

Bitdefender®

GravityZone



INSTALLATION GUIDE

Bitdefender GravityZone Installation Guide

Publication date 2020.12.24

Copyright© 2020 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

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

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

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the

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

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

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document

Table of Contents

Preface	vii
1. Conventions Used in This Guide	vii
1. About GravityZone	1
2. GravityZone Protection Layers	2
2.1. Antimalware	2
2.2. Advanced Threat Control	3
2.3. Advanced Anti-Exploit	3
2.4. Firewall	4
2.5. Content Control	4
2.6. Network Attack Defense	4
2.7. Patch Management	4
2.8. Device Control	5
2.9. Full Disk Encryption	5
2.10. Sandbox Analyzer	5
2.11. Network Traffic Security Analytics (NTSA)	6
2.12. GravityZone Protection Layers Availability	6
3. GravityZone Architecture	7
3.1. GravityZone VA	7
3.1.1. GravityZone Database	7
3.1.2. GravityZone Update Server	8
3.1.3. GravityZone Communication Server	8
3.1.4. Web Console (GravityZone Control Center)	8
3.2. Security Agents	8
3.2.1. Bitdefender Endpoint Security Tools	8
3.2.2. Endpoint Security for Mac	10
3.3. Sandbox Analyzer Architecture	11
4. Requirements	13
4.1. GravityZone Virtual Appliance	13
4.1.1. Supported Formats and Virtualization Platforms	13
4.1.2. Hardware	13
4.1.3. Internet Connection	16
4.2. Control Center	17
4.3. Endpoint Protection	17
4.3.1. Hardware	18
4.3.2. Supported Operating Systems	21
4.3.3. Supported File Systems	26
4.3.4. Supported Browsers	26
4.3.5. Supported Virtualization Platforms	26
4.3.6. Traffic Usage	29
4.4. Sandbox Analyzer On-Premises	30
4.4.1. ESXi Hypervisor	31
4.4.2. Sandbox Analyzer Virtual Appliance	32
4.4.3. Network Security Virtual Appliance	33

4.4.4. Physical Host Requirements and Hardware Scaling	34
4.4.5. Sandbox Analyzer Communication Requirements	35
4.5. Full Disk Encryption	36
4.6. GravityZone Communication Ports	38
5. Installing Protection	39
5.1. GravityZone Installation and Setup	39
5.1.1. Prepare for Installation	39
5.1.2. Deploy GravityZone	40
5.1.3. Control Center Initial Setup	48
5.1.4. Configure Control Center Settings	51
5.1.5. Managing the GravityZone Appliance	75
5.2. License Management	89
5.2.1. Finding a Reseller	89
5.2.2. Entering Your License Keys	89
5.2.3. Checking Current License Details	90
5.2.4. Resetting the license usage count	91
5.3. Installing Security Agents	92
5.3.1. Preparing for Installation	92
5.3.2. Local Installation	93
5.3.3. Remote Installation	98
5.3.4. Preparing Linux Systems for On-access Scanning	103
5.3.5. How Network Discovery Works	105
5.4. Installing Sandbox Analyzer On-Premises	108
5.4.1. Prepare for Installation	108
5.4.2. Deploy Sandbox Analyzer Virtual Appliance	109
5.5. Installing Full Disk Encryption	114
5.6. Credentials Manager	114
5.6.1. Operating System	115
5.6.2. Virtual Environment	116
5.6.3. Deleting Credentials from Credentials Manager	117
6. Updating GravityZone	118
6.1. Updating GravityZone Appliances	118
6.1.1. Manual Update	119
6.1.2. Automatic Update	120
6.2. Configuring Update Server	121
6.3. Downloading Product Updates	122
6.4. Product Offline Updates	122
6.4.1. Prerequisites	122
6.4.2. Setting Up the Online GravityZone Instance	123
6.4.3. Configuring and downloading the initial update files	124
6.4.4. Setting Up the Offline GravityZone Instance	126
6.4.5. Using Offline Updates	129
6.4.6. Using the Web Console	129
7. Uninstalling Protection	131
7.1. Uninstalling Endpoint Protection	131
7.2. Uninstalling Sandbox Analyzer On-Premises	133

7.3. Uninstalling GravityZone Virtual Appliance Roles	134
8. Getting Help	136
8.1. Bitdefender Support Center	136
8.2. Asking for Assistance	137
8.3. Using Support Tool	138
8.3.1. Using Support Tool on Windows Operating Systems	138
8.3.2. Using Support Tool on Linux Operating Systems	139
8.3.3. Using Support Tool on Mac Operating Systems	141
8.4. Contact Information	142
8.4.1. Web Addresses	142
8.4.2. Local Distributors	142
8.4.3. Bitdefender Offices	143
A. Appendices	146
A.1. Supported File Types	146
A.2. Sandbox Analyzer Objects	147
A.2.1. Supported File Types and Extensions for Manual Submission	147
A.2.2. File Types Supported by Content Prefiltering at Automatic Submission	147
A.2.3. Default Exclusions at Automatic Submission	148
A.2.4. Recommended Applications for Detonation VMs	148

Preface

This guide is intended for IT administrators in charge with deploying the GravityZone protection within their organization's premises. IT managers in search for information about GravityZone can find in this guide the GravityZone requirements and available protection modules.

This document aims to explain how to install and configure the GravityZone solution and its security agents on all types of endpoints in your company.

1. Conventions Used in This Guide

Typographical Conventions

This guide uses several text styles for an improved readability. Learn about their aspect and meaning from the table below.

Appearance	Description
sample	Inline command names and syntaxes, paths and filenames, configuration file outputs, input text are printed with <code>monospaced</code> characters.
http://www.bitdefender.com	The URL link is pointing to some external location, on http or ftp servers.
gravityzone-docs@bitdefender.com	E-mail addresses are inserted in the text for contact information.
"Preface" (p. vii)	This is an internal link, towards some location inside the document.
option	All the product options are printed using bold characters.
keyword	Interface options, keywords or shortcuts are highlighted using bold characters.

Admonitions

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.



Note

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.



Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.



Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

1. ABOUT GRAVITYZONE

GravityZone is a business security solution built from ground-up for virtualization and cloud to deliver security services to physical endpoints and virtual machines in private and public cloud.

GravityZone is one product with a unified management console available in the cloud, hosted by Bitdefender, or as one virtual appliance to be installed on company's premises, and it provides a single point for deploying, enforcing and managing security policies for any number of endpoints and of any type, in any location.

GravityZone delivers multiple layers of security for endpoints: antimalware with behavioral monitoring, zero day threat protection, application blacklisting and sandboxing, firewall, device control and content control.

2. GRAVITYZONE PROTECTION LAYERS

GravityZone provides the following protection layers:

- Antimalware
- Advanced Threat Control
- Advanced Anti-Exploit
- Firewall
- Content Control
- Patch Management
- Device Control
- Full Disk Encryption
- Network Traffic Security Analytics (NTSA)

2.1. Antimalware

The antimalware protection layer is based on signature scanning and heuristic analysis (B-HAVE, ATC) against: viruses, worms, Trojans, spyware, adware, keyloggers, rootkits and other types of malicious software.

Bitdefender's antimalware scanning technology relies on the following technologies:

- First, a traditional scanning method is employed where scanned content is matched against the signature database. The signature database contains byte patterns specific to known threats and is regularly updated by Bitdefender. This scanning method is effective against confirmed threats that have been researched and documented. However, no matter how promptly the signature database is updated, there is always a vulnerability window between the time when a new threat is discovered and when a fix is released.
- Against brand-new, undocumented threats, a second layer of protection is provided by **B-HAVE**, Bitdefender's heuristic engine. Heuristic algorithms detect malware based on behavioral characteristics. B-HAVE runs suspicious files in a virtual environment to test their impact on the system and ensure they pose no threat. If a threat is detected, the program is prevented from running.

Scanning Engines

Bitdefender GravityZone is able to automatically set the scanning engines when creating security agent packages, according to the endpoint's configuration.

The administrator can also customize the scan engines, being able to choose between several scanning technologies:

1. **Local Scan**, when the scanning is performed on the local endpoint. The local scanning mode is suited for powerful machines, having security content stored locally.
2. **Hybrid Scan with Light Engines (Public Cloud)**, with a medium footprint, using in-the-cloud scanning and, partially, the local security content. This scanning mode brings the benefit of better resources consumption, while involving off-premise scanning.
3. **Central Scan in Public or Private Cloud**, with a small footprint requiring a Security Server for scanning. In this case, no security content set is stored locally, and the scanning is offloaded on the Security Server.

**Note**

There is a minimum set of engines stored locally, needed to unpack the compressed files.

4. **Central Scan (Public or Private Cloud scanning with Security Server) with fallback* on Local Scan (Full Engines)**
5. **Central Scan (Public or Private Cloud scanning with Security Server) with fallback* on Hybrid Scan (Public Cloud with Light Engines)**

2.2. Advanced Threat Control

For threats that elude even the heuristic engine, another layer of protection is present in the form of Advanced Threat Control (ATC).

Advanced Threat Control continuously monitors running processes and grades suspicious behaviors such as attempts to: disguise the type of process, execute code in another process's space (hijack process memory for privilege escalation), replicate, drop files, hide from process enumeration applications, etc. Each suspicious behavior raises the process rating. When a threshold is reached, an alarm is triggered.

2.3. Advanced Anti-Exploit

Powered by machine learning, Advanced Anti-Exploit is a proactive technology that stops zero-day attacks carried out through evasive exploits. Advanced anti-exploit

catches the latest exploits in real-time and mitigates memory corruption vulnerabilities that can evade other security solutions. It protects the most commonly used applications, such as browsers, Microsoft Office or Adobe Reader, as well as others that you may think of. It watches over system processes and protects against security breaches and hijacking existing processes.

2.4. Firewall

The Firewall controls applications' access to the network and to the Internet. Access is automatically allowed for a comprehensive database of known, legitimate applications. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection.

2.5. Content Control

The Content Control module helps enforce company policies for allowed traffic, web access, data protection and applications control. Administrators can define traffic scan options and exclusions, schedule web access while blocking or allowing certain web categories or URLs, configure data protection rules and define permissions for the use of specific applications.

2.6. Network Attack Defense

The Network Attack Defense module relies on a Bitdefender technology focused on detecting network attacks designed to gain access on endpoints through specific techniques, such as: brute-force attacks, network exploits, password stealers, drive-by-download infection vectors, bots, and Trojans.

2.7. Patch Management

Fully integrated in GravityZone, Patch Management keeps operating systems and software applications up to date and provides a comprehensive view on the patch status for your managed Windows endpoints.

The GravityZone Patch Management module includes several features, such as on-demand / scheduled patch scanning, automatic / manual patching or missing patch reporting.

You can learn more about GravityZone Patch Management supported vendors and products from this [KB article](#).

**Note**

Patch Management is an add-on available with a separate license key for all available GravityZone packages.

2.8. Device Control

The Device Control module allows preventing the sensitive data leakage and malware infections via external devices attached to endpoints by applying blocking rules and exceptions via policy to a vast range of device types (such as USB flash drives, Bluetooth devices, CD/DVD players, storage devices, etc.).

2.9. Full Disk Encryption

This protection layer allows you to provide full disk encryption on endpoints, by managing BitLocker on Windows, and FileVault and diskutil on macOS. You can encrypt and decrypt boot and non-boot volumes, with just a few clicks, while GravityZone handles the entire process, with minimal intervention from the users. Additionally, GravityZone stores the recovery keys needed to unlock volumes when the users forget their passwords.

**Note**

Full Disk Encryption is an add-on available with a separate license key for all available GravityZone packages.

2.10. Sandbox Analyzer

Bitdefender Sandbox Analyzer provides a powerful layer of protection against advanced threats by performing automatic, in-depth analysis of suspicious files which are not signed by Bitdefender antimalware engines yet. The sandbox employs an extensive set of Bitdefender technologies to execute payloads in a contained virtual environment deployed locally, analyze their behavior and report any subtle system changes that is indicative of malicious intent.

Sandbox Analyzer uses a series of sensors to detonate content from network traffic streams, centralized quarantine and ICAP servers.

Additionally, Sandbox Analyzer allows sample manual submission and through API.

**Note**

This module's functionality is provided by Sandbox Analyzer On-Premises, which is available with a separate license key.

2.11. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) is a network security solution that analyzes IPFIX traffic streams for the presence of malicious behavior and malware.

Bitdefender NTSA is meant to act alongside your existing security measures as a complementary safeguard that is capable of covering the blind spots that traditional tools do not monitor.

Traditional network security tools generally attempt to prevent malware infections by inspecting inbound traffic (via sandbox, firewalls, antivirus and so on). Bitdefender NTSA focuses solely on monitoring outbound network traffic for malicious behavior.

2.12. GravityZone Protection Layers Availability

The GravityZone protection layers availability differs according to the endpoint's operating system. To learn more, refer to the [GravityZone Protection Layers Availability](#) KB article.

3. GRAVITYZONE ARCHITECTURE

The unique architecture of GravityZone allows the solution to scale with ease and secure any number of systems. GravityZone can be configured to use multiple virtual appliances and multiple instances of specific roles (Database, Communication Server, Update Server and Web Console) to ensure reliability and scalability.

Each role instance can be installed on a different appliance. Built-in role balancers ensure that the GravityZone deployment protects even the largest corporate networks without causing slowdowns or bottlenecks. Existing load balancing software or hardware can also be used instead of the built-in balancers, if present in the network.

Delivered in a virtual container, GravityZone can be imported to run on any virtualization platform, including VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure.

Integration with VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element and Microsoft Azure reduces the effort of deploying protection for physical and for virtual endpoints.

The GravityZone solution includes the following components:

- [GravityZone Virtual Appliance](#)
- [Security Agents](#)

3.1. GravityZone VA

GravityZone on-premise solution is delivered as a Linux Ubuntu self-configuring hardened virtual appliance (VA), embedded into a virtual machine image, easy to install and configure through a CLI (Command Line Interface). The virtual appliance is available in several formats, compatible with the main virtualization platforms (OVA, XVA, VHD, OVF, RAW).

3.1.1. GravityZone Database

The central logic of GravityZone architecture. Bitdefender uses MongoDB non-relational database, easy to scale and replicate.

3.1.2. GravityZone Update Server

The Update Server has an important role of updating GravityZone solution and endpoint agents by replicating and publishing the needed packages or installation files.

3.1.3. GravityZone Communication Server

The Communication Server is the link between security agents and the database, transferring policies and tasks to protected endpoints and also the events reported by security agents.

3.1.4. Web Console (GravityZone Control Center)

Bitdefender security solutions are managed within GravityZone from a single point of management, Control Center web console, which provides easier management and access to overall security posture, global security threats, and control over all security modules protecting virtual or physical desktops and servers. Powered by a Gravity Architecture, Control Center is capable of addressing the needs of even the largest organizations.

Control Center integrates with the existing system management and monitoring systems to make it simple to automatically apply protection to unmanaged workstations or servers that appear on the Microsoft Active Directory, or that are simply detected in the network.

3.2. Security Agents

To protect your network with Bitdefender, you must install the appropriate GravityZone security agents on network endpoints.

- [Bitdefender Endpoint Security Tools](#)
- [Endpoint Security for Mac](#)

3.2.1. Bitdefender Endpoint Security Tools

GravityZone ensures Windows and Linux physical and virtual machines protection with Bitdefender Endpoint Security Tools, an intelligent environment-aware security agent which adapts to the endpoint type. Bitdefender Endpoint Security Tools can be deployed on any machine, either virtual or physical, providing a flexible scanning system, being an ideal choice for mixed environments (physical, virtual and cloud).

Bitdefender Endpoint Security Tools uses one single policy template for physical and virtual machines, and one installation kit source for any environment (physical or virtual) running Windows.

Protection Layers

The following protection layers are available with Bitdefender Endpoint Security Tools:

- Antimalware
- Advanced Threat Control
- Firewall
- Content Control
- Network Attack Defense
- Patch Management
- Device Control
- Full Disk Encryption

Endpoint Roles

- Power User
- Relay
- Patch Caching Server

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.



Important

This module is available only for supported Windows desktop and server operating systems. For more information, refer to [“Supported Operating Systems” \(p. 21\)](#).

Relay

Endpoint agents with Bitdefender Endpoint Security Tools Relay role serve as communication proxy and update servers for other endpoints in the network. Endpoint agents with relay role are especially required in organizations with isolated networks, where all traffic is made through a single access point.

In companies with distributed networks, relay agents help lowering the bandwidth usage, by preventing protected endpoints to connect directly to the GravityZone appliance.

Once a Bitdefender Endpoint Security Tools Relay agent is installed in the network, other endpoints can be configured via policy to communicate with Control Center through the relay agent.

Bitdefender Endpoint Security Tools Relay agents serve for the following purposes:

- Discovering all unprotected endpoints in the network.
- Deploying the endpoint agent inside the local network.
- Updating protected endpoints in the network.
- Ensuring the communication between Control Center and connected endpoints.
- Acting as proxy server for protected endpoints.
- Optimizing the network traffic during updates, deployments, scanning and other resource-consuming tasks.

Patch Caching Server

Endpoints with Relay role may also act as a Patch Caching Server. With this role enabled, Relays serve for storing software patches downloaded from vendor's websites, and distributing them to target endpoints in your network. Whenever a connected endpoint has software with missing patches, it takes them from the server and not from the vendor's website, thus optimizing the traffic generated and the network bandwidth load.



Important

This additional role is available with a registered Patch Management add-on.

3.2.2. Endpoint Security for Mac

Endpoint Security for Mac is a security agent designed to protect Intel-based Macintosh workstations and laptops. The scanning technology available is **Local Scan**, with security content stored locally.

Protection Layers

The following protection layers are available with Endpoint Security for Mac:

- [Antimalware](#)
- [Advanced Threat Control](#)
- [Content Control](#)

- Device Control
- Full Disk Encryption

3.3. Sandbox Analyzer Architecture

Bitdefender 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.

To use this module with GravityZone, you need to install Sandbox Analyzer On-Premises.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises is delivered as a Linux Ubuntu virtual appliance, embedded into a virtual machine image, easy to install and configure through a command-line interface (CLI). Sandbox Analyzer On-Premises is available in OVA format, deployable on VMware ESXi.

A Sandbox Analyzer On-Premises instance contains the following components:

- **Sandbox Manager.** This component is the sandbox orchestrator. Sandbox Manager connects to the ESXi hypervisor via API and uses its hardware resources to build and operate the malware analysis environment.
- **Detonation virtual machines.** This component consists of virtual machines leveraged by Sandbox Analyzer to execute files and analyze their behavior. The detonation virtual machines can run Windows 7 and Windows 10 64-bit operating systems.

GravityZone Control Center operates as management and reporting console, where you configure security policies and view analysis reports and notifications.

Sandbox Analyzer On-Premises operates the following feeding sensors:

- **Network sensor.** Network Security Virtual Appliance (NSVA) is a virtual appliance deployable in the same virtualized ESXi environment as the Sandbox Analyzer instance. Network sensor extracts content from network streams and submits it to Sandbox Analyzer.
- **ICAP sensor.** Deployed on network attached storage (NAS) devices using ICAP protocol, Bitdefender Security Server supports content submission to Sandbox Analyzer.

In addition to these sensors, Sandbox Analyzer On-Premises supports manual submission and through API. For details, refer to **Using Sandbox Analyzer** chapter in the GravityZone Administrator's Guide.

4. REQUIREMENTS

All of the GravityZone solutions are installed and managed via Control Center.

4.1. GravityZone Virtual Appliance

4.1.1. Supported Formats and Virtualization Platforms

GravityZone is delivered as a virtual appliance (VA). It is available in the following formats, which support most common virtualization platforms:

- OVA (compatible with VMware vSphere, View, VMware Player)
- XVA (compatible with Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (compatible with Microsoft Hyper-V)
- VMDK (compatible with Nutanix Prism)
- OVF (compatible with Red Hat Enterprise Virtualization)*
- OVF (compatible with Oracle VM)*
- RAW (compatible with Kernel-based Virtual Machine or KVM)*

*OVF and RAW packages are archived in tar.bz2 format.

For Oracle VM VirtualBox platform compatibility, refer to [this KB article](#).

Support for other formats and virtualization platforms may be provided on request.

4.1.2. Hardware

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](#)” (p. 75).



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.

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
GravityZone basic features								
Update Server [*]	8	12	14	16	4	4	6	8
Web Console ^{**}					6	10	12	12
Communication Server					6	10	12	18
Database ^{***}					6	6	9	12
Total	8	12	14	16	22	30	39	50
GravityZone with Bitdefender HVI								
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.

RAM (GB)

Component	Number of Endpoints (up to)							
	250	500	1000	3000	5000	10000	25000	50000
GravityZone basic features								
Update Server	16	16	18	20	2	2	3	3
Web Console [*]					8	8	12	16
Communication Server					6	12	12	16
Database ^{**}					8	10	12	12
Total	16	16	18	20	24	32	39	47
GravityZone with Bitdefender HVI								
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.

Free Disk Space (GB)

Component	Number of Endpoints (up to)								
	250	250*	500	1000	3000	5000	10000	25000	50000
GravityZone basic features									
Update Server						80	80	80	80
Web Console						80	80	80	80
Communication Server	120	160	160	200	200	80	80	80	80
Database **						80	120	200	500
Total	120	160	160	200	200	320	360	440	740
GravityZone with Bitdefender HVI									
Update Server			80	80	80	80	80	80	80
Web Console			80	80	80	80	80	80	80
Communication Server	120	160	80	80	80	80	80	80	80
Database **			80	80	100	100	160	300	700
Total	120	160	320	320	340	340	400	540	940



Important

It is highly recommended to use Solid-state drives (SSDs).

* Additional SSD space required when choosing the automatic installation, because it also installs the Security Server. After installation is complete, you can uninstall the Security Server to free disk space.

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

4.1.3. Internet Connection

The GravityZone appliance requires Internet access.

4.2. Control Center

To access the Control Center web console, the following are required:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Recommended screen resolution: 1280 x 800 or higher
- The computer you connect from must have network connectivity to Control Center.



Warning

Control Center will not work / display properly in Internet Explorer 9+ with the Compatibility View feature enabled, which is equivalent with using an unsupported browser version.

