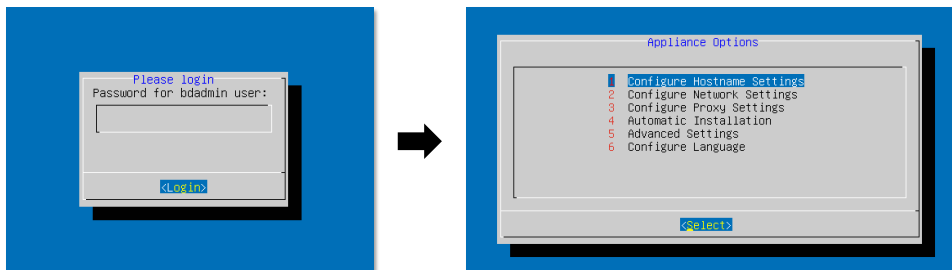
Bitdefender®

34

[Back to Index](#)

## Appliance Deployment

6. Log into the appliance using the `bdadmin`/UNIX password
7. The appliance can be configured from the Appliance Options menu



Bitdefender®

35

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER

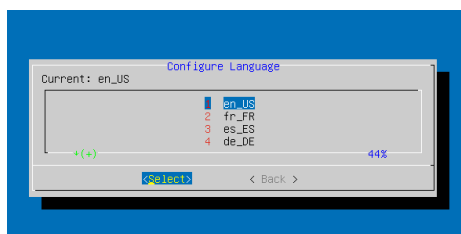
### CONFIGURE LANGUAGE

The default interface language is English.

Available languages: *English, French, Spanish, German, Polish, Romanian, Portuguese, Italian, Russian*

Changing the interface language will also change the keyboard layout accordingly!

➔ You may encounter issues specifying the password for the built-in administrator considering that this was initially configured using an English keyboard layout



Bitdefender®

35

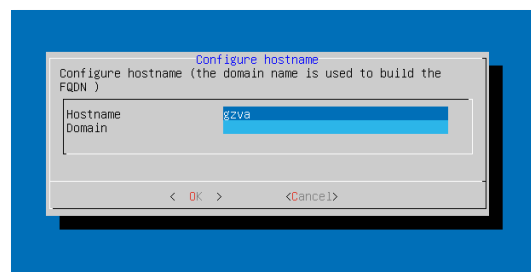
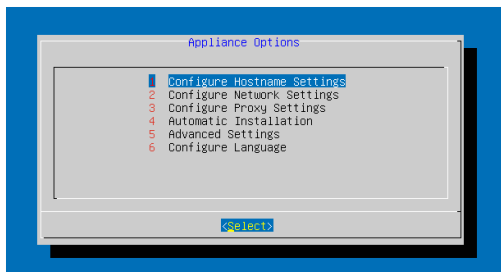
[Back to Index](#)

## CONTROL CENTER

### CONFIGURE HOSTNAME

Communication with the GravityZone roles is performed using IP address or DNS name of the appliance they are installed on.

➔ by default, GravityZone components communicate using IP addresses



Bitdefender®

GravityZone Appliance CLI – Configure Appliance Hostname

37

# GravityZone Basics Handbook

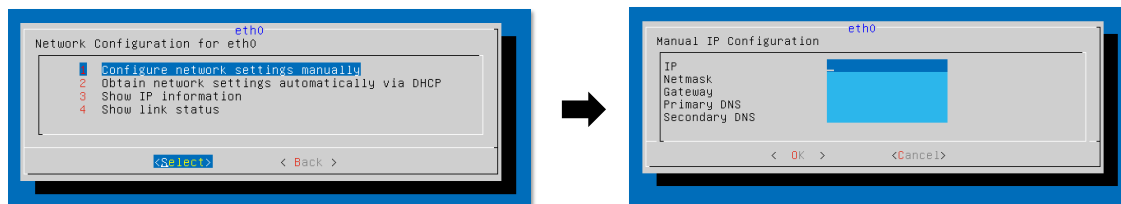
[Back to Index](#)

## CONTROL CENTER CONFIGURE NETWORK SETTINGS

The appliance is configured to automatically obtain network settings from the DHCP server

To manually configure network settings:

Go to *Configure Network Settings* → select *eth0* → choose *Configure network settings manually* → specify required information:



GravityZone Appliance CLI - Manual IP Configuration

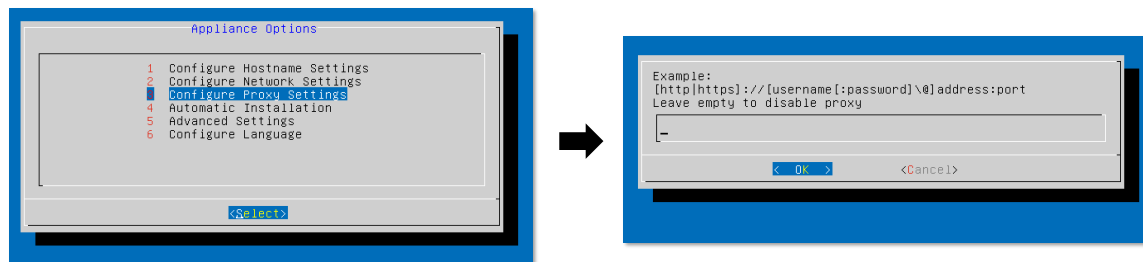
Bitdefender®

33

[Back to Index](#)

## CONTROL CENTER CONFIGURE PROXY SETTINGS

If the network configuration requires a proxy server for connecting to the internet, configure the proxy settings:



GravityZone Appliance CLI – Configure Proxy Settings

Bitdefender®

34

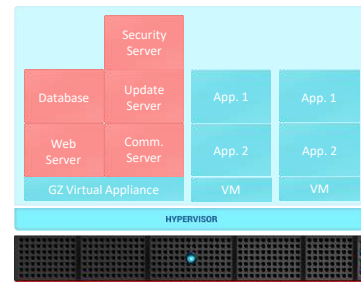
# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER AUTOMATIC INSTALLATION

### Automatic Installation:

- Installs all GravityZone Roles on the same appliance (all-in-one installation)
- The Security Server will also be installed together with the management roles on the appliance
  - ➔ available to use only if your license key allows it
- Recommended only for small environments



Bitdefender®

Automatic Installation = All-In-One Installation

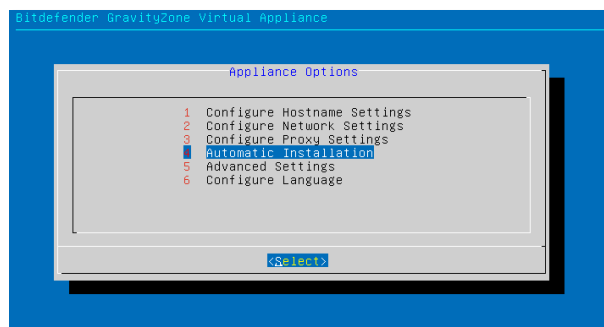
30

## CONTROL CENTER AUTOMATIC INSTALLATION

[Back to Index](#)

### Automatic Installation:

- Select *Automatic Installation* from the main menu of the appliance to start the roles installation:



Bitdefender®

GravityZone Appliance CLI – Automatic Installation

31

# GravityZone Basics Handbook

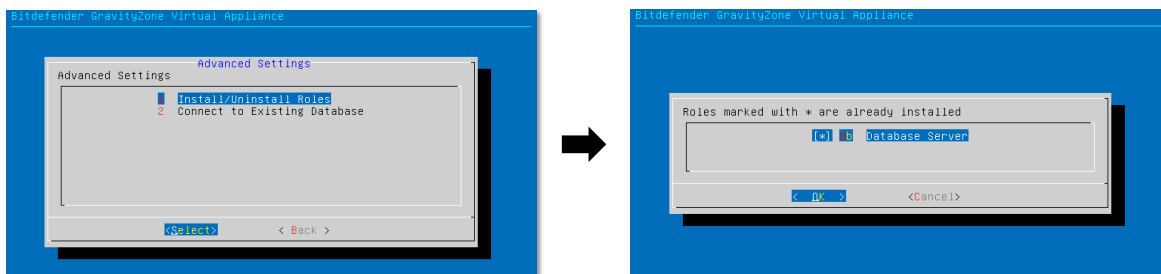
[Back to Index](#)

## CONTROL CENTER

### INSTALL GRAVITYZONE ROLES

#### Manual Installation:

- Manual installation options available under the *Advanced Settings* menu
- The first role that needs to be installed in a new GravityZone deployment is the Database server role
- A prompt to setup the database password will appear



Bitdefender®

GravityZone Appliance CLI – Database Server Installation

32

[Back to Index](#)

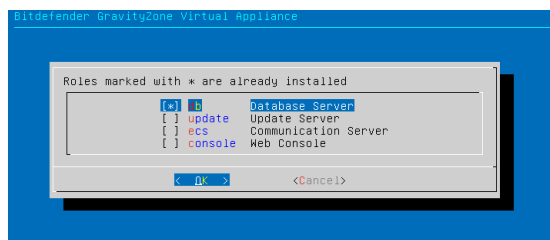
## CONTROL CENTER

### INSTALL GRAVITYZONE ROLES

#### Manual Installation:

- Once the Database Server has been installed, you can install the other roles by choosing *Add or remove roles* from the *Install / Uninstall Roles* appliance menu
- During installation, required files for the Communication Server and Web Server need to be downloaded from the internet

➔ installation takes more time if the internet connection is slow



Bitdefender®

GravityZone Appliance CLI – Install / Uninstall Roles

33

# GravityZone Basics Handbook

[Back to Index](#)

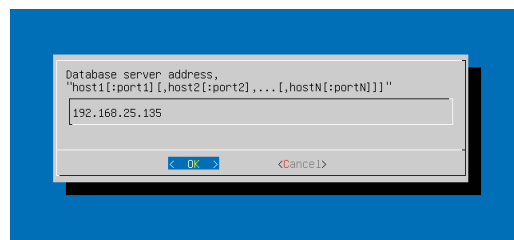
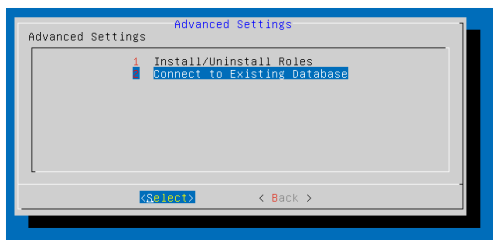
## CONTROL CENTER

### INSTALL GRAVITYZONE ROLES

Cluster Deployment (distributed roles installation):

- Install the Database Server role on the first appliance and configure all other appliances to connect to the existing database instance.

go to **Advanced Settings** → **Connect to Existing Database** in the appliance menu and enter the address of the existing database server (a prompt for the database password will appear):



Bitdefender®

GravityZone Appliance CLI – Connect to Existing Database Server

34

[Back to Index](#)

## CONTROL CENTER

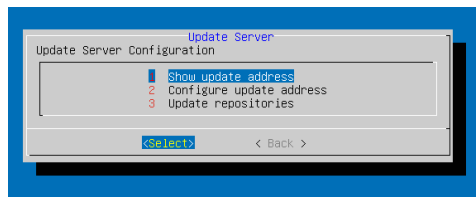
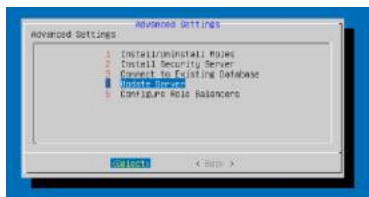
### CONFIGURE UPDATE SERVER

GravityZone virtual appliance requires Internet access for the Bitdefender repositories.

If Internet access cannot be allowed:

1. Configure a separate Bitdefender local Update Server in your organizations DMZ to mirror the repositories
2. Configure the initial GravityZone appliance to access the local Update Server configured at step 1 and download packages and their updates from there

Syntax: `http://<IP/Hostname>:7074`



Bitdefender®

35

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER

### CONFIGURE ROLE BALANCERS

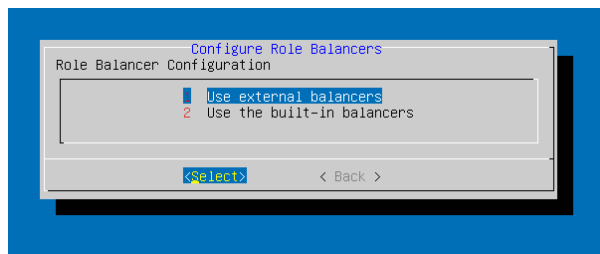
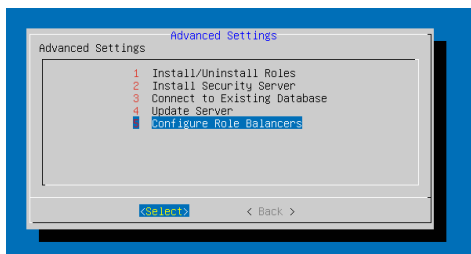
After connection to an existing database, select the *Advanced Settings* → *Configure Role Balancers* option to install built-in load balancers or to specify external balancers to be used

→ the built-in balancers cannot be installed together with other GZ roles on the same appliance

You have to specify the roles you want to balance: *Communication Server*, *Web Console* or *both*

To specify external balancers (software or hardware), use the following syntax for each role to be balanced:

`http(s)://<IP/Hostname>:<Port>`



Bitdefender®

36

[Back to Index](#)

## CONTROL CENTER

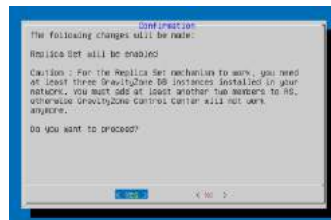
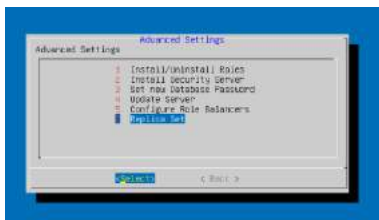
### ENABLE DATABASE REPLICICA SET

Enable the use of a database replica set instead of a single-server database instance in a distributed GravityZone Environment:

1. Install the Database Server Role on the first GravityZone appliance and enable *Replica Set*
2. Add replica set members by installing the database role to the other GravityZone instances in the same GravityZone environment

→ you need at least 3 GravityZone instances installed in your network

→ add up to seven database role instances as replica set members (MongoDB limitation)



Bitdefender®

37

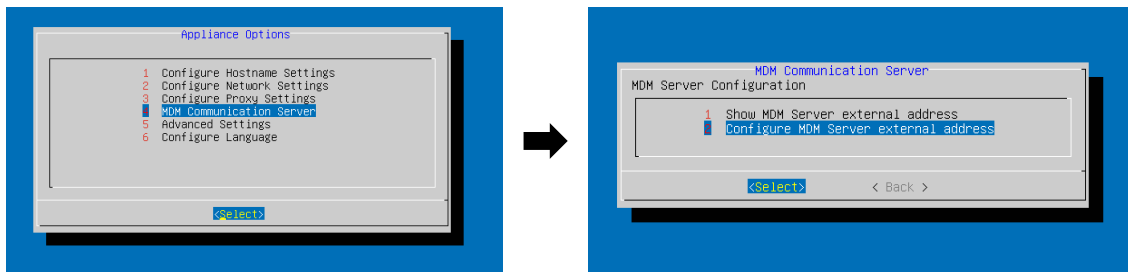
# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER MDM COMMUNICATION SERVER

To be able to manage mobile devices when they are not directly connected to the company network (via Wi-Fi or VPN), configure port forwarding on the corporate gateway for the appliance running the Communication Server role and specify the external address to be used for MDM:

`https://<IP/Domain>:<Port>`



Bitdefender®

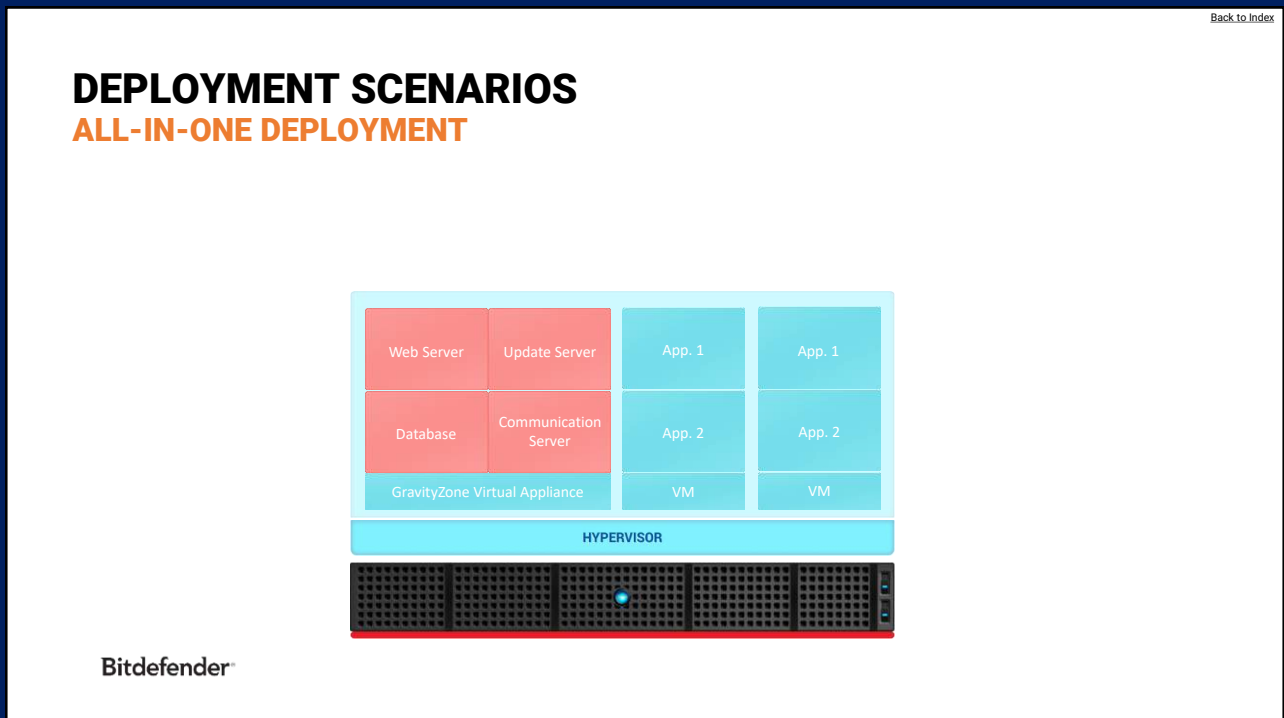
[Back to Index](#)

Bitdefender®

# GravityZone Basics HandBook



100



101

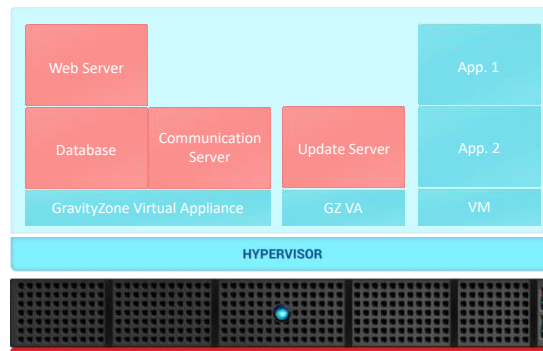
# GravityZone Basics Handbook

[Back to Index](#)

## DEPLOYMENT SCENARIOS

### STAGING

Staging is available only on GravityZone Enterprise Security



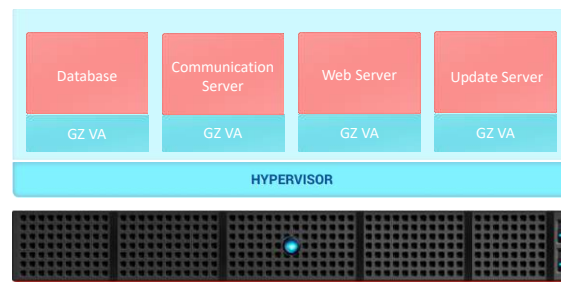
Bitdefender®

102

[Back to Index](#)

## DEPLOYMENT SCENARIOS

### CLUSTER DEPLOYMENT



Bitdefender®

103

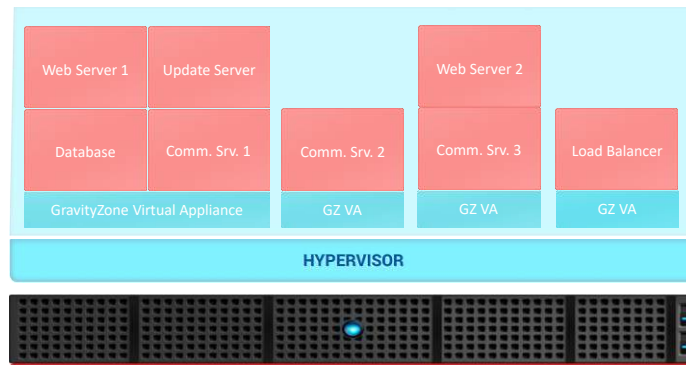
Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## DEPLOYMENT SCENARIOS

### LOAD BALANCED CLUSTER DEPLOYMENT



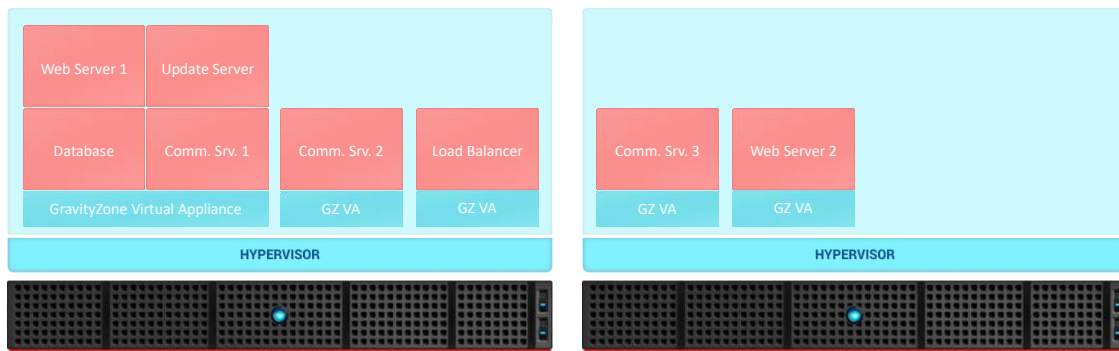
Bitdefender®

104

[Back to Index](#)

## DEPLOYMENT SCENARIOS

### CONTROL CENTER DEPLOYMENT ACROSS MULTIPLE HOSTS



Bitdefender®

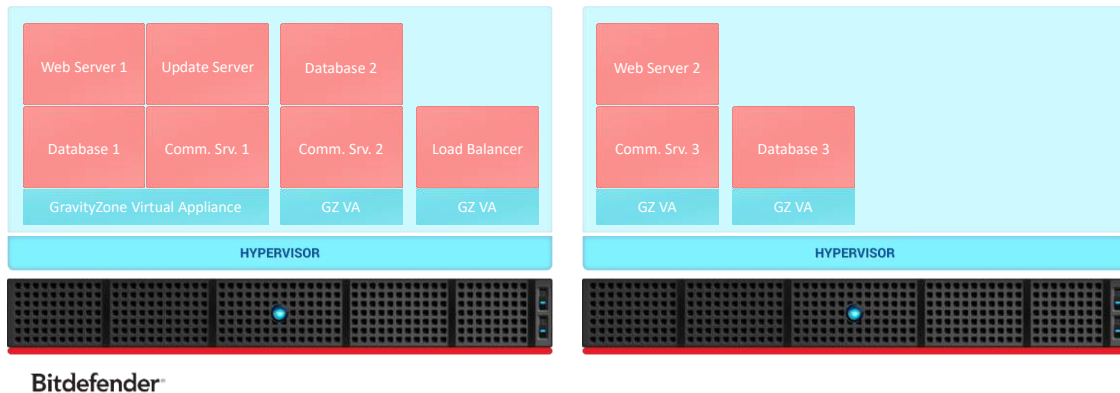
105

# GravityZone Basics Handbook

[Back to Index](#)

## DEPLOYMENT SCENARIOS

### CONTROL CENTER DEPLOYMENT WITH DATABASE REPLICA SET

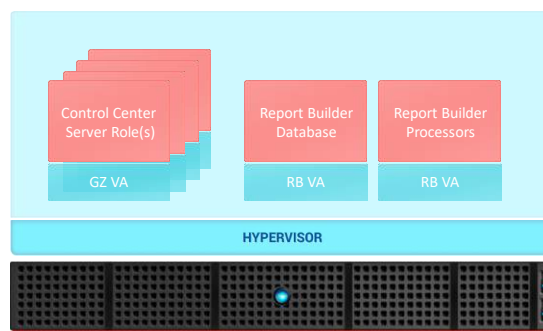


106

[Back to Index](#)

## DEPLOYMENT SCENARIOS

### CONTROL CENTER WITH REPORT BUILDER



Bitdefender®

107

# GravityZone Basics HandBook



## Control Center Configuration

108

Back to Index

## CONTROL CENTER

### INITIAL SETUP

1. Access the Control Center web interface:
  - Using a web browser, access the Control Center web interface by connecting to the IP address of the appliance with the Web Console role installed:  
`https://<IP/Hostname>`

Bitdefender®

109

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER INITIAL SETUP

2. **Authenticate to Control Center using your Bitdefender account:**
  - provides easy access to Bitdefender help & support services
  - stores your Bitdefender GravityZone license keys



The screenshot shows the 'Product Registration' window with a sidebar on the left containing 'MyBitdefender Account', 'License key', and 'Create Account'. The main area is titled 'Enter MyBitdefender Credentials' and includes fields for 'Username' and 'Password'. Below these fields is a link that says 'I don't have a MyBitdefender Account'. There is also a checkbox for 'Use offline registration' and a 'Next' button at the bottom right.

Bitdefender®

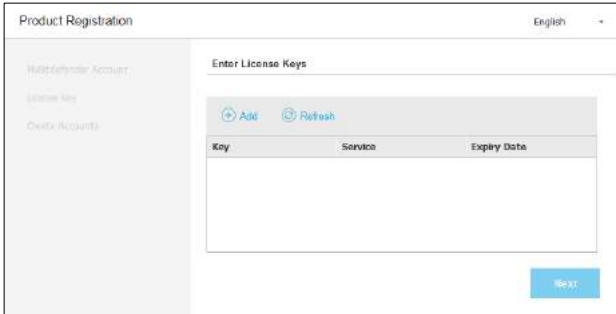
Control Center web interface – My Bitdefender authentication

110

[Back to Index](#)

## CONTROL CENTER INITIAL SETUP

3. **Provide the license keys required for validating the purchased GravityZone security services:**
  - at least one valid license key must be provided to start using GravityZone



The screenshot shows the 'Product Registration' window with the same sidebar. The main area is titled 'Enter License Keys' and features '+ Add' and '+ Refresh' buttons. Below these is a table with columns for 'Key', 'Service', and 'Expiry Date'. A 'Next' button is located at the bottom right.

Bitdefender®

Control Center web interface – Enter License Keys

111

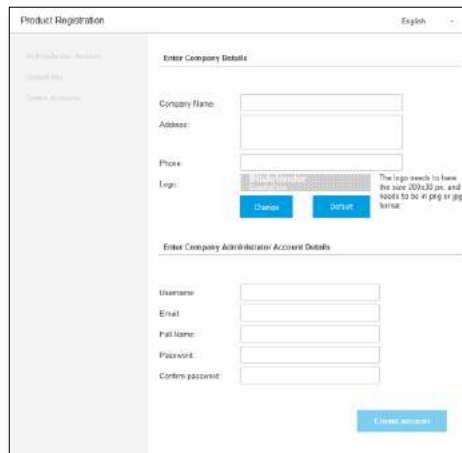
Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER INITIAL SETUP

4. Provide the company details and create a company administrator account



Bitdefender®

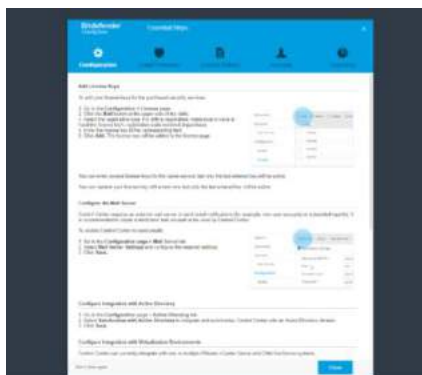
Control Center web interface – Create Accounts

112

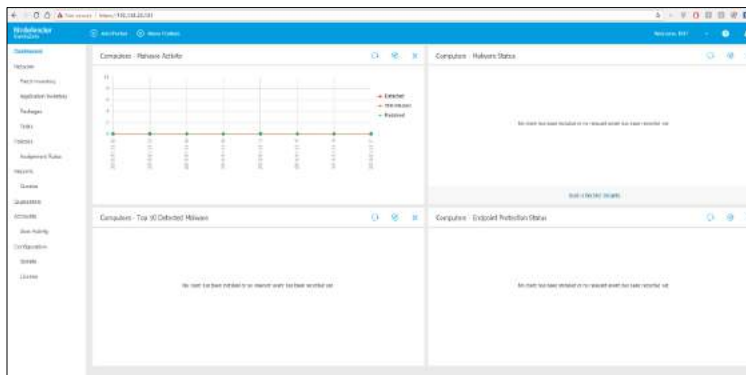
[Back to Index](#)

## CONTROL CENTER INITIAL SETUP

If needed go through the essential tips screen and the Control Center is ready to configure and use



Bitdefender®



113

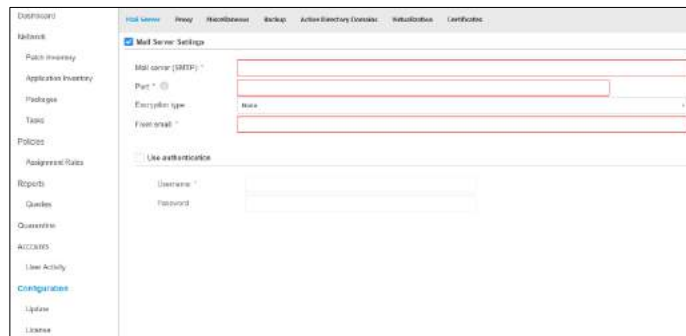
# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 1. Configure Mail Server settings:

- Specify settings for an external mail server if you want to receive e-mail notifications from Control Center

The screenshot shows the 'Mail Server Settings' page in the Bitdefender Control Center. The left sidebar contains a navigation menu with options like Dashboard, Mailbox, Patch Inventory, Application Inventory, Packages, Tasks, Policies, Assignment Rules, Reports, Quarries, Quarantine, Accounts, User Activity, Configuration (highlighted), Updates, and License. The main content area has a tabbed interface with 'Mail Server' selected. Under 'Mail Server Settings', there is a checkbox 'Use Mail Server Settings' which is checked. Below it are input fields for 'Mail server (SMTP)', 'Port', 'Encryption type' (a dropdown menu), and 'From email'. At the bottom, there is a checkbox 'Use authentication' which is unchecked, followed by 'Username' and 'Password' input fields.

Bitdefender®

Control Center web interface – Mail Server Settings

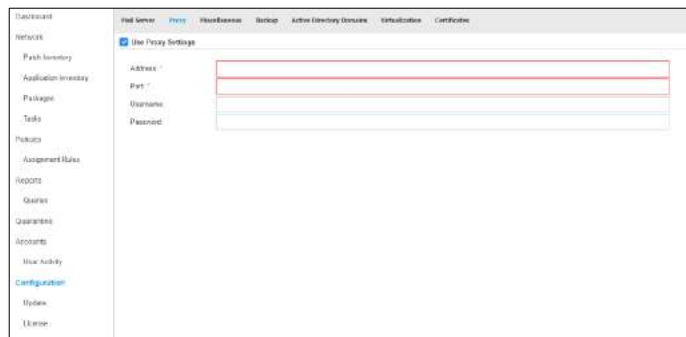
114

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 2. Configure Proxy settings:

- Specify settings for an proxy, with or without authentication

The screenshot shows the 'Proxy Settings' page in the Bitdefender Control Center. The left sidebar is identical to the previous screenshot, with 'Configuration' highlighted. The main content area has a tabbed interface with 'Proxy' selected. Under 'Proxy Settings', there is a checkbox 'Use Proxy Settings' which is checked. Below it are input fields for 'Address', 'Port', 'Username', and 'Password'.

Bitdefender®

Control Center web interface – Proxy Settings

115

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 3. Miscellaneous settings:

- What happens when an unavailable Security Server image or Endpoint Security kit is needed  
➔ **Security Server and Endpoint Security kits are not included by default in the GravityZone appliance**
- Number of concurrent deployments (default = 10)
- Basic deployment method – SSH or API
- NTP Server address (default = pool.ntp.org)  
➔ **UDP port 123 must be open**
- Syslog Server configuration  
➔ **send notifications to a logging server that uses Syslog protocol**
- Mobile push notification check

Bitdefender®

116

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 4. Backup:

- To make sure all your Control Center data are safe, backup the GravityZone database.
- You can manually run as many database backups as you want, or you can schedule periodic backups to run automatically at a specified time interval.
- Information on how to restore from backup



Bitdefender®

117

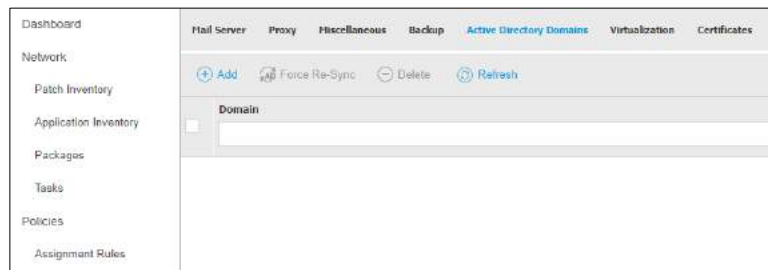
# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 5. Configure Active Directory Integration (1/2):

- If available, you can synchronize the Control Center with multiple Microsoft Active Directories



Bitdefender®

Control Center web interface – Active Directory Synchronization

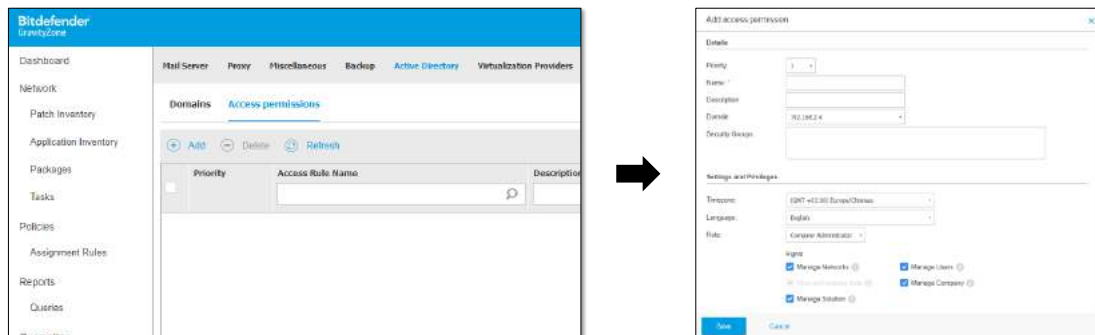
118

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 5. Configure Active Directory Integration (2/2):

- Users within the security groups specified by the access permission rules, can now access GravityZone Control Center with their domain credentials.



Bitdefender®

Control Center web interface – Active Directory Access permissions

119

Bitdefender®

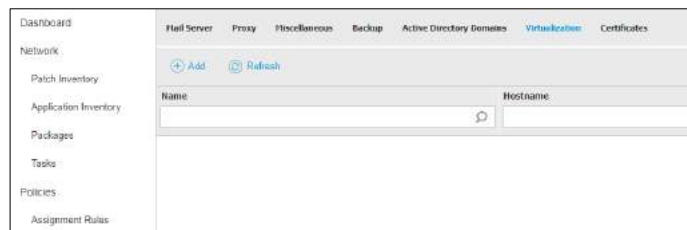
# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 6. Configure integration with virtualization management tools (1/6)

- Control Center can integrate with VMware vCenter Server, Citrix XenServer, Nutanix and Amazon EC2
- You can add multiple virtualization management tools to the Control Center (multiple vCenter Servers and XenServers)



Bitdefender®

Control Center web interface – vCenter / XenServer / Nutanix / Amazon EC2 Synchronization

120

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 6. Configure integration with virtualization management tools (2/6):

- vCenter Server integration
- Integration with VMware vShield or NSX is optional

The screenshot shows a dialog box titled 'Add vCenter Server'. It contains the following sections: 'vCenter Details' with fields for 'Name', 'Hostname/IP', and 'Port' (default 443); 'Authentication' with a checkbox 'Use credentials provided for Active Directory synchronization' and fields for 'User' and 'Password'; 'Installed platform' with radio buttons for 'None' (selected), 'vShield', and 'NSX'; and 'Additional options' with a checked checkbox 'Restrict policy assignment from the network view'. At the bottom are 'Save' and 'Cancel' buttons.

Bitdefender®

Control Center – vCenter Server integration

121

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

6. Configure integration with virtualization management tools (3/6):
  - XenServer integration

Bitdefender®

The screenshot shows the 'Add Xen Server' dialog box. It has a title bar with a close button. The dialog is divided into three sections: 'Xen Server Details', 'Authentication', and 'Options'. Under 'Xen Server Details', there are input fields for 'Name', 'Hostname', and 'Port' (which has '443' pre-filled). Under 'Authentication', there is a checkbox for 'Use credentials provided for Active Directory synchronization' (which is unchecked), and input fields for 'User' and 'Password' (with a placeholder 'Type here the password.'). Under 'Options', there is a checked checkbox for 'Restrict policy assignment from the network view'.

Control Center – XenServer integration

122

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

6. Configure integration with virtualization management tools (4/6):
  - Nutanix Prism Element

Bitdefender®

The screenshot shows the 'Add Nutanix Prism Element' dialog box. It has a title bar with a close button. The dialog is divided into three sections: 'Nutanix Server Details', 'Authentication', and 'Options'. Under 'Nutanix Server Details', there are input fields for 'Name', 'Hostname', and 'Port' (which has '9490' pre-filled). Under 'Authentication', there are input fields for 'User' and 'Password' (with a placeholder 'Type here the password.'). Under 'Options', there is a checked checkbox for 'Restrict policy assignment from the network view'.

Control Center – Nutanix Server integration

123

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 6. Configure integration with virtualization management tools (5/6):

- Amazon EC2

The screenshot shows a dialog box titled "Add Amazon EC2 Integration". It contains the following fields and sections:

- Amazon EC2 Integration Details:** A "Name:" text input field.
- Authentication:** Includes an "Information" icon and text: "Make sure that the AWS account matching the entered credentials has IAMReadOnlyAccess and AmazonEC2ReadOnlyAccess predefined permissions." Below this are "Access Key ID:" and "Secret Access Key:" text input fields. The "Secret Access Key:" field has a placeholder text "Type here the Secret Access Key".
- Options:** A checkbox labeled "Restrict policy assignment from the network view" which is checked.
- At the bottom are "Save" and "Cancel" buttons.

Control Center – Amazon EC2 integration

Bitdefender®

124

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 6. Configure integration with virtualization management tools (6/6):

- Azure

The screenshot shows a dialog box titled "Add Azure Integration". It contains the following fields and sections:

- Azure Integration Details:** A "Name:" text input field.
- Authentication:** Includes an "Information" icon and text: "To view the Azure inventory in GravityZone, the Azure app must have Reader permissions." Below this are "Active Directory ID:", "Application ID:", and "Application Secret:" text input fields. The "Application Secret:" field has a placeholder text "Type here the Application Secret".
- Options:** A checkbox labeled "Restrict policy assignment from the network view" which is checked.
- At the bottom are "Save" and "Cancel" buttons.

Control Center – Amazon EC2 integration

Bitdefender®

125

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 7. Add certificates (1/2)

- Certificates for the GravityZone communication services can be added under the Certificates tab
- Certificates can be signed by your company (self-signed) or by an external Certificate Authority (CA)
- Supported formats:
  - PEM (.pem, .crt, .cet, .key),
  - DER (.der, .cer),
  - PKCS#7 (.p7b, .p7c),
  - PKCS#12 (.p12, .pfx)

Bitdefender®

126

[Back to Index](#)

## CONTROL CENTER CONFIGURATION

### 7. Add certificates (2/2)

Certificate	Description
Control Center Security	Identify the Control Center web console as a trusted website in the web browser.
Endpoint - Security Server Communication	Ensures a secure communication between the security agents and the Security Server (Multi-Platform) they have assigned
Communication Server	Needed to secure communication between the Communication Server and iOS mobile devices
Apple MDM Push	Required to ensure secure communication between the Communication Server and the Apple Push Notifications service (APNs) servers when sending push notifications
iOS MDM Identity and Profile Signing	Used by the Communication Server to sign identity certificates and configuration profiles sent to mobile devices
iOS MDM Trust Chain	Needed to ensure that iOS mobile devices trust the Communication Server certificate and the iOS MDM Identity and Profile Signing certificate

Bitdefender®

127

# GravityZone Basics HandBook



128

Back to Index

## CONTROL CENTER UPDATE

The Update Server Role is designed to serve as the centralized update distribution point for the GravityZone deployment.

- Downloads all available GravityZone updates from the Bitdefender update servers
- GravityZone components can be configured to download all updates from the local update server instead of the internet

Bitdefender®

129

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER

### UPDATE

Check the current GravityZone version and update the GravityZone appliances (if an update is available) under the Update page → GravityZone Update tab

Current Status

Your console is up to date. [View changelog](#) [Update](#)

☐ Enable automatic update

Infrastructure

Virtual appliance	IP	Roles	Current Version	Available version	Status
gsvr	192.168.25.135	Database Server	6.3.3-6	6.3.5-1	Not updated
gsvr	192.168.25.136	Update Server	6.3.3-6	6.3.5-1	Not updated
gsvr	192.168.25.137	Communication Server	6.3.3-6	6.3.5-1	Not updated
gsvr	192.168.25.138	Web Console	6.3.3-6	6.3.5-1	Not updated

Page 1 of 1

Bitdefender®

Control Center – GravityZone Update

130

[Back to Index](#)

## CONTROL CENTER

### DOWNLOAD PACKAGES

View information about the existing GravityZone component packages under the Update page → Components tab

- Download installation packages you plan to install in your network or update existing packages

i.e.: *If you plan to protect a VMware virtualization environment with vShield, you should download the **Security Server (VMware with vShield)** package.*

*If you plan to protect a Citrix Xen virtualization environment, download the **Security Server (Citrix XenServer)** package.*

Bitdefender®

131

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER CONFIGURE UPDATE SERVER

The Update Server configuration can be edited under the Update page → Components tab → Settings

- Update Server is configured to check for and download updates from `upgrade.bitdefender.com:80`
- Updates are published in the network through port 7074

Use the following syntax when configuring clients to download updates from the local Update Server:

`<update_server_IP>:7074`

Bitdefender®

132

[Back to Index](#)

## CONTROL CENTER CONFIGURE UPDATE SERVER

By default, the Update Server downloads updates from the Internet every hour

→ **Bitdefender recommends not to change the default Update Server settings:**

The screenshot shows the 'Update Server Settings' window. On the left, four orange callout boxes point to specific settings:

- The Address where packages are downloaded from** points to the 'Packages Address' field, which contains `download.bitdefender.com/SMB/Hyd`.
- Generic update address resolved to the closest server in your region** points to the 'Update Address' field, which contains `upgrade.bitdefender.com:80`.
- Download kits automatically when needed** points to the 'Update period (hours)' dropdown, which is set to `1`.
- Act as gateway for data sent by BEST clients** points to the 'Real time malware reporting gateway role' checkbox, which is checked.

The 'Update Server Configuration' section includes the following settings:

- ☐ Enable Staging
- ☐ Automatically download security server kits
- ☐ Automatically download endpoint kits
- ☒ Real time malware reporting gateway role
- ☒ Crash submitter gateway role
- ☒ Registration server gateway role

Control Center – Update – Components – Update Settings

133

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER

### STAGING (AVAILABLE ON GRAVITYZONE ENTERPRISE ONLY)

Staging enables you to test newer kits or product updates in an enclosed and controlled environment before publishing them in your production network

- staging environment should mirror production as closely as possible for the purposes of testing
- disabled by default

Staging can be enabled under the Update page → Components → Settings

Bitdefender®

Update Server Settings

☒ Enable Staging ⓘ

Production Server Configuration

Packages Address: \* download.bitdefender.com/SMB/Hydr

Update Address: \* upgrade.bitdefender.com:80

Port: ⓘ 7074

IP: ⓘ 192.168.230.181

Update – Components – Update Settings

134

[Back to Index](#)

## CONTROL CENTER

### STAGING PREREQUISITES

1. The Update Server must be installed alone on the virtual appliance.

If you have the Update Server together with other roles on the appliance, uninstall it and reinstall it again on another GravityZone appliance

2. The Update Server appliance virtual disk must be of at least 120 GB
3. The Web Console appliance virtual disk must be of at least 120 GB

Bitdefender®

135

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER STAGING SETTINGS

The screenshot shows the 'Update Server Settings' and 'Staging Server Configuration' sections of the Bitdefender GravityZone Control Center. Callouts point to specific settings:

- Enable Staging:** A checkbox in the 'Update Server Settings' section.
- Port on which updates will be published in the staging environment:** The 'Port' field in the 'Staging Server Configuration' section, set to 7077.
- Update Server IP address:** The 'IP' field in the 'Staging Server Configuration' section, set to 192.168.230.181.
- Select if you want to automatically download and publish new kits:** A checkbox for 'Automatically download security server kits' in the 'Packages' section.
- Select if you want to automatically download product updates:** A checkbox for 'Automatically download updates' in the 'Products Update' section.

Bitdefender®

Update – Components – Update Settings

136

[Back to Index](#)

## CONTROL CENTER STAGING ACTIONS

Action	Description	Availability
Download	Get the package or update on your GravityZone appliance	Packages & Updates
Publish	Make it available for the production environment	Packages & Updates
Add to staging	Make update available to the staging / test environment*	Updates
Delete	Delete package or update from the GravityZone appliance	Packages & Updates

\*The staging / staging environment is user created

137

# GravityZone Basics HandBook

[Back to Index](#)

## CONTROL CENTER

### STAGING PACKAGES

1. Download the package you want to test on your GravityZone appliance
2. Save the package to disk
3. Configure package settings in the package configuration windows that will be displayed
4. Install the kit on testing endpoints
5. Monitor behavior
6. If the package installs successfully and the endpoints have normal behavior, publish the package to the production environment

Bitdefender®

138

[Back to Index](#)

## CONTROL CENTER

### STAGING UPDATES

**You can use staging only with updates for security agents and not Security Servers!**

1. Configure the test environment to get updates from the Staging Server:  
`<update_server_IP>:7077` (default port for staging updates)
2. Select an update you want to test
3. Download the update to your GravityZone appliance
4. Select the downloaded update and click the Add to staging action
5. Monitor behavior
6. If the update installs successfully and the endpoints have normal behavior, publish the update to the production environment

Bitdefender®

139

# GravityZone Basics HandBook



140

Back to Index

## CONTROL CENTER

### LICENSING

You will only license the GravityZone Security Services but not the Control Center or the GravityZone appliances!

GravityZone Security Services can be licensed as a bundle or separately

- At least one valid license key must be provided for using GravityZone
- Each license key will be checked on the Bitdefender servers
- If the GravityZone appliance does not have internet access you will need to use offline registration
  - ➔ offline registration code associated to the purchased license key will be provided by the Bitdefender support department with special approval from PM team.

Bitdefender®

141

# GravityZone Basics Handbook

[Back to Index](#)

## CONTROL CENTER

### LICENSING

To enter a new license key or view the current license details, go to the Configuration → License page

Licensing options:

- Subscription for 1, 2 or 3 years
- Bundle or 1 license key per security service
- Unlimited no. of units

Security Service	Licensing	Options
Security for Virtualized Environments	Per # of VMs or # of CPUs	# of VDI and # of VS or # of CPUs (sockets)
Security for Endpoints	Per # of physical Endpoints	# of Workstations and # of Servers
Security for Mobile Devices	Per # of Mobile Devices	
Security for Exchange	Per # of Mailboxes	
Add-on keys for Encryption and Patch Management		

Bitdefender®

[Back to Index](#)

Bitdefender®

# GravityZone Basics HandBook



144

Back to Index

## DASHBOARD

### PORTLETS

- The console dashboard provides you with an overview of the security status of your systems.
- Allows you to quickly identify any issues that might require your attention.
- Fully customizable portlets → users can select the target computer groups for portlets and the information to be displayed.

Bitdefender®

Computers - Windows activity

Computers - Windows applications

Computers - Windows status

Computers - Windows protection status

145

Bitdefender®

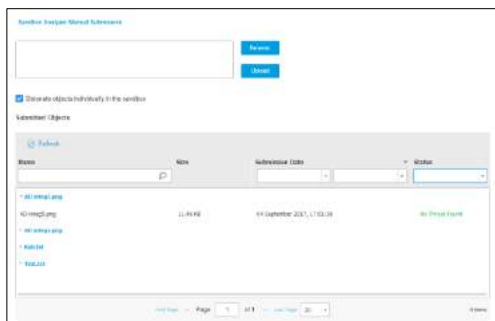
# GravityZone Basics Handbook

[Back to Index](#)

## DASHBOARD TOOLS

The Control Center provides access to the Tools area:

Sandbox Analyzer manual submission (Elite)



Bitdefender®

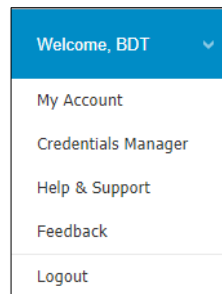
146

[Back to Index](#)

## DASHBOARD MY ACCOUNT (ON PREMISE CONSOLE VIEW)

By pointing to the username in the upper-right corner of the console, you will be able to access the options below:

- My Account
- Credentials Manager
- Help & Support
- Feedback
- Logout



Bitdefender®

147

# GravityZone Basics Handbook

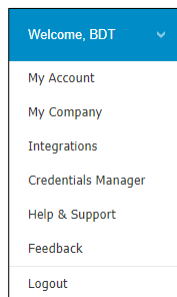
[Back to Index](#)

## DASHBOARD

### MY ACCOUNT (CLOUD CONSOLE VIEW)

By pointing to the username in the upper-right corner of the console, you will be able to access the options below:

- My Account
- My Company
- Integrations
- Credentials Manager
- Help & Support
- Feedback
- Logout



Bitdefender®

143

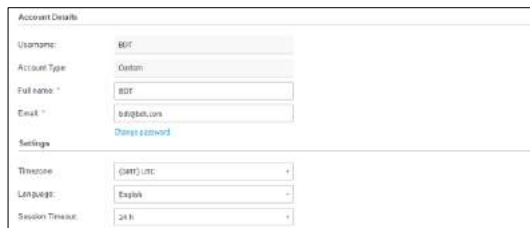
[Back to Index](#)

## DASHBOARD

### MY ACCOUNT

The account details and API keys can be configured:

- Username, Account type, Full name, Email
- Time zone, Language, Session Timeout
- API keys
- Preferences



Bitdefender®

149

# GravityZone Basics Handbook

[Back to Index](#)

## DASHBOARD

### MY COMPANY (AVAILABLE IN THE CLOUD CONSOLE ONLY)

#### Company details:

- Company details
- License key
- Partner information
- Logo
- Add-on key
- Partner change

Company Details

Company Name:

Address:

My Company ID:

Phone:

Logo:

[Change](#) [Cancel](#)

License

License Key	Expiry date	Licensed	Not licensed	Total	Available for servers	Mailboxes
<input type="text"/>	02 August 2018	4	1	10	4	0/15

Add on key:  [Add](#)

Type:  Key:  Remove:

Encryption:

Bitdefender Partner

Company Name:

ID:

Address:

Phone:

☐ Link this company to MyBitdefender (optional)

Bitdefender®

150

[Back to Index](#)

## DASHBOARD

### INTEGRATIONS (AVAILABLE IN THE CLOUD CONSOLE ONLY)

#### The GravityZone console can integrate with:

- ConnectWise
- Amazon EC2
- Microsoft Windows Defender ATP

Bitdefender GravityZone

Dashboard

Incidents

Blocklist

Network

Packages

Tasks

Policies

Assignment Rules

Reports

[Add](#) [Delete](#) [Refresh](#)

Add ConnectWise Integration

Add Amazon EC2 Integration

Add Microsoft Windows Defender ATP Integration

Bitdefender®

151

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## DASHBOARD CREDENTIALS MANAGER

Setup credentials for Operating System, Virtual Environment, Exchange

➔ Format must be username@domain when deploying through a Relay

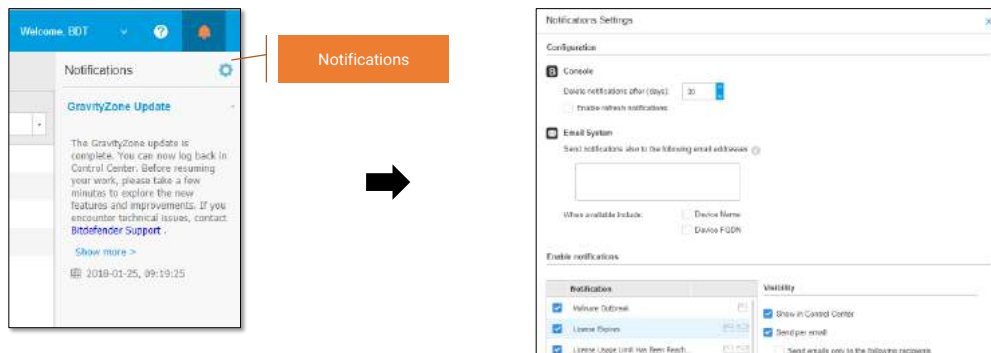
The screenshot shows the 'Credentials' section of the GravityZone dashboard. At the top, there are tabs for 'Operating System', 'Virtual Environment', and 'Exchange'. Below these is a table with columns for 'Username', 'Password', and 'Description'. The table is currently empty. At the bottom, there is a pagination bar showing 'Page 0 of 0' and 'Last Page 20'. A note at the bottom states: 'For Active Directory machines, enter the domain username as USERNAME@DOMAIN (when deploying through a relay) or DOMAIN\USERNAME, where DOMAIN is the NetBios name of the domain. For Workgroup machines, it suffices to enter only the username, without the workgroup name.'

152

[Back to Index](#)

## DASHBOARD NOTIFICATIONS

Clicking on the Notifications Bell ➔ Notifications Cogwheel, allows the user to setup the Control Center notifications



Bitdefender®

153

Bitdefender®

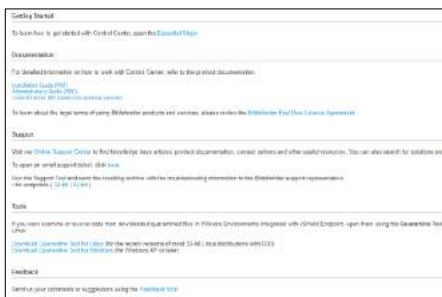
# GravityZone Basics Handbook

[Back to Index](#)

## DASHBOARD

### HELP & SUPPORT / FEEDBACK

- Documentation, Support, Tools



- Customer feedback

A screenshot of the 'New Customer Feedback' form. It includes fields for 'Full Name', 'Email', 'Phone Number', and 'Country'. There is a 'Feedback Details' section with a 'Category' dropdown, a 'Feedback for' dropdown, and a 'Comments' text area. At the bottom, there is a 'Overall Rating' section with radio buttons for 'Poor', 'Fair', 'Intermediate', 'Good', and 'Excellent'. There are 'Send' and 'Cancel' buttons at the bottom right.

Bitdefender®

154

[Back to Index](#)

## DASHBOARD

### LICENSING (CLOUD CONSOLE ONLY)

#### My Company:

- License key
- Add-on key

A screenshot of the 'License' management interface in the GravityZone dashboard. It shows a 'License Key' input field with a 'Check' button. Below this is a table with columns: 'Expiry date:', 'Licensed:', 'Not licensed:', 'Total:', 'Available for servers:', and 'Mailboxes:'. The table contains one row with values: '02 August 2018', '4', '1', '10', '4', and '0/15'. There is an 'Add-on key:' input field with an 'Add' button. Below this is a table with columns: 'Type:', 'Key:', and 'Remove:'. The table contains one row with values: 'Encryption', an empty key field, and a remove button with an 'X' icon.

Bitdefender®

155

# GravityZone Basics Handbook



156

Back to Index

## NETWORK

### NETWORK VIEW

- Computers and Virtual Machines
- Virtual Machines
- Mobile Devices
- Custom Groups
- Deleted
- Filters

The screenshot shows the Bitdefender GravityZone interface. On the left is a sidebar with a 'Network' section highlighted. The main area is titled 'Computers and Virtual Machines' and shows a list of items: 'Virtual Machines', 'Mobile Devices', 'Computers and Virtual Machines', 'Custom Groups', and 'Deleted'. On the right, there is a table with columns 'Name' and 'OS'. The table contains two rows: 'Custom Groups' and 'Deleted'.

Name	OS
Custom Groups	
Deleted	

Bitdefender®

157

# GravityZone Basics Handbook

[Back to Index](#)

## NETWORK

### NETWORK VIEW

Depending on status and type the network view will populate with the endpoints, with or without BEST installed

Managed computer, no issues

Managed computer, with issues

Managed computer, Relay

Managed virtual machine

Security Server

Managed computer, offline, with issues

Name	OS	IP	Last Seen
<input type="checkbox"/>			
<input type="checkbox"/> CLIENT05	Windows 7 Professional	192.168.230.162	Online
<input type="checkbox"/> CLIENT06	Windows 7 Professional	192.168.230.163	Online
<input type="checkbox"/> DC-01	Microsoft Windows Server 2003	192.168.230.161	Online
<input type="checkbox"/> RDVM-PC	Windows 7 Professional	192.168.230.132	Online
<input type="checkbox"/> bitdefender-sva	Linux	192.168.230.145	Online
<input type="checkbox"/> WIN-AJ1QGLBVCP2	Windows Server 2008 R2 Enterprise	192.168.230.131	13 May 2015, 15:06:03

Bitdefender®

158

[Back to Index](#)

## NETWORK

### NETWORK VIEW

Tasks are related to the GravityZone Security Services and differ based on the type of network objects

Available Tasks for each Security Service:

Computers and Virtual Machines

Virtual Machines

Mobile Devices

Scan

Patch Scan

Patch Install

Exchange Scan

Install

Uninstall client

Update client

Recover/repair client

Restart machine

Network Discovery

Applications Discovery

Update Security Server

Uninstall Custom Tool

Scan

Patch Scan

Patch Install

Exchange Scan

Install

Uninstall client

Update client

Reconfigure Client

Network Discovery

Applications Discovery

Restart machine

Install Security Server

Uninstall Security Server

Update Security Server

Install HIPS Supplemental Pack

Uninstall HIPS Supplemental Pack

Update HIPS Supplemental Pack

Uninstall Custom Tool

Lock

Unlock

Wipe

Scan

Locate

Bitdefender®

159

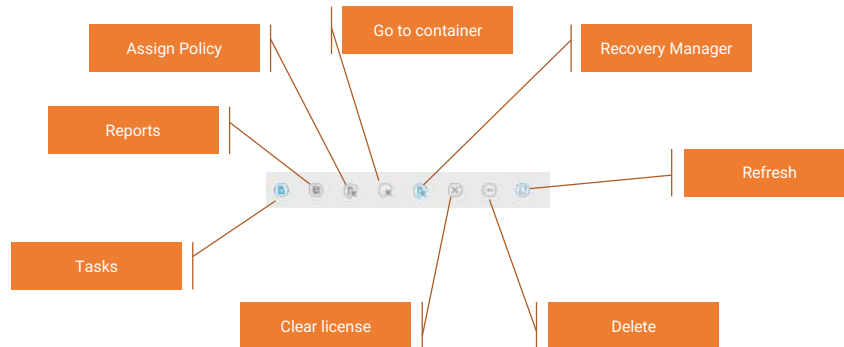
# GravityZone Basics Handbook

[Back to Index](#)

## NETWORK

### NETWORK VIEW

Network view options



Bitdefender®

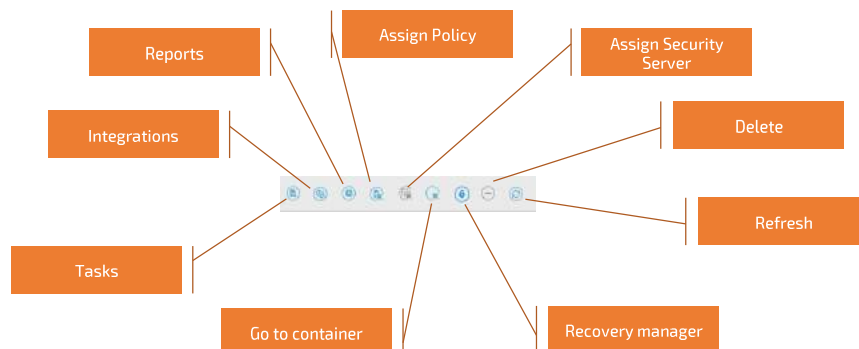
160

[Back to Index](#)

## NETWORK

### NETWORK VIEW (CLOUD CONSOLE)

Network view options



Bitdefender®

161

Bitdefender®

# GravityZone Basics HandBook



162

Back to Index

## PACKAGES

### PACKAGE VIEW

Lists the default and custom installation packages for Endpoint Security Tools and Security Server.  
Allows you to create custom installation packages according to your security requirements.

Add custom installation package

Download installation package

Dashboard	<a href="#">+ Add</a> <a href="#">+ Download</a> <a href="#">- Delete</a> <a href="#">Refresh</a>		
Network	Name	Type	Language
Patch Inventory	<input type="text"/>	<input type="text"/>	
Application Inventory	<input checked="" type="checkbox"/> BEST	BEST	English
Packages	<input type="checkbox"/> Security Server Virtual Appliance	Security Server	

Bitdefender®

163

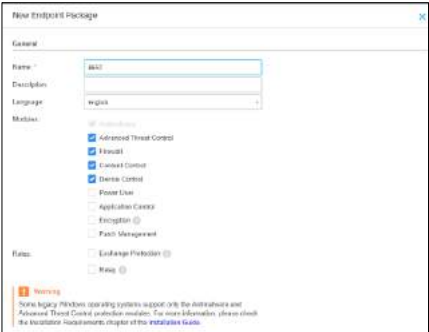
# GravityZone Basics Handbook

[Back to Index](#)

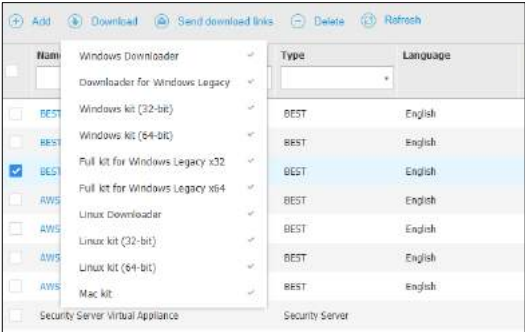
## PACKAGES

### CREATE AND DOWNLOAD

- The Add option allows the user to create the packages with specific modules, roles and settings
- The Download option allows the user to download the packages locally (Windows, Linux, MAC)



Bitdefender®



[Back to Index](#)

Bitdefender®

# GravityZone Basics HandBook



155

Back to Index

## TASKS

### TASKS

Administrative tasks can be ran remotely on network objects (computers, virtual machines or mobile devices)

View and manage tasks on the Tasks page:

Dashboard

Network

Patch Inventory

Application Inventory

Packages

**Tasks**

Policies

Restart Delete Refresh

Name	Task type	Status	Start period
<input type="checkbox"/> Restart Client 2018-01-30	Restart	Pending (0 / 1)	30 January 2018, 11:44:01
<input type="checkbox"/> Update Task 2018-01-30	Update	Pending (0 / 1)	30 January 2018, 11:43:52

Click to view execution progress

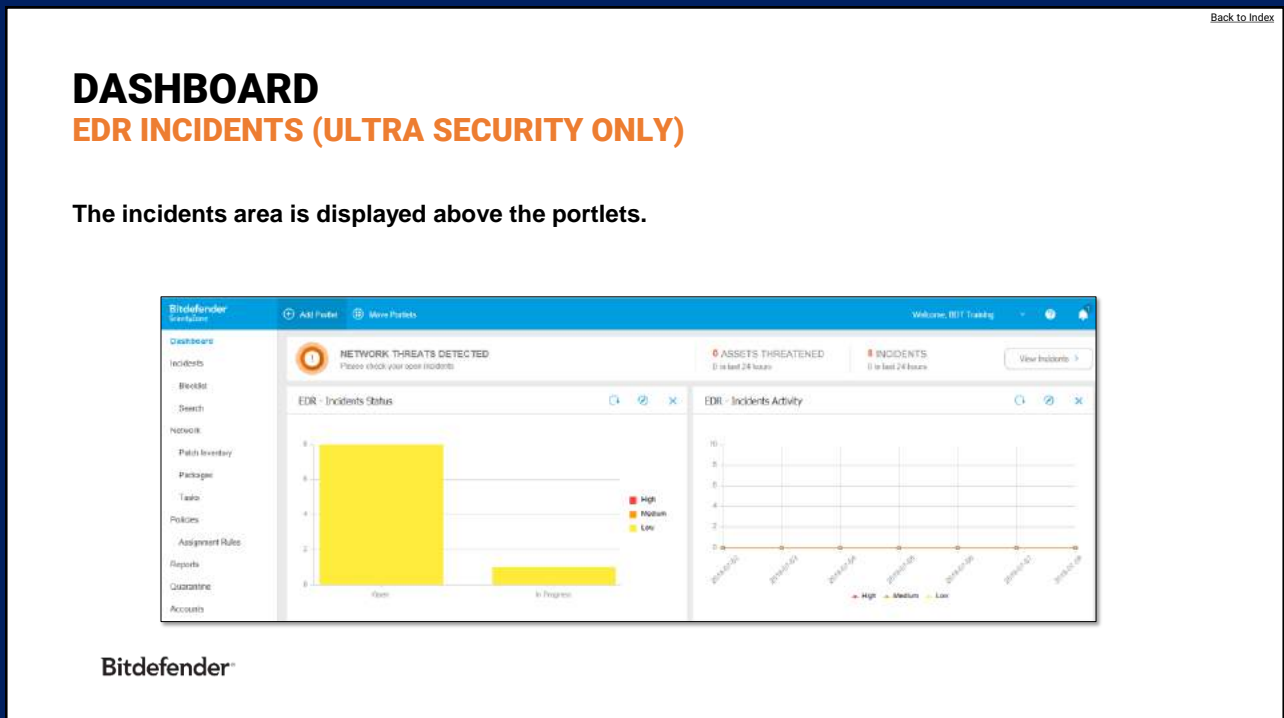
Bitdefender®

157

# GravityZone Basics HandBook



158



159

# GravityZone Basics Handbook

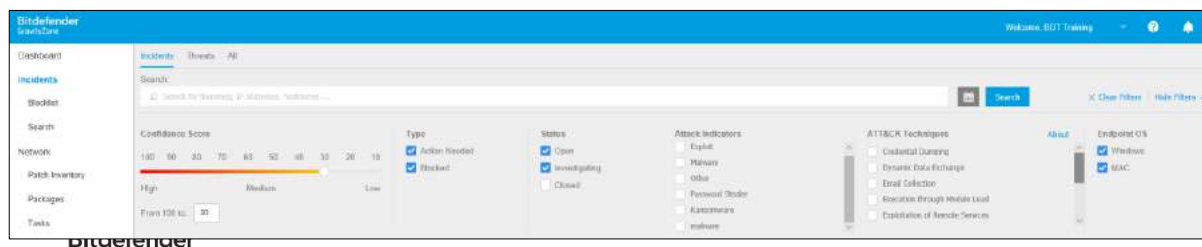
[Back to Index](#)

## INCIDENTS

### EDR

GravityZone ATS integrates layered next-gen endpoint protection and easy-to-use EDR platform to protect against even the most elusive cyber threats. It contains two major components:

- The EDR Sensor, that collects, process, and reports endpoint and application behavior data.
- The Security Analytics, a backend component used to interpret metadata collected by the EDR Sensor.



170

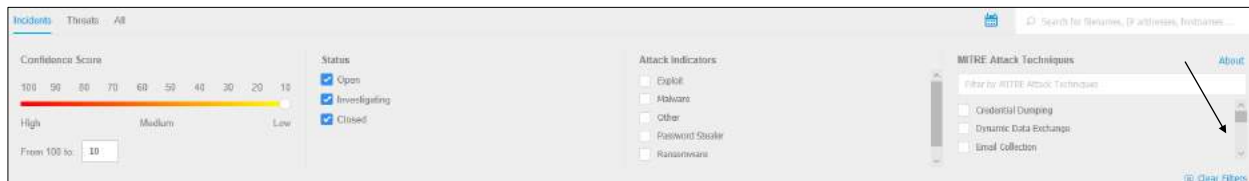
[Back to Index](#)

## INCIDENTS

### FILTER SECURITY EVENTS

The Incidents page lists security events with the following filtering options:

- **Confidence Score** - This context is based on the attack indicators, and MITRE Techniques, if applicable. The default range is set from 100 to 10.
- **Status (Open, Investigating and Closed)** - Once closed, a security event will no longer be updated.
- **Attack Indicators** - Filter security events by attack indicator. The option changes dynamically, based on the attack indicators found in the listed security events.
- **MITRE Techniques (MITRE ATT&CK knowledge base)** - Filter security by MITRE's ATT&CK knowledge base, if applicable. The options change dynamically, based on the techniques found in the listed security events
- **Search filter** - Use the search filter at the action bar to enter filenames, IP addresses, hostnames, or IOCs



Bitdefender®

\*Click **About** to open MITRE's Technique Matrix in a new tab.

171

# GravityZone Basics Handbook

[Back to Index](#)

## INCIDENTS

### EDR

- Threats - This card is triggered by minor security events that can be resolved easily.
- Incidents - This card is triggered by major security events that require your attention.

99	#10 Created at 30 Jan 2020	Blocked	View	Imported Endpoints: 1	Files and processes blocked: 157	View
Main Indicators: Malware, Ransomware : ATTACK Techniques: Collection - Email Collection						
99	#11 Created at 30 Jan 2020	Blocked	View	Imported Endpoints: 1	Files and processes blocked: 157	View
Main Indicators: Malware, Ransomware : ATTACK Techniques: Collection - Email Collection						
99	#12 Created at 30 Jan 2020	Blocked	View	Imported Endpoints: 1	Files and processes blocked: 121	View
Main Indicators: Malware, Ransomware : ATTACK Techniques: Collection - Email Collection						
99	#13 Created at 30 Jan 2020	Blocked	View	Imported Endpoints: 1	Files and processes blocked: 169	View
Main Indicators: Malware, Ransomware : ATTACK Techniques: Collection - Email Collection						

\*The cards include information such as the type of action that was performed, origin of attack, attack vectors and other indicators of compromise (IOCs) tied to the security event.

\*Remediation solutions become available based on the analyzed metadata. Furthermore, Sandbox integration allows for further investigation against security threats.

Bitdefender®

172

[Back to Index](#)

## INCIDENTS

### VIEW SECURITY EVENT DETAILS

This area provides more detailed information and remediation actions that you can take.

You can view the following information:

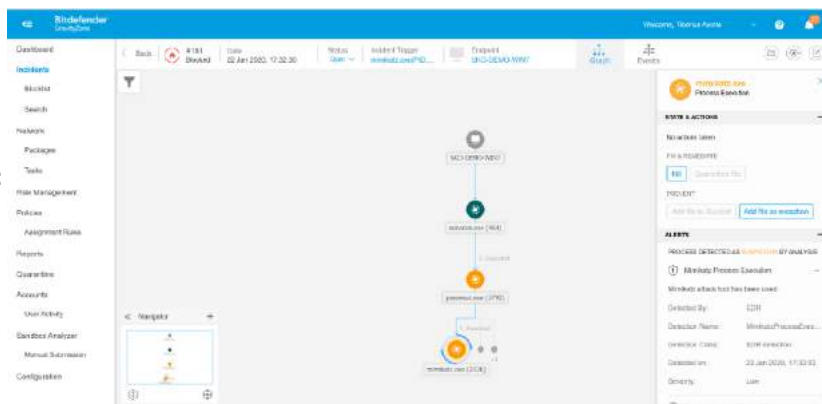
- Security event description and tags.
- Security Event Map
- Node Details

Use the following tabs

to investigate security events:

- Graph
- Events

Bitdefender®



173

# GravityZone Basics Handbook

[Back to Index](#)

## INCIDENTS

### VIEW SECURITY EVENT DETAILS

- Summary

In the Summary tab you can investigate security events and take actions. Security events are briefly described at the beginning of the tab.

- Timeline

Use Timeline to view timestamped detections in a chronological order.

- Take Action

- ✓ Quick Reaction – Kill, Quarantine or Patch Install
- ✓ Isolate - isolates the endpoint from the network while retaining communication with GravityZone services.
- ✓ Investigate - external analysis through Virus Total, Sandbox and Google
- ✓ Network Action - Add to Blocklist and Add Exception

**Note:** Actions are available if the corresponding module is also installed. Ex: Patch install requires Patch Management.

**Note:** For more details, refer to the [GravityZone Guide](#), starting from page 231.

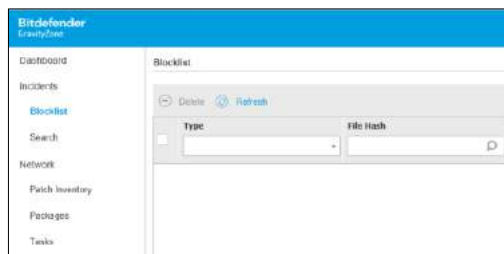
Bitdefender®

174

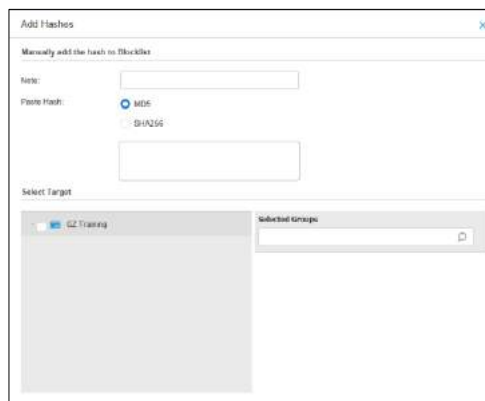
## INCIDENTS

### EDR BLOCKLIST

- View and edit blocklisted files
- Add items to the blocklist based on MD5 or SHA256 hashes for the whole company or specific targets.



Bitdefender®



[Back to Index](#)

175

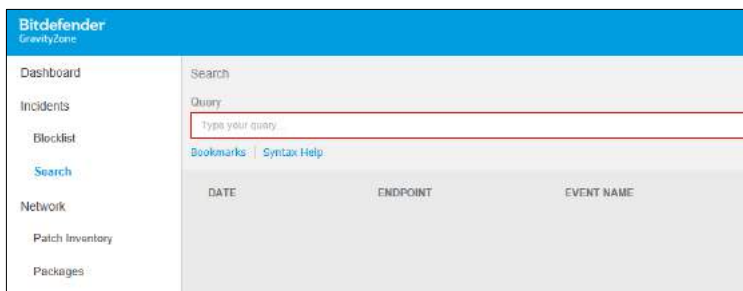
# GravityZone Basics Handbook

[Back to Index](#)

## INCIDENTS

### EDR SEARCH

The Search page allows you to go through past events based on complex criteria.



Bitdefender®

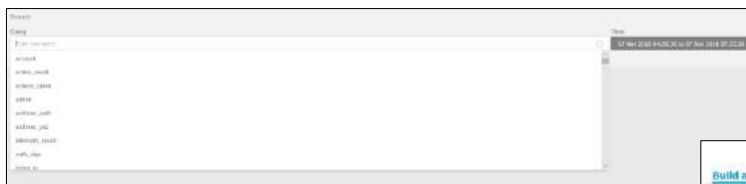
176

[Back to Index](#)

## INCIDENTS

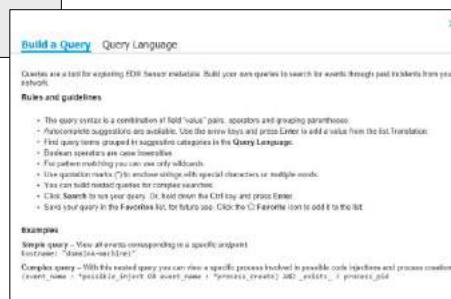
### EDR SEARCH

To view the events you are interested in, you must build queries using the query language available in GravityZone.



The query language provides the vocabulary (fields and operators) and the syntax with which you can build queries.

Bitdefender®



177

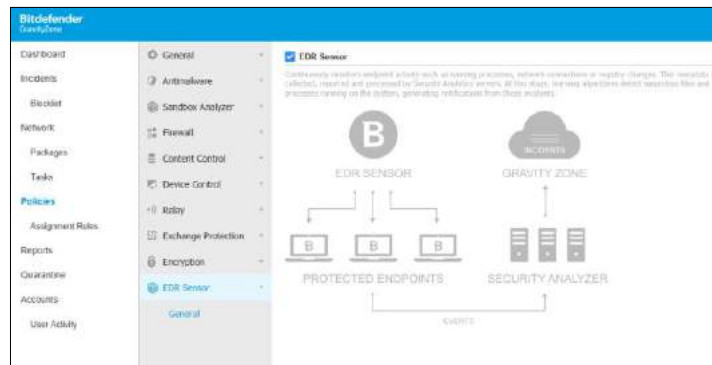
# GravityZone Basics Handbook

[Back to Index](#)

## INCIDENTS

### EDR SENSOR POLICY

Allows you to enable or disable the EDR Sensor to continuously monitor endpoint activity such as running processes, network connections or registry changes.



Bitdefender®

178

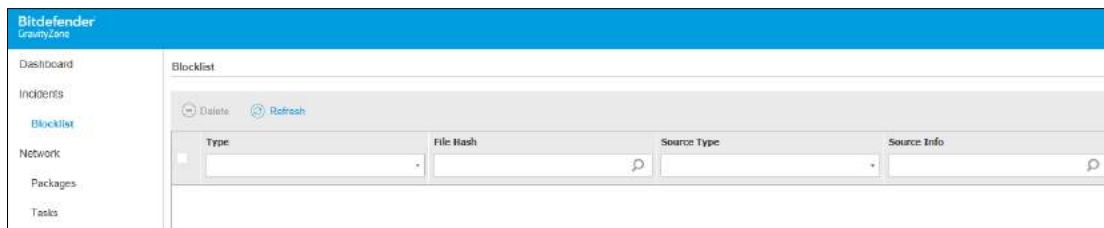
[Back to Index](#)

## INCIDENTS

### BLOCKLIST

GravityZone Ultra integrates layered next-gen endpoint protection and easy-to-use EDR platform to protect against even the most elusive cyber threats. It offers:

- Prevention
- Automated detection
- Investigation and response tools



Bitdefender®

179

# GravityZone Basics HandBook



180

[Back to Index](#)

## POLICIES

### HYPERDETECT CONFIGURATION

Hyper Detect is a feature available in the GravityZone Elite / Ultra / Enterprise, which uses specialized local machine models, behavior analysis techniques trained to spot hacking tools, exploits and malware obfuscation techniques, in the pre-execution stage:

- Targeted attack
- Suspicious file and network traffic
- Exploits
- Ransomware
- Grayware

Bitdefender®

181

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## HYPERDETECT CONFIGURATION

Hyper Detect will be installed with the FileScan and TrafficScan modules (supports HTTP and HTTPS traffic).

The installation will be made silently via product update and there is no need to reconfigure the client in order to add this new feature.

When a new GravityZone Elite license key is added in web console, the Hyper Detect feature will be visible under the Antimalware tab, by default, enabled in Report Only mode. It can be used as a visibility tool to monitor the threat activity in the organization.

The screenshot shows the 'HyperDetect' configuration window. At the top, there's a checkbox for 'HyperDetect' which is checked. Below it, a descriptive text states: 'This feature is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. It can be customized to suit your organization's security requirements.' The 'Protection Level' section has three radio buttons: 'Permissive', 'Normal', and 'Aggressive'. The 'Normal' level is selected. Below this, there's a table with four rows of threat types, each with a checkbox and three radio buttons corresponding to the protection levels. All four rows are checked, and the 'Normal' level is selected for all. The 'Actions' section has two dropdown menus for 'Files' and 'Network traffic', both set to 'Report Only'. There are also two checkboxes for 'Extend reporting on higher levels', both of which are unchecked. A 'Reset to default' button is at the bottom.

	Permissive	Normal	Aggressive
<input checked="" type="checkbox"/> Targeted Attack	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Suspicious files and network traffic	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Exploits	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Ransomware	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Grayware	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Actions ⓘ

Files: Report Only ☐ Extend reporting on higher levels

Network traffic: Report Only ☐ Extend reporting on higher levels

[Reset to default](#)

Bitdefender®

182

[Back to Index](#)

Bitdefender®

183

# GravityZone Basics Handbook



134

Back to Index

## SANDBOX ANALYZER

### OVERVIEW

The Sandbox Analyzer page provides a unified interface for viewing, filtering and searching automatic and manual submissions to the sandbox environment. The page consists in two main areas: the filters and the submission cards.

The screenshot displays the Bitdefender Sandbox Analyzer web interface. At the top, there's a search bar with a 'Search' button and a 'Select a sample' link. Below the search bar, there are several filter sections: 'Analysis Result' with radio buttons for 'Clean', 'Infected', and 'Unsupported'; 'Severity Score' with a color-coded scale from 0 to 100; 'Submission Type' with checkboxes for 'Manual' and 'Automatic'; 'Submission Status' with checkboxes for 'Final', 'Pending Analysis', and 'Failed'; and 'AT&T Technologies (selected)' with a list of specific technologies. The main area shows a list of submission cards. Each card includes a status icon (green for 'Clean'), the sample name, a severity score, a file and process hash, the submission date, the environment (e.g., 'Cloud Sandbox'), and a 'View' button. The cards are dated 'YESTERDAY' and '11 MAR 2019'.

Bitdefender®

135

# GravityZone Basics HandBook

[Back to Index](#)

## SANDBOX ANALYZER

### SUBMISSION CARDS

The submission cards are displayed by days, in reverse chronological order. Each card includes the following data:

- Analysis result
- Sample name
- Submission type
- Hash (MD5)
- ATT&CK techniques Managing Sandbox Analyzer
- Severity score
- Files and processes involved
- Submission endpoint
- Sandbox Analyzer instance (i.e. Cloud Sandbox)

Bitdefender®

136

[Back to Index](#)

## SANDBOX ANALYZER

### SUBMISSION CARDS – DETAILS

Each submission card includes a link to the behavioral analysis report, if available. To open the report, click the View button at the right side of the card.

The behavioral analysis report consists of two sections:

- Submission details – includes general information about the sample, such as name, hash, result, severity score, files and processes involved, the endpoint that submitted the sample, submission type and time.
- Behavior–displays all the security events captured during analysis

**Note:** If the analysis report is not needed anymore the submission card can be deleted from the list. The analysis data will still be available in the Sandbox Analyzer Results (Deprecated) report

Bitdefender®

137

# GravityZone Basics Handbook

[Back to Index](#)

## SANDBOX ANALYZER SUBMISSION CARDS – DETAILS

The screenshot shows the Bitdefender GravityZone interface for the Sandbox Analyzer. The top navigation bar includes the Bitdefender logo, 'GravityZone', 'Sandbox Analyzer', and a status indicator 'Infected'. The main content area is divided into two sections: 'SUBMISSION DETAILS' and 'BEHAVIOUR'.

**SUBMISSION DETAILS**

**File Info**

Filename	Smarts.exe
MDS	N/A

**General Info**

Analysis Result	Infected
Severity Score	N/A
Files and Processes Involved	N/A
Submitted From Endpoint	N/A
Environment	N/A
Submission Type	Manual
Submission Time	15.02.2016 14:48:01

**BEHAVIOUR**

The sample performs various changes on the system so it can remain hidden. Such changes include hiding files in file extensions, modifying security, notifications or system settings, deleting the origin of file, changing file attributes or other actions. Moreover, the sample creates copies on the system to ensure persistence and continue its actions for a long period of time. These files can be executable files that confuse the actions done by the sample, or configuration/storage files in which the sample can store the information required to continue the activities. The sample writes additional files on the system, which may be used to restore logs, including ensuring persistence. The new files can be executables that continue the sample's actions or storage/configuration files that hold data information for the sample. Apart from that, the sample performs certain actions over the network. This can include connecting to remote hosts or sending and reading data from different domains. The sample connects to certain domains to download files which it uses to accomplish its purpose or further infect the system.

This behavior is fulfilled through the following activity:

The original file %userprofile%\Downloads\smarts.exe connects to the domains 50.130.70.73, www.wicar.org.

Writes several files on the system. The new files can have various uses including storing sensitive information gathered by the sample or being configuration files. For this sample, the original file %userprofile%\Downloads\smarts.exe writes multiple files in the folder %userprofile%\Downloads.

Bitdefender®

189

[Back to Index](#)

## SANDBOX ANALYZER MANUAL SUBMISSION

From the Sandbox Analyzer > Manual Submission, you can send samples of suspicious objects to Sandbox Analyzer, to determine whether they are threats or harmless files.

The screenshot shows the 'Manual Submission' form in the Bitdefender GravityZone interface. The form has two tabs: 'General' and 'Settings', with 'General' selected. The 'Samples' section has a radio button for 'File' selected, followed by a text input field and a 'Browse' button. Below this is a radio button for 'URL'. The 'Detection Settings' section has a text input field for 'Command-line arguments' and a checked checkbox for 'Detect samples individually'. At the bottom is a 'Submit' button.

**Note:** Manual Submission is compatible with all web browsers required by Control Center, except Internet Explorer 9.

Bitdefender®

190

Bitdefender®

# GravityZone Basics HandBook

[Back to Index](#)

## SANDBOX ANALYZER

### MANUAL SUBMISSION

This page includes settings that apply per session, therefore you have to configure them each time you make a submission.

- **Samples**
  - **Files** - You can select up to five objects that do not exceed 50 MB together.
  - **URL** - fill in the corresponding field with any URL you want to analyze. You can submit to Sandbox Analyzer only one URL per session.
- **Detonation Settings**
  - **Command-line arguments** –The command-line arguments apply to all submitted samples during analysis.
  - **Detonate samples individually** - select the check box to have the files from bundle analyzed one by one.

Bitdefender®

190

[Back to Index](#)

## SANDBOX ANALYZER

### GENERAL SETTINGS

- **Time limit for sample detonation (minutes)** – allocate a fixed amount of time to complete the sample analysis. The default value is 4 minutes, but sometimes the analysis may take more time. If interrupted when incomplete, the analysis may contain inaccurate results.
- **Number of reruns allowed** – in case of unexpected errors, Sandbox Analyzer tries to detonate the sample as configured until completes the analysis. The default value is 2.
- **Pre-filtering** – select this option to exclude from detonation samples already analyzed.
- **Internet access during detonation** – during analysis, some samples require internet connection to complete the analysis. For best result, it is recommended to keep this option enabled.

Bitdefender®

191

# GravityZone Basics Handbook

[Back to Index](#)

## SANDBOX ANALYZER

### GENERAL SETTINGS

Upload

General Settings

Detonation configurations

Time limit for sample detonation (minutes): \*

4

Number of reruns allowed: \*

2

Pre-filtering:

☒

Internet access during detonation:

☒

Bitdefender®

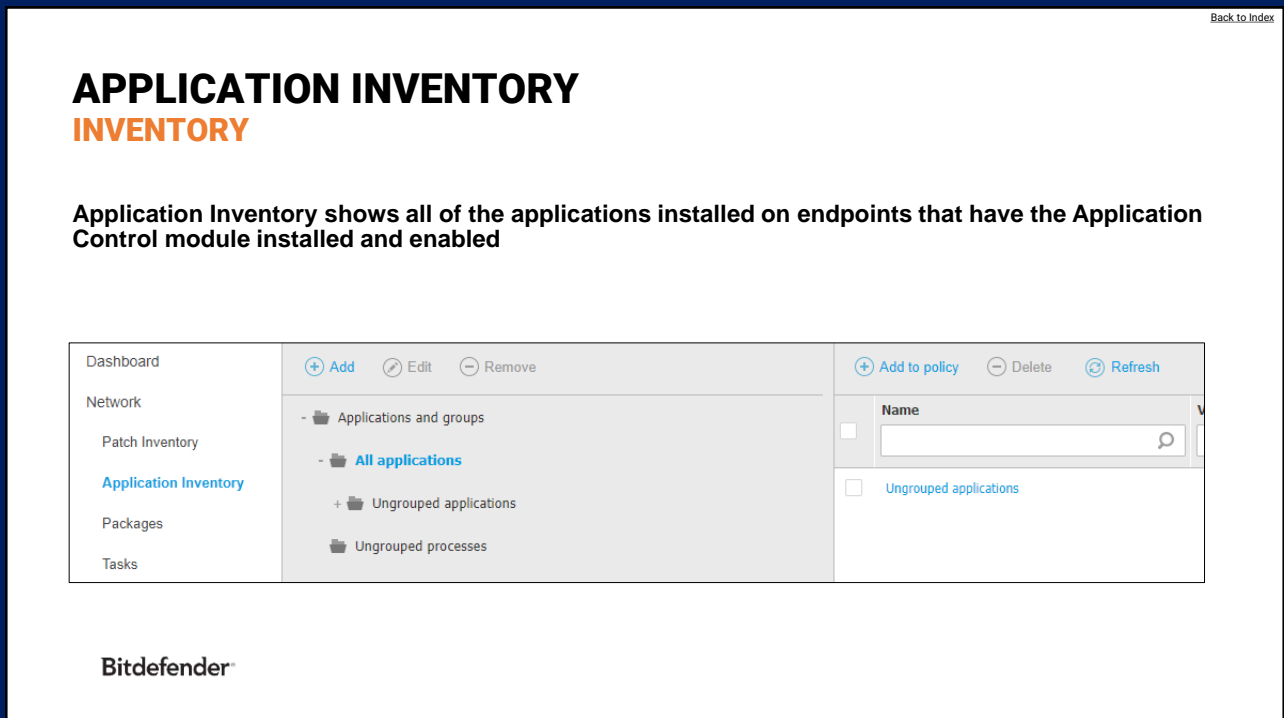
[Back to Index](#)

Bitdefender®

# GravityZone Basics HandBook



194



195

# GravityZone Basics Handbook

[Back to Index](#)

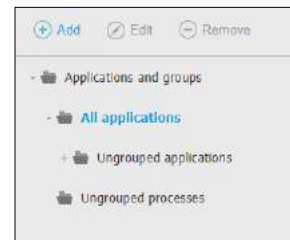
## APPLICATION INVENTORY

### APPLICATIONS

- The applications are grouped per categories
- Uncertain applications and processes are stacked in the Ungrouped Applications and Ungrouped Processes folders
- Custom folders can be created



3D Builder 1.1	3D Builder 12	12
3D Builder 1.2	3D Builder 14	14
3D Builder 1.4	64 bit driver installer 1	1
64 bit driver installer 1	7-Zip 0	0
7-Zip 0	7-Zip 15	15
7-Zip 15	7-Zip 15.08 beta (x64) 15	15
7-Zip 15.08 beta (x64) 15	7-Zip 15.14 (x64) 15	15



Bitdefender®

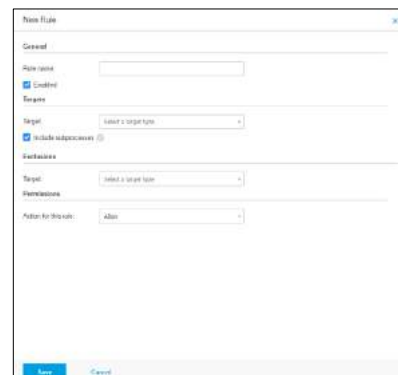
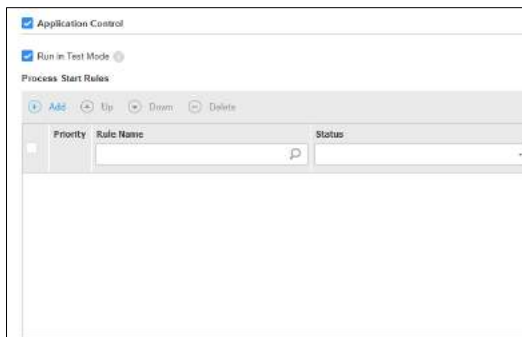
196

[Back to Index](#)

## APPLICATION INVENTORY

### APPLICATIONS

- **Test Mode** – applications are not blocked. Reports will show applications what normally would have been blocked.
- **Create rules** to block or whitelist specific applications.



Bitdefender®

197

# GravityZone Basics HandBook



## REPORTS

## CHECK NETWORK SECURITY STATUS

**Reports will be generated based on the information stored in the product database.**

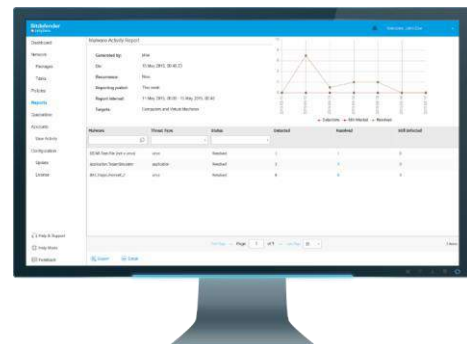
**Several different types of reports are available for each GravityZone Security Service.**

**Can be generated on-demand or scheduled to be generated later or at specific time intervals.**

- **scheduled reports can be sent by e-mail**

**Custom reporting period available.**

**Can be sent by e-mail to the administrator or exported as a \*.pdf (Report Summary) / \*.csv (Report Details).**



Bitdefender®

# GravityZone Basics HandBook



200

Back to Index

## QUARANTINE

Allows you to remotely manage quarantined files

Centralized management of quarantined files is available for:

- **Security for Endpoints:** quarantined files stored locally on each managed computer
- **Security for Exchange:** contains emails and attachments. The Antimalware module quarantines email attachments, where as Antispam, Content and Attachment Filtering quarantine the whole email.
- **Security for Virtualized Environments (Multi-Platform):** quarantined files stored locally on each managed virtual machine
- **Security for Virtualized Environments (VMware vShield or NSX):** centralized quarantine, files stored on the Security Server appliance
  - ➔ files can be deleted or downloaded to a custom path

Note: Exclusions can be automatically added for the restored items

Bitdefender®

201

# GravityZone Basics Handbook

[Back to Index](#)

## QUARANTINE

### CENTRALIZED QUARANTINE

Centralized Quarantine (policy option) sends an archived copy of each local quarantined file to a network share.

After enabling this option, each quarantined file from the managed endpoints is copied and packed in a password-protected ZIP archive to the specified network location. The archive name is the hash of the quarantined file.

☒ Centralized Quarantine

Archive password:

Click here to set the password

Confirm password:

Please re-enter password

Share Path:

Share Username:

Share Password:

Note: The archive size limit is 100 MB. If the archive exceeds 100 MB, it will not be saved on the network shared location.

Bitdefender®

202

[Back to Index](#)

Bitdefender®

203

Bitdefender®

# GravityZone Basics HandBook



204

## Accounts

You can create a custom user or add a user from Active Directory

- When adding a user from AD, user details are imported from AD and synchronized regularly
- Users log in to Control Center using AD user password

A user can have one of the following roles:

- Partner (Cloud Console only)
- Company Administrator
- Network Administrator
- Security Analyst (create, edit and delete reports)
- Custom (allows manual selection of user rights)

For every user you can restrict access to a specific GravityZone service or to specific areas of the network

Bitdefender®

205

# GravityZone Basics Handbook

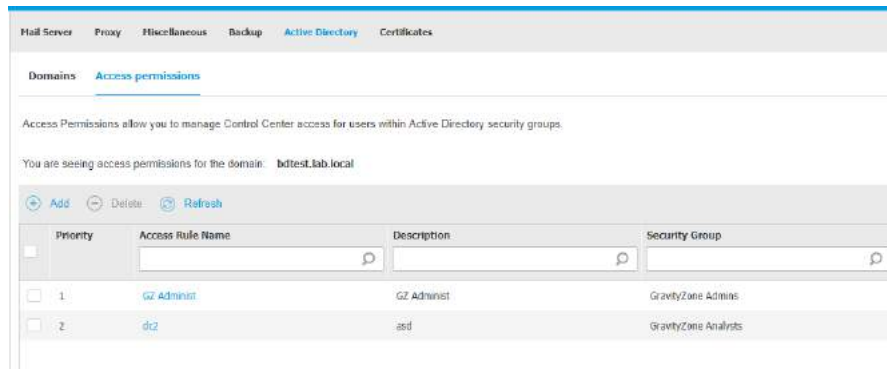
[Back to Index](#)

## User Management

### ACTIVE DIRECTORY - ACCESS PERMISSIONS

Specific to the On-Premises installation, once the integration with Active Directory is configured, access permissions rules can be created based on AD security groups.

This allows GravityZone access management directly from AD.



Bitdefender®

206

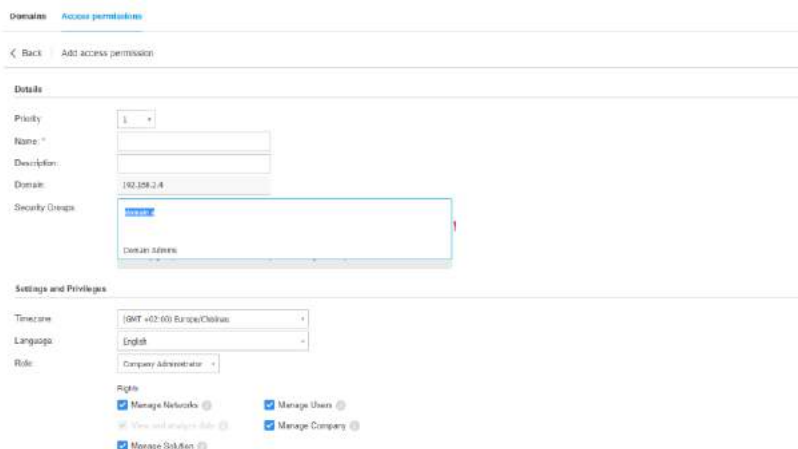
[Back to Index](#)

## User Management

### ACTIVE DIRECTORY - ACCESS PERMISSIONS

When creating a rule you need:

- To set a name
- Select a AD Security Group
- Select the roles needed
- Select the network section(s) where the access is granted



Bitdefender®

207

# GravityZone Basics HandBook

[Back to Index](#)

## ACCOUNTS

### USER RIGHTS

Account Role	Allowed Child Accounts	User Rights
Company Administrator	Company Administrators, Network Administrators, Reporter	Manage Solution Manage Company Manage Users Manage Networks Manage Reports
Network Administrator	Network Administrators, Reporters	Manage Users Manage Networks Manage Reports
Security Analyst	-	Manage Reports
Custom	Custom, depending on the selected User Rights	Custom

Bitdefender®

208

[Back to Index](#)

## ACCOUNTS

### USER RIGHTS DESCRIPTION

User Rights	Description
Manage Networks	Create and download installation packages; deploy Endpoint Security on computers, Security Server on hosts, BD Tools on VMs; manage security policies, tasks and quarantined files
Manage Users	Create, edit or delete user accounts
View and Analyze Data	Create, edit and delete reports
Manage Company	Manage the GravityZone license keys and edit your company's details
Manage Solution	Configure Control Center settings (mail server and proxy settings, integration with Active Directory and virtualization platforms, security certificates and GravityZone updates)

Bitdefender®

209

# GravityZone Basics Handbook

[Back to Index](#)

## ACCOUNTS

### USER ACTIVITY

Logs operations and actions.

Define a search using available filters to display recorded events you are interested in.

The screenshot displays the Bitdefender GravityZone Control Center interface for 'User Activity'. On the left, there is a sidebar with navigation links: Dashboard, Network, Packages, Tasks, Policies, Configuration, Update, and License. An orange box labeled 'Filters' points to the top of the table. The table has columns: User, Role, Action, Area, Target, and Created. It lists three entries for user 'jdoe' who performed 'Custom' actions in the 'Tasks' area. Below the table, there is a 'Details' section with a 'Summary' and 'More Event Information'. An orange box labeled 'Log Details' points to the 'Summary' section.

User	Role	Action	Area	Target	Created
jdoe	Custom	Created	Tasks	DC-01	14 May 2015, 15:11:22
jdoe	Custom	Created	Tasks	CLIENT06	14 May 2015, 12:30:11
jdoe	Custom	Created	Package	Endpoint Security Tools	14 May 2015, 11:39:12

**Details**

**Summary**  
jdoe created a new task Reconfigure client settings 2015-05-14.

**More Event Information**

Task Name: Reconfigure client ...  
Task Type: Reconfigure Client ...

Bitdefender®

Control Center – User Activity

210

[Back to Index](#)

## Companies

(Cloud only)

Bitdefender®

211

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## Companies

### TYPES

#### Partner Companies accounts

- Intended for companies that sell the security solution to other companies (service providers, distributors or resellers of the service)

#### Customer Companies accounts

- Intended for companies that use the security solution to protect their computer networks. Such companies can install, configure, manage and monitor their own protection.
- A customer company must be linked to at least one company administrator user account.

Bitdefender®

212

[Back to Index](#)

## Create Companies accounts

1. Access the Control Center
2. Go to Companies
3. Click Add
4. Add the Company name and fill in the other details requested
5. Under Company Settings select the company type (Partner or Customer)

Type: Partner

☒ Manage Networks

☒ Allow your partner to assist with the security management of this company

License

Type: Monthly Subscription

☒ Reserve seats 20 (40 still available)

Partner

Customer

6. Select the **license type** (*Trial, Licensed or Monthly subscription*)
7. When selecting **Licensed** you can enter an yearly key or enable "Monthly subscription". Under "Monthly subscription", partners can limit the number of seats by entering a specific number in the *Reserve seats* field.

Bitdefender®

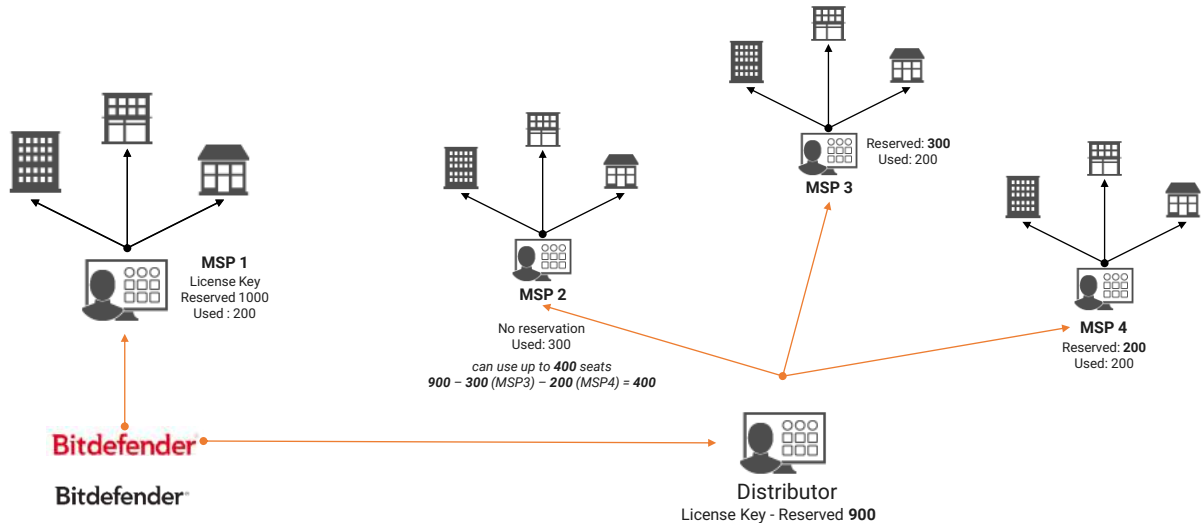
213

Bitdefender®

# GravityZone Basics Handbook

[Back to Index](#)

## MONTHLY SUBSCRIPTION RESERVE SEATS



214

[Back to Index](#)

## MONTHLY SUBSCRIPTION FEATURES

Available:

- Security Server
- GravityZone Security for Exchange
- Encryption

Not available

- Hyper Detect
- Sandboxing

Bitdefender®

215

# GravityZone Basics HandBook



216

[Back to Index](#)

## SECURITY FOR EXCHANGE

### SECURING THE MESSAGING AND COLLABORATION ENVIRONMENT

Bitdefender Security for Exchange provides antimalware, antispam, antiphishing, attachment and content filtering seamlessly integrated with the Microsoft Exchange Server.

The diagram illustrates the Bitdefender Security for Exchange architecture. At the top, there are two server icons: a desktop monitor on the left and a rack server on the right, connected by a horizontal line. Below them is a long horizontal line representing the network or data flow. Underneath this line are four server icons, each with a label: "Security for Virtualized Environments", "Security for Exchange", "Security for Endpoints", and "Security for Mobile". The "Security for Exchange" icon is highlighted with a blue border.

Bitdefender®

217

# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR EXCHANGE

### HOW PROTECTION WORKS

Filters all Exchange email traffic – incoming, outgoing and internal, regardless of the protocol or mail client used to send emails:

- Desktop clients using MAPI or POP3/SMTP (Microsoft as well as other popular mail client software)
- Mobile clients using Exchange ActiveSync
- Web access via Outlook Web App (OWA)
- Mobile access via Outlook Web App (OWA)

Additionally, allows scanning the Exchange mailbox and public folder databases for malware, by using Exchange Web Services API from Microsoft.

Bitdefender®

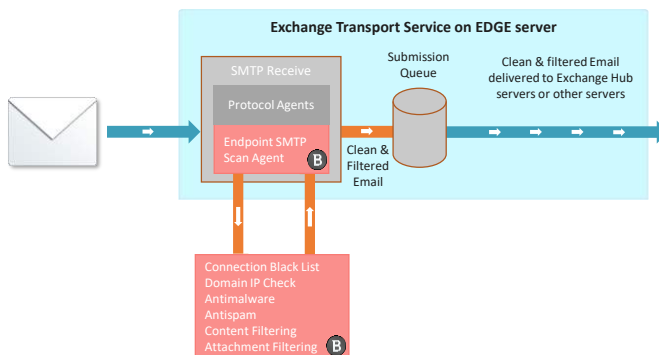
218

[Back to Index](#)

## SECURITY FOR EXCHANGE

### INTEGRATION WITH EXCHANGE TRANSPORT SERVICE

Edge Server:



Bitdefender®

219

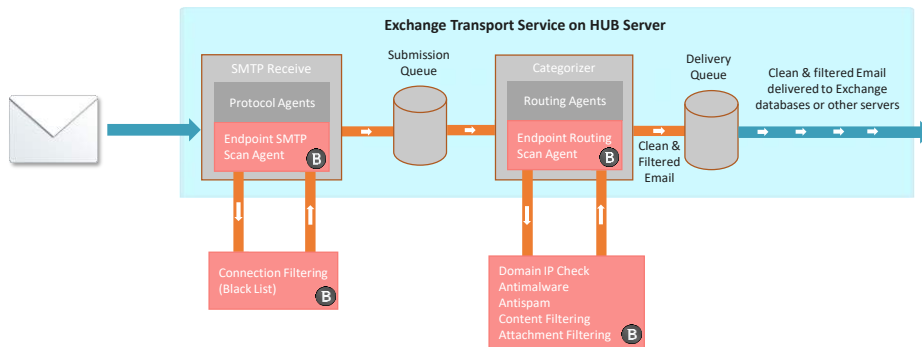
# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR EXCHANGE

### INTEGRATION WITH EXCHANGE TRANSPORT SERVICE

Hub Server:



Bitdefender®

220

[Back to Index](#)

## SECURITY EXCHANGE

### SUPPORTED MS EXCHANGE ENVIRONMENTS

Security for Exchange supports the following Microsoft Exchange versions and roles:

- Exchange Server 2019 / 2016 / 2013 with Edge Transport or Mailbox role
- Exchange Server 2010 with Edge Transport, Hub Transport or Mailbox role
- Exchange Server 2007 with Edge Transport, Hub Transport or Mailbox role

Security for Exchange is compatible with Microsoft Exchange Database Availability Groups (DAGs).

Bitdefender®

221

# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR EXCHANGE

### EXCHANGE INTEGRATION

Bitdefender Endpoint Security Tools with Exchange Protection automatically integrates with the Exchange Servers, depending on the server role. For each role only the compatible features are installed:

Features	MS Exchange 2019/2016/2013		MS Exchange 2007/2010		
	Edge	Mailbox	Edge	Hub	Mailbox
<b>Transport Level</b>					
Antimalware	✓	✓	✓	✓	
Antispam	✓	✓	✓	✓	
Content Filtering	✓	✓	✓	✓	
Attachment Filtering	✓	✓	✓	✓	
<b>Exchange Store</b>					
Antimalware On-demand scanning		✓			✓

Bitdefender®

222

[Back to Index](#)

## Exchange Protection Settings

Bitdefender Endpoint Security Tools integrates with the mail transport agents to scan all email traffic.

By default, transport level scanning is enabled. Bitdefender Endpoint Security Tools is filtering the email traffic and, if required, informs the users of the taken actions by adding a text in the email body.

Antimalware scanning is performed at two levels:

- Transport Level
- Exchange Store

Bitdefender®

223

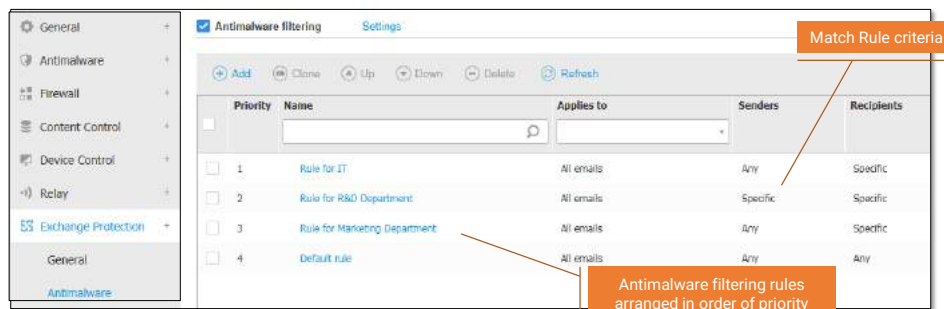
# GravityZone Basics Handbook

[Back to Index](#)

## EXCHANGE PROTECTION SETTINGS

### SCANNING AT TRANSPORT LEVEL

The antimalware filtering relies on rules. Each email that reaches the mail server is checked against the antimalware filtering rules, by order of priority, until it matches a rule. The email is then processed according to the options specified by that rule.



Policies → Exchange Protection → Antimalware Filtering Rules

Bitdefender®

224

[Back to Index](#)

## EXCHANGE PROTECTION SETTINGS

### EXCHANGE STORE SCANNING

Exchange Protection uses Exchange Web Services (EWS) from Microsoft to allow scanning the Exchange mailbox and public folder databases.

You can configure the antimalware module to run on-demand scan tasks regularly on the target databases, according to the schedule you specify.

- ➔ On-demand scanning is available only for Exchange Servers with the Mailbox role installed.
- ➔ On-demand scanning increases resource consumption and, depending on the scanning options and the number of objects to be scanned, can take considerable time to complete.

Bitdefender®

225

# GravityZone Basics Handbook

[Back to Index](#)

## EXCHANGE PROTECTION SETTINGS

### EXCHANGE STORE SCANNING

On-demand scanning requires an Exchange administrator account (service account) to impersonate Exchange users and to retrieve the target objects to be scanned from the user mailboxes and public folders.

→ It is recommended to create a dedicated account for this purpose.

The Exchange administrator account must meet the following requirements:

- It is a member of the Organization Management group (Exchange 2019, 2016, 2013 and 2010)
- It is a member of the Exchange Organization Administrators group (Exchange 2007)
- It has a mailbox attached.

Bitdefender®

226

[Back to Index](#)

## SECURITY FOR EXCHANGE

### INSTALL

To protect your Exchange Servers, you must install Bitdefender Endpoint Security Tools with Exchange Protection role on each of them.

Options to deploy Bitdefender Endpoint Security Tools on Exchange Servers:

- Local installation, by downloading and running the installation package on the server.
- Remote installation, by running an Install task.
- Remote, by running the Reconfigure Client task, if Bitdefender Endpoint Security Tools already offers file system protection on the server.

Bitdefender®

227

# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR EXCHANGE

### BUILT-IN EXCHANGE ANTIMALWARE

The built-in Exchange 2013 Antimalware agent is automatically disabled during installation of Endpoint Security Tools with Exchange Protection.

→ prevent unwanted results (inconsistent reporting, difficult to trace back what happened to a missing email)

It is also recommended to disable any other 3rd party antimalware / filtering agents installed on the server.

View installed transport agents:

- Open Exchange Management Shell on the Exchange Server and run the following command  
`Get-TransportAgent`

Bitdefender®

228

[Back to Index](#)

## SECURITY FOR EXCHANGE

### POLICY CONFIGURATION

For each of the Exchange protection settings, rules can be created and applied per user groups. The user can also choose what action should BEST take when encountering infected or suspicious files.

- General
  - User groups
  - Domain IP Check (Antispoofing)
- Antimalware
  - Antimalware filtering
  - Exclusions
- Antispam
  - Real-time Blackhole List (RBL) Settings
  - Whitelist
- Content Control
  - Content filtering
  - Attachment filtering

Bitdefender®

229

# GravityZone Basics Handbook

[Back to Index](#)

## LICENSING

### MAILBOX COUNT

GravityZone Security for Exchange protects automatically all mailboxes on the Exchange Server.

→ Your license key should cover all available mailboxes on the mail server

The protected mailboxes count shown in the license information window of the web console = mailboxes count on the Exchange Server, which can be determined by running the following command in the Exchange Management Shell:

`(Get-Mailbox).count`

```
[PS] C:\Users\Administrator\Desktop>(Get-Mailbox).count
10
[PS] C:\Users\Administrator\Desktop>_
```

*(Get-Mailbox).count Command*

Bitdefender®

230

[Back to Index](#)

Bitdefender®

231

# GravityZone Basics Handbook



232

## VOLUME ENCRYPTION CONFIGURATION

- The Volume Encryption module allows you to provide full disk encryption by managing BitLocker on Windows machines.
- You can encrypt and decrypt boot and non-boot volumes, with just one click, while GravityZone handles the entire process, with minimal intervention from the users.
- BitLocker is a full disk encryption feature included with Windows Vista and later. It is designed to protect data by providing encryption for entire volumes.
- GravityZone stores the recovery keys needed to unlock volumes when the users forget their passwords.

Bitdefender®

Note: GravityZone does not support encryption for volumes already encrypted with BitLocker, FileVault and other third-party tools. The volumes must be unencrypted when applying a GravityZone policy to encrypt them.

Note: GravityZone Encryption does not support multiple users. Only the user who encrypted the computer can log in to the system with the password he configured during the encryption process.



233

Bitdefender®

# GravityZone Basics HandBook

[Back to Index](#)

## VOLUME ENCRYPTION RECOVERY

To recover the key, you will need to identify the machine in network and use the dedicated wizard.

If the recovery is made for the boot partition, the Recovery key ID will be taken from the BitLocker prompt before boot, entered in the GZ Recovery manager and the Recovery key will be revealed.

For other partitions, the operation can be performed from Windows Explorer with right click on the partition.

Bitdefender®

234

[Back to Index](#)

Bitdefender®

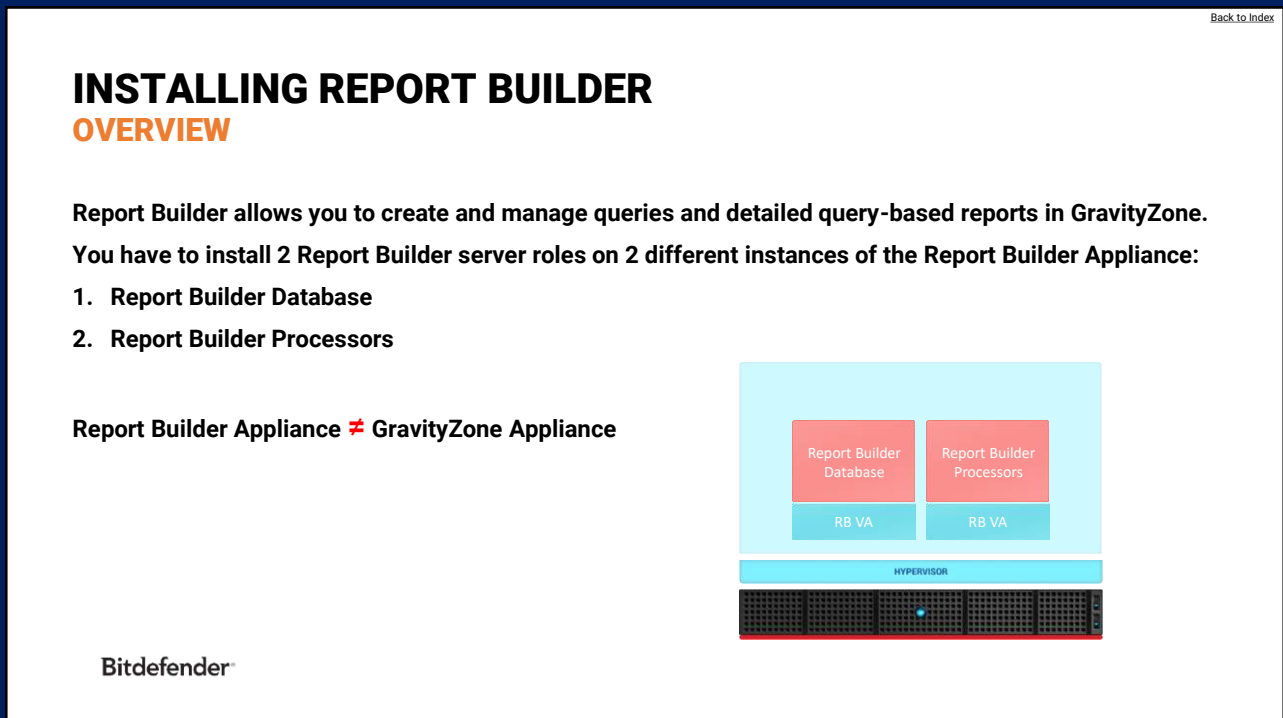
235

Bitdefender®

# GravityZone Basics Handbook



236



237

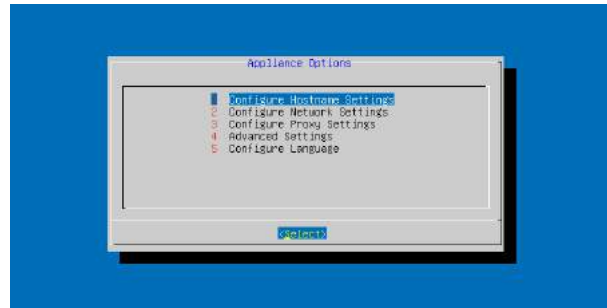
# GravityZone Basics Handbook

[Back to Index](#)

## INSTALLING REPORT BUILDER

### DATABASE

1. Import the Report Builder appliance in your virtualized environment and power it on
2. Configure password for the built-in `bdadmin` system administrator
3. Configure hostname and network settings and proxy settings if needed



Bitdefender®

GravityZone Report Builder Appliance CLI

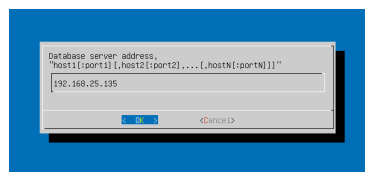
238

[Back to Index](#)

## INSTALLING REPORT BUILDER

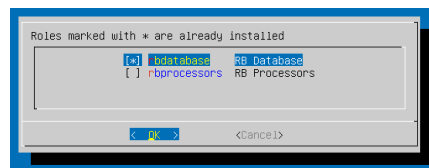
### DATABASE

4. Go to *Advanced Settings* → *Connect to Existing Database* in the appliance menu and enter the IP address and password of the GravityZone database:



5. Go to *Advanced Settings* → *Add or remove roles* and select the installation of the *RB Database*.

➔ **You cannot install RB Database and RB Processors on the same Appliance**



Bitdefender®

239

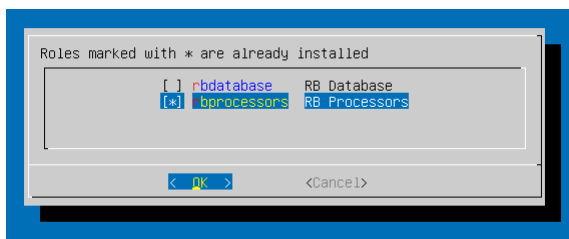
# GravityZone Basics Handbook

[Back to Index](#)

## INSTALLING REPORT BUILDER

### PROCESSORS

6. Import RBVA in your virtualized environment and power it on
7. Configure password for the built-in `bdadmin` system administrator
8. Configure hostname and network settings and proxy settings if needed
9. Go to *Advanced Settings* → *Connect to Existing Database* in the appliance menu and enter the IP address and password of the GravityZone database
10. Go to *Advanced Settings* → *Add or remove roles* and select the installation of the *RB Database*.



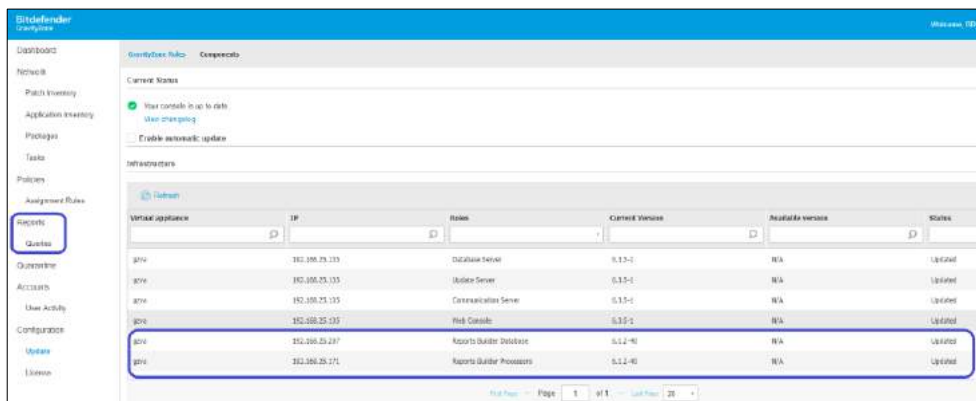
Bitdefender®

GravityZone Report Builder Appliance CLI → Add or remove roles

240

## Installing Report Builder

Report Builder Database and Processors roles are also displayed in the infrastructure section of the Control Center web console, under *Configuration* → *Update*, along with other GravityZone roles:



Virtual appliance	IP	Roles	Current version	Available version	Status
gztv	192.168.25.133	Database Server	5.1.2-1	N/A	Updated
gztv	192.168.25.133	Update Server	5.1.2-1	N/A	Updated
gztv	192.168.25.133	Communication Server	5.1.2-1	N/A	Updated
gztv	192.168.25.133	Web Console	5.1.2-1	N/A	Updated
gztv	192.168.25.247	Report Builder Database	5.1.2-40	N/A	Updated
gztv	192.168.25.271	Report Builder Processors	5.1.2-40	N/A	Updated

Bitdefender®

241

# GravityZone Basics Handbook

[Back to Index](#)

## REPORTS

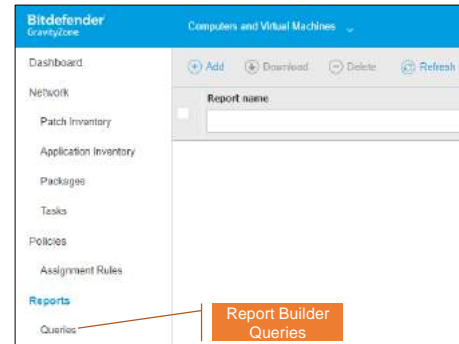
### REPORT BUILDER

With queries, you can take advantage of the multiple benefits comparing to the standard GravityZone reports:

- Comprehensive reports which, unlike standard reports, have summary and details integrated together in the same PDF document.
- Queries can retrieve information for the past two years.
- High level of customization. While standard GravityZone reports offer you the possibility to opt between a couple of predefined options, with queries there is no bound in choosing your data filters.

**Query Types – Endpoint Status, Endpoint Events, Exchange Events**

**Templates – Add, clone and fast search for specific templates in the Templates Manager window**



Bitdefender®

242

[Back to Index](#)

Bitdefender®

243

# GravityZone Basics HandBook



244

Back to Index

## PATCH MANAGEMENT CONFIGURATION

- Fully Integrated in the GravityZone, Patch Management Module enable organizations to keep systems up to date across entire Windows install base
- GravityZone Patch Management manages software updates for Windows operating systems and the largest collection of software applications in the market
- The patching module delivers updates for the entire fleet of workstations, physical servers or virtual servers

Bitdefender®

245

# GravityZone Basics Handbook

[Back to Index](#)

## PATCH MANAGEMENT FEATURES

### Automatic Patching

- Scheduled scanning for missing patches
- Different scheduling for security and non-security patches
- Automatic patching only on a set of vendors/products
- Postpone reboot for patches that needs requires restart

### Manual Patching

- Discovery and install patch tasks
- Success/Fail patching reports

Bitdefender®

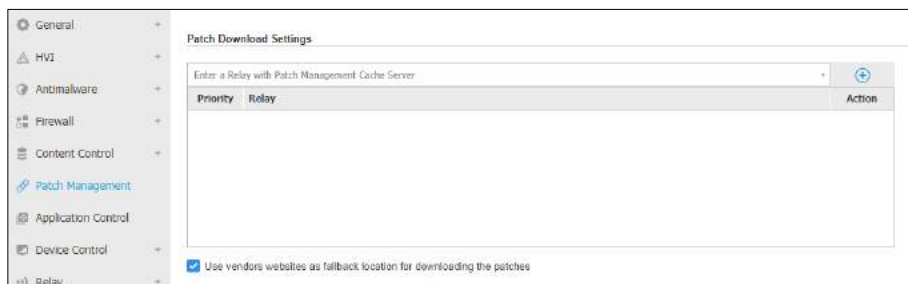
246

[Back to Index](#)

## PATCH MANAGEMENT POLICY SETTINGS

### Patch Download Settings

- Relay
- Vendor website



Bitdefender®

247

# GravityZone Basics Handbook

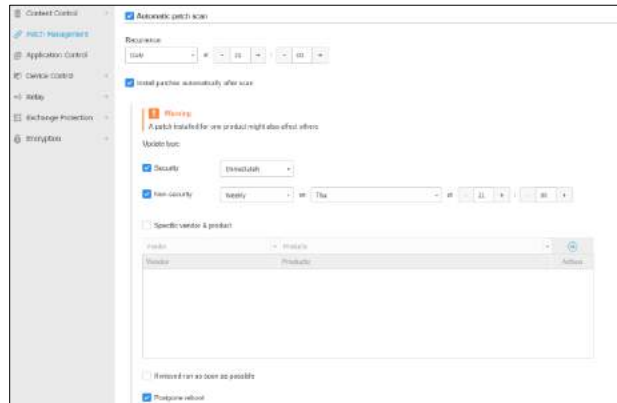
[Back to Index](#)

## PATCH MANAGEMENT

### POLICY SETTINGS

Automatic patch scan

- Security or Non-security options
- Specific vendors
- Postpone reboot



Bitdefender®

243

[Back to Index](#)

## PATCH MANAGEMENT

### PATCH INVENTORY

- Detailed information centering patches – CVE, BuletinID...
- Quick deployment of missing patches
- Patch blacklisting – temporary prevent installation of patches that might break workflow
- Postpone reboot for patches that requires restart

Bitdefender®

249

# GravityZone Basics Handbook

[Back to Index](#)

## PATCH MANAGEMENT

### PATCH STATUS REPORT

Check the update status of the software that is installed in your network. The report reveals the following details:

- Target machine (endpoint name, IP and operating system)
- Security patches (installed patches, failed patches, missing security and non-security patches)
- Status and last modified time for checked-out endpoints

Bitdefender®

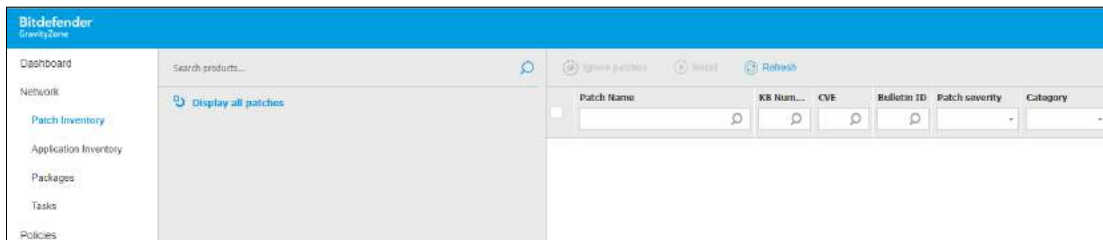
250

[Back to Index](#)

## PATCH INVENTORY

### PATCH MANAGEMENT

- Part of Patch Management
- Patch Inventory includes all patches for the software installed on the endpoints
- GravityZone discovers the patches the software needs through Patch Scan tasks and then adds it to the inventory
- Can be configured from the Policy



Bitdefender®

251

# GravityZone Basics HandBook

[Back to Index](#)

## Security for Virtual Environment

252

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS PLATFORM-AGNOSTIC SECURITY SOLUTION FOR DATACENTERS



Bitdefender®

253

Bitdefender®

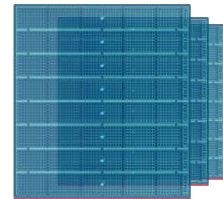
# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS

Provides security that is build specifically for the virtualized environments allowing organizations to maintain higher consolidation ratios across their datacenters.

- Compatible with VMware, Citrix, Microsoft Hyper-V, Red Hat, Oracle VM
- Integrates with vShield Endpoint and NSX for agentless antimalware
- Supports Windows and Linux VMs



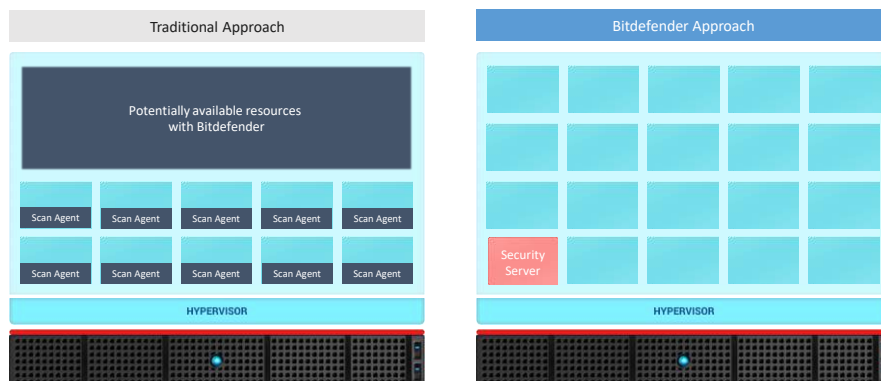
Bitdefender®

254

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS

### TRADITIONAL VS. BITDEFENDER APPROACH



Bitdefender®

255

Bitdefender®

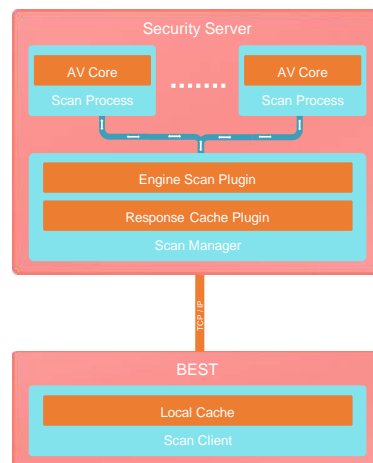
# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS

### SCANNING WORKFLOW

1. The local cache is first queried
2. If a corresponding entry does not exist in the local cache, the response cache (global cache) is queried
3. If a corresponding entry does not exist in the response cache, the object is subjected to scanning
4. File chunks, capable of containing malicious code, sent for scanning to Security Server
5. A response that is the result of scanning is used to populate the response cache and local cache. A response that results from querying the response cache is used to populate the local cache



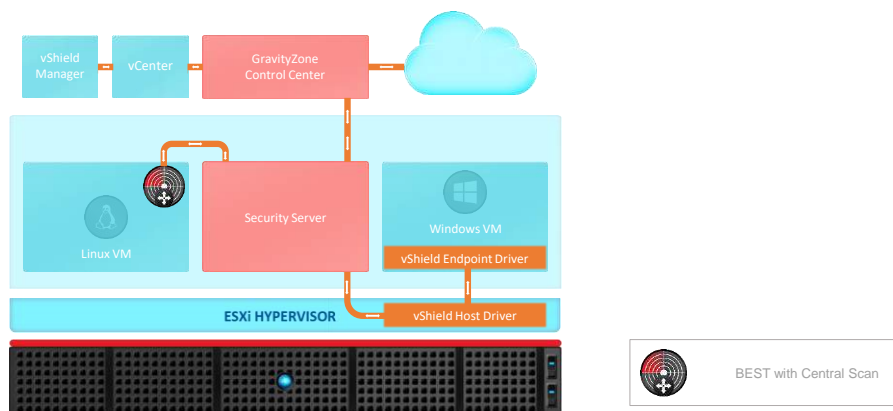
Bitdefender®

256

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS

### VMWARE ENVIRONMENTS WITH VSHIELD ENDPOINT



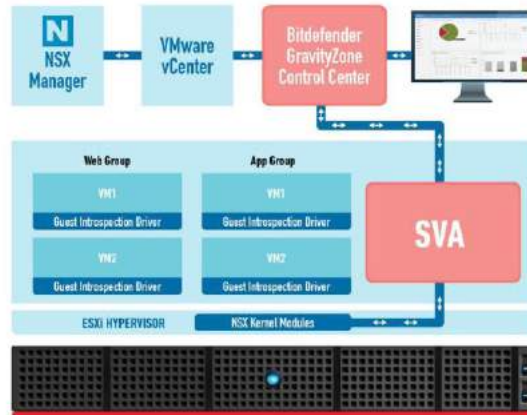
Bitdefender®

257

# GravityZone Basics HandBook

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS VMWARE ENVIRONMENTS WITH NSX

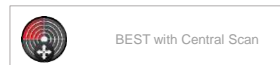
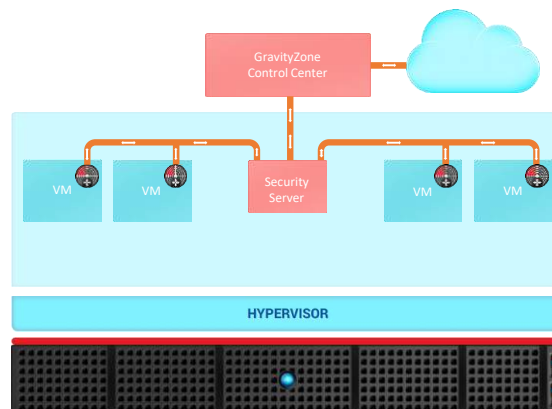


Bitdefend

258

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS MULTIPLATFORM ARCHITECTURE



Bitdefender®

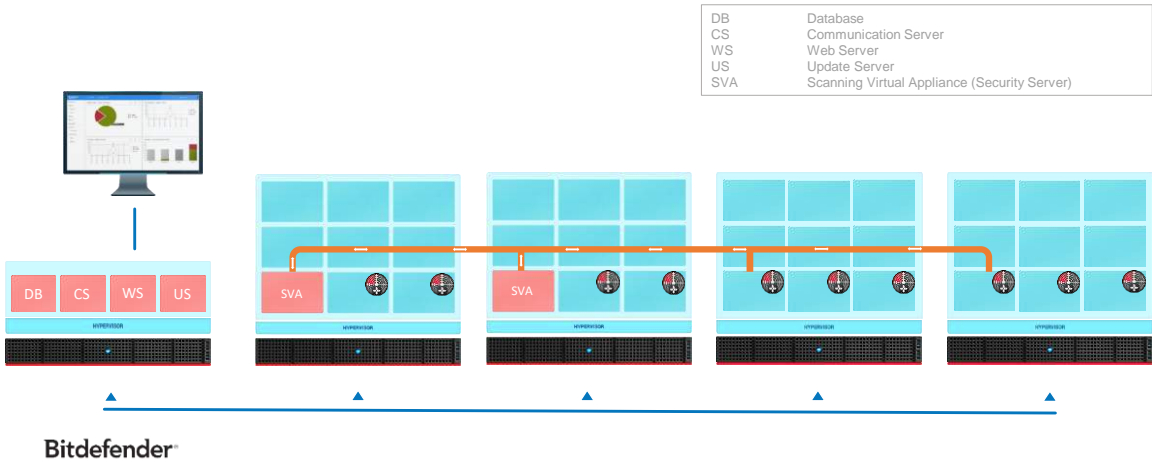
259

Bitdefender®

# GravityZone Basics HandBook

[Back to Index](#)

## SECURITY FOR VIRTUALIZED ENVIRONMENTS MULTIPLATFORM ARCHITECTURE



250

[Back to Index](#)

Bitdefender®

251

Bitdefender®

# GravityZone Basics Handbook



262

## Security Server

(not available on GravityZone Business Security)

Security Server is a dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware clients, acting as a scan server.

The diagram illustrates the Security Server architecture. At the top right, there is a server rack icon with a grid of 10 slots. One slot is highlighted in red and labeled "Security Server". Below the rack is a "HYPERVISOR" label. A blue line connects the "Security Server" to a horizontal bus line. From this bus line, four arrows point down to four client devices: a laptop, two desktop monitors, and a server rack. Each device has a Bitdefender logo on its screen. The Bitdefender logo is a red circle with a white crosshair and a red dot in the center.

Bitdefender®

263

# GravityZone Basics HandBook

[Back to Index](#)

## Security Server

VMware vShield and NSX Architecture:

- Security Server is installed on every physical host in the datacenter that contains VMs that needs protection

Multiplatform Architecture:

- Security Server is installed on one or more hosts so as to accommodate the number of virtual machines and physical clients to be protected
  - ➔ consider the number of protected systems, resources available for Security Server on hosts, as well as network connectivity between Security Server and the protected systems

Bitdefender™

204

[Back to Index](#)

## Security Server Remote Deployment

Bitdefender™

205

# GravityZone Basics HandBook

[Back to Index](#)

## SECURITY SERVER

### REMOTE DEPLOYMENT

If Control Center is integrated with vCenter Server, XenServer or Nutanix, you can **remotely deploy** Security Server on hosts from Control Center:

1. Go to Network page → select Virtual Machines
2. Browse the corresponding inventory → select the check boxes corresponding to the hosts on which you plan to install the Security Server
3. Go to Tasks → choose Install Security Server
4. Specify the deployment settings for the appliance

Bitdefender®

256

[Back to Index](#)

## Security Server Manual Installation

Bitdefender®

257

# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY SERVER MANUAL INSTALLATION

Download Security Server Appliance packages for from Control Center:

1. Go to Network → Packages page
2. Select the *Default Security Server* package
3. Click the Download icon → choose the package type from the menu (OVA, XVA or VHD)
4. Save the package to the desired location and deploy it on the host using your preferred VM deployment tool.

Bitdefender®

268

[Back to Index](#)

## SECURITY SERVER MANUAL INSTALLATION

Configure Security Server appliance:

1. Log in CLI console of the Security Server VM with the following credentials:

- User: *root*
- Password: *sve*

2. Run the configuration script:

```
$ sudo sva-setup
```

3. Configure the appliance with DHCP/static network settings
4. Enter the Communication Server IP address and port (default: 8443)

```
ECS_Server_IP:8443
```

5. Enter the Update Server address and port (default: 7074)

```
Update_Server_IP:7074
```

Bitdefender®

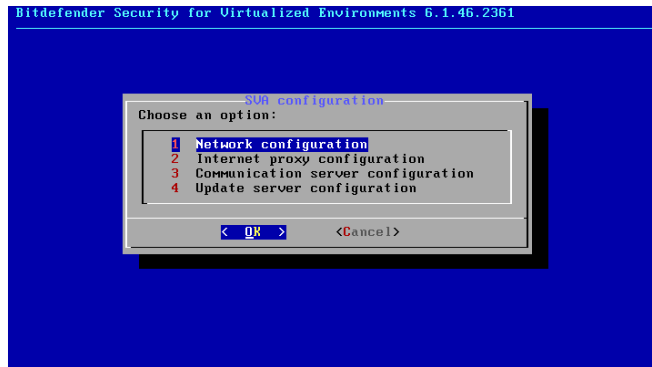
269

# GravityZone Basics Handbook

[Back to Index](#)

## SECURITY SERVER MANUAL INSTALLATION

Configure Security Server appliance:



Bitdefender®

Security Server Configuration

270

[Back to Index](#)

## ENDPOINT PROTECTION SECURITY SERVER REQUIREMENTS

Number of protected VMs	RAM	CPUs (HVI)
1-50 VMs	2 GB	2 CPUs
51-100 VMs	2 GB	4 CPUs
101-200 VMs	4 GB	6 CPUs

In VMware environments with vShield Endpoint / NSX:

- Security Server must be installed on each ESXi host to be protected.
- 40 GB disk space

In other environments:

- Bitdefender recommends installing Security Server on each physical host for improved performance.
- 16 GB disk space

Bitdefender®

271

Bitdefender®

# GravityZone Basics HandBook



272