4.3. Endpoint Protection

To protect your network with Bitdefender, you must install the GravityZone security agents on network endpoints. For this purpose, you need a Control Center user with administrator privileges over the services you need to install and over the network endpoints under your management.

Requirements for the security agent are different, based on whether has additional server roles, such as Relay, Exchange Protection or Patch Caching Server. For more information on the agent's roles, refer to [“Security Agents” \(p. 8\)](#).

4.3.1. Hardware

Security Agent Without Roles

CPU

Target Systems	CPU Type	Supported Operating Systems (OSes)
Workstations	Intel® Pentium compatible processors, 2 GHz or faster	Microsoft Windows desktop OSes
	Intel® Core 2 Duo, 2 GHz or faster	macOS
Smart Devices	Intel® Pentium compatible processors, 800 MHz or faster	Microsoft Windows embedded OSes
Servers	Minimum: Intel® Pentium compatible processors, 2.4 GHz	Microsoft Windows Server OSes and Linux OSes
	Recommended: Intel® Xeon multi-core CPU, 1.86 GHz or faster	



Warning

ARM processors are currently not supported.

Free RAM Memory

At Installation (MB)

OS	SINGLE ENGINE					
	Local Scanning		Hybrid Scanning		Centralized 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
macOS	1024	1024	n/a	n/a	n/a	n/a

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	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

* The measurements cover the daily endpoint client usage, without taking into account additional tasks, such as on-demand scans or product updates.

Free Disk Space

At Installation (MB)

OS	SINGLE ENGINE						DUAL ENGINE			
	Local Scanning		Hybrid Scanning		Centralized 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	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

For Daily Usage (MB)*

OS	Antivirus (Single Engine)			Protection Modules				
	Local	Hybrid	Centralized	Behavioral Scan	Firewall	Content Control	Power User	Update Server
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

* The measurements cover the daily endpoint client usage, without taking into account additional tasks, such as on-demand scans or product updates.

Security Agent with Relay Role

The Relay role needs hardware resources additionally to the basic security agent's configuration. These requirements are to support the Update Server and installation packages hosted by the endpoint:

Number of connected endpoints	CPU to support Update Server	RAM	Free disk space for Update Server
1-300	minimum Intel® Core™ i3 or equivalent processor, 2 vCPU per core	1 GB	10 GB
300-1000	minimum Intel® Core™ i5 or equivalent processor, 4 vCPU per core	1 GB	10 GB



Warning

- ARM processors are currently not supported.
- Relay agents require SSD disks, to support the high amount of read/write operations.



Important

- If you want to save the installation packages and updates to another partition than the one where the agent is installed, make sure both partitions have sufficient free disk space (10 GB), otherwise the agent aborts installation. This is required only at installation.
- On Windows endpoints, local to local symbolic links must be enabled.

Security Agent With Patch Caching Server Role

The agent with Patch Caching Server role must meet the following cumulative requirements:

- All hardware requirements of the simple security agent (without roles)
- All hardware requirements of the Relay role

- Additionally 100 GB of free disk space to store the downloaded patches

**Important**

If you want to save the patches to another partition than the one where the agent is installed, make sure both partitions have sufficient free disk space (100 GB), otherwise the agent aborts installation. This is required only at installation.

4.3.2. Supported Operating Systems

Windows Desktop

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

**Warning**

Bitdefender does not support Windows Insider Program builds.

Windows Tablet and Embedded

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard

- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Windows Server

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Linux



Important

Linux endpoints use license seats from the pool of licenses for server operating systems.

- Ubuntu 14.04 LTS or higher
- Red Hat Enterprise Linux / CentOS 6.0 or higher⁽²⁾
- SUSE Linux Enterprise Server 11 SP4 or higher
- OpenSUSE Leap 42.x
- Fedora 25 or higher⁽¹⁾
- Debian 8.0 or higher
- Oracle Linux 6.3 or higher
- Amazon Linux AMI 2016.09 or higher
- Amazon Linux 2



Warning

(1) On Fedora 28 and higher, Bitdefender Endpoint Security Tools requires manual installation of the `libnsl` package, by running the following command:

```
sudo dnf install libnsl -y
```

(2) For minimal installations of CentOS Bitdefender Endpoint Security Tools requires manual installation of the `libnsl` package, by running the following command:

```
sudo yum install libnsl
```

Active Directory Prerequisites

When integrating Linux endpoints with an Active Directory domain via the System Security Services Daemon (SSSD), ensure that the **ldbsearch**, **krb5-user**, and **krb5-config** tools are installed and kerberos is configured properly.

```
/etc/krb5.conf

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    default_realm = DOMAIN.NAME
    dns_lookup_realm = true
    dns_lookup_kdc = true
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    fcc-mit-ticketflags = true
    default_keytab_name = FILE:/etc/krb5.keytab

[realms]
    DOMAIN.NAME = {
        kdc = dc1.domain.name
        kdc = dc2.domain.name
        admin_server = dc.domain.com
        default_domain = domain.com
    }
```

```
[domain_realm]
domain.name = DOMAIN.NAME
.domain.name = DOMAIN.NAME

[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```



Note

All entries are case sensitive.

On-access Scanning Support


On-access scanning is available for all supported guest operating systems. On Linux systems, on-access scanning support is provided in the following situations:

Kernel Versions	Linux Distributions	On-access Requirements
2.6.38 or higher*	Red Hat Enterprise Linux / CentOS 6.0 or higher Ubuntu 14.04 or higher SUSE Linux Enterprise Server 11 SP4 or higher OpenSUSE Leap 42.x Fedora 25 or higher Debian 9.0 or higher Oracle Linux 6.3 or higher Amazon Linux AMI 2016.09 or higher	Fanotify (kernel option) must be enabled.

Kernel Versions	Linux Distributions	On-access Requirements
2.6.38 or higher	Debian 8	Fanotify must be enabled and set to enforcing mode and then the kernel package must be rebuilt. For details, refer to this KB article .
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender provides support via DazukoFS with prebuilt kernel modules.
All other kernels	All other supported systems	The DazukoFS module must be manually compiled. For more details, refer to "Manually compile the DazukoFS module" (p. 103).

* With certain limitations described below.

On-access Scanning Limitations

Kernel Versions	Linux Distributions	Details
2.6.38 or higher	All supported systems	On-access scanning monitors mounted network shares only under these conditions: <ul style="list-style-type: none"> • Fanotify is enabled on both remote and local systems. • The share is based on the CIFS and NFS file systems. <div>  Note On-access scanning does not scan network shares mounted using SSH or FTP. </div>
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.

macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Content Control not supported in macOS Big Sur (11.0).

4.3.3. Supported File Systems

Bitdefender installs on and protects the following file systems:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.



Note

On-access scanning support is not provided for NFS and CIFS/SMB.

4.3.4. Supported Browsers

Endpoint browser security is verified to be working with the following browsers:

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

4.3.5. Supported Virtualization Platforms

Security for Virtualized Environments provides out-of-the-box support for the following virtualization platforms:

- VMware vSphere & vCenter Server 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

**Note**

The Workload Management functionality in vSphere 7.0 is not supported.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (including Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- 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)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism with AOS 5.6, 5.11 STS
- Nutanix Prism with AHV 20170830.115, 20170830.301 and 20170830.395 Community Edition
- Nutanix Prism version 2018.01.31 (Community Edition)

**Note**

Support for other virtualization platforms may be provided on request.

Supported Cloud Platforms

Along with on premise virtualization environments, GravityZone can also integrate with the following cloud platforms:

- **Amazon EC2**

As Amazon EC2 customer, you can integrate the inventory of EC2 instances grouped by Regions and Availability Zones with the GravityZone network inventory.

- **Microsoft Azure**

As Microsoft Azure customer, you can integrate the Microsoft Azure virtual machines grouped by Regions and Availability Zones with the GravityZone network inventory.

Compatibility with Desktop and Application Virtualization Technologies

GravityZone is compatible with the following virtualization technologies, starting with Bitdefender Endpoint Security Tools version 6.6.16.226:

- **VMware:**

VMware V-App (same version with vCenter Server)

VMware ThinApp 5.2.6

VMware AppVolumes 2.180



Important

It is recommended not to install in Application Stack or Writable Volumes.

- **Microsoft:**

Microsoft App-V 5.0, 5.1

Microsoft FSLogix 2.9.7237

- **Citrix:**

Citrix App Layering 19.10

Citrix Appdisks 7.12



Important

Assign policies based on user rules so that Device Control would not prevent OS and platform layers creation.

You may need to configure the GravityZone Firewall rules to allow network traffic for each of these applications. For more information, refer to [Citrix App Layering Product Documentation](#).

Supported Virtualization Management Tools

Control Center currently integrates with the following virtualization management tools:

- VMware vCenter Server
- Citrix XenServer
- Nutanix Prism Element

To set up integration, you must provide the username and password of an administrator.

4.3.6. Traffic Usage

• Product updates traffic between endpoint client and update server

Each periodical Bitdefender Endpoint Security Tools product update generates the following download traffic on each endpoint client:

- On Windows OS: ~20 MB
- On Linux OS: ~26 MB
- On macOS: ~25 MB

• Downloaded security content updates traffic between endpoint client and Update Server (MB / day)

Update Server Type	Scan Engine Type		
	Local	Hybrid	Centralized
Relay	65	58	55
Bitdefender Public Update Server	3	3.5	3

• Central Scan traffic between endpoint client and Security Server

Scanned Objects	Traffic Type		Download (MB)	Upload (MB)
Files*	First scan		27	841
	Cached scan		13	382
Websites**	First scan	Web traffic	621	N/A
		Security Server	54	1050
	Cached Scan	Web traffic	654	N/A
		Security Server	0.2	0.5

* The provided data has been measured for 3.49 GB of files (6,658 files), of which 1.16 GB are Portable Executable (PE) files.

** The provided data has been measured for the top-ranked 500 websites.

- **Hybrid scan traffic between endpoint client and Bitdefender Cloud Services**

Scanned Objects	Traffic Type	Download (MB)	Upload (MB)
Files*	First scan	1.7	0.6
	Cached scan	0.6	0.3
Web traffic**	Web traffic	650	N/A
	Bitdefender Cloud Services	2.6	2.7

* The provided data has been measured for 3.49 GB of files (6,658 files), of which 1.16 GB are Portable Executable (PE) files.

** The provided data has been measured for the top-ranked 500 websites.

- **Traffic between Bitdefender Endpoint Security Tools Relay clients and update server for downloading security content**

Clients with Bitdefender Endpoint Security Tools Relay role download ~16 MB / day* from update server.

* Available with Bitdefender Endpoint Security Tools clients starting from 6.2.3.569 version.

- **Traffic between endpoint clients and Control Center web console**

An average traffic of 618 KB / day is generated between endpoint clients and Control Center web console.

4.4. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises has specific requirements as follows:

- [ESXi Hypervisor](#) (the virtualization platform that will run the environment).
- [Sandbox Analyzer Virtual Appliance](#) (the management appliance that will control the detonation virtual machines).
- [Network Security Virtual Appliance](#) (a VM that encapsulates a network sensor capable of extracting payload from network traffic).

- Connectivity to an existing GravityZone Control Center used for high-level management of the sandbox environment.
- Internet connection for downloading the Sandbox Analyzer Virtual Appliance, with minimum bandwidth of 5 MBps.

**Important**

Make sure there are not other applications or processes that may block the internet connection while downloading and installing Sandbox Analyzer.

4.4.1. ESXi Hypervisor

Sandbox Analyzer Virtual Appliance is available in OVA format, deployable on a single physical host running VMware ESXi hypervisor (version 6.5 or 6.7).

Hardware Requirements for the Physical Host

- CPU: the total number of CPU cores (considering hyperthreading) can be extrapolated by using the calculation presented in the section [“Physical Host Requirements and Hardware Scaling”](#) (p. 34).
- RAM: the total amount of RAM needed for the physical host can be extrapolated by using the calculation presented in the section [“Physical Host Requirements and Hardware Scaling”](#) (p. 34).
- Disk space: at least 1TB of SSD storage (adequate for 8-VM detonation environment, scalable with at least 50 GB for each additional detonation VM).
- Network: one dedicated physical network interface card (NIC).

This NIC can be split into two virtual NICs, with the following mappings:

- One NIC for the management interface.
- One NIC for the detonation network.

**Note**

It is recommended to use dedicated physical NICs with the same mappings as the above mentioned vNICs if the hardware configuration allows it.

Software Requirements

Supported versions of ESXi server: 6.5 or higher, VMFS version 5.

Additional configuration on ESXi host:

- SSH enabled on startup.
- NTP service configured and active.
- The **start/stop with host** option enabled.



Note

Sandbox Analyzer is compatible with the trial version of VMware ESXi. However, for production deployments it is recommended to run on a licensed version of ESXi.

4.4.2. Sandbox Analyzer Virtual Appliance

Sandbox Analyzer Virtual Appliance provides virtually unlimited scalability, as long as the underlying hardware resources are available.

Of the total amount of ESXi available resources, Sandbox Analyzer shares CPU and RAM between Sandbox Manager and the detonation virtual machines.

Sandbox Manager Minimum System Requirements

- 6 vCPUs
- 20 GB of RAM
- 600 GB of disk space

Sandbox Manager has three internal virtual NICs allocated as follows:

- One NIC for communication with the management console (GravityZone Control Center).
- One NIC for internet connectivity.
- One NIC for communication with detonation VMs.



Note

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

Detonation Virtual Machines

System Requirements

- 4 vCPUs (overprovisioned in 4:1 ratio, refer to [“Physical Host Requirements and Hardware Scaling”](#) (p. 34))

- 3 GB of RAM
- 50 GB of disk space

Sandbox Analyzer On-Premises provides support for custom virtual machine images. This allows for sample detonation in a runtime environment that mimics a realistic production environment.

Creating a virtual machine image requires the following conditions:

- The virtual machine image is in VMDK format, version 5.0.
- Supported operating systems for building detonation virtual machines:
 - Windows 7 64-bit (any patch level)
 - Windows 10 64-bit (any patch level)



Important

- The operating system must be installed on the second partition in the partition table and mounted at drive C: (default Windows installation configuration).
- Local "Administrator" account must be enabled and have an empty password string (password disable).
- Before exporting the VM image, you must correctly license the operating system and all installed software in the virtual machine image.

Virtual Machine Image Software

Sandbox Analyzer supports for detonation a wide range of file formats and types. For details, refer to ["Sandbox Analyzer Objects"](#) (p. 147).

For conclusive reports, make sure you have installed in the custom image the software that can open a particular file type you want to detonate. For details, refer to ["Recommended Applications for Detonation VMs"](#) (p. 148).

4.4.3. Network Security Virtual Appliance

Network Security Virtual Appliance operates the network sensor, which extracts payloads from network streams and submits it to Sandbox Analyzer. The minimal hardware requirements are:

- 4 vCPUs
- 4 GB of RAM

- 1 TB of disk space
- 2 vNICs

4.4.4. Physical Host Requirements and Hardware Scaling

The scaling algorithm of the Sandbox Analyzer environment considers the following formula, where "K" equals the number of detonation slots (or detonation VMs):

- Sandbox Analyzer VA vCPU = 6 vCPUs + K x 1 vCPU
- Sandbox Analyzer VA RAM = 20 GB RAM + K x 2GB

Similarly, the scaling algorithm for the host is the following:

- ESXi Host vCPU = 6 vCPUs + K x 2 vCPU
- ESXi Host RAM = 20 GB RAM + K x 5 GB

The main difference between Sandbox Analyzer VA and ESXi resources are given by the resources allocated to each detonation VM.

Therefore, a typical detonation environment (8 VMs) would have the following requirements:

- Sandbox Analyzer VA vCPU = 6 vCPUs + 8 x 1 vCPU = 14 vCPUs
- Sandbox Analyzer VA RAM = 20 GB RAM + 8 x 2GB = 36GB RAM
- ESXi Host vCPU = 6 vCPUs + 8 x 2 vCPUs = 22 vCPUs

**Note**

Each detonation VM needs 1 vCPU allocated for the Sandbox Analyzer VA and 1 vCPU for the detonation VM. The detonation VM will be provisioned with 4 vCPUs, but they will be overprovisioned in a 4:1 ratio, resulting in only 1 vCPU being needed for the ESXi host.

- ESXi Host RAM = 20 GB RAM + 8 x 5 GB = 60 GB RAM

**Note**

RAM is used in a 1:1 ratio between Sandbox Analyzer VA, detonation VMs and the ESXi host. Thus, each detonation VM will require 5 GB of RAM from the ESXi host, out of which 2 GB will be allocated to the Sandbox Analyzer VA and 3 GB will be allocated for detonation VM itself.

The resulting physical host requires, in the above-mentioned scenario, at least 22 CPU cores (including hyperthreading) and at least 60 GB of RAM, with an additional 10-20% of RAM reserved for the hypervisor itself.

Typically, detonation of a sample takes nine minutes to execute and generate the detonation report, and it uses all provisioned resources. It is recommended to design your sandboxing environment starting with the detonation capacity (files/hour) and then transform this metric into needed resources at host and VM level.

4.4.5. Sandbox Analyzer Communication Requirements

Sandbox Analyzer On-Premises components use certain communication ports bound to specific network interfaces, in order to communicate between themselves and/or with Bitdefender's public servers.

The sandboxing environment requires three network interfaces:

- **eth0 – Management network interface.** It connects to GravityZone and to the ESXi host.

It is recommended to be connect eth0 to the same network as the ESXi management interface. It is also recommended to map it to a dedicated physical adapter.

The following table describes the network communication requirements for eth0:

Direction	Communication ports (on TCP)	Source/destination
Outbound	8443	GravityZone Communication Server
	443	GravityZone Virtual Appliance
	80	GravityZone Virtual Appliance
	22	ESXi host
	443	ESXi host API
Inbound	8443	Any

- **eth1 – Detonation network.** It does not require any configuration. The installation process creates the necessary virtual resources.

- **eth2 – Internet access network.** It is recommended to have unrestricted and unfiltered connection to the internet.

It is recommended that the management network and the internet access network are assigned to different subnets.

GravityZone Virtual Appliance requires access to Sandbox Analyzer Virtual Appliance on port 443 (on TCP) to view and download Sandbox Analyzer reports.

GravityZone Virtual Appliance requires connectivity to Sandbox Analyzer Virtual Appliance on port 443 (on TCP) for requesting the status of the detonated samples.

4.5. Full Disk Encryption

GravityZone Full Disk Encryption allows you to operate BitLocker on Windows endpoints and FileVault and the diskutil command-line utility on macOS endpoints via Control Center.

To ensure data protection, this module provides full disk encryption for boot and non-boot volumes, on fixed disks, and it stores the recovery keys in case the users forget their passwords.

The Encryption module uses the existing hardware resources in your GravityZone environment.

From the software perspective, the requirements are almost the same as for BitLocker, FileVault and the diskutil command-line utility and most of the limitations refer to these tools.

On Windows

GravityZone Encryption supports BitLocker, starting with version 1.2, on machines with and without a Trusted Platform Module (TPM) chip.

GravityZone supports BitLocker on the endpoints with the following operating systems:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro

- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (with TPM)
- Windows 7 Enterprise (with TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (with TPM)

*BitLocker is not included on these operating systems and must be installed separately. For more information about deploying BitLocker on Windows Server, refer to these KB articles provided by Microsoft:

- <https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server>
- [https://technet.microsoft.com/en-us/library/cc732725\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx)



Important

GravityZone does not support encryption on Windows 7 and Windows 2008 R2 without TPM.

For detailed BitLocker requirements, refer to this KB article provided by Microsoft: [https://technet.microsoft.com/en-us/library/cc766200\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx)

On Mac

GravityZone supports FileVault and diskutil on macOS endpoints running the following operating systems:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

4.6. GravityZone Communication Ports

GravityZone is a distributed solution, meaning that its components communicate with each other through the use of the local network or the Internet. Each component uses a series of ports to communicate with the others. You need to make sure these ports are open for GravityZone.

For detailed information regarding GravityZone ports, refer to [this KB article](#).

5. INSTALLING PROTECTION

GravityZone is a client-server solution. To protect your network with Bitdefender, you must deploy the GravityZone server roles, register your license, configure installation packages and deploy them via security agents on endpoints.

5.1. GravityZone Installation and Setup

To make sure installation goes smoothly, follow these steps:

1. [Prepare for installation](#)
2. [Deploy and set up GravityZone](#)
3. [Connect to Control Center and set up the first user account](#)
4. [Configure Control Center settings](#)

5.1.1. Prepare for Installation

For installation, you need a GravityZone virtual appliance image. After you deploy and set up the GravityZone appliance, you can remotely install the client or download the necessary installation packages from the Control Center web interface.

The GravityZone appliance image is available in several different formats, compatible with the main virtualization platforms. You can obtain the download links by registering for a trial on the [Bitdefender website](#).

For installation and initial setup, you must have the following at hand:

- DNS names or fixed IP addresses (either by static configuration or via a DHCP reservation) for the GravityZone appliances
- Username and password of a domain administrator
- vCenter Server, XenServer details (hostname or IP address, communication port, administrator username and password)
- License keys (check the trial registration or purchase email)
- Outgoing mail server settings
- If needed, proxy server settings
- Security certificates

5.1.2. Deploy GravityZone

A GravityZone deployment consists of one or several appliances running the server roles. The number of appliances depends on various criteria, such as: the size and design of your network infrastructure, or the GravityZone features you will use. Server roles are of three types: basic, auxiliary and optional.



Important

Auxiliary and optional roles are available only to certain GravityZone solutions.

GravityZone Role	Role Type	Deployment
Database Server	Basic (Required)	At least one instance of each role.
Update Server		A GravityZone appliance can run one, several or all of these roles.
Web Console		
Communication Server		
N/A	Optional	N/A

Depending on how you distribute the GravityZone roles, you will deploy one or more GravityZone appliances. The Database Server is the first to be installed.

In a scenario with multiple GravityZone appliances, you will install the Database Server role on the first appliance and configure all other appliances to connect to the existing database instance.

You can deploy more instances of Database Server, Web Console, and Communication Server roles. In this case, you will use Replica Set for Database Server, and load balancers for Web Console and Communication Server on the GravityZone appliances.

To deploy and set up GravityZone:

1. Download the GravityZone virtual appliance image from the Bitdefender website (link provided in registration or purchase email).
2. Import the GravityZone virtual appliance image in your virtualized environment.
3. Power on the appliance.
4. From your virtualization management tool, access the console interface of the GravityZone appliance.
5. Configure the password for `bdadmin`, the built-in system administrator.

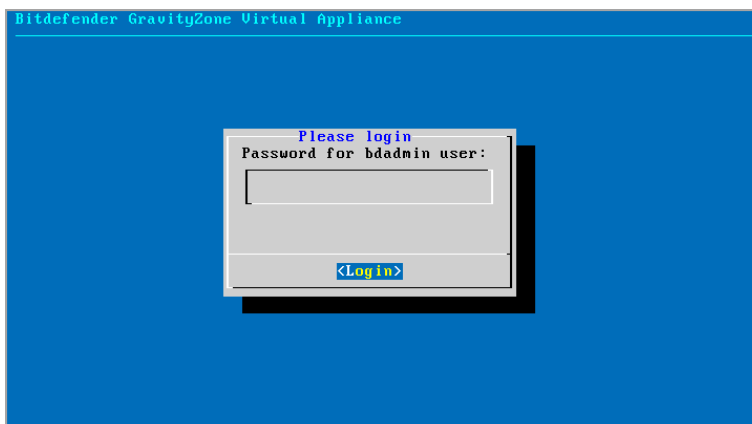
```
You need to change the initial password for badmin user. Choose an option:
[c]ontinue
[e]xit

NOTE: On this terminal, the exit option restarts this verification,
      unless initial password is changed. Otherwise the installer will run.

New password:
```

Appliance console interface: enter new password

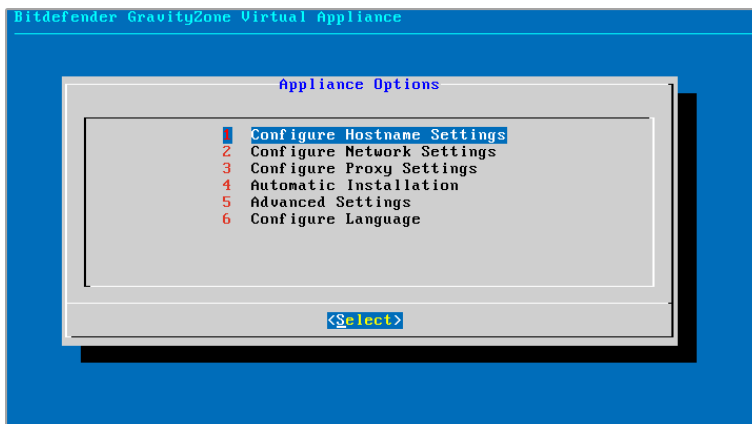
6. Log in with the password you have just set.



Appliance console interface: login

You will access the appliance configuration interface.

Use the arrow keys and the `Tab` key to navigate through menus and options. Press `Enter` to select a specific option.



Appliance console interface: main menu

7. If you need to change the interface language, select the option **Configure Language**. For configuration details, refer to [“Configure Language”](#) (p. 48).
8. [Configure the appliance hostname](#).
9. [Configure the network settings](#).
10. [Configure the proxy settings](#). (if needed)
11. Install the GravityZone server roles. You have two options:
 - [Automatic Installation](#). Select this option if you need to deploy only one GravityZone appliance in your network.
 - [Advanced Settings](#). Select this option if you need to deploy GravityZone manually or in a distributed architecture.

After deploying and setting-up the GravityZone appliance, you can anytime edit the appliance settings using the configuration interface. For more information regarding the GravityZone appliance configuration, refer to [“Managing the GravityZone Appliance”](#) (p. 75).

Configure Hostname Settings

Communication with the GravityZone roles is performed using the IP address or DNS name of the appliance they are installed on. By default, the GravityZone components communicate using IP addresses. If you want to enable communication

via DNS names, you must configure GravityZone appliances with a DNS name and make sure it correctly resolves to the configured IP address of the appliance.

Prerequisites:

- Configure the DNS record in the DNS server.
- The DNS name must correctly resolve to the configured IP address of the appliance. Therefore, you must make sure the appliance is configured with the correct IP address.

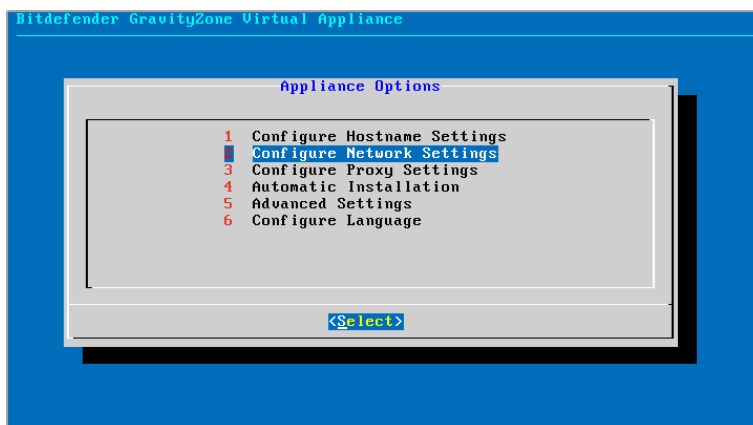
To configure the hostname settings:

1. From the main menu, select **Configure Hostname Settings**.
2. Enter the hostname of the appliance and the Active Directory domain name (if needed).
3. Select **OK** to save the changes.

Configure Network Settings

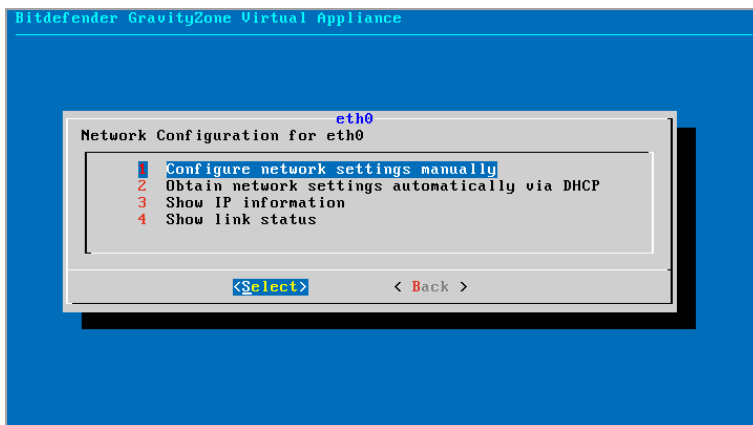
You can configure the appliance to automatically obtain network settings from the DHCP server or you can manually configure network settings. If you choose to use DHCP, you must configure the DHCP Server to reserve a specific IP address for the appliance.

1. From the main menu, select **Configure Network Settings**.



Appliance console interface: network settings option

2. Select the network interface.
3. Select the configuration method:
 - **Configure network settings manually.** You must specify the IP address, network mask, gateway address and DNS server addresses.
 - **Obtain network settings automatically via DHCP.** Use this option only if you have configured the DHCP Server to reserve a specific IP address for the appliance.



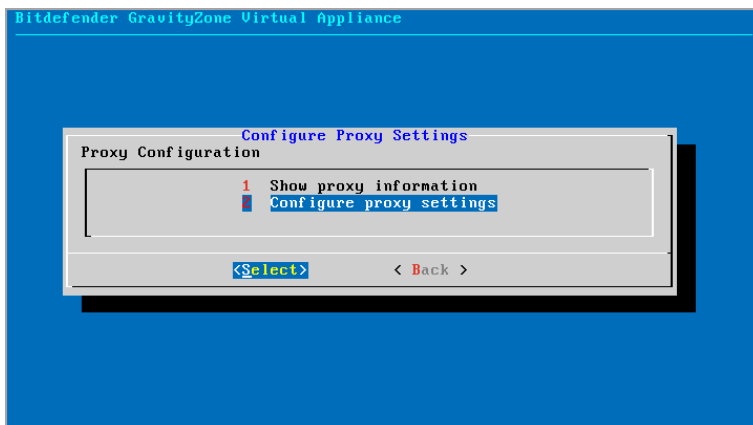
Appliance console interface: network configuration

4. You can check current IP configuration details or link status by selecting the corresponding options.

Configure Proxy Settings

If you want the appliance to connect to the Internet through a proxy server, you must configure the proxy settings.

1. From the main menu, select **Configure Proxy Settings**.
2. Select **Show proxy information** to check if proxy is enabled.
3. Select **OK** to return to the previous screen.
4. Select again **Configure proxy settings**.



Appliance console interface: configure proxy settings

5. Enter the proxy server address. Use the following syntax:

- If the proxy server does not require authentication:

`http(s)://<IP/hostname>:<port>`

- If the proxy server requires authentication:

`http(s)://<username>:<password>@<IP/hostname>:<port>`

6. Select **OK** to save the changes.

Automatic Installation

During automatic installation all basic roles install on the same appliance. For a distributed GravityZone deployment, refer to [“Advanced Settings” \(p. 46\)](#).



Important

Automatic deployment will also install the Security Server, embedded into the GravityZone appliance. You can remove this role afterwards because your license type restricts its use.

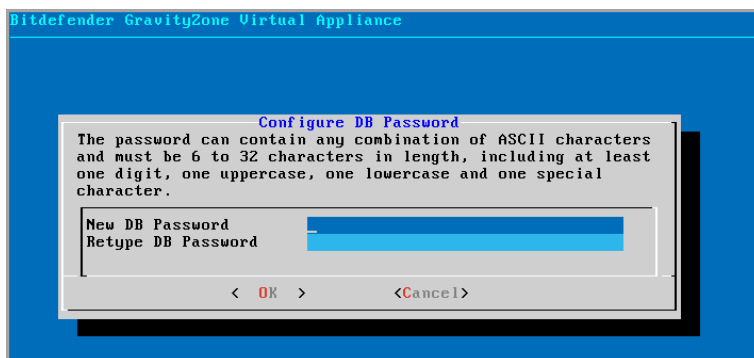
The option to install roles automatically is available only at the initial setup of GravityZone.

To install the roles automatically:

1. From the main menu, select **Automatic Installation**.

2. Read and accept the End User License Agreement (EULA) to continue.
3. Confirm the roles to be installed.
4. Set the password for the Database Server.

The password can contain any combination of ASCII characters and must be 6 to 32 characters in length, including at least one digit, one uppercase, one lowercase and one special character.



Appliance console interface: configure database password

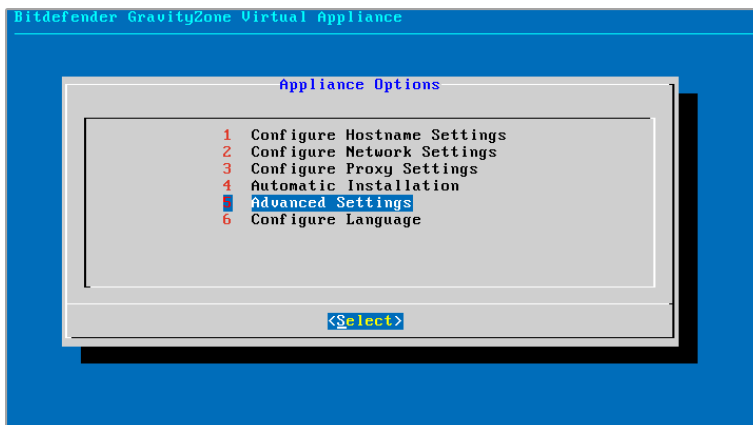
5. Wait until installation process is complete.

Advanced Settings

Use this option to install only a part or all of the GravityZone roles, individually, or to extend your GravityZone infrastructure. You can install the roles on one or more appliances. This installation method is required when staging updates or in distributed GravityZone architectures to scale GravityZone in large networks and to ensure high availability of the GravityZone services.

To install the roles individually:

1. From the main menu, select **Advanced Settings**.



Appliance console interface: install roles

2. Select **Install/Uninstall Roles** to install the appliance in a GravityZone environment with a single database server.



Note

The other options are for extending the GravityZone deployment to a distributed architecture. For more information, refer to [“Connect to Existing Database”](#) (p. 86) or to [“Connect to Existing Database \(Secure VPN Cluster\)”](#) (p. 87).

3. Select **Add or remove roles**. A confirmation message will appear.
4. Press `Enter` to continue.
5. Press the `Space` bar and then the `Enter` key to install the Database Server role. You must confirm your choice by pressing `Enter` again.
6. Set the database password.
The password can contain any combination of ASCII characters and must be 6 to 32 characters in length, including at least one digit, one uppercase, one lowercase and one special character.
7. Press `Enter` and wait for the installation to complete.
8. Install the other roles. by choosing **Add or remove roles** from the **Install/Uninstall Roles** menu and then the roles to install.

- a. Choose **Add or remove roles** from the **Install/Uninstall Roles** menu.
- b. Read the End User License Agreement. Press `Enter` to accept and continue.

**Note**

This is required only once after installing the Database Server.

- c. Select the roles to install. Press the `Space` bar to select a role and `Enter` to proceed.
- d. Press `Enter` to confirm and then wait for the installation to complete.

**Note**

Each role is normally installed within a few minutes. During installation, required files are downloaded from the Internet. Consequently, the installation takes more time if the Internet connection is slow. If the installation hangs, redeploy the appliance.

Configure Language

Initially, the appliance configuration interface is in English.

To change the interface language:

1. Select **Configure Language** from the main menu.
2. Select the language from the available options. A confirmation message will appear.

**Note**

You may need to scroll down to view your language.

3. Select **OK** to save the changes.

5.1.3. Control Center Initial Setup

After deploying and setting up the GravityZone appliance, you must access the Control Center web interface and configure your Company Administrator account.

1. In the address bar of your web browser, enter the IP address or the DNS hostname of the Control Center appliance (using the `https://` prefix). A configuration wizard will appear.

2. Provide the license key required for validating the purchased GravityZone solution. You can also provide any GravityZone add-on key you may have.

Check the trial registration or purchase email to find your license keys.

- a. Click the **+ Add** button at the upper side of the table. A configuration window will appear.
- b. Select the license registration type (online or offline).
- c. Enter the license key in the **License key** field. For offline registration, you are required to provide also the registration code.
- d. Wait until the license key is validated. Click **Add** to finish.

The license key and its expiry date will appear in the license table.



Note

- During the initial setup, you must provide a valid basic license key to start using GravityZone. You can afterwards add license keys for add-ons, or to modify the existing ones.
- You can use the add-ons as long as a valid basic license is provided. Otherwise you will view the features, but you will be unable to use them.

Product Registration

MyBitdefender Account
License key
Create Accounts

English ▼

Enter License Keys

+ Add

⌛ Refresh

Key	Service	Expiry Date

Next

Initial setup - Provide license key

3. Click **Next** to continue.
4. Fill in your company information, such as company name, address and phone.

5. You can change the logo displayed in Control Center and also in your company's reports and email notifications as follows:
 - Click **Change** to browse for the image logo on your computer. The image file format must be .png or .jpg and the image size must be 200x30 pixels.
 - Click **Default** to delete the image and reset to the image provided by Bitdefender.
6. Specify the required details for your company administrator account: username, email address and a password. The password must contain at least one upper case character, at least one lower case character and at least one digit or special character.

Product Registration

MyBitdefender Account

License key

Create Accounts


English ▼

Enter Company Details

Company Name:

Address:

Phone:

Logo:  The logo needs to have the size 200x30 px, and needs to be in png or jpg format

Change **Default**

Enter Company Administrator Account Details

Username:

Email:

Full Name:

Password:

Confirm password:

Create account

Initial setup - Configure your account

7. Click **Create account**.

The company administrator account will be created and you will automatically log on with the new account to Bitdefender Control Center.

5.1.4. Configure Control Center Settings

After the initial setup, you need to configure Control Center settings. As Company Administrator, you can do the following:

- Configure mail, proxy and other general settings.
- Run or schedule a Control Center database backup.
- Set up integration with Active Directory and virtualization management tools (vCenter Server, XenServer).
- Install security certificates.

The screenshot shows the Bitdefender GravityZone web interface. The top navigation bar is blue with the Bitdefender GravityZone logo on the left and a user profile 'Welcome, Admin' on the right. A left sidebar contains a menu with items like Dashboard, Network, Packages, Tasks, Policies, Reports, Quarantine, Accounts, and Configuration (which is highlighted). The main content area has a sub-header with tabs: Mail Server, Proxy, Miscellaneous, Backup, Active Directory, Virtualization, and Certificates. The 'Mail Server' tab is active, showing 'Mail Server Settings'. The settings include: 'Mail server (SMTP): *' with the value 'mail.comp.com'; 'Port: *' with the value '25'; 'Encryption type:' with a dropdown set to 'None'; 'From email: *' with the value 'noreply@comp.com'; and an unchecked checkbox for 'Use authentication'. Below this, there is a 'Username: *' field.

Mail Server settings

Mail Server

Control Center requires an external mail server to send email communications.



Note

It is recommended to create a dedicated mail account to be used by Control Center.

To enable Control Center to send emails:

1. Go to the **Configuration** page.
2. Select the **Mail Server** tab.

3. Select **Mail Server Settings** and configure the required settings:
 - **Mail server (SMTP).** Enter the IP address or hostname of the mail server that is going to send the emails.
 - **Port.** Enter the port used to connect to the mail server.
 - **Encryption type.** If the mail server requires an encrypted connection, choose the appropriate type from the menu (SSL, TLS or STARTTLS).
 - **From email.** Enter the email address that you want to appear in the From field of the email (sender's email address).
 - **Use authentication.** Select this check box if the mail server requires authentication. You must specify a valid username / email address and password.
4. Click **Save**.

Control Center automatically validates the mail settings when you save them. If the provided settings cannot be validated, an error message informs you of the incorrect setting. Correct the setting and try again.

Proxy

If your company connects to the Internet through a proxy server, you must configure the proxy settings:

1. Go to the **Configuration** page.
2. Select the **Proxy** tab.
3. Select **Use Proxy Settings** and configure the required settings:
 - **Address** - type in the IP address of the proxy server.
 - **Port** - type in the port used to connect to the proxy server.
 - **Username** - type in a user name recognized by the proxy.
 - **Password** - type in the valid password of the previously specified user.
4. Click **Save**.

Miscellaneous

From the **Configuration** page > **Miscellaneous** tab you can configure the following general preferences:

- **When an unavailable kit is needed.** You can configure an automated action for this situation by choosing one of the following options:
 - **Download the package automatically**
 - **Notify the administrator and do not download**
- **Concurrent deployments.** Administrators can remotely deploy security components by running installation tasks. Use this option to specify the maximum number of simultaneous deployments that can be performed at a time.

For example, if the maximum number of concurrent deployments is set to 10 and a remote client installation task is assigned to 100 computers, Control Center will initially send 10 installation packages through the network. In this case, the client installation is performed simultaneously on a maximum number of 10 computers, all the other sub-tasks being in pending state. As soon as a sub-task is done, another installation package is sent, and so on.

- **Enforce two-factor authentication for all accounts.** The two-factor authentication (2FA) adds an extra layer of security to GravityZone accounts, by requiring an authentication code in addition to Control Center credentials. This feature requires downloading and installing the either the Google Authenticator, Microsoft Authenticator, or any two-factor TOTP (Time-Based One-Time Password Algorithm) authenticator app - compatible with the standard RFC6238 - on the user's mobile device, then linking the app to the GravityZone account and using it with each Control Center login. The authentication app generates a six-digit code each 30 seconds. To complete the Control Center login, after entering the password, the user will have to provide also the six-digit authentication code.

Two-factor authentication is enabled by default when creating a company. After that, at login, a configuration window will prompt users to enable this feature. Users will have the option to skip enabling 2FA for three times only. At the fourth login attempt, skipping the 2FA configuration will not be possible and the user will not be allowed to log in.

If you want to deactivate the 2FA enforcement for all GravityZone accounts in your company, just uncheck the option. You will be prompted with a confirmation message before the changes come into effect. From this point on, users will still have 2FA activated, but they will be able to deactivate it from their account settings.

**Note**

- You can view the 2FA status for a user account in the **Accounts** page.
- If a user with 2FA enabled cannot log in to GravityZone (because of new device or lost secret key), you can reset its two-factor authentication activation from the user account page, under **Two-factor authentication** section. For more details, refer to **User Accounts > Managing Two-factor Authentication** chapter from the Administrator's Guide.

- **NTP Server Settings.** The NTP server is used to synchronize time between all GravityZone appliances. A default NTP server address is provided, which you can change in the **NTP Server Address** field.

**Note**

For the GravityZone appliances to communicate with the NTP Server, 123 (UDP) port must be open.

- **Enable Syslog.** By enabling this feature, you allow GravityZone to send notifications to a logging server that uses the Syslog protocol. This way you have the possibility to better monitor GravityZone events.

To view or configure the list of notifications sent to the Syslog server, refer to the **Notifications** chapter from GravityZone Administrator's Guide.

To enable logging to a remote Syslog server:

1. Select the **Enable Syslog** check box.
2. Enter the server name or IP, the preferred protocol and the port Syslog listens to.
3. Select in the format in which to send the data to the Syslog server:
 - **JSON Format.** JSON is a lightweight data-interchange format that is completely independent from any programming language. JSON represents the data in human readable text format. In JSON format, the details of each event are structured into objects, each object consisting in a name/value pair.

For example:

```
{  
  "name": "Login from new device",
```

```
"created": "YYYY-MM-DDThh:mm:ss+hh:ss",
"company_name": "companyname",
"user_name": "username",
"os": "osname",
"browser_version": "browserversion",
"browser_name": "browsername",
"request_time": "DD MMM YYYY, hh:mm:ss +hh:ss",
"device_ip": "computerip"
}
```

For more information, refer to www.json.org.

This is the default format in GravityZone.

- **Common Event Format (CEF)**. CEF is an open standard developed by ArcSight, which simplifies log management.

For example:

```
CEF:0|Bitdefender|GZ|<GZ version>|NNNNN|Login from new
device|3|start=MMM DD YYYY hh:mm:ss+hh:mm
BitdefenderGZCompanyName=companyname suser=username
BitdefenderGZLoginOS=osname
BitdefenderGZAuthenticationBrowserName=browsername
BitdefenderGZAuthenticationBrowserVersion=browserversion
dvchost=computerip
```

For more information, refer to [ArcSight Common Event Format \(CEF\) Implementation Standard](#).

In the **Notifications** chapter of the Administrator's Guide, you can view the available notification types for each format.

4. Click the **+** **Add** button from the **Action** column.

Click **Save** to apply the changes.

Backup


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

Each database backup command creates a `tgz` file (GZIP Compressed Tar Archive file) to the location specified in the backup settings.

When several administrators have manage privileges over the Control Center settings, you can also configure the **Notification Settings** to alert you each time a database backup has been completed. For more information, refer to the **Notifications** chapter from GravityZone Administrators Guide.

Creating Database Backups

To run a database backup:

1. Go to the **Configuration** page in Control Center and click the **Backup** tab.
2. Click the  **Backup Now** button at the upper side of the table. A configuration window will appear.
3. Select the type of location where the backup archive will be saved:

- **Local**, for saving the backup archive to the GravityZone appliance. In this case, you have to specify the path to the specific directory from the GravityZone appliance where the archive will be saved.

The GravityZone appliance has a Linux directory structure. For example, you can choose to create the backup to the `tmp` directory. In this case, enter `/tmp` in the **Path** field.

- **FTP**, for saving the backup archive to a FTP server. In this case, enter the FTP details in the following fields.
 - **Network**, for saving the backup archive to a network share. In this case, enter the path to the network location that you want (for example, `\\computer\folder`), the domain name and the domain user credentials.
4. Click the **Test Settings** button. A text notification will inform you if the specified settings are valid or invalid.


To create a backup, all the settings have to be valid.

5. Click **Generate**. The **Backup** page will be displayed. A new backup entry will be added to the list. Check the **Status** of the new backup. When the backup is completed, you will find the `tgz` archive at the specified location.

**Note**

The list available in the **Backup** page contains the logs of all created backups. These logs do not provide access to the backup archives; they only display details of the created backups.

To schedule a database backup:

1. Go to the **Configuration** page in Control Center and click the **Backup** tab.
2. Click the  **Backup Settings** button at the upper side of the table. A configuration window will appear.
3. Select **Scheduled Backup**.
4. Configure the backup interval (daily, weekly or monthly) and the start time.
For example, you can schedule backups to run weekly, every Friday, starting at 22:00.
5. Configure the scheduled backup location.
6. Select the type of location where the backup archive will be saved:
 - **Local**, for saving the backup archive to the GravityZone appliance. In this case, you have to specify the path to the specific directory from the GravityZone appliance where the archive will be saved.
The GravityZone appliance has a Linux directory structure. For example, you can choose to create the backup to the `tmp` directory. In this case, enter `/tmp` in the **Path** field.
 - **FTP**, for saving the backup archive to a FTP server. In this case, enter the FTP details in the following fields.
 - **Network**, for saving the backup archive to a network share. In this case, enter the path to the network location that you want (for example, `\\computer\folder`), the domain name and the domain user credentials.
7. Click the **Test Settings** button. A text notification will inform you if the specified settings are valid or invalid.
To create a backup, all the settings have to be valid.
8. Click **Save** to create the scheduled backup.

Restoring a Database Backup

When from various reasons your GravityZone instance is working improperly (failed updates, dysfunctional interface, corrupted files, errors, etc.), you can restore the GravityZone database from a backup copy using:

- The same appliance
- A fresh GravityZone image
- The Replica Set feature

Choose the option that best suits your situation and proceed with the restoration procedure only after you have carefully read the prerequisites described hereinafter.

Restoring the Database to the Same GravityZone VA

Prerequisites

- A SSH connection to the GravityZone appliance, using the **root** privileges.
You can use **putty** and **bdadmin**'s credentials to connect to the appliance via SSH, then run the command `sudo su` to switch to the **root** account.
- The GravityZone infrastructure has not changed since the backup.
- The backup is more recent than April 30th, 2017 and the GravityZone version is higher than 6.2.1-30. If otherwise, contact the Technical Support team.
- In distributed architectures, GravityZone has not been configured to use database replication (Replica Set).

To verify the configuration, follow these steps:

1. Open the `/etc/mongodb.conf` file.
2. Check that `replSet` is not configured, as in the example below:

```
# replSet = setname
```



Note

To restore the database when Replica Set is enabled, refer to [“Restoring the database in a Replica Set environment”](#) (p. 63).

- No CLI processes are running.

To make sure all CLI processes are stopped, run the following command:

```
# killall -9 perl
```

- The **mongoconsole** package is installed on the appliance.

To verify the condition is met, run this command:

```
# /opt/bitdefender/bin/mongoshellrestore --version
```

The command should not return any errors, otherwise run:

```
# apt-get update  
# apt-get install --upgrade mongoconsole
```

Restoring the database

1. Go to the location containing the database archive:

```
# cd /directory-with-backup
```

, where **directory-with-backup** is the path to the location with the backup files.

For example:

```
# cd /tmp/backup
```

2. Restore the database.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password' \  
--authenticationDatabase admin --gzip --drop --archive < \  
gz-backup-$YYYY-$MM-$DD(timestamp).tar.gz
```

**Important**

Make sure to replace `GZ_db_password` with the actual password of the GravityZone Database Server and the timestamp variables in the archive's name with the actual date.

For example, the actual date should look like this:

```
gz-backup-2019-05-17 (1495004926) .tar.gz
```

3. Restart the appliances.

Database restoration is now complete.

Restoring the Database From a Decommissioned GravityZone VA

Prerequisites

- A fresh GravityZone VA installation:
 - With the same IP as the old appliance
 - Having **ONLY** the Database Server role installed.
- You can download the GravityZone VA image from [here](#).
- A SSH connection to the GravityZone virtual appliance, using the **root** privileges.
- The GravityZone infrastructure has not changed since the backup was made.
- The backup is more recent than April 30th, 2017.
- In distributed architectures, GravityZone has not been configured to use database replication (Replica Set).

If you use Replica Set in your GravityZone environment, you also have the Database Server role installed on other appliance instances.

To restore the database when Replica Set is enabled, refer to [“Restoring the database in a Replica Set environment”](#) (p. 63).

Restoring the database

1. Connect to the GravityZone appliance via SSH and switch to **root**.
2. Stop VASync:

```
# stop vasync
```

3. Stop CLI:

```
# # killall -9 perl
```

4. Go to the location where the backup is:

```
# cd /directory-with-backup
```

, where `directory-with-backup` is the path to the location with the backup files.

For example:

```
# cd /tmp/backup
```

5. Restore the database.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password' \  
--authenticationDatabase=admin --gzip --drop \  
--archive='/home/bdadmin/gz-backup-YYYY-MM-DD(timestamp).tar.gz
```



Important

Make sure to replace `GZ_db_password` with the actual password of the GravityZone Database Server and the timestamp variables in the archive's name with the actual date.

For example, the actual date should look like this:

```
gz-backup-2019-05-17(1495004926).tar.gz
```

6. Restore the old appliance ID:

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ-db_password' \  
--eval print(db.applianceInstalls.findOne({name:'db'}).\  
applianceId) --quiet > /opt/bitdefender/etc/applianceid
```

**Important**

Make sure to replace `GZ_db_password` with the actual password of the GravityZone Database Server.

7. Remove the reference to the old roles.

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ_db_password' --eval\  
'db.applianceInstalls.remove({ip:db.applianceInstalls.findOne(  
{name:"db"}).ip,name:{"$ne": "db"}});' --quiet devdb
```

**Important**

Make sure to replace `GZ_db_password` with the actual password of the GravityZone Database Server.

8. Start VASync:

```
# start vasync
```

9. Start CLI:

```
# /opt/bitdefender/eltiw/installer
```

10. Install the other roles.

```
# dpkg -l gz*
```

Note that the database schema has been successfully upgraded to the latest version:

```
> db.settings.findOne().database  
{
```

```
"previousVersion" : "000-002-009",
"ranCleanUpVersions" : {
  "b0469c84f5bf0bec0b989ae37161b986" : "000-002-008"
},
"updateInProgress" : false,
"updateTimestamp" : 1456825625581,
"version" : "000-002-011"
}
```

11. Restart the appliance.

Database restoration is now complete.

Restoring the database in a Replica Set environment

If you have deployed the database in a Replica Set environment, you can find the official restore procedure on the [mongoDB online manual](#) (English only).



Note

The procedure requires advanced technical skills and should be done only by a trained engineer. If you encounter difficulties, please contact our [Technical Support](#) to assist you in restoring the database.

Active Directory

Through Active Directory integration, you are able to import into Control Center the existing inventory from Active Directory on-premises and from Active Directory hosted in Microsoft Azure, simplifying security deployment, management, monitoring and reporting. Additionally, Active Directory users can be assigned different user roles in Control Center.

To integrate and synchronize GravityZone with an Active Directory domain:

1. Go to **Configuration > Active Directory > Domains** and click **+ Add**.
2. Configure the required settings:
 - Synchronization interval (in hours)
 - Active Directory domain name (including the domain extension)
 - Username and password of a domain administrator
 - Location in Network Inventory where to display the AD endpoints:
 - Keep AD structure and ignore empty OUs
 - Ignore AD structure, import to Custom Groups

- Keep AD structure only with selected OUs
- The Domain Controllers with which Control Center is synchronizing. Expand the **Request Domain Controller** section and choose the controllers from the table.

3. Click **Save**.



Important

Whenever the user password changes, remember to also update it in Control Center.

Access Permissions

With access permissions you can grant GravityZone Control Center access to Active Directory (AD) users, based on access rules. To integrate and synchronize AD domains, refer to [Active Directory](#). For more information on managing user accounts via access rules, refer to the **User Accounts** chapter from the GravityZone Installation Guide.

Virtualization Providers

GravityZone can currently integrate with VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 and Microsoft Azure.

- [“Integrating with vCenter Server”](#) (p. 64)
- [“Integrating with XenServer”](#) (p. 65)
- [“Integrating with Nutanix Prism Element”](#) (p. 66)
- [“Integrating with Amazon EC2”](#) (p. 67)
- [“Integrating with Microsoft Azure”](#) (p. 69)
- [“Managing Platform Integrations”](#) (p. 70)



Important

Whenever you set up a new integration with another vCenter Server, XenServer, Nutanix Prism Element or Microsoft Azure, remember to also review and update access privileges for existing users.

Integrating with vCenter Server

You can integrate GravityZone with one or multiple vCenter Server systems. vCenter Server systems in Linked Mode must be added separately to Control Center.

To set up integration with a vCenter Server:

1. Go to the **Configuration** page in Control Center and navigate to **Virtualization Providers > Management Platforms**.
2. Click the **+ Add** button at the upper side of the table and choose **vCenter Server** from the menu. A configuration window will appear.
3. Specify the vCenter Server details.
 - Name of the vCenter Server system in Control Center
 - Hostname or IP address of the vCenter Server system
 - vCenter Server port (default 443)
4. Specify the credentials to be used to authenticate with the vCenter Server. The user whose credentials you provide must have root or administrator permissions on the vCenter Server.
5. **Restrict policy assignment from the network view.** Use this option to control the network administrators permission to change the virtual machines policies via the **Computers and Virtual Machines** view in the **Network** page. When this option is selected, administrators can change the virtual machines policies only from the **Virtual Machines** view of the network inventory.
6. Click **Save**. You will be asked to accept the security certificates for vCenter Server and NSX Manager. These certificates ensure a secure communication between GravityZone and VMware components, resolving the risk of man-in-the-middle attacks.

You can verify if the correct certificates were installed by checking the browser's site information for each VMware component against the certificate information displayed in Control Center.

7. Select the check boxes to accept using the certificates.
8. Click **Save**. You will be able to view the vCenter Server in the active integrations list.

In the end, you can view that the vCenter Server is synchronizing. Wait for a couple of minutes until synchronization finishes.

Integrating with XenServer

You can integrate GravityZone with one or multiple XenServer systems.

To set up integration with a XenServer:

1. Go to the **Configuration** page in Control Center and click the **Virtualization Providers** tab.

2. Click the **+** **Add** button at the upper side of the table and choose **XenServer** from the menu. A configuration window will appear.
3. Specify the XenServer details.
 - Name of the XenServer system in Control Center
 - Hostname or IP address of the XenServer system
 - XenServer port (default 443)
4. Specify the credentials to be used to authenticate with the XenServer. You can choose to use the credentials provided for integration with Active Directory or a different set of credentials.
5. **Restrict policy assignment from the network view.** Use this option to control the network administrators permission to change the virtual machines policies via the **Computers and Virtual Machines** view in the **Network** page. When this option is selected, administrators can change the virtual machines policies only from the **Virtual Machines** view of the network inventory.
6. Click **Save**. You will be able to view the vCenter Server in the active integrations list and that it is synchronizing. Wait for a couple of minutes until synchronization finishes.

Integrating with Nutanix Prism Element

You can integrate GravityZone with one or multiple Nutanix Prism Element clusters, whether they are registered to Nutanix Prism Central or not.

To set up integration with Nutanix Prism Element:

1. Go to the **Configuration** page in Control Center and click the **Virtualization Providers** tab.
2. Click the **+** **Add** button at the upper side of the table and choose **Nutanix Prism Element** from the menu. A configuration window will appear.
3. Specify the Nutanix Prism Element details:
 - Name of the Nutanix Prism Element in Control Center.
 - The IP address of a Controller Virtual Machine (CVM) from the Nutanix Prism Element cluster or the IP address of the Cluster Virtual IP.
 - Nutanix Prism Element port (default 9440).
4. Specify the credentials to be used to authenticate with Nutanix Prism Element.

**Important**

The user whose credentials you provide must have Cluster Admin or User Admin privileges in Nutanix Prism Element.

5. **Restrict policy assignment from the network view.** Use this option to control the network administrators' permission to change the virtual machines policies via the **Computers and Virtual Machines** view in the **Network** page. When this option is selected, administrators can change the virtual machines policies only from the Virtual Machines view of the network inventory.

6. Click **Save**. You will be asked to accept the security certificates for Nutanix Prism. These certificates ensure a secure communication between GravityZone and Nutanix Prism Element, resolving the risk of man-in-the-middle attacks.

You can verify if the correct certificates were installed by checking the browser's site information for each Nutanix Prism Element cluster or CVM against the certificate information displayed in Control Center.

7. Select the check boxes to accept using the certificates.

8. Click **Save**.

If you entered a CVM IP to configure the integration, you will be asked in a new window if you want to use the Cluster Virtual IP instead of the CVM IP:

- Click **Yes** to use the Cluster Virtual IP for integration. The Cluster Virtual IP will replace the CVM IP in the Nutanix Prism Element details.
- Click **No** to further use the CVM IP.

**Note**

As best practice, it is recommended to use the Cluster Virtual IP rather than the CVM IP. This way, the integration remains active even when a particular host becomes unavailable.

- In the **Add Nutanix Prism Element** window, click **Save**.

You will be able to view the Nutanix Prism Element in the active integrations list. Wait for a couple of minutes until the synchronization finishes.

Integrating with Amazon EC2

You can integrate GravityZone with your Amazon EC2 inventory and protect your EC2 instances hosted in the Amazon cloud.

Prerequisites:

- The access and secret keys of a valid AWS account
- The AWS account must have the following permissions:
 - `IAMReadOnlyAccess`
 - `AmazonEC2ReadOnly` for all AWS regions

You can create several Amazon EC2 integrations. For each integration, you need to provide a valid AWS user account.



Note

It is not possible to add multiple integrations using the credentials of IAM roles created for the same AWS account.

To set up integration with Amazon EC2:

1. Go to the **Configuration** page in Control Center and click the **Virtualization Providers** tab.
2. Click the **+ Add** button at the upper side of the table and choose **Amazon EC2 Integration** from the menu. A configuration window will appear.
3. Specify the Amazon EC2 integration details:
 - The integration name. When adding several Amazon EC2 integrations, you can identify them by name.
 - The access and secret keys of the AWS user account.
4. **Restrict policy assignment from the network view.** Use this option to control the network administrators permission to change the virtual machines policies via the **Computers and Virtual Machines** view in the **Network** page. When this option is selected, administrators can change the virtual machines policies only from the **Virtual Machines** view of the network inventory.
5. Click **Save**. If the provided credentials are valid, the integration will be created and added to the grid.

Wait a few moments while GravityZone synchronizes with the Amazon EC2 inventory.

Integrating with Microsoft Azure

You can integrate GravityZone with Microsoft Azure and protect your virtual machines hosted in the Microsoft cloud.

Prerequisites:

- Azure application with Reader permission
- Active Directory ID
- Application ID
- Application Secret

For details about obtaining the required credentials and setting up the Azure application, refer to this [KB article](#).

You can create several Microsoft Azure integrations. For each integration, you must have a valid Active Directory ID.


To set up integration with Microsoft Azure:

1. Go to the **Configuration** page in Control Center and click the **Virtualization Providers** tab.
2. Click the **+ Add** button at the upper side of the table and choose **Azure Integration** from the menu. A configuration window will appear.
3. Specify the Azure integration details:
 - **The integration name.** When adding several Azure integrations, you can identify them by name.
 - **Active Directory ID.** Each instance of Azure Active Directory has a unique identifier available in the Microsoft Azure account details.
 - **Application ID.** Each Azure application has a unique identifier available in the application details.
 - **Application Secret.** The application secret is the value displayed when saving a key in the Azure application settings.
4. Select the option **Restrict policy assignment from the network view** to change the policy only from the **Virtual Machines** view. If deselected, you can change the policy from the **Computers and Virtual Machines** view.
5. Click **Save**. If the provided credentials are valid, the integration will be created and added to the grid.


Wait a few moments while GravityZone synchronizes with the Microsoft Azure inventory.


Managing Platform Integrations

To edit or update a platform integration:

1. In Control Center, go to the **Configuration > Virtualization Providers** tab.
2. Click the  **Edit** button in the **Action** column.
3. Configure the rule settings as needed. For more information, refer to one of the following sections, whichever is applicable:
 - [“Integrating with vCenter Server” \(p. 64\)](#)
 - [“Integrating with XenServer” \(p. 65\)](#)
 - [“Integrating with Nutanix Prism Element” \(p. 66\)](#)
 - [“Integrating with Amazon EC2” \(p. 67\)](#)
 - [“Integrating with Microsoft Azure” \(p. 69\)](#)
4. Click **Save**. Wait a couple of minutes until the server re-syncs.


Nutanix Prism Element, Amazon EC2 and Microsoft Azure integrations are automatically synchronized every 15 minutes. You can manually synchronize an integration at any time, as follows:

1. In Control Center, go to the **Configuration > Virtualization Providers** tab.
2. Click the  **Resync Inventory** button in the **Action** column.
3. Click **Yes** to confirm the action.

The  **Resync Inventory** button is especially useful when the integration status changes and requires synchronization, as in the following situations:

- For the Nutanix Prism Element integration:
 - The user has no more administrative privileges in the inventory.
 - The user becomes invalid (changed or deleted password).
 - The security certificate becomes invalid.
 - There is a connection error.
 - A host is added or removed in the Nutanix Prism Element cluster.
- For the Microsoft Azure integration:
 - A subscription is added or removed in Microsoft Azure.

- Virtual machines are added or removed in the Microsoft Azure inventory.

You can also synchronize the integration by clicking the  **Edit** button, then clicking **Save**.

To make sure the latest information is being displayed, click the **Refresh** button at the upper side of the table.


Security Providers

GravityZone Security for Virtualized Environments integrates with the VMware NSX-T Data Center through NSX-T Manager.

Integrating with NSX-T Manager

NSX-T Manager is the management plane of your vCenter Servers integrated with an NSX-T Data Center. For the integration to work, you will need to set up the integration for vCenter Servers associated with the NSX-T Manager. For more information, refer to [Integrating with vCenter Server](#).

To setup integration with NSX-T Manager:

1. In Control Center, navigate to **Configuration > Virtualization Providers > Security Providers**.
2. Click the  **Add** button at the upper side of the table. A configuration window will appear.
3. Specify the NSX-T integration details:
 - Name of the NSX-T integration.
 - Hostname or the IP address of the associated vCenter Server system.
 - NSX-T port (default 433).
4. Specify the credentials to authenticate with the vCenter Server. You can choose to use the credentials provided for integration with Active Directory or a different set of credentials. The user whose credentials you provide must have root or administrator permissions on the vCenter Server.
5. Click **Save**.

The Control Center is now integrated with NSX-T. To apply endpoint protection to your VMs through GravityZone Guest Introspection policy, refer to the [Configure and apply endpoint protection to VMware NSX-T guest VMs through GravityZone Guest Introspection policy](#) KB article.

**Note**

GravityZone can only be used to protect the associated vCenter Server.

NTSA

Within this section you can configure the integration with Bitdefender Network Traffic Security Analytics, an enterprise security solution that accurately detects breaches and provides insights into advanced attacks by analyzing network traffic. To learn more about this solution, refer to the [Bitdefender NTSA documentation](#).

**Important**

The NTSA integration section is available only after providing an NTSA valid license key in the **Configuration > License** page.

To configure the NTSA integration, you need to have the NTSA solution installed in your environment and credentials to access the NTSA web console.

During the integration, you will be required to provide the NTSA web console address (IP or Hostname) and a token (pairing key) generated in the NTSA web console, as explained hereinafter.

Configure the NTSA integration

1. Log in to GravityZone Control Center.
2. Go to the **Configuration** page and click the NTSA tab.
3. Enable the **Integrate with Network Traffic Security Analytics (NTSA)** option.
4. Enter the following data:
 - The NTSA web console address (IP / Hostname).
 - The port used by GravityZone to communicate with NTSA (443 by default).
 - The pairing key (token) generated by NTSA web console as follows:
 - a. Access your NTSA web console and go to the **Licensing** page.
 - b. Select the option **Integration with GravityZone**.
 - c. Click **Generate a Pairing Key**. The key will appear automatically.
 - d. Use the **Copy to clipboard** button to get the pairing key.
 - e. Click **OK** to confirm.

5. Verify that the displayed host fingerprint matches the hash of SSL certificate from the NTSA appliance, then enable the option **I accept the certificate**.
6. Click **Save**.

When the configuration completed successfully, the integration will be displayed as **Synchronized**. The NTSA integration can have the following statuses:

- **N/A**: the integration has not been configured yet.
- **Synchronized**: the integration is configured and enabled.
- **Invalid token**: the pairing key from the NTSA web console is invalid.
- **Connection error**: could not connect to the specified NTSA web console address (invalid IP / Hostname).
- **Certificate error**: the current fingerprint of the SSL certificate from the NTSA appliance does not match the initially accepted fingerprint.
- **Unknown error**: there is an unknown communication error.

The **Last status change** field displays the date and time of the last successful change of integration settings, or when the integraton status has changed.

Once the integration with NTSA is configured, you may disable / enable the integration using the check box available at the upper side of the **NTSA** page.

Linking your GravityZone and NTSA accounts

After configuring the integration, your GravityZone and NTSA accounts will be linked and you can easily navigate to the NTSA web console as follows:

1. In GravityZone Control Center, click the **NTSA** button placed on the lower-left corner of the window.
2. You will be forwarded to the login page of the NTSA web console. After entering your NTSA login credentials, you can start navigating the NTSA web console.

You only need to enter your NTSA credentials the first time. Afterwards, you will be granted access to the NTSA web console automatically by clicking the **NTSA** button, without being prompted to log in.

Deleting the NTSA integration

Deleting the NTSA license key from the **Configuration > License** page will also delete the NTSA integration.

**Note**

Your NTSA account and GravityZone will be unlinked in the following situations:

- The NTSA license key has been removed.
- Your NTSA password has been changed.
- Your GravityZone password has been changed.
- The NTSA integration settings have been modified.

Certificates

For your GravityZone deployment to operate correctly and in a secure manner, you must create and add the security certificate in Control Center.

The screenshot shows the Bitdefender GravityZone Control Center interface. The top navigation bar is blue with the Bitdefender GravityZone logo on the left and a user profile 'Welcome, Admin' on the right. A left sidebar contains a menu with items: Dashboard, Network, Packages, Tasks, Policies, Assignment Rules, Reports, Quarantine, Accounts, User Activity, Configuration (highlighted), Update, and License. The main content area has a sub-navigation bar with links: Mail Server, Proxy, Miscellaneous, Backup, Active Directory, Virtualization, and Certificates (highlighted). Below this is a table with the following data:

Certificate	Common Name	Issued By	Expire Date
Control Center Security	N/A	N/A	N/A

The Certificates page

Control Center supports the following certificate formats:

- PEM (.pem, .crt, .cer, .key)
- DER (.der, .cer)
- PKCS#7 (.p7b, .p7c)
- PKCS#12 (.p12, .pfx)

Control Center Security Certificate

The Control Center Security certificate is needed to identify the Control Center web console as a trusted website in the web browser. Control Center uses by default an SSL certificate signed by Bitdefender. This built-in certificate is not recognized by web browsers and triggers security warnings. To avoid browser security warnings, add an SSL certificate signed by your company or by an external Certificate Authority (CA).

To add or replace the Control Center certificate:

1. Go to the **Configuration** page and click the **Certificates** tab.
2. Click the certificate name.
3. Choose the certificate type (with separate or embedded private key).
4. Click the **Add** button next to the **Certificate** field and upload the certificate.
5. For certificates with separate private key, click the **Add** button next to the **Private key** field and upload the private key.
6. If the certificate is password protected, enter the password in the corresponding field.
7. Click **Save**.

Repository

This tab displays information about the security agent updates including product versions stored on the Update Server and versions available in the Bitdefender official repository, update rings, the date and time of the update and last check for new versions.



Note

The product versions are not available for Security Servers.

5.1.5. Managing the GravityZone Appliance

The GravityZone appliance comes with a basic configuration interface, available from the management tool used for managing the virtualized environment where you have deployed the appliance.

These are the available main options after the first GravityZone appliance deployment:

- [Configure Hostname Settings](#)
- [Configure Network Settings](#)
- [Configure Proxy Settings](#)
- [MDM Communication Server](#)
- [Advanced Settings](#)
- [Configure Language](#)

Use the arrow keys and the `Tab` key to navigate through menus and options. Press `Enter` to select a specific option.

Configure Hostname and Settings

Communication with the GravityZone roles is performed using the IP address or DNS name of the appliance they are installed on. By default, the GravityZone components communicate using IP addresses. If you want to enable communication via DNS names, you must configure GravityZone appliances with a DNS name and make sure it correctly resolves to the configured IP address of the appliance.

Prerequisites:

- Configure the DNS record in the DNS server.
- The DNS name must correctly resolve to the configured IP address of the appliance. Therefore, you must make sure the appliance is configured with the correct IP address.

To configure the hostname settings:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Configure Hostname Settings**.
3. Enter the hostname of the appliance and the Active Directory domain name (if needed).
4. Select **OK** to save the changes.

Configure Network Settings

You can configure the appliance to automatically obtain network settings from the DHCP server or you can manually configure network settings. If you choose to use

DHCP, you must configure the DHCP Server to reserve a specific IP address for the appliance.

To configure the network settings:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Configure Network Settings**.
3. Select the network interface (default `eth0`).
4. Select the configuration method:
 - **Configure network settings manually.** You must specify the IP address, network mask, gateway address and DNS server addresses.
 - **Obtain network settings automatically via DHCP.** Use this option only if you have configured the DHCP Server to reserve a specific IP address for the appliance.
5. You can check current IP configuration details or link status by selecting the corresponding options.

Configure Proxy Settings

If the appliance connects to the Internet through a proxy server, you must configure the proxy settings.



Note

The proxy settings can also be configured from Control Center, **Configuration > Proxy** page. Changing the proxy settings in one location automatically updates them in the other location too.

To configure the proxy settings:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Configure Proxy Settings**.
3. Select **Configure proxy settings**.
4. Enter the proxy server address. Use the following syntax:
 - If the proxy server does not require authentication:
`http(s)://<IP/hostname>:<port>`

- If the proxy server requires authentication:

`http(s)://<username>:<password>@<IP/hostname>:<port>`

5. Select **OK** to save the changes.

Select **Show proxy information** to check the proxy settings.

MDM Communication Server



Note

This configuration is required only for mobile device management, if your license key covers the Security for Mobile service. The option appears in the menu after installing the [Communication Server role](#).

In the default GravityZone setup, mobile devices can be managed only when they are directly connected to the corporate network (via Wi-Fi or VPN). This happens because when enrolling mobile devices they are configured to connect to the local address of the Communication Server appliance.

To be able to manage mobile devices over the Internet, no matter where they are located, you must configure the Communication Server with a publicly reachable address.

To be able to manage mobile devices when they are not connected to the company network, the following options are available:

- Configure port forwarding on the corporate gateway for the appliance running the Communication Server role.
- Add an additional network adapter to the appliance running the Communication Server role and assign it a public IP address.

In both cases, you must configure the Communication Server with the external address to be used for mobile device management:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **MDM Communication Server**.
3. Select **Configure MDM Server external address**.
4. Enter the external address.

Use the following syntax: `https://<IP/Domain>:<Port>`.

- If you use port forwarding, you must enter the public IP address or domain name and the port open on the gateway.
 - If you use a public address for the Communication Server, you must enter the public IP address or domain name and the Communication Server port. The default port is 8443.
5. Select **OK** to save the changes.
 6. Select **Show MDM Server external address** to check the settings.

Advanced Settings

The advanced settings cover several options for manual deployment, environment extension and security enhancements:

- [Install/Uninstall Roles](#)
- [Install Security Server](#)
- [Set New Database Password](#)
- [Update Server](#)
- [Configure Role Balancers](#)
- [Replica Set](#)
- [Enable Secure VPN Cluster](#)
- [Connect to Existing Database](#)
- [Connect to Existing Database \(Secure VPN Cluster\)](#)
- [Check Secure VPN Cluster](#)

The options availability vary depending on the installed roles and the enabled services. For example, if the Database Server role is not installed on the appliance, you can only install roles or connect to a GravityZone database deployed in your network. Once the Database Server role has installed on the appliance, the options for connecting to another database become unavailable.

Install/Uninstall Roles

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

- **Database Server**
- **Update Server**

- **Web Console**
- **Communication Server**
- **Incidents Server**

A GravityZone deployment requires running one instance of each role. Consequently, depending on how you prefer to distribute the GravityZone roles, you will deploy one to four GravityZone appliances. The Database Server role is the first to be installed. In a scenario with multiple GravityZone appliances, you will install the Database Server role on the first appliance and configure all other appliances to connect to the existing database instance.



Note

You can install additional instances of specific roles using role balancers. For more information, refer to [“Configure Role Balancers”](#) (p. 83).

To install the GravityZone roles:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Advanced Settings**.
3. Select **Install/Uninstall Roles**.
4. Select **Add or remove roles**.
5. Proceed according to the current situation:
 - If this is the initial GravityZone appliance deployment, press the `Space` bar and then `Enter` to install the Database Server role. You must confirm your choice by pressing `Enter` again. Configure the database password and then wait for the installation to complete.
 - If you have already deployed another appliance with the Database Server role, choose **Cancel** and return to the **Add or remove roles** menu. You must then choose **Configure Database Address** and enter the address of the database server. Make sure you set a database password before accessing this option. If you don't know the database password, configure a new one by selecting **Advanced Settings > Set a new database password** from the main menu.

Use the following syntax: `http://<IP/Hostname>:<Port>`. The default database port is 27017. Enter the primary database password.

6. Install the other roles by choosing **Add or remove roles** from the **Install/Uninstall Roles** menu and then the roles to install. For each role you want to install or uninstall, press the `Space` bar to select or deselect the role and then press `Enter` to proceed. You must confirm your choice by pressing `Enter` again and then wait for the installation to complete.



Note

Each role is normally installed within a few minutes. During installation, required files are downloaded from the Internet. Consequently, the installation takes more time if the Internet connection is slow. If the installation hangs, redeploy the appliance.

You can view the installed roles and their IPs, by selecting one of the following options from the **Install/Uninstall Roles** menu:

- **Show locally installed roles**, to view only the roles installed on that appliance.
- **Show all installed roles**, to view all roles installed in your GravityZone environment.

Install Security Server



Note

The Security Server will be available to use only if your license key allows it.

You can install the Security Server from the GravityZone appliance configuration interface, directly on the GravityZone appliance, or from Control Center as a stand alone appliance. The advantages of installing the Security Server from the appliance are:

- Suitable for GravityZone deployments with a single appliance having all roles.
- You can view and use the Security Server without having to integrate GravityZone with a virtualization platform.
- Less deployment operations to perform.

Prerequisites:

The GravityZone appliance must have the Database Server role installed, or it must be configured to connect to an existing database.

To install the Security Server from the appliance interface:

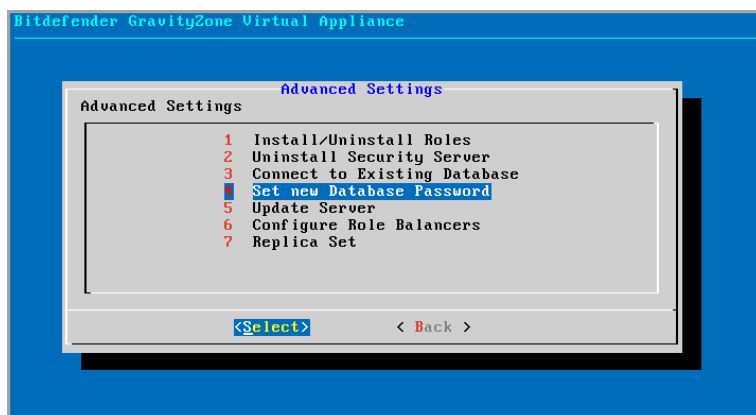
1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Advanced Settings**.
3. Select **Install Security Server**. A confirmation message will appear.
4. Press `Enter` to continue and wait until the installation finishes.

**Note**

You can uninstall this Security Server only from the **Advanced Settings** menu of the appliance interface.

Set New Database Password

When installing the Database Server role, you are required to set up a password to protect the database. In case you want to change it, set a new one by accessing **Advanced Settings > Set a new database password** from the main menu.



Appliance console interface: Set New Database Password option

Follow the guidelines to set up a strong password.

Configure Update Server

The GravityZone appliance is by default configured to update from the Internet. If you prefer, you can set your installed appliances to update from the local Bitdefender update server (the GravityZone appliance with the Update Server role installed).

To set the update server address:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Advanced Settings**.
3. Select **Update Server**.
4. Select **Configure update address**.
5. Enter the IP address or hostname of the appliance running the Update Server role. The default Update Server port is 7074.

Configure Role Balancers

To ensure reliability and scalability, you can install multiple instances of specific roles (Incidents Server, Communication Server, Web Console).

Each role instance is installed on a different appliance.

All instances of a specific role must be connected to the other roles via a role balancer.

The GravityZone appliance includes built-in balancers that you can install and use. If you already have balancing software or hardware within your network, you can choose to use them instead of the built-in balancers.

Built-in role balancers cannot be installed together with roles on a GravityZone appliance.

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Advanced Settings**.
3. Select **Configure Role Balancers**.
4. Select the desired option:
 - **Use external balancers.** Select this option if your network infrastructure already includes balancing software or hardware that you can use. You must enter the balancer address for each role that you want to balance. Use the following syntax:
`http(s)://<IP/Hostname>:<Port>.`
 - **Use the built-in balancers.** Select this option to install and use the built-in balancer software.

**Important**

To install multiple instances of the Incidents Server role you may only use the built-in balancer.

5. Select **OK** to save the changes.

Replica Set

With this option you can enable the use of a database replica set instead of a single-server database instance. This mechanism allows creating multiple database instances across a distributed GravityZone environment, ensuring the database high-availability in the case of a failure.

**Important**

Database replication is available only for fresh installations of GravityZone appliance starting with version 5.1.17-441.

Configuring Replica Set

At first, you have to enable Replica Set on the first installed GravityZone appliance. Then, you will be able to add replica set members by installing the database role to the other GravityZone instances in the same environment.

**Important**

- Replica Set requires at least three members to work.
- You can add up to seven database role instances as replica set members (MongoDB limitation).
- It is recommended to use an odd number of database instances. An even number of members will only consume more resources for the same results.

To enable the database replication in your GravityZone environment:

1. Install the Database Server role on the first GravityZone appliance. For more information, refer to [“Install/Uninstall Roles”](#) (p. 79).
2. Configure the other appliances to connect to the first database instance. For more information, refer to [“Connect to Existing Database”](#) (p. 86).
3. Go to the main menu of the first appliance, select **Advanced Settings** and then select **Replica Set** to enable it. A confirmation message will appear.
4. Select **Yes** to confirm.

5. Install the Database Server role on each of the other GravityZone appliances.

As soon as the above steps have been completed, all database instances will start working as a replica set:

- A primary instance is elected, being the only one to accept write operations.
- The primary instance writes all changes made to its data set to a log.
- The secondary instances replicate this log and apply the same changes to their data sets.
- When the primary instance becomes unavailable, the replica set will elect one of the secondary instances as primary.
- When a primary instance does not communicate with the other members of the set for more than 10 seconds, the replica set will attempt to select another member to become the new primary.

Removing Replica Set Members

To remove replica set members, just choose from their appliance console interface (menu-based interface) **Install/Uninstall Roles > Add or Remove Roles** and deselect **Database Server**.



Note

You can remove a replica set member only if at least four database instances have been installed in the network.

Enable Secure VPN Cluster

The GravityZone roles have several internal services that communicate exclusively between them. For a more secure environment, you can isolate these services by creating a VPN cluster for them. Either these services are on the same appliance or on more, they will then communicate via a secure channel.



Important

- This feature requires a standard GravityZone deployment, without any custom tools installed.
- Once the cluster is enabled, you cannot disable it.

To secure the internal services on the appliances:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Advanced Settings**.
3. Select Enable **Secure VPN Cluster**.
A message informs you of the changes that will be made.
4. Select **Yes** to confirm and proceed with the VPN installation.
When complete, a confirmation message is displayed.

From now on, all roles on the appliance are installed in secured mode and the services will communicate through the VPN interface. Any new appliance you add to the environment must join the VPN cluster. For more information, refer to [“Connect to Existing Database \(Secure VPN Cluster\)”](#) (p. 87).

Connect to Existing Database

In a GravityZone distributed architecture, you need to install the Database Server role on the first appliance and then configure all other appliances to connect to the existing database instance. This way, all appliances will share the same database.

Important

It is recommended to enable Secure VPN Cluster and to connect to a database within such cluster. For more information, refer to:

- [“Enable Secure VPN Cluster”](#) (p. 85)
- [“Connect to Existing Database \(Secure VPN Cluster\)”](#) (p. 87)

To connect the appliance to a GravityZone database outside a Secure VPN Cluster:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Advanced Settings**.
3. Select **Connect to Existing Database**.



Note

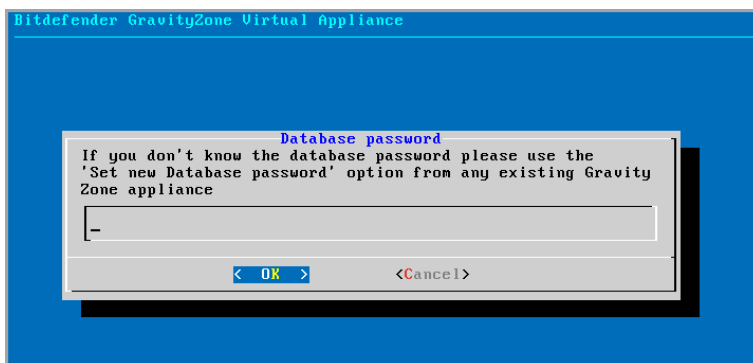
Make sure you set a database password before accessing this option. If you don't know the database password, set a new one by accessing **Advanced Settings > Set a new database password** from the main menu.

4. Select **Configure Database Server address**.
5. Enter the database address, using the following syntax:

`<IP/Hostname>:<Port>`

Specifying the port is optional. The default port is 27017.

6. Enter the primary database password.



Appliance console interface: enter database password

7. Select **OK** to save the changes.
8. Select **Show Database Server address** to make sure the address has been correctly configured.

Connect to Existing Database (Secure VPN Cluster)

Use this option when you need to extend your GravityZone deployment with more appliances, and Secure VPN Cluster is enabled. This way, the new appliance will share the same database with the existing deployment in a secure mode.

For more information on Secure VPN Cluster, refer to [“Enable Secure VPN Cluster” \(p. 85\)](#).

Prerequisites

Before proceeding, make sure to have the following at hand:

- Database Server IP address
- Password for the **bdadmin** user on the appliance with the Database Server role

Connect to Database

To connect the appliance to a GravityZone database within a Secure VPN Cluster:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Advanced Settings**.
3. Select **Connect to Existing Database (Secure VPN Cluster)**.
You will be informed of the requirements and alternatives, if they are not met.
4. Select **OK** to acknowledge and continue.
5. Enter the IP address of the Database Server within the Secure VPN Cluster.
6. Enter the password for the **bdadmin** user on the appliance with the Database Server.
7. Select **OK** to save the changes and continue.

When the process is complete, you receive a confirmation message. The new appliance becomes a member of the cluster and it will communicate with the other appliances in a secure way. All appliances will share the same database.

Check the Secure VPN Cluster Status

This option is available only after you have previously enabled the secure VPN cluster. Select this option to check which appliances in your GravityZone deployment have not yet secured their services. You may need to investigate further and see if the appliances are online and accessible.

Configure Language

To change the appliance configuration interface language:

1. Select **Configure Language** from the main menu.
2. Select the language from the available options. A confirmation message will appear.



Note

You may need to scroll down to view your language.

3. Select **OK** to save the changes.

5.2. License Management

GravityZone is licensed with a single key for all security services.

Besides the basic security services, GravityZone also provides important protection features as add-ons. Each add-on is licensed with a separate key and you can use it only together with a basic valid license. If the main license is invalid, you will view the features settings, but you will be unable to use them.

You can choose to test GravityZone and decide if it is the right solution for your organization. To activate your evaluation period, you must enter the trial license key from the registration email in Control Center.

To continue using GravityZone after the trial period expires, you must purchase a license key and use it to register the product.

To purchase a license, contact a Bitdefender reseller or contact us by email at enterprisesales@bitdefender.com.

GravityZone license key can be managed from the **License** page in Control Center. When your current license key is about to expire, a message will appear in the console informing you that it needs to be renewed. To enter a new license key or view the current license details, go to the **License** page.

5.2.1. Finding a Reseller

Our resellers will assist you with all the information you need and help you choose the best licensing option for you.


To find a Bitdefender reseller in your country:

1. Go to the [Partner Locator](#) page on Bitdefender website.
2. Select the country you reside in to view contact information of available Bitdefender partners.
3. If you do not find a Bitdefender reseller in your country, feel free to contact us by email at enterprisesales@bitdefender.com.

5.2.2. Entering Your License Keys

GravityZone license registration can be done online or offline (when internet connection is not available). In both cases, you need to provide a valid license key. For offline registration, you will also need the offline registration code associated to the license key.

To change the current license key or to register an add-on:

1. Log in to Control Center using a company administrator account.
2. Go to the **Configuration > License** page.
3. Click the  **Add** button at the upper side of the table.
4. Select the registration type:
 - **Online.** In this case, enter a valid license key in the **License key** field. The license key will be checked and validated online.
 - **Offline,** when an internet connection is not available. In this case, you need to provide the license key and also its registration code.

If the license key is not valid, a validation error is displayed as tooltip over the **License key** field.

5. Click **Add**. The license key will be added to the **License** page, where you can check its details.
6. Click **Save** to apply the changes. Control Center restarts and you need to log in again to view the changes.

**Note**

You can use the add-ons as long as a compatible basic license is valid. Otherwise you will view the features, but you will be unable to use them.

5.2.3. Checking Current License Details

To view your license details:

1. Log in to Control Center using a company administrator account.
2. Go to the **Configuration > License** page.

Bitdefender

GravityZone

Welcome, Admin

Dashboard

Network

Packages

Tasks

Policies

Assignment Rules

Reports

Quarantine

Accounts

User Activity

Configuration

Update

License

+ Add

⌂ Reset

- Delete

↻ Refresh

<input type="checkbox"/>	Key	Status	Expiry Date	Usage
<input type="checkbox"/>	<div></div>	Active	21 Dec 2015, 195 days...	0/50 Entities, Available

The License page

3. In the table, you can view details about the license key.
 - License key
 - License key status
 - Expiry date and remaining license period




Important

When license expires, the protection modules of the installed agents are disabled. As a result, endpoints are no longer protected and you cannot perform any scan task. Any new installed agent will enter in trial period.

- License usage count

5.2.4. Resetting the license usage count

You can find out information about your license key's usage count in the **License** page, under the **Usage** column.

If you need to update the usage information, select the license key and click the  **Reset** button at the upper side of the table.

5.3. Installing Security Agents

To protect your physical and virtual endpoints, you must install a security agent on each of them. Besides managing protection on the local endpoint, the security agent also communicates with Control Center to receive the administrator's commands and to send the results of its actions.

You can install the security agents on physical and virtual endpoints [by running installation packages locally](#) or [by running installation tasks remotely](#) from Control Center.

It is very important to carefully read and follow the instructions to prepare for installation.

In normal mode, the security agents have a minimal user interface. It only allows users to check protection status and run basic security tasks (updates and scans), without providing access to settings.

By default, the display language of the user interface on protected Windows endpoints is set at installation time based on the language of your GravityZone account.

To install the user interface in another language on certain Windows endpoints, you can create an installation package and set the preferred language in its configuration options. This option is not available for Mac and Linux endpoints. For more information on creating installation packages, refer to [“Creating Installation Packages” \(p. 93\)](#).

5.3.1. Preparing for Installation

Before installation, follow these preparatory steps to make sure it goes smoothly:

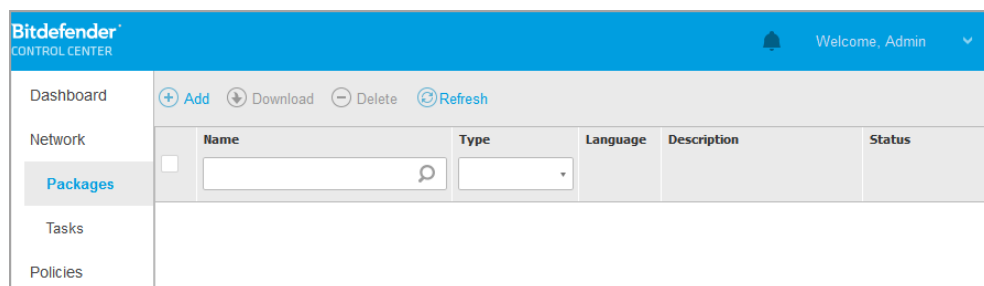
1. Make sure the target endpoints meet the [minimum system requirements](#). For some endpoints, you may need to install the latest operating system service pack available or free up disk space. Compile a list of endpoints that do not meet the necessary requirements so that you can exclude them from management.
2. The installation requires administrative privileges and Internet access. If the target endpoints are in an Active Directory domain, you should use domain administrator credentials for remote installation. Otherwise, make sure you have the necessary credentials at hand for all endpoints.
3. Endpoints must have network connectivity to the GravityZone appliance.

- It is recommended to use a static IP address for the Relay server. If you do not set a static IP, use the machine's hostname.

5.3.2. Local Installation

One way to install the security agent on an endpoint is to locally run an installation package.

You can create and manage installation packages in the **Network > Packages** page.



The Packages page

Once the first client has been installed, it will be used to detect other endpoints in the same network, based on the Network Discovery mechanism. For detailed information on network discovery, refer to [“How Network Discovery Works”](#) (p. 105).

To locally install the security agent on an endpoint, follow the next steps:

- [Create an installation package](#) according to your needs.



Note

This step is not mandatory if an installation package has already been created for the network under your account.

- [Download the installation package](#) on the target endpoint.

You can alternately [send the installation package download links by email](#) to several users in your network.

- [Run the installation package](#) on the target endpoint.

Creating Installation Packages

To create an installation package:

1. Connect and log in to Control Center.
2. Go to the **Network > Packages** page.
3. Click the **+ Add** button at the upper side of the table. A configuration window will appear.

General

Name: *

Description:

Language:

Modules:


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

Create Packages - Options

4. Enter a suggestive name and description for the installation package you want to create.
5. From the **Language** field, select the desired language for the client's interface.
6. Select the target endpoint role:
7. **Miscellaneous.** You can configure the following options on several types of files from the target endpoints:
 - **Submit crash dumps.** Select this option so that memory dump files will be sent to Bitdefender Labs for analysis if the security agent crashes. The crash dumps will help our engineers find out what caused the problem and prevent it from occurring again. No personal information will be sent.
 - **Submit quarantined files to Bitdefender Labs every (hours).** By default, quarantined files are automatically sent to Bitdefender Labs every hour. You can edit the time interval between quarantined files are being sent. The

sample files will be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

- **Submit suspicious executables to Bitdefender.** Select this option so that files that seem untrustworthy or with suspicious behavior will be sent to Bitdefender Labs for analysis.

8.  **Important**
When using custom path, make sure you have the right installation package for each operating system.
9. If you want to, you can set a password to prevent users from removing protection. Select **Set uninstall password** and enter the desired password in the corresponding fields.
10. If the target endpoints are in Network Inventory under **Custom Groups**, you can choose to move them in a specified folder immediately after the security agent deployment finishes.
Select **Use custom folder** and choose a folder in the corresponding table.
11. Under **Deployer** section, choose the entity to which the target endpoints will connect for installing and updating the client:
- **GravityZone Appliance**, when endpoints connect directly to GravityZone Appliance.
For this case, you can also define:
 - A custom Communication Server by entering its IP or Hostname, if required.
 - Proxy settings, if target endpoints communicate with GravityZone Appliance via proxy. In this case, select **Use proxy for communication** and enter the required proxy settings in the fields below.
 - **Endpoint Security Relay**, if you want to connect the endpoints to a Relay client installed in your network. All machines with Relay role detected in your network will show-up in the table displayed below. Select the Relay machine that you want. Connected endpoints will communicate with Control Center only via the specified Relay.

 **Important**

12. Click **Save**.

The newly created package will be added to the list of packages.




Note

The settings configured within an installation package will apply to endpoints immediately after installation. As soon as a policy is applied to the client, the settings configured within the policy will be enforced, replacing certain installation package settings (such as communication servers or proxy settings).

Downloading Installation Packages

To download the installation packages of the security agents:

1. Log in to Control Center from the endpoint on which you want to install protection.
2. Go to the **Network > Packages** page.
3. Select the installation package you want to download.
4. Click the  **Download** button at the upper side of the table and select the type of installer you want to use. Two types of installation files are available:
 - **Downloader.** The downloader first downloads the full installation kit from the Bitdefender cloud servers and then starts the installation. It is small in size and it can be run both on 32-bit and 64-bit systems (which makes it easy to distribute). On the downside, it requires an active Internet connection.
 - **Full Kit.** The full installation kits are bigger in size and they have to be run on the specific operating system type.

The full kit is to be used to install protection on endpoints with slow or no Internet connection. Download this file to an Internet-connected endpoint, then distribute it to other endpoints using external storage media or a network share.



Note

Available full kit versions:

- **Windows OS:** 32-bit and 64-bit systems

5. Save the file to the endpoint.




Warning

- The downloader executable must not be renamed, otherwise it will not be able to download the installation files from Bitdefender server.

6. Additionally, if you have chosen the Downloader, you can create an MSI package for Windows endpoints. For more information, refer to [this KB article](#).

Send Installation Packages Download Links by Email

You may need to quickly inform other users that an installation package is available to download. In this case, follow the steps described hereinafter:

1. Go to the **Network > Packages** page.
2. Select the installation package that you want.
3. Click the  **Send download links** button at the upper side of the table. A configuration window will appear.
4. Enter the email of each user you want to receive the installation package download link. Press **Enter** after each email.

Please make sure that each entered email address is valid.

5. If you want to view the download links before sending them by email, click the **Installation links** button.
6. Click **Send**. An email containing the installation link is sent to each specified email address.

Running Installation Packages

For the installation to work, the installation package must be run using administrator privileges.

The package installs differently on each operating system as follows:

- On Windows and macOS operating systems:
 1. On the target endpoint, download the installation file from Control Center or copy it from a network share.
 2. If you have downloaded the full kit, extract the files from the archive.
 3. Run the executable file.

Once the security agent has been installed, the endpoint will show up as managed in Control Center (**Network** page) within a few minutes.

5.3.3. Remote Installation

Control Center allows you to remotely install the security agent on endpoints from environments integrated with Control Center and on other endpoints detected in the network by using installation tasks. In VMware environments, remote installation relies on VMware Tools, while in Citrix XenServer and Nutanix Prism Element environments, it relies on Windows administrative shares and SSH.

Once the security agent is installed on an endpoint, it may take a few minutes for the rest of the network endpoints to become visible in Control Center.

Bitdefender Endpoint Security Tools includes an automatic network discovery mechanism that allows detecting endpoints that are not in Active Directory. Detected endpoints are displayed as **unmanaged** in the **Network** page, in **Computers** view, under **Custom Groups**. Control Center automatically removes Active Directory endpoints from the detected endpoints list.

To enable network discovery, you must have Bitdefender Endpoint Security Tools already installed on at least one endpoint in the network. This endpoint will be used to scan the network and install Bitdefender Endpoint Security Tools on unprotected endpoints.

For detailed information on network discovery, refer to [“How Network Discovery Works”](#) (p. 105).

Remote Installation Requirements

For remote installation to work:

- On Windows:
 - The `admin$` administrative share must be enabled. Configure each target workstation not to use advanced file sharing.
 - Configure User Account Control (UAC) depending on the operating system running on the target endpoints. If the endpoints are in an Active Directory domain, you can use a group policy to configure User Account Control. For details, refer to [this KB article](#).

**Note**

Remote deployment works only on modern operating systems, starting with Windows 7 / Windows Server 2008 R2, for which Bitdefender provides full support. For more information, refer to [“Supported Operating Systems”](#) (p. 21).

- On Linux: SSH must be enabled.
- On macOS: remote login and file sharing must be enabled.


Running Remote Installation Tasks

To run a remote installation task:

1. Connect and log in to Control Center.
2. Go to the **Network** page.
3. Choose **Computers and Virtual Machines** from the views selector.
4. Select the desired group from the left-side pane. The entities contained in the selected group are displayed in the right-side pane table.

**Note**

Optionally, you can apply filters to display unmanaged endpoints only. Click the **Filters** menu and select the following options: **Unmanaged** from the **Security** tab and **All items recursively** from the **Depth** tab.

5. Select the entities (endpoints or groups of endpoints) on which you want to install protection.
6. Click the  **Tasks** button at the upper side of the table and choose **Install**. The **Install Client** wizard is displayed.

Install client

Options

☒ Now

☐ Scheduled

☐ Automatically reboot (if needed)

Credentials Manager

User	Password	Description	Action
<input type="checkbox"/> tester	*****		

Save **Cancel**

7. Under **Options** section, configure the installation time:

- **Now**, to launch the deployment immediately.
- **Scheduled**, to set up the deployment recurrence interval. In this case, select the time interval that you want (hourly, daily or weekly) and configure it according to your needs.



Note

For example, when certain operations are required on the target machine before installing the client (such as uninstalling other software and restarting the OS), you can schedule the deployment task to run every 2 hours. The task will start on each target machine every 2 hours until the deployment is successful.

8. If you want target endpoints to automatically restart for completing the installation, select **Automatically reboot (if needed)**.
9. Under the **Credentials Manager** section, specify the administrative credentials required for remote authentication on target endpoints. You can add the credentials by entering the user and password for each target operating system.



Important

For Windows 8.1 stations, you need to provide the credentials of the built-in administrator account or a domain administrator account. To learn more, refer to [this KB article](#).

To add the required OS credentials:

- a. Enter the user name and password of an administrator account in the corresponding fields from the table header.

If computers are in a domain, it suffices to enter the credentials of the domain administrator.

Use Windows conventions when entering the name of a user account:

- For Active Directory machines use these syntaxes: `username@domain.com` and `domain\username`. To make sure that entered credentials will work, add them in both forms (`username@domain.com` and `domain\username`).
- For Workgroup machines, it suffices to enter only the user name, without the workgroup name.

Optionally, you can add a description that will help you identify each account more easily.

- b. Click the  **Add** button. The account is added to the list of credentials.



Note

Specified credentials are automatically saved to your [Credentials Manager](#) so that you do not have to enter them the next time. To access the Credentials Manager, just point to your username in the upper-right corner of the console.



Important

If the provided credentials are invalid, the client deployment will fail on the corresponding endpoints. Make sure to update the entered OS credentials in the Credentials Manager when these are changed on the target endpoints.

10. Select the check boxes corresponding to the accounts you want to use.



Note

A warning message is displayed as long as you have not selected any credentials. This step is mandatory to remotely install the security agent on endpoints.

11. Under **Deployer** section, choose the entity to which the target endpoints will connect for installing and updating the client:

- **GravityZone Appliance**, when endpoints connect directly to GravityZone Appliance.

In this case, you can also define:

- A custom Communication Server by entering its IP or Hostname, if required.
- Proxy settings, if target endpoints communicate with GravityZone Appliance via proxy. In this case, select **Use proxy for communication** and enter the required proxy settings in the fields below.
- **Endpoint Security Relay**, if you want to connect the endpoints to a Relay client installed in your network. All machines with Relay role detected in your network will show-up in the table displayed below. Select the Relay machine that you want. Connected endpoints will communicate with Control Center only via the specified Relay.



Important

Port 7074 must be open, for the deployment through the Relay agent to work.

Deployer

Deployer:

Endpoint Security Relay

Name	IP	Custom Server Name/IP	Label
CO_SUPA	192.168.0.183		N/A
FC-WIN7-X64-01	192.168.3.80		N/A

First Page

Page

1

of 1

Last Page

20

2 items

12. Use the **Additional targets** section if you want to deploy the client to specific machines from your network that are not shown in the network inventory. Expand the section and enter the IP addresses or hostnames of those machines in the dedicated field, separated by a comma. You can add as many IPs as you need.
13. You need to select one installation package for the current deployment. Click the **Use package** list and select the installation package that you want. You can find here all the installation packages previously created for your account and also the default installation package available with Control Center.
14. If needed, you can modify some of the selected installation package's settings by clicking the button **Customize** next to the **Use package** field.

The installation package's settings will appear below and you can make the changes that you need. To find out more about editing installation packages, refer to [“Creating Installation Packages” \(p. 93\)](#).

If you want to save the modifications as a new package, select the **Save as package** option placed at the bottom of the package settings list, and enter a name for the new installation package.

15. Click **Save**. A confirmation message will appear.

You can view and manage the task in the **Network > Tasks** page.

5.3.4. Preparing Linux Systems for On-access Scanning

Bitdefender Endpoint Security Tools for Linux includes on-access scanning capabilities that work with specific Linux distributions and kernel versions. For more information, refer to [system requirements](#).

Next you will learn how to manually compile the DazukoFS module.

Manually compile the DazukoFS module

Follow the steps below to compile DazukoFS for the system's kernel version and then load the module:

1. Download the proper kernel headers.
 - On **Ubuntu** systems, run this command:

```
$ sudo apt-get install linux-headers-`uname -r`
```

- On **RHEL/CentOS** systems, run this command:

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. On **Ubuntu** systems, you need `build-essential`:

```
$ sudo apt-get install build-essential
```

3. Copy and extract the DazukoFS source code in a preferred directory:

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
# tar -xzf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Compile the module:

```
# make
```

5. Install and load the module:

```
# make dazukofs_install
```

Requirements for using on-access scanning with DazukoFS

For DazukoFS and on-access scanning to work together, a series of conditions must be met. Please check if any of the statements below apply to your Linux system and follow the guidelines to avoid issues.

- The SELinux policy must be either disabled or set to **permissive**. To check and adjust the SELinux policy setting, edit the `/etc/selinux/config` file.
- Bitdefender Endpoint Security Tools is exclusively compatible with the DazukoFS version included in the installation package. If DazukoFS is already installed on the system, remove it prior to installing Bitdefender Endpoint Security Tools.
- DazukoFS supports certain kernel versions. If the DazukoFS package shipped with Bitdefender Endpoint Security Tools is not compatible with the system's kernel version, the module will fail to load. In such case, you can either update the kernel to the supported version or recompile the DazukoFS module for your kernel version. You can find the DazukoFS package in the Bitdefender Endpoint Security Tools installation directory:

```
/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz
```

- When sharing files using dedicated servers such as NFS, UNFSv3 or Samba, you have to start the services in the following order:
 1. Enable on-access scanning via policy from Control Center.

For more information, refer to GravityZone Administrator's Guide.

2. Start the network sharing service.

For NFS:

```
# service nfs start
```

For UNFSv3:

```
# service unfs3 start
```

For Samba:

```
# service smb start
```



Important

For the NFS service, DazukoFS is compatible only with NFS User Server.

5.3.5. How Network Discovery Works

Besides integration with Active Directory, GravityZone also includes an automatic network discovery mechanism intended to detect workgroup computers.

GravityZone relies on the **Microsoft Computer Browser** service and **NBTscan** tool to perform network discovery.

The Computer Browser service is a networking technology used by Windows-based computers to maintain updated lists of domains, workgroups, and the computers within them and to supply these lists to client computers upon request. Computers detected in the network by the Computer Browser service can be viewed by running the **net view** command in a command prompt window.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFLL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

The Net view command

The NBTscan tool scans computer networks using NetBIOS. It queries each endpoint in the network and retrieves information such as IP address, NetBIOS computer name, and MAC address.



Important

Control Center does not use network information from Active Directory or from the network map feature. Network map relies on a different network discovery technology: the Link Layer Topology Discovery (LLTD) protocol.

Control Center processes the browse list, appending newly detected computers to its **Unmanaged Computers** list. Previously detected computers are not deleted after a new network discovery query, so you must manually exclude & delete computers that are no longer on the network.

- If the Relay is installed on a workgroup computer, only computers from that workgroup will be visible in Control Center.
- If the Relay is installed on a domain computer, only computers from that domain will be visible in Control Center. Computers from other domains can be detected if there is a trust relationship with the domain where the Relay is installed.

Subsequent network discovery queries are performed regularly every hour. For each new query, Control Center divides the managed computers space into visibility areas and then designates one Relay in each area to perform the task. A visibility area is a group of computers that detect each other. Usually, a visibility area is defined by a workgroup or domain, but this depends on the network topology and configuration. In some cases, a visibility area might consist of multiple domains and workgroups.

If a selected Relay fails to perform the query, Control Center waits for the next scheduled query, without choosing another Relay to try again.

More about the Microsoft Computer Browser Service

Quick facts about the Computer Browser service:

- Works independent of Active Directory.
- Runs exclusively over IPv4 networks and operates independently within the boundaries of a LAN group (workgroup or domain). A browse list is compiled and maintained for each LAN group.
- Typically uses connectionless server broadcasts to communicate between nodes.
- Uses NetBIOS over TCP/IP (NetBT).
- Requires NetBIOS name resolution. It is recommended to have a Windows Internet Name Service (WINS) infrastructure up and running in the network.
- Is not enabled by default in Windows Server 2008 and 2008 R2.

For detailed information on the Computer Browser service, check the [Computer Browser Service Technical Reference](#) on Microsoft Technet.

Network Discovery Requirements

To successfully discover all the computers (servers and workstations) that will be managed from Control Center, the following are required:

- Computers must be joined in a workgroup or domain and connected via an IPv4 local network. Computer Browser service does not work over IPv6 networks.
- Several computers in each LAN group (workgroup or domain) must be running the Computer Browser service. Primary Domain Controllers must also run the service.
- NetBIOS over TCP/IP (NetBT) must be enabled on computers. Local firewall must allow NetBT traffic.
- If using a Linux Relay to discover other Linux or Mac endpoints, you must either install Samba on target endpoints, or join them in Active Directory and use DHCP. This way, NetBIOS will be automatically configured on them.
- File sharing must be enabled on computers. Local firewall must allow file sharing.
- A Windows Internet Name Service (WINS) infrastructure must be set up and working properly.

- Network discovery must be enabled (**Control Panel > Network and Sharing Center > Change Advanced Sharing Settings**).

To enable this feature, the following services must be started:

- DNS Client
 - Function Discovery Resource Publication
 - SSDP Discovery
 - UPnP Device Host
- In environments with multiple domains, it is recommended to set up trust relationships between domains so that computers can access browse lists from other domains.

5.4. Installing Sandbox Analyzer On-Premises

To make sure installation goes smoothly, follow these steps:

1. [Prepare for Installation](#)
2. [Deploy Sandbox Analyzer Virtual Appliance](#)
3. [Deploy Network Security Virtual Appliance](#)

5.4.1. Prepare for Installation

Before installing Sandbox Analyzer On-Premises, make sure that:

- The VMware ESXi hypervisor is installed and configured. For details, refer to the [vSphere Installation and Setup](#) documentation, section 2: "Installing and Setting Up ESXi".
- Bitdefender GravityZone virtual appliance is deployed and configured.



Note

Regarding the VMware ESXi hypervisor, make sure:

- ESXi version is 6.5 or later.
- VMFS datastore version is 5.
- SSH is enabled in **Startup policy** with the **Start and stop with host** configuration.
- NTP service is active and configured.

The Sandbox Analyzer On-Premises license key controls the number of maximum concurrent detonations. Since each detonation requires a running virtual machine

instance, the number of concurrent detonations reflect in the number of virtual machines created. For details about adding license keys in GravityZone Control Center, refer to [“Entering Your License Keys”](#) (p. 89).

5.4.2. Deploy Sandbox Analyzer Virtual Appliance

To deploy the Sandbox Analyzer Virtual Appliance:

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



Note

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

- **Bitdefender Network** - this is the network where other Bitdefender components reside (`eth0` interface). Sandbox Analyzer and the GGravityZone appliance must be in the same network and they must communicate through `eth0`.
 - **Private Detonation Network** - Sandbox Analyzer uses this network for internal communication (`eth1` interface). This network must be isolated from any other network segments.
 - **Internet Access Network** - Sandbox Analyzer uses this network for obtaining the latest updates (`eth2` interface). The `eth2` interface should not have the same IP or network as `eth0`.
6. Power on the appliance.
 7. From your virtualization management tool, access the console interface of the Sandbox Analyzer Virtual Appliance.
 8. When prompted for credentials, use `root` for username and `sve` for password.
 9. Access the configuration menu by running the following command:

```
/opt/bitdefender/bin/sandbox-setup
```

10. In the **Sandbox configuration** menu, make the following settings:

- a. **Network configuration.** Select this option to configure the management NIC. Sandbox Analyzer will use this network interface to communicate with GravityZone.

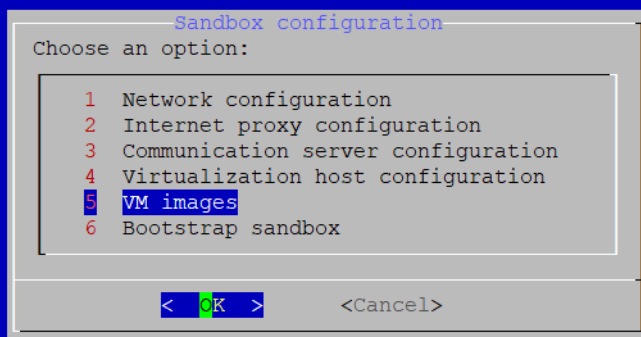
The IP address can be manually specified or automatically through DHCP.



Note

If the GravityZone appliance is in another network than `eth0`, you must add a static route in **Network Configuration > BitDefender Network > Routes** for Sandbox Analyzer to function properly.

Bitdefender Security for Virtualized Environments (Sandbox) 1.0.1.8513



Sandbox Analyzer appliance console

- b. **Internet proxy configuration.** For installation to succeed, Sandbox Analyzer requires internet connection. If the case, you can configure Sandbox Analyzer to use a proxy server by specifying these details:
 - **Host** - IP or FQDN of the proxy server. Use the following syntax:
`http://<IP/Hostname>:<Port>`.
 - **User and password** - you need to type in the password twice.

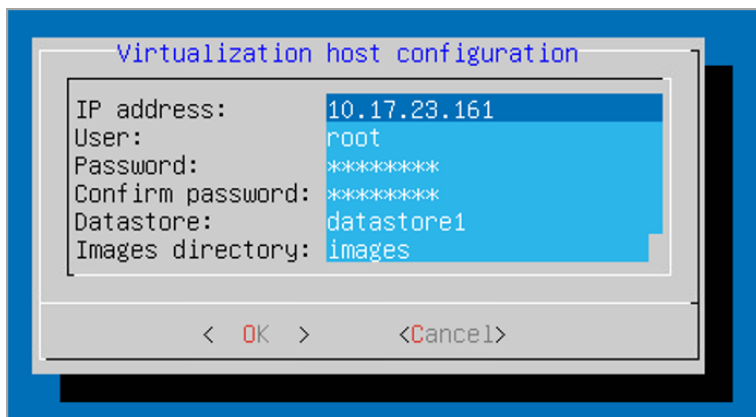
- **Domain** - the Active Directory domain, if the case.
- c. **Communication server configuration.** Specify either the IP address or the hostname of the appliance running the Communication Server role.

Use the following syntax: `http://<IP/Hostname>:<Port>`. The default port is 8443.

**Note**

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

- d. **Virtualized host configuration.** Sandbox Analyzer uses ESXi server to provision the malware analysis infrastructure. Using **Virtualized host configuration**, you connect the Sandbox Analyzer appliance to the ESXi host by providing the following information:
 - The ESXi server IP address.
 - Root credentials for accessing the ESXi host.
 - Datastore dedicated to Sandbox Analyzer.
Type in the datastore name as displayed by ESXi.
 - Name of the folder used on datastore for storing virtual machines images.
If this folder does not exist, you must create it on the datastore before saving the Sandbox Analyzer configuration.



Sandbox Analyzer appliance console

- e. **VM Images.** To build detonation virtual machines for Sandbox Analyzer, you need to copy the VMDK files containing the desired images into the **Images** folder specified in the the **Virtualized host configuration** menu. For each image, you can do in the **VM Images** menu the following settings:
 - i. In the **Image configuration** menu, specify the image name (as it will be displayed in GravityZone Control Center) and the operating system.



Note

The folder containing the VM images is periodically scanned and new entries are reported to GravityZone. These entries are visible in Control Center, in the **Sandbox Analyzer > Infrastructure > Image Management** page.

In certain situations, when using Sandbox Analyzer, you may encounter issues with the detonation virtual machines. To address these issues, you need to disable the anti-fingerprinting option. For details, refer to [“Anti-fingerprinting Techniques” \(p. 113\)](#).

- ii. In the **DMZ hosts** menu, you can whitelist the hostnames that third-party services and components embedded in the virtual machines require to communicate with Sandbox Manager. For details, refer to [“DMZ Hosts” \(p. 114\)](#)

- iii. In the **Cleanup** menu, you can remove VM images that you do not need anymore.
- f. **Bootstrap sandbox.** Once you have added the Sandbox Analyzer configuration details, proceed with the installation by selecting this option. The status of the installation will be reflected in GravityZone Control Center, in the **Sandbox Analyzer > Infrastructure** page.

Anti-fingerprinting Techniques

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

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

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

A quick remedy to such rare occurrences consists in rebuilding the image with the anti-fingerprinting techniques disabled. To do so, follow the steps below:

1. Log into GravityZone Control Center and delete the image.
2. Log into Sandbox Analyzer appliance and launch the Sandbox Analyzer appliance console by running the following command:

```
/opt/bitdefender/bin/sandbox-setup
```

3. Go to **VM Images > Image Configuration**.
4. Select the image that is causing problems.
5. Go to **Anti-fingerprinting** option.
6. Deselect the corresponding check box to disable anti-fingerprinting techniques.

DMZ Hosts

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

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

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

5.5. Installing Full Disk Encryption

GravityZone Full Disk Encryption comes as a service that requires activation based on license key. To do this, you must go to **Configuration > License** and enter the license key.

For detailed information about license keys, refer to [“License Management” \(p. 89\)](#).

The Bitdefender security agents support Full Disk Encryption starting with version 6.2.22.916 on Windows and 4.0.0173876 on Mac. To make sure that the agents are fully compatible with this module, you have two options:

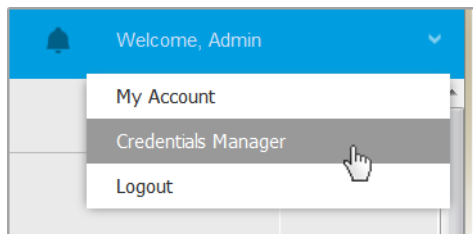
- Install the security agents with the Encryption module included.
- Use the **Reconfigure** task.

For detailed information about using Full Disk Encryption within your network, refer to the **Security Policies > Encryption** chapter in the GravityZone Administrator's Guide.

5.6. Credentials Manager

The Credentials Manager helps you define the credentials required for accessing the available vCenter Server inventories and also for remote authentication on different operating systems in your network.

To open the Credentials Manager, click your username in the upper-right corner of the page and choose **Credentials Manager**.



The Credentials Manager menu

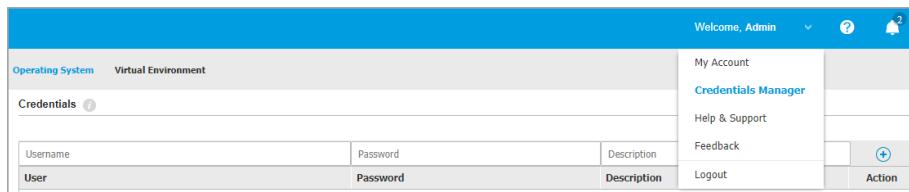
The **Credentials Manager** window contains two tabs:

- [Operating System](#)
- [Virtual Environment](#)

5.6.1. Operating System

From the **Operating System** tab, you can manage the administrator credentials required for remote authentication during installation tasks sent to computers and virtual machines in your network.

To add a set of credentials:



Credentials Manager

1. Enter the user name and password of an administrator account for each target operating system in the corresponding fields at the upper side of the table heading. Optionally, you can add a description that will help you identify each account more easily. If computers are in a domain, it suffices to enter the credentials of the domain administrator.

Use Windows conventions when entering the name of a user account:

- For Active Directory machines use these syntaxes: `username@domain.com` and `domain\username`. To make sure that entered credentials will work, add them in both forms (`username@domain.com` and `domain\username`).
 - For Workgroup machines, it suffices to enter only the user name, without the workgroup name.
2. Click the **+** **Add** button at the right side of the table. The new set of credentials is added to the table.

**Note**

If you have not specified the authentication credentials, you will be required to enter them when you run installation tasks. Specified credentials are automatically saved to your Credentials Manager so that you do not have to enter them the next time.

5.6.2. Virtual Environment

From the Virtual Environment tab, you can manage the authentication credentials for the available virtualized server systems.

To access the virtualized infrastructure integrated with Control Center, you must provide your user credentials for each virtualized server system available. Control Center uses your credentials to connect to the virtualized infrastructure, displaying only resources you have access to (as defined in the virtualized server).

To specify the credentials required for connecting to a virtualized server:

1. Select the server from the corresponding menu.

**Note**

If the menu is unavailable, either no integration has been configured yet or all necessary credentials have already been configured.

2. Enter your username and password and a suggestive description.
3. Click the **+** **Add** button. The new set of credentials is added to the table.

**Note**

If you do not configure your authentication credentials in Credentials Manager, you will be required to enter them when you try to browse the inventory of any


virtualized server system. Once you have entered your credentials, they are saved to your Credentials Manager so that you do not need to enter them the next time.

**Important**

Whenever you change your virtualized server user password, remember to also update it in Credentials Manager.

5.6.3. Deleting Credentials from Credentials Manager

To delete obsolete credentials from the Credentials Manager:

1. Point to the row in the table containing the credentials you want to delete.
2. Click the  **Delete** button at the right side of the corresponding table row. The selected account will be deleted.

6. UPDATING GRAVITYZONE

Bitdefender publishes all product and security content updates through the Bitdefender servers on the Internet. All updates are encrypted and digitally signed so that they cannot be tampered with.

GravityZone includes an Update Server role, designed to serve as the centralized update distribution point for your GravityZone deployment. Update Server checks for and downloads all available GravityZone updates from the Bitdefender update servers on the Internet, making them available in the local network. The GravityZone components can be configured to automatically update from the local update server instead of the Internet.

When a new update is available, the GravityZone appliance or the security agent checks the digital signature of the update for authenticity, and the contents of the package for integrity. Next, each update file is parsed and its version is checked against the installed one. Newer files are downloaded locally and checked against their MD5 hash to make sure they are not altered.

If in any moment a check is not passed, the update process stops, returning an error. Otherwise, the update is considered valid and ready to be installed.

To update the GravityZone appliances installed in your environment and the installation packages of the GravityZone components, log in with a company administrator account and go to the **Configuration > Update** page.

6.1. Updating GravityZone Appliances

Through GravityZone appliance updates, Bitdefender releases new features and improvements of existing ones. These are visible into Control Center.

Before running an update, it is recommended you check the following:

- The update status
- Any information or warning messages that may appear.
- The changelog

To check the update status:

1. Go to the **Configuration > Update > GravityZone Roles** page.

2. Under the **Current Status** section, glance over the message that points the general status of your deployment. If GravityZone needs updating, the **Update** button becomes available.
3. Under the **Infrastructure** section, inspect the details for each GravityZone role deployed in your network. Because roles update independently, for each role you can view: the name of the appliance hosting it, its IP address, current version, the latest version available, and update status.

To check the changelog:

1. Go to the **Configuration > Update > GravityZone Roles** page.
2. Click the **View changelog** link. A pop-up window displays a list with all versions and changes they included.

Release Notes for each new product version are also published on the [Bitdefender Support Center](#).

You can update GravityZone in two ways:

- [Manually](#)
- [Automatically](#)

6.1.1. Manual Update

Choose this method if you want to have full control of when the update should roll out.

To manually update GravityZone:

1. Go to the **Configuration > Update > GravityZone Roles** page.
2. Click the **Update** button (if available).

The update may take a while. Please wait until it is complete.

3. Clear the browser cache.

During the update, Control Center logs out all users and informs them of an in-progress update. You will be able to view a detailed progress of the update process.

When the update is complete, Control Center displays the Login page.

6.1.2. Automatic Update

By installing updates automatically, you are sure that GravityZone is always updated with the latest features and security patches.

GravityZone has two types of automatic updates:

- [Product updates](#)
- [Third party software updates](#)

Product Updates

These updates bring new features in GravityZone and resolve issues resulted from these features.

Because updates are disruptive for GravityZone users, they are designed to run based on a schedule. You can schedule the update to take place at convenient hours. By default, automatic product updates are disabled.

To enable and schedule product updates:

1. Go to **Configuration > Update > GravityZone Roles** page.
2. Select the **Enable automatic GravityZone product updates** check box.
3. Set the **Recurrence** to **Daily, Weekly** (select one or more weekdays) or **Monthly**.
4. Define an **Interval**. You can schedule a time for the update process to begin when a new update is available.

GravityZone displays by default a warning message to all Control Center users 30 minutes before the automatic update starts. To disable the warning, clear the check box **Enable the 30 minutes downtime alert before update**.

Third Party Software Updates

GravityZone virtual appliance embeds a series of software products provided by other vendors. This type of updates aims to patch such software as soon as possible, diminishing possible security risks.

These updates run silently and do not interrupt the work with Control Center.

By default, this option is enabled. To disable this option:

1. Go to **Configuration > Update > GravityZone Roles** page.
2. Clear the check box **Enable automatic security updates for 3rd party GravityZone components**.

Third party software patches will then be released once with the GravityZone product update.

6.2. Configuring Update Server

By default, the Update Server downloads updates from the Internet every hour. It is recommended not to change the default Update Server settings.

To check and configure the Update Server settings:

1. Go to the **Update** page in Control Center and click the **Components** tab.
2. Click the **Settings** button at the upper side of the pane on the left side to display the **Update Server Settings** window.
3. Under **Update Server Configuration**, you can check and configure the main settings.
 - **Packages Address.** The address where packages are downloaded from.
 - **Update Address.** Update Server is configured to check for and download updates from `upgrade.bitdefender.com:80`. This is a generic address that is automatically resolved to the closest server that stores Bitdefender updates in your region.
 - **Port.** When configuring the various GravityZone components to update from Update Server, you must provide this port. The default port is `7074`.
 - **IP.** The IP address of the Update Server.
 - **Update period (hours).** If you want to change the update period, type a new value in this field. The default value is `1`.
4. You can configure the Update Server to automatically download the endpoint kits.
5. Update Server can act as gateway for data sent by the Bitdefender client products installed in the network to the Bitdefender servers. This data may include anonymous reports regarding virus activity, product crash reports and data used for online registration. Enabling the gateway roles is useful for traffic control and in networks with no Internet access.

**Note**

You can disable the product modules that send statistical or crash data to Bitdefender Labs anytime you want. You can use policies to remotely control these options on the computers and virtual machines managed by Control Center.

6. Click **Save**.

6.3. Downloading Product Updates

You can view information about the existing GravityZone component packages under the **Components** tab. Available information includes current version, update version (if any) and the status for update operations you initiate.

To update a GravityZone component:

1. Go to the **Update** page in Control Center and click the **Components** tab.
2. Click the component you want to update in the **Product** list. All available versions will be displayed in the **Packages** table. Select the check box corresponding to the version you want to download.

**Note**

New packages will be in the **Not downloaded** state. Once a newer version is released by Bitdefender, the oldest undownloaded version will be removed from the table.

3. Click **Actions** at the upper side of the table and select **Publish**. The selected version will be downloaded and the status will change accordingly. Refresh the table contents by clicking the **Refresh** button and check the corresponding status.

6.4. Product Offline Updates

GravityZone uses by default an update system connected to the Internet. For isolated networks, Bitdefender offers an alternative, making the components and security content updates available offline as well.

6.4.1. Prerequisites

To use offline updates, you need:

- A GravityZone instance installed in a network with internet access (“online instance”). The online instance must have:
 - Direct internet access
 - Access on ports 80 and 443. For more details about the ports used by GravityZone, refer to [this KB article](#).
 - Only the Database and Update Server installed roles
- One or several GravityZone instances installed in a network without internet access (“offline instances”)
- Both GravityZone instances must have the same appliance version

6.4.2. Setting Up the Online GravityZone Instance

During this phase, you will deploy a GravityZone instance to a network with internet access, and then configure it to perform as offline update server.

1. Deploy GravityZone to a machine with internet connection.
2. Install only the Database and Update Server roles.
3. Access the machine's TTY terminal in your virtual environment (or connect to it via SSH).
4. Log in with the `bdadmin` user and the password you have set.
5. Run the command `sudo su` to gain **root** privileges.
6. Run the following commands to install the offline `gzou-mirror` package:

```
# apt update
# gzcli update
# apt install gzou-mirror
```

The `gzou-mirror` has the following roles:

- Configure the Update Server to generate automatically offline update archives.
- Set up a web service to the online instance, providing configuration and download options for the offline update archives.

6.4.3. Configuring and downloading the initial update files

During this phase, you will configure the update archive settings via the web service installed on the online instance, and then create the archive files required for [setting up the offline instance](#). Then, you will have to download the update files and place them to a portable media device (USB stick).

1. Access the web service through a URL of this form: `https://Online-Instance-Update-Server-IP-or-Hostname`, with the username `bdadmin` and the password you have set.

Appliance Status

[Download archives](#)
[Generate support bundle](#)

Current job: -

Next archive will be created on: Tue Aug 14 2018 17:55:07 GMT+0300 (Eastern European Summer Time) [Create...](#)

Free disk space: 86.59 GiB

Kits

- ☒ Bitdefender Security Tools (BEST)
- ☐ Bitdefender Security Tools (BEST) Legacy
- ☒ Bitdefender Security Tools (BEST)
- ☐ Bitdefender Endpoint Security
- ☐ Bitdefender Endpoint Security
- ☐ Bitdefender Tools
- ☐ Bitdefender Tools

Settings

Archive creation interval (in hours):

Number of FULL archives to keep on disk:

Number of LITE archives to keep on disk:

Apply

The online instance - Web Service

2. Configure the offline update archive as follows:
 - Under **Kits**: select the endpoint agent kits you want to include in the offline update archive.
 - Under **Settings**, edit your update archive preferences.

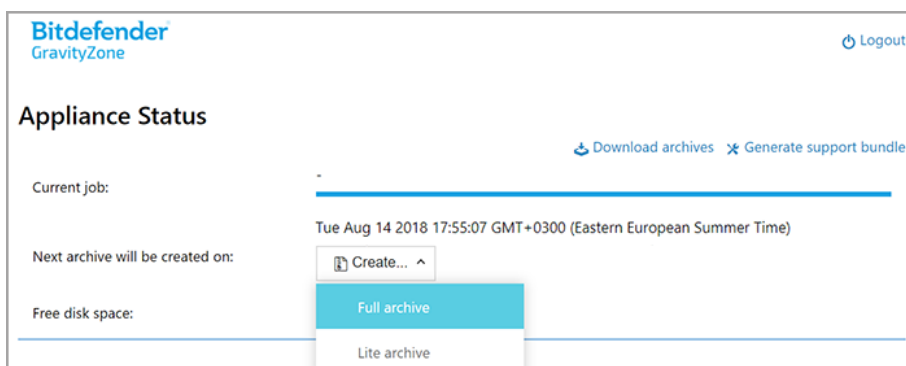
A CRON job installed on the online instance will check every minute if there are new update files available and if the free disk space is bigger than 10GB. At each period set by the **Archive creation interval (in hours)** option, the CRON job will create the following files:

- **Full archive (product + security content)**, when new update files are available
- **Lite archive** (security content only), when there are no new update files

The archives will be created in the following location:

<https://Online-Instance-Update-Server-IP-or-Hostname/snapshots>

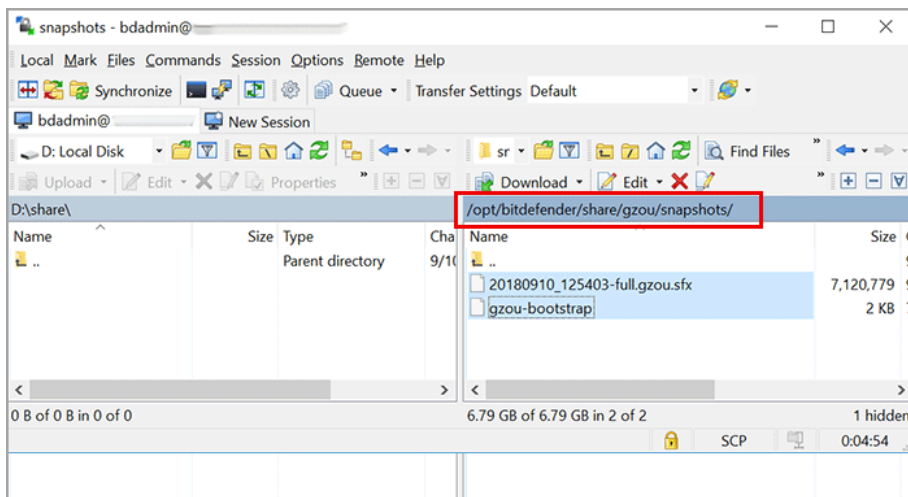
3. Click **Create > Full** archive to create the first full archive. Wait until the archive is created.



The online instance - Web Service: Creating the archive

4. Download the full update archive and the `gzou-bootstrap` file from the online instance. You have several options at hand:
 - Via the web service: click **Download archives** to access the page containing the links to the update files. Click the full update archive and the `gzou-bootstrap` file links to download them on your endpoint.
 - Use your preferred SCP/SCTP client (WinSCP, for example) to establish a SCP session with the online instance and transfer the abovementioned files to any location in your online network. The default path on the online instance is:

```
opt/bitdefender/share/gzou/snapshots
```



Transferring update files using SCP

- Via SAMBA share. Use a read-only SAMBA share to retrieve the offline update archives from the following location:

\\Online-Instance-Update-Server-IP-or-Hostname\gzou-snapshots



Note

The credentials for accessing the SAMBA share, if requested, are the same with the online instance credentials (bdadmin user and password).

6.4.4. Setting Up the Offline GravityZone Instance

During this step, you will deploy and configure the offline instance to receive updates via the archives generated by the online instance. Unless stated otherwise, all commands must be run as **root**.

1. Deploy GravityZone to a machine from the isolated environment.
2. Install only the Database and Update Server roles.
3. Transfer the update archive and the `gzou-bootstrap` file downloaded from the online instance to the `/home/bdadmin` directory of the offline instance using a portable media device (USB stick).

**Important**

For the offline update to work, make sure that:

- The update archive and the `gzou-bootstrap` are in the same folder.
- The update archive is a **full** archive.

4. Execute the `gzou-bootstrap` file as follows:

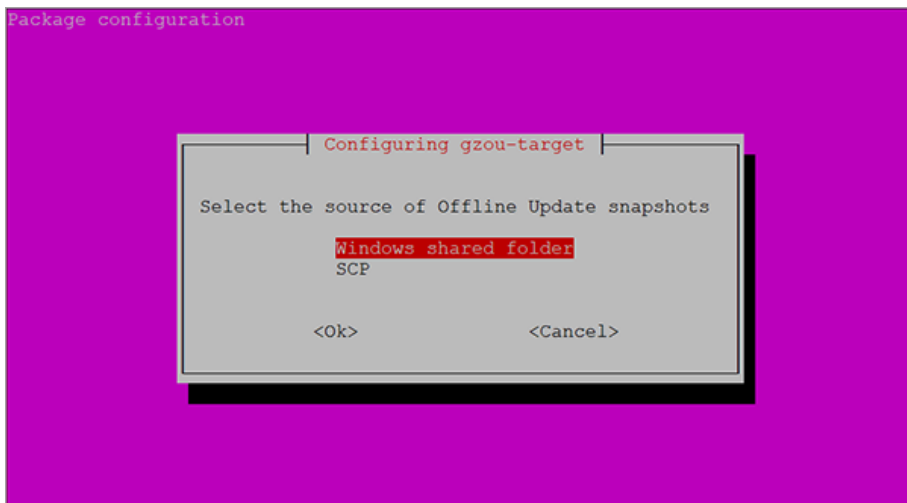
- a. Access the machine's TTY terminal in your virtual environment (or connect to it via SSH).
- b. Transform `gzou-bootstrap` into an executable:

```
#chmod +x gzou-bootstrap
```

- c. Run: `./gzou-bootstrap`

5. Choose the method of transferring the update archives to the offline instance:

- Select **Windows shared folder** (Samba share). In this case, you will have to specify the path to a Windows share from the isolated network, where the offline instance will automatically connect to retrieve the update archives. Enter the credentials required to access the specified location.
- Select **SCP** if you will manually transfer the files to the `/opt/bitdefender/share/gzou/snapshots/` folder of the offline instance via SCP.



Offline GravityZone Instance - Configuring the update files transfer mode



Note

If you want to change the transfer method at a later time:

- Access the offline instance's TTY terminal in your virtual environment (or connect to it via SSH).
- Log in with the `bdadmin` user and the password you have set.
- Run the command `sudo su` to gain root privileges.
- Run:

```
# rm -f /opt/bitdefender/etc/gzou-target.json
# dpkg-reconfigure gzou-target
```

The configuration dialog will appear, where you can make the changes that you want.

- Switch to the offline GravityZone console command line and install the rest of the roles.
- Access the offline console from your web browser and insert your license key (in offline mode).

6.4.5. Using Offline Updates

Once you have set up the GravityZone instances, follow these steps to update your offline installation:

1. Download the latest offline update archive from the online instance to your preferred network share. For more details, refer to [“Configuring and downloading the initial update files”](#) (p. 124).
2. Use a USB stick to transfer the update archive to the configured Samba share from the isolated network. For more details, refer to [“Setting Up the Offline GravityZone Instance”](#) (p. 126).

The files will be automatically pulled into the following offline instance directory:

```
/opt/bitdefender/share/gzou/snapshots/
```

6.4.6. Using the Web Console

Access the web console by entering the IP/Hostname of the appliance in the web browser. You can edit the available options:

- [Control Center](#)
- [General Settings](#)

Control Center

The **Appliance Status** displays the details of the last job performed (archive type, date and time), and the next scheduled job.

You have the option to:

- **Create Security Content Archive**
- **Create Full Archive**

In the **Created Archives** section, you can download security content and full archives.

Select the archive(s) from the available list, and click the **Download** button.

You can also view the available space on the appliance disk.

General Settings

You can define a download schedule for the GravityZone kits.

1. Click the **Edit Settings** button.

2. Select one or more kits from the **Available Kits** list.
3. In the **Schedule** section, you can define an interval for creating the archives, as well as the number of archives to keep on disk.
4. Click the **Apply** button to save your changes.

7. UNINSTALLING PROTECTION

You can uninstall and reinstall GravityZone components in such cases as when you need to use a license key for another machine, to fix errors or when you upgrade.

To correctly uninstall Bitdefender protection from endpoints in your network, follow the instructions described in this chapter.

- [Uninstalling Endpoint Protection](#)
- [Uninstalling GravityZone Server Roles](#)

7.1. Uninstalling Endpoint Protection

You have two options to uninstall the security agents:

- [Remotely](#) in Control Center
- [Manually](#) on the target machine

Remote Uninstallation

To uninstall Bitdefender protection from any managed endpoint remotely:

1. Go to **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the container you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
4. Select the endpoints from which you want to uninstall the Bitdefender security agent.
5. Click **Tasks** at the upper-side of the table and choose **Uninstall client**. A configuration window is displayed.
6. In the **Uninstall agent** task window you can choose whether to keep the quarantined files on the endpoint or to delete them.

For VMware vShield integrated environments, you must select the required credentials for each machine, otherwise the uninstallation fails. Select **Use credentials for vShield integration**, then add the required data in the Credentials Manager table displayed below.

7. Click **Save** to create the task. A confirmation message appears.

You can view and manage the task in **Network > Tasks**.

If you want to reinstall security agents, refer to [“Installing Security Agents”](#) (p. 92).

Local Uninstallation

To manually uninstall the Bitdefender security agent from a Windows machine:

1. Depending on your operating system:
 - In Windows 7, go to **Start > Control Panel > Uninstall a program** under **Programs** category.
 - In Windows 8, go to **Settings > Control Panel > Uninstall a program** under **Program** category.
 - In Windows 8.1, right-click on **Start** button, then choose **Control Panel > Programs & features**.
 - In Windows 10, go to **Start > Settings > System > Apps & features**.
2. Select the Bitdefender agent from the programs list.
3. Click **Uninstall**.
4. Enter the Bitdefender password, if enabled in the security policy. During uninstallation, you can view the progress of the task.

To manually uninstall the Bitdefender security agent from a Linux machine:

1. Open the terminal.
2. Gain root access using the `su` or `sudo su` commands.
3. Navigate using the `cd` command to the following path:
`/opt/BitDefender/bin`
4. Run the script:

```
# ./remove-sve-client
```

5. Enter the Bitdefender password to continue, if enabled in the security policy.

To manually uninstall the Bitdefender agent from a Mac:

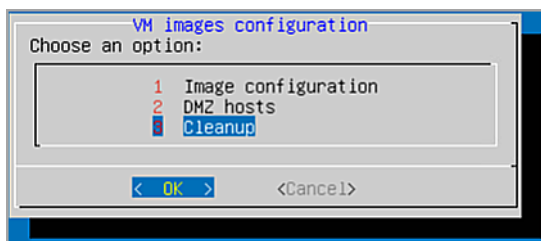
1. Go to **Finder > Applications**.
2. Open the Bitdefender folder.

3. Double-click **Bitdefender Mac Uninstall**.
 4. In the confirmation window, click both **Check** and **Uninstall** to continue.
- If you want to reinstall security agents, refer to [“Installing Security Agents”](#) (p. 92).

7.2. Uninstalling Sandbox Analyzer On-Premises

To uninstall Sandbox Analyzer On-Premises:

1. Remove the virtual machine (VM) images from the Sandbox Analyzer appliance console.
 - a. Log into Sandbox Analyzer appliance interface.
Use the arrow keys and the **Tab** key to navigate through menus and options.
Press **Enter** to select a specific option.
 - b. In the **Sandbox configuration** menu, go to the **VM images** option.
 - c. In the **VM images configuration** menu, go to the **Cleanup** option.



Sandbox Analyzer appliance console - Sandbox configuration - Cleanup

- d. Confirm that you want to remove the installed virtual machine images.
Wait for this action to complete. During this action, data associated with the virtual machine images will also be deleted.
2. Delete the Sandbox Analyzer Virtual Appliance:
 - a. Power off the Sandbox Analyzer Virtual Appliance.
 - b. Delete the appliance from the ESXi inventory.

7.3. Uninstalling GravityZone Virtual Appliance Roles

You can uninstall the GravityZone virtual appliance roles through the menu-based interface. Even if you remove one of them, your network is still protected. Nevertheless, you need at least one instance of each role for GravityZone to run properly.

In a scenario with a single appliance with all GravityZone roles, when removing one role, the endpoints will continue to be protected, although some of the appliance features will not be available, depending on each role.

In a scenario with multiple GravityZone appliances, you can safely uninstall a role as long as another instance of the same role is available. By design, multiple instances of Communication Server and Web Console roles can be installed on different appliances and connected to the other roles via a role balancer. Hence, if you uninstall one instance of a specific role, its function is taken over by other ones.

When needed, you can uninstall Communication Server from one appliance while assigning its function to another instance of this role. For a smooth migration, follow these steps:

1. In Control Center, go to the **Policies** page.
2. Select an existing policy or click **+Add** to create a new one.
3. Under **General** section, go to **Communication**.
4. In the **Endpoint Communication Assignment** table, click the **Name** field. The list of detected communication servers is displayed.
5. Select the communication server you want for endpoints to relate.
6. Click the **+ Add** button at the right side of the table. If you have in the list more than one communication server, you can configure their priority using the up and down arrows at the right side of each entity.
7. Click **Save** to create the policy. The endpoints will communicate with Control Center via the specified communication server.
8. In GravityZone command-line interface, uninstall the old Communication Server role.

**Warning**

If you uninstall the old Communication Server without first setting up the policy, communication will be permanently lost and you will need to reinstall the security agents.

To uninstall GravityZone virtual appliance roles:

1. Log in to the console interface from your virtualization management tool (for example, vSphere Client). Use the arrow keys and the `Tab` key to navigate through menus and options. Press `Enter` to select a specific option.
2. Select **Advanced Settings**.
3. Select **Install/Uninstall Roles**.
4. Go to **Add or remove roles**.
5. Using the `Space` bar, deselect any role you want to uninstall, then press `Enter`. A confirmation window appears, informing you the role will be removed.
6. Press `Enter` to continue and wait for the uninstallation to complete.

If you want to reinstall a role, refer to [“Install/Uninstall Roles” \(p. 79\)](#).

8. GETTING HELP

Bitdefender strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issue with or if you have any question about your Bitdefender product, go to our [online Support Center](#). It provides several resources that you can use to quickly find a solution or an answer. Or, if you prefer, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.



Note

You can find out information about the support services we provide and our support policy at the Support Center.

8.1. Bitdefender Support Center

[Bitdefender Support Center](#) is the place where you will find all the assistance you need with your Bitdefender product.

You can use several resources to quickly find a solution or an answer:

- Knowledge Base Articles
- Bitdefender Support Forum
- Product Documentation

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

Knowledge Base Articles

The Bitdefender Knowledge Base is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about virus prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their

way into the Bitdefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Knowledge Base for business products is available any time at <http://www.bitdefender.com/support/business.html>.

Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others. You can post any problem or question related to your Bitdefender product.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at <http://forum.bitdefender.com>, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Business Protection** link to access the section dedicated to business products.

Product Documentation

Product documentation is the most complete source of information about your product.

The easiest way to reach the documentation is from the **Help & Support** page of Control Center. Click your username in the upper-right corner of the console, choose **Help & Support** and then the link of the guide you are interested in. The guide will open in a new tab of your browser.

You can also check and download the documentation at [Support Center](#), in the **Documentation** section available on each product support page.

8.2. Asking for Assistance

You can ask for assistance through our online Support Center. Fill in the [contact form](#) and submit it.

8.3. Using Support Tool

The GravityZone Support Tool is designed to help users and support technicians easily obtain the information needed for troubleshooting. Run the Support Tool on affected computers and send the resulting archive with the troubleshooting information to the Bitdefender support representative.

8.3.1. Using Support Tool on Windows Operating Systems

Running the Support Tool application

To generate the log on the affected computer, use one of these methods:

- **Command-line**

For any issues with BEST, installed on the computer.

- **Installation issues**

For situations where BEST is not installed on the computer and the installation fails.

Command-line method

Using command line you can collect logs directly from the affected computer. This method is useful in situations where you do not have access to GravityZone Control Center or the computer does not communicate with the console.

1. Open Command Prompt with administrative privileges.
2. Go to the product installation folder. The default path is:

```
C:\Program Files\Bitdefender\Endpoint Security
```

3. Collect and save the logs by running this command:

```
Product.Support.Tool.exe collect
```

The logs are saved by default to C:\Windows\Temp.

Optionally, if you want to save the Support Tool log in a custom location, use the option path:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Example:

```
Product.Support.Tool.exe collect path="D:\Test"
```

While the command is executing, you can notice a progress bar on the screen. When the process is complete, the output displays the name of the archive containing the logs and its location.

To submit the logs to Bitdefender Enterprise Support access `C:\Windows\Temp` or the custom location and find the archive file named `ST_[computername]_[currentdate]`. Attach the archive to your support ticket for further troubleshooting.

Installation issues

1. To download BEST Support Tool click [here](#).
2. Run the executable file as administrator. A window will be prompted.
3. Choose a location to save the logs archive.

While the logs are collected, you will notice a progress bar on the screen. When the process is complete, the output displays the name of the archive and its location.

To submit the logs to Bitdefender Enterprise Support, access the selected location and find the archive file named `ST_[computername]_[currentdate]`. Attach the archive to your support ticket for further troubleshooting.

8.3.2. Using Support Tool on Linux Operating Systems

For Linux operating systems, the Support Tool is integrated with the Bitdefender security agent.

To gather Linux system information using Support Tool, run the following command:

```
# /opt/BitDefender/bin/bdconfigure
```

using the following available options:

- `--help` to list all Support Tool commands

- `enablelogs` to enable product and communication module logs (all services will be automatically restarted)
- `disablelogs` to disable product and communication module logs (all services will be automatically restarted)
- `deliverall` to create:
 - An archive containing the product and communication module logs, delivered to the `/tmp` folder in the following format:
`bitdefender_machineName_timeStamp.tar.gz`.

After the archive is created:

1. You will be prompted if you want to disable logs. If needed, the services are automatically restarted.
 2. You will be prompted if you want to delete logs.
- `deliverall -default` delivers the same information as with the previous option, but default actions will be taken on logs, without the user to be prompted (the logs are disabled and deleted).

You can also run the `/bdconfigure` command right from the BEST package (full or downloader) without having the product installed.

To report a GravityZone issue affecting your Linux systems, follow the next steps, using the options previously described:

1. Enable product and communication module logs.
2. Try to reproduce the issue.
3. Disable logs.
4. Create the logs archive.
5. Open an email support ticket using the form available on the **Help & Support** page of Control Center, with a description of the issue and having the logs archive attached.

The Support Tool for Linux delivers the following information:

- The `etc`, `var/log`, `/var/crash` (if available) and `var/epag` folders from `/opt/BitDefender`, containing the Bitdefender logs and settings
- The `/var/log/BitDefender/bdinstall.log` file, containing installation information

- The `network.txt` file, containing network settings / machine connectivity information
- The `product.txt` file, including the content of all `update.txt` files from `/opt/BitDefender/var/lib/scan` and a recursive full listing of all files from `/opt/BitDefender`
- The `system.txt` file, containing general system information (distribution and kernel versions, available RAM and free hard-disk space)
- The `users.txt` file, containing user information
- Other information concerning the product related to the system, such as external connections of processes and CPU usage
- System logs

8.3.3. Using Support Tool on Mac Operating Systems

When submitting a request to the Bitdefender Technical Support Team, you need to provide the following:

- A detailed description of the issue you are encountering.
- A screenshot (if applicable) of the exact error message that appears.
- The Support Tool log.

To gather Mac system information using Support Tool:

1. Download the [ZIP archive](#) containing the Support Tool.
2. Extract the **BDProfiler.tool** file from the archive.
3. Open a Terminal window.
4. Navigate to the location of the **BDProfiler.tool** file.

For example:

```
cd /Users/Bitdefender/Desktop;
```

5. Add execute permissions to the file:

```
chmod +x BDProfiler.tool;
```

6. Run the tool.

For example:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Press **Y** and enter the password when asked to provide the administrator password.

Wait for a couple of minutes until the tool finishes generating the log. You will find the resulted archive file (**Bitdefenderprofile_output.zip**) on your Desktop.

8.4. Contact Information

Efficient communication is the key to a successful business. During the past 18 years Bitdefender has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

8.4.1. Web Addresses

Sales Department: enterprisesales@bitdefender.com

Support Center: <http://www.bitdefender.com/support/business.html>

Documentation: gravityzone-docs@bitdefender.com

Local Distributors: <http://www.bitdefender.com/partners>

Partner Program: partners@bitdefender.com

Media Relations: pr@bitdefender.com

Virus Submissions: virus_submission@bitdefender.com

Spam Submissions: spam_submission@bitdefender.com

Report Abuse: abuse@bitdefender.com

Website: <http://www.bitdefender.com>

8.4.2. Local Distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to <http://www.bitdefender.com/partners>.
2. Go to **Partner Locator**.

3. The contact information of the Bitdefender local distributors should be displayed automatically. If this does not happen, select the country you reside in to view the information.
4. If you do not find a Bitdefender distributor in your country, feel free to contact us by email at enterprisesales@bitdefender.com.

8.4.3. Bitdefender Offices

The Bitdefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

United States

Bitdefender, LLC

PO Box 667588

Pompano Beach, FL 33066

United States

Phone (sales&technical support): 1-954-776-6262

Sales: sales@bitdefender.comWeb: <http://www.bitdefender.com>Support Center: <http://www.bitdefender.com/support/business.html>

France

Bitdefender

49, Rue de la Vanne

92120 Montrouge

Fax: +33 (0)1 47 35 07 09

Phone: +33 (0)1 47 35 72 73

Email: b2b@bitdefender.frWebsite: <http://www.bitdefender.fr>Support Center: <http://www.bitdefender.fr/support/business.html>

Spain

Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª

08037 Barcelona

España

Fax: (+34) 93 217 91 28
Phone (office&sales): (+34) 93 218 96 15
Phone (technical support): (+34) 93 502 69 10
Sales: comercial@bitdefender.es
Website: <http://www.bitdefender.es>
Support Center: <http://www.bitdefender.es/support/business.html>

Germany

Bitdefender GmbH

Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Phone (office&sales): +49 (0) 2304 94 51 60
Phone (technical support): +49 (0) 2304 99 93 004
Sales: firmenkunden@bitdefender.de
Website: <http://www.bitdefender.de>
Support Center: <http://www.bitdefender.de/support/business.html>

UK and Ireland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Phone (sales&technical support): (+44) 203 695 3415
Email: info@bitdefender.co.uk
Sales: sales@bitdefender.co.uk
Website: <http://www.bitdefender.co.uk>
Support Center: <http://www.bitdefender.co.uk/support/business.html>

Romania

BITDEFENDER SRL

Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470

Sales: sales@bitdefender.ro

Website: <http://www.bitdefender.ro>

Support Center: <http://www.bitdefender.ro/support/business.html>

United Arab Emirates

Bitdefender FZ-LLC

Dubai Internet City, Building 17

Office # 160

Dubai, UAE

Phone (sales&technical support): 00971-4-4588935 / 00971-4-4589186

Fax: 00971-4-44565047

Sales: sales@bitdefender.com

Web: <http://www.bitdefender.com>

Support Center: <http://www.bitdefender.com/support/business.html>

A. Appendices

A.1. Supported File Types

The antimalware scanning engines included in the Bitdefender security solutions can scan all types of files that may contain threats. The list below includes the most common types of files that are being analyzed.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo

A.2. Sandbox Analyzer Objects

A.2.1. Supported File Types and Extensions for Manual Submission

The following file extensions are supported and can be manually detonated in Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer is able to detect the above-mentioned file types also if they are included in archives of the following types: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

A.2.2. File Types Supported by Content Prefiltering at Automatic Submission

Content prefiltering will determine a particular file type through a combination which implies the object content and extension. That means that an executable having the `.tmp` extension will be recognized as an application and, if found suspicious, it will be sent to Sandbox Analyzer.

- Applications - files having the PE32 format, including but not limited to the following extensions: `exe`, `dll`, `com`.
- Documents - files having the document format, including but not limited to the following extensions: `xlsx`, `xls`, `ppt`, `doc`, `docx`, `dot`, `chm`, `xlm`, `docm`, `dotm`, `potm`, `potx`, `ppam`, `ppax`, `pps`, `ppsm`, `pptx`, `sldm`, `sldx`, `xlam`, `xlm`, `xltm`, `rtf`, `pdf`.

- **Scripts:** ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.
- **Archives:** zip, jar, 7z, bz, bz2, tgz, msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.
- **Emails (saved in the file system):** eml, tnef.

A.2.3. Default Exclusions at Automatic Submission

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.

A.2.4. Recommended Applications for Detonation VMs

Sandbox Analyzer On-Premises requires certain applications to be installed on the detonation virtual machines so that they open the submitted samples.

Applications	File Types
Microsoft Office suite	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Windows default	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml