Bitdefender

GravityZone

Digitally signed by Celonenco Vitalie
Date: 2022.10.27 17:11:37 EEST
Reason: MoldSign Signature
Location: Moldova

INSTALLATION GUIDE

Bitdefender GravityZone Installation Guide

Publication date 2021.03.23

Copyright© 2021 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 viii
1. Conventions Used in This Guide viii
1. About GravityZone 1
2. GravityZone Protection Layers 2
2.1. Antimalware 2
2.2. Advanced Threat Control 3
2.3. HyperDetect 4
2.4. Advanced Anti-Exploit 4
2.5. Firewall 4
2.6. Content Control 5
2.7. Network Attack Defense 5
2.8. Patch Management 5
2.9. Device Control 5
2.10. Full Disk Encryption 6
2.11. Security for Exchange 6
2.12. Application Control 6
2.13. Sandbox Analyzer 6
2.14. Hypervisor Memory Introspection (HVI) 7
2.15. Network Traffic Security Analytics (NTSA) 8
2.16. Security for Storage 8
2.17. Security for Mobile 8
2.18. GravityZone Protection Layers Availability 9
3. GravityZone Architecture 10
3.1. GravityZone VA 10
3.1.1. GravityZone Database 10
3.1.2. GravityZone Update Server 11
3.1.3. GravityZone Communication Server 11
3.1.4. Web Console (GravityZone Control Center) 11
3.1.5. Report Builder Database 11
3.1.6. Report Builder Processors 11
3.2. Security Server 11
3.3. HVI Supplemental Pack 12
3.4. Security Agents 12
3.4.1. Bitdefender Endpoint Security Tools 12
3.4.2. Endpoint Security for Mac 15
3.4.3. GravityZone Mobile Client 15
3.4.4. Bitdefender Tools (vShield) 15
3.5. Sandbox Analyzer Architecture 16
4. Requirements 18
4.1. GravityZone Virtual Appliance 18
4.1.1. Supported Formats and Virtualization Platforms 18
4.1.2. Hardware 18
4.1.3. Internet Connection 23

4.2. Control Center 24
4.3. Endpoint Protection 24
4.3.1. Hardware 25
4.3.2. Supported Operating Systems 28
4.3.3. Supported File Systems 34
4.3.4. Supported Browsers 34
4.3.5. Supported Virtualization Platforms 34
4.3.6. Security Server 38
4.3.7. Traffic Usage 40
4.4. Exchange Protection 41
4.4.1. Supported Microsoft Exchange Environments 41
4.4.2. System Requirements 42
4.4.3. Other Software Requirements 42
4.5. Sandbox Analyzer On-Premises 42
4.5.1. ESXi Hypervisor 43
4.5.2. Sandbox Analyzer Virtual Appliance 44
4.5.3. Network Security Virtual Appliance 45
4.5.4. Physical Host Requirements and Hardware Scaling 45
4.5.5. Sandbox Analyzer Communication Requirements 47
4.6. HVI 48
4.7. Full Disk Encryption 53
4.8. Storage Protection 54
4.9. Mobile Protection 55
4.9.1. Supported Platforms 55
4.9.2. Connectivity Requirements 55
4.9.3. Push Notifications 55
4.9.4. iOS Management Certificates 56
4.10. Report Builder 56
4.10.1. Hardware 56
4.10.2. GravityZone Product Versions 57
4.11. GravityZone Communication Ports 57

5. Installing Protection 58
5.1. GravityZone Installation and Setup 58
5.1.1. Prepare for Installation 58
5.1.2. Deploy GravityZone 59
5.1.3. Control Center Initial Setup 68
5.1.4. Configure Control Center Settings 71
5.1.5. Managing the GravityZone Appliance 103
5.2. License Management 117
5.2.1. Finding a Reseller 117
5.2.2. Entering Your License Keys 118
5.2.3. Checking Current License Details 118
5.2.4. Resetting the license usage count 119
5.2.5. Deleting License Keys 120
5.3. Installing Endpoint Protection 120
5.3.1. Installing Security Server 120
5.3.2. Installing Security Agents 130
5.4. Installing Sandbox Analyzer On-Premises 154

5.4.1. Prepare for Installation ... 154
5.4.2. Deploy Sandbox Analyzer Virtual Appliance ... 155
5.4.3. Deploy Network Security Virtual Appliance ... 160
5.5. Installing Full Disk Encryption ... 162
5.6. Installing Exchange Protection ... 162
5.6.1. Preparing for Installation ... 163
5.6.2. Installing Protection on Exchange Servers ... 163
5.7. Installing HVI ... 163
5.8. Installing Storage Protection ... 167
5.9. Installing Mobile Devices Protection ... 167
5.9.1. Configure External Address for Communication Server ... 168
5.9.2. Create and Organize Custom Users ... 170
5.9.3. Add Devices to Users ... 171
5.9.4. Install GravityZone Mobile Client on Devices ... 172
5.10. Installing Report Builder ... 173
5.10.1. Installing Report Builder Database ... 174
5.10.2. Installing Report Builder Processors ... 175
5.11. Credentials Manager ... 176
5.11.1. Operating System ... 177
5.11.2. Virtual Environment ... 178
5.11.3. Deleting Credentials from Credentials Manager ... 179
5.12. Bitdefender GravityZone and HIPAA ... 179
5.12.1. GravityZone Cloud Solution ... 179
5.12.2. GravityZone On-Premises Solution ... 179
6. Updating GravityZone ... 182
6.1. Updating GravityZone Appliances ... 182
6.1.1. Manual Update ... 183
6.1.2. Automatic Update ... 184
6.2. Configuring Update Server ... 185
6.3. Downloading Product Updates ... 186
6.4. Staging Updates ... 186
6.4.1. Prerequisites ... 187
6.4.2. Using Staging ... 188
6.5. Product Offline Updates ... 194
6.5.1. Prerequisites ... 194
6.5.2. Setting Up the Online GravityZone Instance ... 195
6.5.3. Configuring and downloading the initial update files ... 195
6.5.4. Setting Up the Offline GravityZone Instance ... 198
6.5.5. Using Offline Updates ... 201
6.5.6. Using the Web Console ... 201
7. Uninstalling Protection ... 203
7.1. Uninstalling Endpoint Protection ... 203
7.1.1. Uninstalling Security Agents ... 203
7.1.2. Uninstalling Security Server ... 205
7.2. Uninstalling HVI ... 206
7.3. Uninstalling Exchange Protection ... 208
7.4. Uninstalling Sandbox Analyzer On-Premises ... 208

7.5. Uninstalling Mobile Devices Protection 209
7.6. Uninstalling Report Builder 211
7.7. Uninstalling GravityZone Virtual Appliance Roles 212
8. Getting Help 214
8.1. Bitdefender Support Center 214
8.2. Asking for Assistance 215
8.3. Using Support Tool 216
8.3.1. Using Support Tool on Windows Operating Systems 216
8.3.2. Using Support Tool on Linux Operating Systems 217
8.3.3. Using Support Tool on Mac Operating Systems 219
8.4. Contact Information 220
8.4.1. Web Addresses 220
8.4.2. Local Distributors 220
8.4.3. Bitdefender Offices 221
A. Appendices 224
A.1. Supported File Types 224
A.2. Sandbox Analyzer Objects 225
A.2.1. Supported File Types and Extensions for Manual Submission 225
A.2.2. File Types Supported by Content Prefiltering at Automatic Submission 225
A.2.3. Default Exclusions at Automatic Submission 226
A.2.4. Recommended Applications for Detonation VMs 226

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 `monospaced` 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. viii)	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, mobile devices, virtual machines in private, public cloud and Exchange mail servers.

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 and for Microsoft Exchange mail servers: antimalware with behavioral monitoring, zero day threat protection, application control and sandboxing, firewall, device control, content control, anti-phishing and antispam.

2. GRAVITYZONE PROTECTION LAYERS

GravityZone provides the following protection layers:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Advanced Anti-Exploit
- Firewall
- Content Control
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Application Control
- Sandbox Analyzer
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

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)**

* When using a dual engines scanning, if the first engine is unavailable, the fallback engine will be used. Resource consumption and network utilization will depend on the used 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. HyperDetect

Bitdefender HyperDetect is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage. HyperDetect contains machine learning models and stealth attack detection technology against threats such as: zero-day attacks, advanced persistent threats (APT), obfuscated malware, fileless attacks (misuse of PowerShell, Windows Management Instrumentation etc.), credential stealing, targeted attacks, custom malware, script-based attacks, exploits, hacking tools, suspicious network traffic, potentially unwanted applications (PUA), ransomware.

Note
This module is an add-on available with a separate license key.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. 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.

2.9. 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.).

2.10. 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.

2.11. Security for Exchange

Bitdefender Security for Exchange provides antimalware, antispam, antiphishing, attachment and content filtering seamlessly integrated with the Microsoft Exchange Server, to ensure a secure messaging and collaboration environment and increase productivity. Using award-winning antimalware and antispam technologies, it protects the Exchange users against the latest, most sophisticated malware, and against attempts to steal users' confidential and valuable data.

Important
Security for Exchange is designed to protect the entire Exchange organization to which the protected Exchange Server belongs. This means it protects all active mailboxes, including user/room/equipment/shared mailboxes.
In addition to Microsoft Exchange protection, the license also covers the endpoint protection modules installed on the server.

2.12. Application Control

The Application Control module prevents malware, zero-day attacks and enhances security without impacting productivity. Application Control enforces flexible application whitelisting policies that identify and prevent the installation and execution of any unwanted, untrusted or malicious applications.

2.13. 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 hosted by Bitdefender or 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 managed endpoints, network traffic streams, centralized quarantine and ICAP servers.

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

2.14. Hypervisor Memory Introspection (HVI)

It is widely known that highly organized, profit-driven attackers seek unknown vulnerabilities (zero-day vulnerabilities), or use one-off, purpose-built exploits (zero-day exploits) and other tools. Attackers also use advanced techniques to delay and sequence attack payloads to mask malicious activity. Newer, profit-driven attacks are built to be stealthy and defeat traditional security tools.

For virtualized environments, the problem is now resolved, HVI protecting datacenters with a high density of virtual machines against advanced and sophisticated threats that the signature-based engines cannot defeat. It enforces strong isolation, ensuring real-time detection of the attacks, blocking them as they happen and immediately removing the threats.

Whether the protected machine is Windows or Linux, server or desktop, HVI provides insight at a level that is impossible to achieve from within the guest operating system. Just as the hypervisor controls hardware access on behalf of each guest virtual machine, HVI has intimate knowledge of both user-mode and kernel-mode in-guest memory. The result is HVI has complete insight into guest memory, and therefore full context. At the same time, HVI is isolated from the protected guests, just as the hypervisor itself is isolated. By operating at the hypervisor level and leveraging the hypervisor functionalities, HVI overcomes technical challenges of traditional security to reveal malicious activity in datacenters.

HVI identifies attack techniques rather than attack patterns. This way, the technology is able to identify, report and prevent common exploitation techniques. The kernel is protected against rootkit hooking techniques that are used during the attack kill chain to provide stealth. User-mode processes are also protected against code injection, function detouring, and code execution from stack or heap.

2.15. 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.

2.16. Security for Storage

GravityZone Security for Storage delivers real-time protection for leading file-sharing and network-storage systems. System and threat-detection algorithm upgrades happen automatically - without requiring any efforts from you or creating disruptions for end-users.

Two or more GravityZone Security Servers Multi-Platform perform the role of ICAP server providing antimalware services to Network-Attached Storage (NAS) devices and file-sharing systems compliant with the Internet Content Adaptation Protocol (ICAP, as defined in RFC 3507).

When a user requests to open, read, write, or close a file from a laptop, workstation, mobile, or other device, the ICAP client (a NAS or file-sharing system) sends a scan request to Security Server and receives a verdict regarding the file. Depending on the result, Security Server allows access, denies access or deletes the file.

Note
This module is an add-on available with a separate license key.

2.17. Security for Mobile

Unifies enterprise-wide security with management and compliance control of iPhone, iPad and Android devices by providing reliable software and update distribution via Apple or Android marketplaces. The solution has been designed to enable controlled adoption of bring-your-own-device (BYOD) initiatives by enforcing usage policies consistently on all portable devices. Security features include screen

lock, authentication control, device location, remote wipe, detection of rooted or jailbroken devices and security profiles. On Android devices the security level is enhanced with real-time scanning and removable media encryption. As a result, mobile devices are controlled and sensitive business information residing on them is protected.

2.18. 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 Server
- HVI Supplemental Pack
- 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 from a single point of management, Control Center web console. This provides easier management and access to overall security posture, global security threats, and control over all security modules protecting virtual or physical desktops, servers and mobile devices. 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, servers or mobile devices that appear on the Microsoft Active Directory, VMware vCenter, Nutanix Prism Element or Citrix XenServer or that are simply detected in the network.

3.1.5. Report Builder Database

The Report Builder Database role provides the data required for creating query-based reports.

3.1.6. Report Builder Processors

The Report Builder Processors role is essential for creating, managing and storing the query-based reports that use information from Report Builder Database.

3.2. Security Server

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

There are three Security Server versions, for each type of virtualization environments:

- **Security Server for VMware NSX.** This version automatically installs on each host in the cluster where the Bitdefender has been deployed.
- **Security Server for VMware vShield Endpoint.** This version must be installed on each host to be protected.
- **Security Server Multi-Platform.** This version is for various other virtualized environments and it must be installed on one or more hosts so as to accommodate the number of protected virtual machines. When using HVI, a Security Server must be installed on each host that contains virtual machines to be protected.

3.3. HVI Supplemental Pack

The HVI pack ensures the link between the hypervisor and the Security Server on that host. This way, the Security Server is able to monitor the memory in use on the host it is installed, based on the GravityZone security policies.

3.4. 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
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

3.4.1. 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).

In addition to file system protection, Bitdefender Endpoint Security Tools also includes mail server protection for Microsoft Exchange Servers.

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
- HyperDetect
- Firewall
- Content Control
- Network Attack Defense
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Application Control

Endpoint Roles

- Power User
- Relay
- Patch Caching Server
- Exchange Protection

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. 28).

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 large distributed networks, relay agents help lowering the bandwidth usage, by preventing protected endpoints and security servers 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.

Exchange Protection

Bitdefender Endpoint Security Tools with Exchange role can be installed on Microsoft Exchange Servers with the purpose of protecting the Exchange users from email-borne threats.

Bitdefender Endpoint Security Tools with Exchange role protects both the server machine and the Microsoft Exchange solution.

3.4.2. 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

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client extends security policies with ease to on any number of Android and iOS devices, protecting them against unauthorized usage, riskware and loss of confidential data. Security features include screen lock, authentication control, device location, remote wipe, detection of rooted or jailbroken devices and security profiles. On Android devices the security level is enhanced with real-time scanning and removable media encryption.

GravityZone Mobile Client is exclusively distributed via Apple App Store and Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools is a light agent for VMware virtualized environments that are integrated with vShield Endpoint. The security agent installs on virtual machines protected by Security Server, to allow you to take advantage of the additional functionality it provides:

- Allows you to run Memory and Process Scan tasks on the machine.
- Informs the user about the detected infections and actions taken on them.
- Adds more options for antimalware scan exclusions.

3.5. 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.

Sandbox Analyzer is available in two variants:

- Sandbox Analyzer Cloud, hosted by Bitdefender.
- Sandbox Analyzer On-Premises, available as a virtual appliance that can be deployed locally.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud contains the following components:

- **Sandbox Analyzer Portal** – a hosted communication server used for handling requests between endpoints and the Bitdefender sandbox cluster.
- **Sandbox Analyzer Cluster** – the hosted sandbox infrastructure where the sample behavioral analysis occurs. At this level, the submitted files are detonated on virtual machines running Windows 7.

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

Bitdefender Endpoint Security Tools, the security agent installed on endpoints, acts as a feeding sensor to Sandbox Analyzer.

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:

- **Endpoint sensor**. Bitdefender Endpoint Security Tools for Windows acts as feeding sensor installed on endpoints. The Bitdefender agent uses advanced machine learning and neural network algorithms to determine suspicious content and to submit it to Sandbox Analyzer, including objects from centralized quarantine.
- **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. 103).

Bitdefender HVI also requests a significant amount of resources. If you use this service, please check out the tables with specific data. For complete requirements of the service, refer to "HVI" (p. 48).

If using Application Control, refer to "Application Control" (p. 21).

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	120	**160**	160	200	200	80	80	80	80
Web Console						80	80	80	80
Communication Server						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	120	160	80	80	80	80	80	80	80
Web Console			80	80	80	80	80	80	80
Communication Server			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.

Application Control

Counting on the number of endpoints using Application Control, GravityZone has specific hardware and deployment requirements:

Number of endpoints	Minimum recommended GravityZone configuration
< 500	All roles installed on one appliance
500 - 2999	Distributed environment, one role per each appliance
3000 - 4999	Distributed environment: • 3 x Database Server role • 2 x Communication Server role • 1 x Web Console role • 1 x Update Server role
5000 - 9999	Distributed environment: • 3 x Database Server role • 2 x Communication Server role • 1 x Web Console role • 1 x Update Server role
10000 - 24999	Distributed environment: • 3 x Database Server role • 2 x Communication Server role • 2 x Web Console role • 1 x Update Server role
25000 - 49999	Distributed environment: • 3 x Database Server role • 2 x Communication Server role • 2 x Web Console role • 1 x Update Server role
50000 <	Distributed environment: • 3 x Database Server configured in replica set with at least 3 members

Number of endpoints	Minimum recommended GravityZone configuration
	• 2 x Communication Server role • 2 x Web Console role • 1 x Update Server role

If you have endpoints with a high volume of installed applications, meaning high volatility in the entire infrastructure, consider the next level of specifications to make sure that everything works as intended.

For distributed environments, each role should have this minimum hardware configuration:

- 4 x vCPUs
- 8 GB of RAM
- 120 GB thin provisioned SDD storage

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 optimized protection, you can also install Security Servers. 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. 12).

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
	Apple M1	
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	

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

- 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 Exchange Protection Role

The quarantine for Exchange Servers requires additional hard-disk space on the partition where the security agent is installed.

The quarantine size depends on the number of items stored and their size.

By default, the agent is installed on the system partition.

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.

Requirements for VMware vShield Environments

These are Bitdefender Tools requirements and footprint for systems integrated in VMware environments with vShield Endpoint.

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

*5 MB when the Silent Mode option is enabled and 10 MB when it is disabled. When Silent Mode is enabled, Bitdefender Tools graphical user interface (GUI) is not loaded automatically at system startup, freeing up associated resources.

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 (1)(2)
- Windows 8 (3)
- Windows 7

Warning
(1) VMware vShield platform (Agentless version) support for Windows 8.1 (32/64 bit) is available starting with VMware vSphere 5.5 – ESXi build 1892794 and above.
(2) In VMware NSX, the OS version is supported starting with vSphere 5.5 Patch 2.
(3) In VMware NSX, the OS version is supported starting with vSphere 5.5.

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[(1)(2)]
- Windows Server 2012[(3)(4)]
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2[(4)]

Warning
(1) VMware vShield platform (Agentless version) support for Windows Server 2012 R2 (64 bit) is available starting with VMware vSphere 5.5 – ESXi build 1892794 and above.
(2) In VMware NSX, the OS version is supported starting with vSphere 5.5 Patch 2.
(3) In VMware NSX, the OS version is supported starting with vSphere 5.5.
(4) VMware NSX does not support the 32-bit versions of Windows 2012 and 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.
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.

Kernel Versions	Linux Distributions	On-access Requirements
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. 149).

* 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: • **Fanotify** is enabled on both remote and local systems. • The share is based on the CIFS and NFS file systems. **Note** On-access scanning does not scan network shares mounted using SSH or FTP.
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.x)
- macOS Catalina (10.15)

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

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 update 1, 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, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (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, 5.18 STS
- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 Community Edition

Note
Support for other virtualization platforms may be provided on request.

Integration with VMware NSX-V Requirements

- ESXi 5.5 or later for each server
- vCenter Server 5.5 or later
- NSX Manager 6.2.4 or later
- VMware Tools 9.1.0 or later, with Guest Introspection thin agent.
  - For Windows Virtual Machines refer to the following VMware Docs article.
  - For Linux Virtual Machines refer to the following VMware Docs article.

Note
VMware recommends using the following VMware Tools versions:
- 10.0.8 or later, to resolve slow VMs after upgrading VMware Tools in NSX / vCloud Networking and Security (VMware Knowledge Base article 2144236).
- 10.0.9 and later for Windows 10 support.

Important
It is recommended that you keep all VMware products updated with the latest patch.

Integration with VMware NSX-T Data Center Requirements

- VMware NSX-T Manager 2.4, 2.5, 3.0 or 3.1
- ESXi compatible with the NSX-T Manager version
- vCenter Server & vSphere compatible with the NSX-T Manager version
- VMware Tools with Guest Introspection thin agent, compatible with the NSX-T Manager version

For more compatibility details, refer to these VMware webpages:

- VMware Compatibility Guide – GravityZone vs. NSX-T Manager
- VMware Product Interoperability Matrices - NSX-T Data Center vs. VMware vCenter and VMware Tools

Integration with Nutanix Prism Element Requirements

- Credentials of a Nutanix Prism Element user with administrative privileges (Cluster Admin or User Admin)
- Nutanix Prism with AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism with AOS 5.6, 5.11 5.18 STS
- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 Community Edition

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. Security Server

Security Server is a preconfigured virtual machine running on an Ubuntu Server with the following versions:

- 16.04 (VMware NSX and Multi-Platform)
- 12.04 LTS (VMware vShield)

Memory and CPU

The memory and CPU resource allocation for the Security Server depends on the number and type of VMs running on the host. The following table lists the recommended resources to be allocated:

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

Security Server for NSX comes with a predefined hardware configuration (CPU and RAM), which you can adjust in VMware vSphere Web Client by turning off the machine, editing its settings and then turning it back on. For detailed information, refer to "Installing Security Server for VMware NSX" (p. 121).

HDD Space

Environment	HDD Space Provisioning
VMware NSX-V / NSX-T	40 GB
VMware with vShield Endpoint	40 GB
Other	16 GB

Security Server Distribution on Hosts

Environment	Security Server vs. Hosts
VMware NSX-V / NSX-T	Security Server automatically installs on each ESXi host in the cluster to be protected, at the time of the Bitdefender service deployment.
VMware with vShield Endpoint	Security Server must be installed on each ESXi host to be protected.
Other	Although not mandatory, Bitdefender recommends installing Security Server on each physical host for improved performance.

Network Latency

The communication latency between Security Server and the protected endpoints must be under 50 ms.

Storage Protection Load

The impact of Storage Protection on Security Server when scanning 20 GB is as follows:

Storage Protection status	Security Server resources	Security Server load	Transfer time (mm:ss)
Disabled (baseline)	N/A	N/A	10:10
Enabled	4 vCPU 4 GB RAM	Normal	10:30
Enabled	2 vCPU 2 GB RAM	Heavy	11:23

Note
These results are obtained with a sample of varied file types (.exe, .txt, .doc, .eml, .pdf, .zip etc.), ranging from 10 KB to 200 MB. The transfer duration corresponds to 20 GB of data contained in 46,500 files.

4.3.7. 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. Exchange Protection

Security for Exchange is delivered through Bitdefender Endpoint Security Tools, which is able to protect both the file system and the Microsoft Exchange mail server.

4.4.1. Supported Microsoft Exchange Environments

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

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

- Exchange Server 2007 with Edge Transport, Hub Transport or Mailbox role

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

4.4.2. System Requirements

Security for Exchange is compatible with any physical or virtual 64-bit server (Intel or AMD) running a supported Microsoft Exchange Server version and role. For details regarding the Bitdefender Endpoint Security Tools system requirements, refer to "Security Agent Without Roles" (p. 25).

Recommended server resource availability:

- Free RAM memory: 1 GB
- Free HDD space: 1 GB

4.4.3. Other Software Requirements

- For Microsoft Exchange Server 2013 with Service Pack 1: KB2938053 from Microsoft.
- For Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 or higher

4.5. 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.

4.5.1. 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. 45).
- 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. 45).
- 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.

4.5.2. 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. 45))
- 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. 225).

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. 226).

4.5.3. 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

4.5.4. 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 1vCPU
- 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 1vCPU = 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.

4.5.5. 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.

4.6. HVI

HVI operates with the help of two components: Security Server and HVI Supplemental Pack. These products need to be installed on the hosts in your virtualized environment where you have virtual machines you want to protect.

Before you deploy HVI on hosts, make sure that the following requirements are met:

Supported Virtualization Platforms

- Citrix XenServer 7.1 Enterprise Edition or higher, with latest patches

  Important
  For any XenServer starting with version 7.1 that reached EOL, Bitdefender provides HVI support for two additional months. After this period, we recommend updating to a XenServer version supported by Citrix. For more information, refer to Citrix Legacy Products Matrix and Citrix Product Matrix.

- Citrix Hypervisor 8.0 Enterprise Edition or higher, with latest patches

  Warning
  For Citrix Hypervisor 8.0 you must install patch XS80E004.

Supported Guest Virtual Machines

The virtual machines you want to protect with HVI must meet the following conditions:

1. The machines are in HVM Virtualization Mode, meaning that they are fully virtualized.
2. The machines run a supported operating system:
   - **Windows Desktop Operating Systems (32-bit and 64-bit)**

     Windows 10 Windows 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 (Restone 2)
Windows 10 Anniversary Update (Redstone 1)
Windows 10 November Update (Threshold 2)
Windows 10
Windows 8.1
Windows 8
Windows 7

- **Windows Server Operating Systems (64-bit)**
  Windows Server 2019
  Windows Server 2016
  Windows Server 2012 / Windows Server 2012 R2
  Windows Server 2008 R2
- **Linux Operating Systems (64-bit)**

Distribution	Version	Kernel version
Debian	10	4.19
Debian	9	4.9
Debian	8	3.16
Ubuntu	20.04 LTS	5.4
Ubuntu	18.04 LTS	4.15
Ubuntu	16.04 LTS	4.4
Ubuntu	14.04 LTS	3.13.139 and later
CentOS	8.2	4.18
CentOS	8	4.18
CentOS	7	3.10

Distribution	Version	Kernel version
Red Hat Enterprise Linux	8.2	4.18
Red Hat Enterprise Linux	8	4.18
Red Hat Enterprise Linux	7	3.10
Red Hat Enterprise Linux	6.8 / 6.9 / 6.10	2.36.32
SUSE Linux Enterprise Server	15 SP1	4.12
SUSE Linux Enterprise Server	12 SP4	4.12
SUSE Linux Enterprise Server	12 SP3	4.4
SUSE Linux Enterprise Server	12 SP2	4.4
SUSE Linux Enterprise Server	12 SP1	3.12
Oracle Linux	Earlier than 7.5	4.1 (UEK/RHCK)
Oracle Linux	7.5 and later	4.14 (UEK/RHCK)

Hardware Requirements for GravityZone VA

- **Required 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
Update Server*	8	4	4	4	4	4	6	8
Web Console**		6	8	8	10	10	12	12
Communication Server		6	8	8	10	10	16	20
Database***		6	6	6	6	6	9	12
Total	**8**	**22**	**26**	**26**	**30**	**30**	**43**	**52**

* Recommended when no Relays are deployed.

** For each active integration, add one vCPU on the virtual appliance with Web Console role.
*** In case of distributed installation of roles, along with Replica Set: for each additional Database instance, add the specified number to the total amount.

- **Required RAM (GB)**

Component	Number of Endpoints (up to)							
	250	500	1000	3000	5000	10000	25000	50000
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.

- **Required Disk Space (GB)**

Update Server	120	160	80	80	80	80	80	80	80
Web Console			80	80	80	80	80	80	80
Communication Server			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**

* 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.

Hardware Requirements for Hosts

- **CPU microarchitecture:**
  - Any Intel® Sandy Bridge processor or later, with support for Intel® Virtualization Technology.
  - VT-x or VT-d extensions must be enabled in BIOS.
- **Free HDD space:** Besides the space required by the Security Server, HVI requires another 9 MB for the Supplemental Pack on each host.

Security Server Requirements

Memory and CPU resource allocation for the Security Server depends on the number and type of VMs running on the host. The following table lists the recommended resources to be allocated:

Number of protected VMs	RAM	CPUs
1-50 VMs	6 GB	4 CPUs
51-100 VMs	8 GB	6 CPUs
101-200 VMs	16 GB	8 CPUs

Free HDD space: You must provision 8 GB disk space on each host for the Security Server.

For an optimal performance in a XenAPP environment, scale the Security Server's resources based on your configuration, as follows:

Number of XenApp VDAs	VDA		Security Server	
	CPUs	RAM (GB)	CPUs	RAM (GB)
1 VDA	4 / 8	12 / 24	2	4
2 VDA	4 / 8	12 / 24	2	8
4 VDA	8	24	2	16
8 VDA	4	12	4	16

Guest Virtual Machines Requirements

In a usual environment setup, for optimal performance and VM consolidation ratio, it is recommended to have the following minimum hardware configuration for the guest virtual machines:

- **vCPU:** 2 x vCPU
- **RAM:** 3 GB

4.7. 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

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

On Mac

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

- macOS Big Sur (11.x)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

4.8. Storage Protection

Supported storage and file-sharing solutions:

- ICAP-compatible network-attached storage (NAS) and storage-area network (SAN) systems from Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle®, and others
- Nutanix® Files 3.x up to 3.7.1.
- Citrix® ShareFile

4.9. Mobile Protection

4.9.1. Supported Platforms

Security for Mobile supports the following types of mobile devices and operating systems:

- Apple iPhones and iPad tablets (iOS 8.1+)
- Google Android smartphones and tablets (4.2+)

4.9.2. Connectivity Requirements

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

4.9.3. Push Notifications

Security for Mobile uses push notifications to alert mobile clients when policy updates and tasks are available. Push notifications are sent by the Communication Server via the service provided by the operating system manufacturer:

- Firebase Cloud Messaging (FCM) service for Android devices. For FCM to work, the following are required:
  - Google Play Store must be installed.
  - Devices running Android 4.2 or higher.
  - To send push notifications, a number of ports must be open.
- Apple Push Notifications service (APNs) for iOS devices. For more information, refer to this Apple KB article.

You can check whether mobile push notifications are working correctly in the **Mobile Push Notifications Check** section in **Configuration > Miscellaneous**.

To learn more about GravityZone Mobile Device Management workflow, please refer to this KB article.

4.9.4. iOS Management Certificates

To set up the infrastructure for iOS mobile device management, you must provide a number of security certificates.

For more information, refer to "Certificates" (p. 97).

4.10. Report Builder

The Report Builder roles require to run on separate instances of the GravityZone Virtual Appliance: the first virtual appliance must have the Report Builder Database role installed, the second one must have the Report Builder Processors role installed.

4.10.1. Hardware

The Report Builder roles require the following hardware resources:

Required CPU

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

RAM (GB)

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

Free Hard-Disk Space (GB)

Virtual Appliance	Number of Endpoints					
	250	1000	5000	10000	25000	50000
Database*	15	20	50	90	210	400

Virtual Appliance	Number of Endpoints					
	250	1000	5000	10000	25000	50000
Processors**	50	200	1000	1950	4800	9500

* The disk usage of the Report Builder Database virtual appliance is provided for events stored for one year.
** The disk usage of the Report Builder Processors virtual appliance is provided considering 10 reports per month on average, with a subset of 15 columns each one. The Report Builder Processors virtual appliance requires more space because it stores all the reports created with data from Report Builder Database.

4.10.2. GravityZone Product Versions

Starting with GravityZone version 6.5.5-1, the Report Builder roles are delivered with the GravityZone Virtual Appliance.

Before this version, the Report Builder roles were delivered as a separate virtual appliance compatible with Bitdefender GravityZone version 6.1.27-537 and later.

4.11. 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. Some protection layers require additional components to be installed and configured.

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 for all security services components 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, vShield Manager, 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 Update Server Web Console Communication Server	Basic (Required)	At least one instance of each role. A GravityZone appliance can run one, several or all of these roles.
Report Builder Database Report Builder Processors	Auxiliary	One appliance for each role
Security Server	Optional	Recommended only in small networks or if low on resources. Otherwise, deploy a stand-alone Security Server from Control Center, after GravityZone deployment is complete.

Depending on how you distribute the GravityZone roles, you will deploy one or more GravityZone appliances (at least three appliances if you use Report Builder). 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.

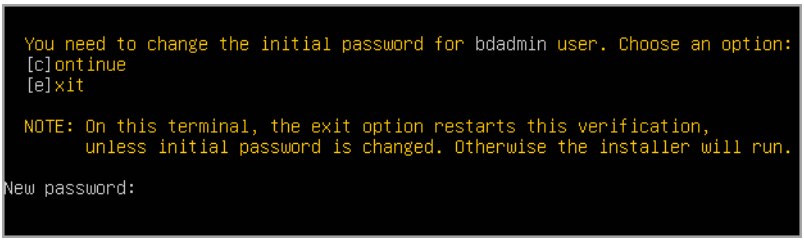
You can deploy more instances of Database Server, Web Console, and Communication Server roles. In this case, you will use Replica Set for Database Server, and load balancers for Web Console and Communication Server on the GravityZone appliances.

It is recommended to install the Report Builder roles after you set up GravityZone, meaning: installing the basic GravityZone roles, configuring Control Center, updating

GravityZone, and deploying protection on endpoints. Also, you need to first install Report Builder Database, followed by Report Builder Processors. For details, refer to "Installing Report Builder" (p. 173).

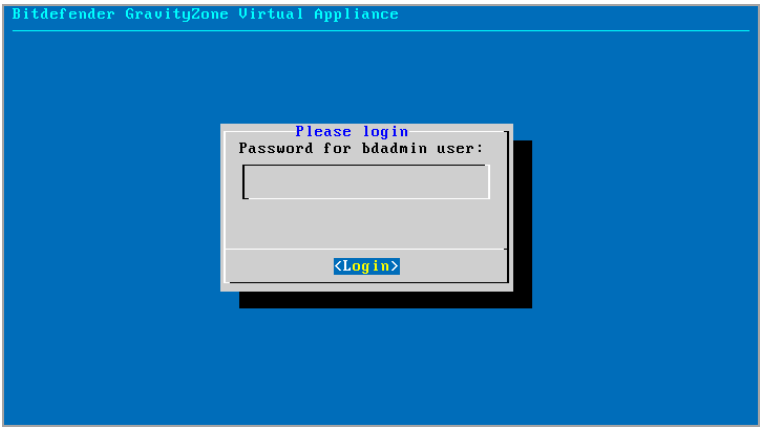
To deploy and set up GravityZone:

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.



Appliance console interface: enter new password

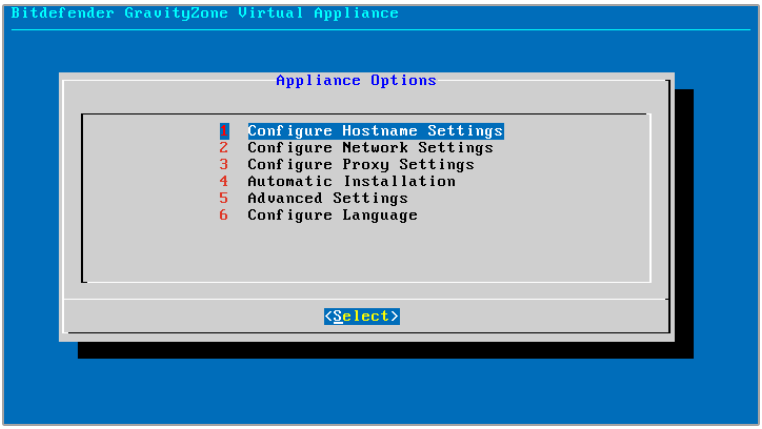
6. Log in with the password you have just set.



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. 68).

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. 103).

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.

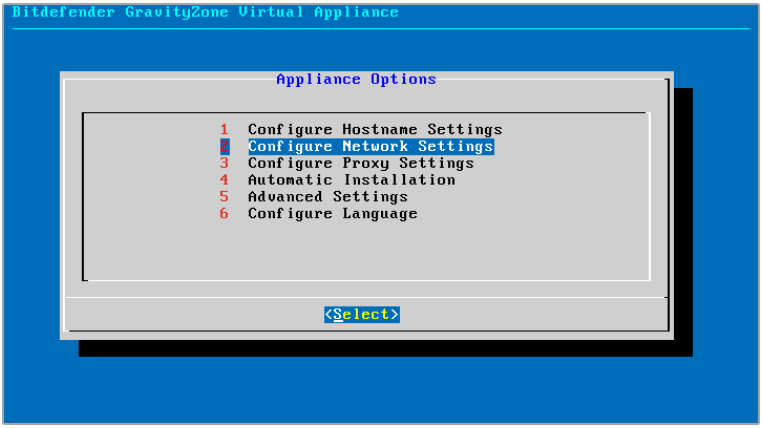
To configure the hostname settings:

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

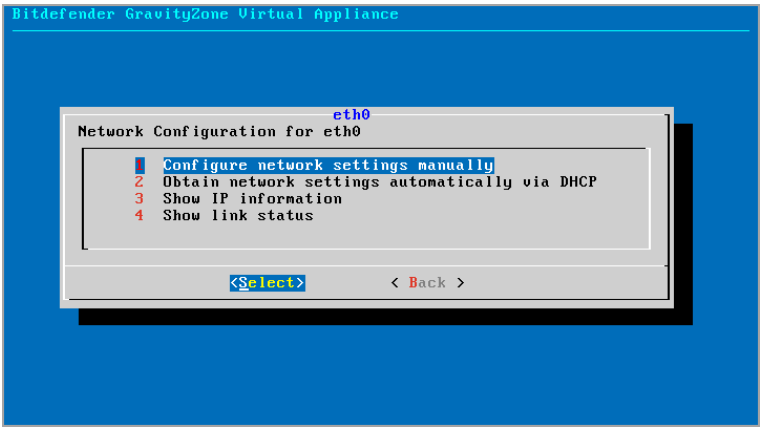
You can configure the appliance to automatically obtain network settings from the DHCP server or you can manually configure network settings. If you choose to use DHCP, you must configure the DHCP Server to reserve a specific IP address for the appliance.

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.



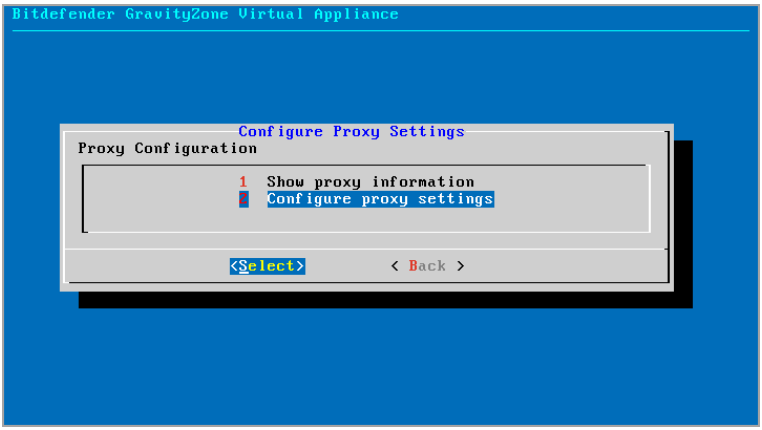
Appliance console interface: network configuration

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. 66).

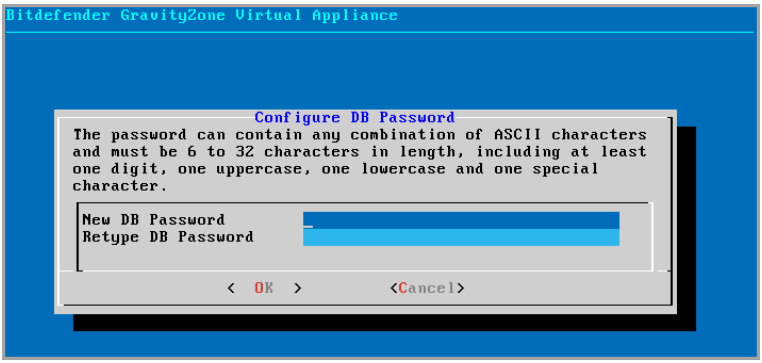
Important
Automatic deployment will also install the Security Server, embedded into the GravityZone appliance. For information about Security Server, refer to "GravityZone Architecture" (p. 10).
The option to install roles automatically is available only at the initial setup of GravityZone.

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

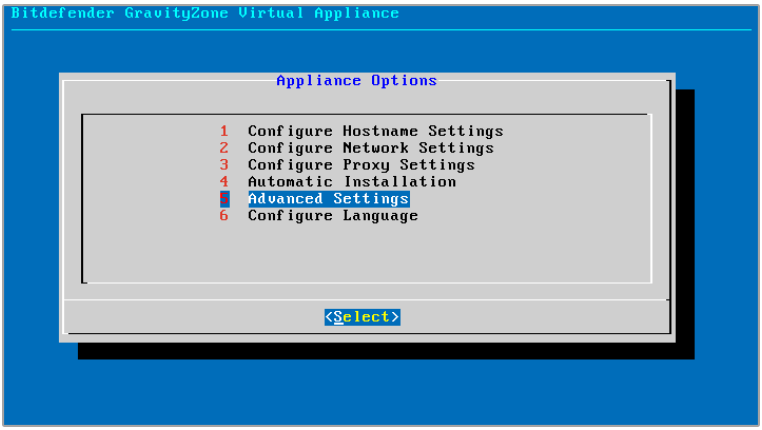
5. Wait until installation process is complete.

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. 114) or to "Connect to Existing Database (Secure VPN Cluster)" (p. 115).

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 keys required for validating the purchased GravityZone security services. 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).

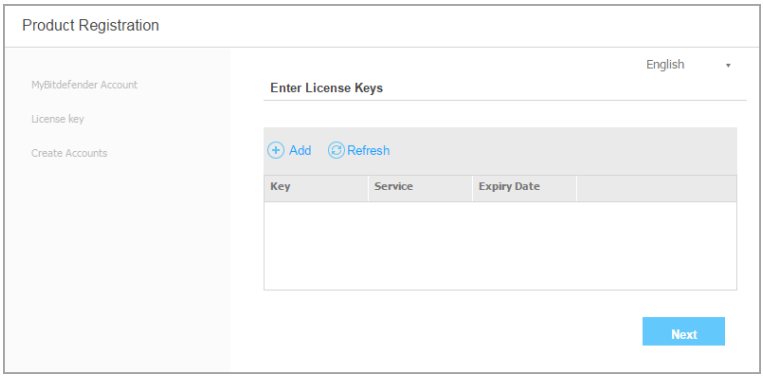
   c. Enter the license key in the **License key** field. For offline registration, you are required to provide also the registration code.

   d. Wait until the license key is validated. Click **Add** to finish.

   The license key will appear in the license table. You can also view the security service, status, expiry date and current usage for each license key in the corresponding columns.

   Note

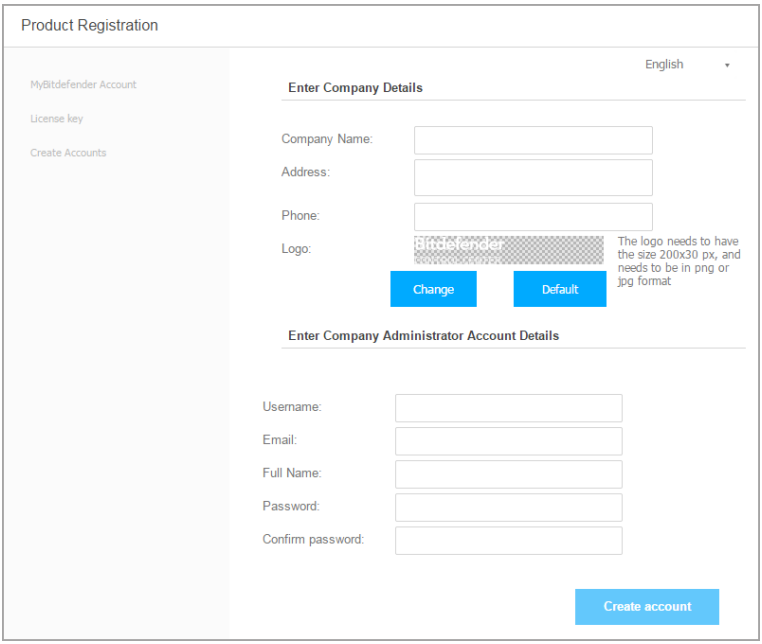
   - During the initial setup, at least one valid license key must be provided to start using GravityZone. You can afterwards add more license and add-on keys or to modify the existing ones.
   - You can use the add-ons as long as a valid basic license is provided. Otherwise you will view the features,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



Initial setup - Provide license keys

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.



Initial setup - Configure your account

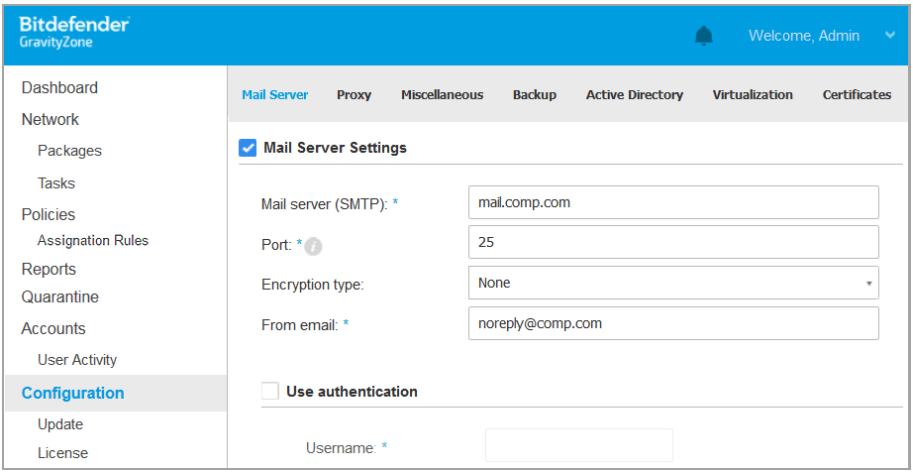
7. Click **Create account**.

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.



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 Security Server image is needed.** The GravityZone appliance does not include by default the Security Server virtual machine images. If an administrator tries to download a Security Server image or to run a Security Server installation task, the action is going to fail. You can configure an automated action for this situation by choosing one of the following options:
  - **Download the image automatically**
  - **Notify the administrator and do not download**

  Note
  To avoid interference with administrator's work, you can manually download the necessary Security Server packages from the **Update** page, on the **Product Update** tab. For more information, refer to "Downloading Product Updates" (p. 186).

- **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. 83).

- 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. 83).

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. 85)
- “Integrating with XenServer” (p. 88)
- “Integrating with Nutanix Prism Element” (p. 88)
- “Integrating with Amazon EC2” (p. 90)
- “Integrating with Microsoft Azure” (p. 91)
- “Managing Platform Integrations” (p. 92)

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. 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. Choose the VMware platform installed in your environment and configure the settings accordingly:
   - **None**. Select this option for NSX-T or if there is no VMware specific platform is installed and click **Save**. Accepting the self signed security certificate is required for the integration.

     To configure NSX-T Manager integration and apply endpoint protection to your VMs through GravityZone Guest Introspection policy, refer to the following KB article.
   - **vShield**. Specify the details of the vShield Manager system integrated with the vCenter Server.
     - Hostname or IP address of the vShield Manager system
     - vShield Manager port (default `443`)

- **NSX-V**. Specify the details of the NSX Manager integrated with the vCenter Server.

  Note
  To upgrade from VMware vShield to NSX, refer to this KB article.

  – Hostname or IP address of the NSX Manager
  – NSX Manager port (default `443`)
  – Username and password used to authenticate on NSX Manager.

    These credentials will be saved on the protected entity, not in Credentials Manager.
  – Select the **Tag if a virus is found** check box to use the default NSX security tags when malware is found on the virtual machine.

    A machine may be tagged with three different security tags, depending on the risk level of the threat:

    - `ANTI_VIRUS.VirusFound.threat=low`, applying on machine when Bitdefender finds low risk malware, which it can delete.
    - `ANTI_VIRUS.VirusFound.threat=medium`, applying on the machine if Bitdefender cannot delete the infected files, but instead it disinfects them.
    - `ANTI_VIRUS.VirusFound.threat=high`, applying on the machine if Bitdefender can neither delete, nor disinfect the infected files, but blocks access to them.

    When threats of different risk levels are detected on the same machine, all associated tags will be applied. For example, a machine on which high and low risk malware were found, will have both security tags.

    Note
    You can find the security tags in VMware vSphere, under **Networking & Security > NSX Managers >** `NSX Manager` **> Manage > Security Tags** tab.
    Though you can create as many tags as you want, only the three mentioned tags work with Bitdefender.

6. **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.

7. 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.

8. Select the check boxes to accept using the certificates.
9. Click **Save**. You will be able to view the vCenter Server in the active integrations list.
10. If you use the NSX-V platform:
    a. Go to the **Update > Components** tab.
    b. Download and then publish the **Security Server (VMware with NSX)** package. For more information on how to update GravityZone components, refer to "Updating GravityZone" (p. 182).
    c. Go to the **Configuration > Virtualization Providers** tab.
    d. In the **Action** column, click the **Register** button corresponding to the vCenter integrated with NSX to register the Bitdefender service with VMware NSX Manager.

Warning
When the security certificate is expired and the vCenter tries to synchronize, a pop-up will prompt you to update it. Enter the configuration window of the vCenter Server integration, click **Save**, accept the new certificates and then click **Save** again.

After registration, Bitdefender adds to VMware vSphere console:
- Bitdefender service
- Bitdefender service manager
- Three new default service profiles for permissive, normal and aggressive scanning modes.

Note
You can view these service profiles also in the **Policies** page of Control Center. Click the **Columns** button at the upper-right side of the right pane to view additional information.

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 asked in a new window if you want to use the Cluster Virtual IP instead of the CVM IP:

   a. 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.

   b. 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.

c. 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. 85)
   - “Integrating with XenServer” (p. 88)
   - “Integrating with Nutanix Prism Element” (p. 88)
   - “Integrating with Amazon EC2” (p. 90)
   - “Integrating with Microsoft Azure” (p. 91)
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 remove a vShield, XenServer, Nutanix Prism Element, Amazon EC2 or Microsoft Azure integration:

1. In Control Center, go to the **Configuration > Virtualization Providers** tab.
2. Click the **Delete** button in the **Action** column, corresponding to the integration to be removed.
3. Click **Yes** to confirm the action.

To remove an NSX integration:

1. Log in to VMware vSphere console and delete all Bitdefender policies and Security Servers.
2. In Control Center, go to the **Configuration > Virtualization Providers** tab.
3. In the **Action** column, corresponding to the integration to be removed, click **Unregister** and then **Delete**.
4. Click **Yes** to confirm the action.

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

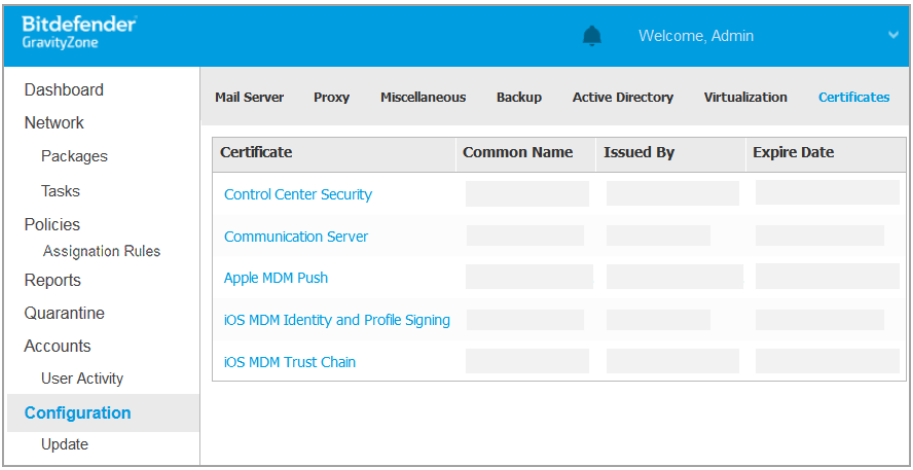
Deleting the NTSA license key from the **Configuration > License** page will also delete the NTSA integration.

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 a number of security certificates in Control Center.



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)

Note
The following certificates are required exclusively for managing security on Apple iOS devices:

- Communication Server Certificate
- Apple MDM Push Certificate
- iOS MDM Identity and Profile Signing Certificate
- iOS MDM Trust Chain Certificate

If you do not plan to roll out iOS mobile device management, you do not need to provide these certificates.

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**.

Endpoint - Security Server Communication Security Certificate

This certificate ensures a secure communication between the security agents and the Security Server (Multi-Platform) they have assigned.

During its deployment, the Security Server generates a default self-signed certificate. You can replace this built-in certificate by adding one of your choice in Control Center.

To add or replace an Endpoint - Security Server Communication 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**. A warning message may appear if the certificate is self-signed or expired. If expired, please renew your certificate.
8. Click **Yes** to continue uploading the certificate. Immediately after the upload finishes, Control Center sends the security certificate to the Security Servers.

If needed, you can revert to the original built-in certificate of each Security Server, as follows:

1. Click the certificate name in the **Certificates** page.
2. Choose **No certificate (use default)** as the certificate type.
3. Click **Save**.

Communication Server Certificate

The Communication Server certificate is used to secure communication between the Communication Server and iOS mobile devices.

Requirements:

- This SSL certificate can be signed either by your company or by an external Certificate Authority.

  Warning
  The certificate may be invalidated if it not issued by a public/trusted Certificate Authority (for example, self-signed certificates).

- The certificate common name must match exactly the domain name or IP address used by mobile clients to connect to the Communication Server. This is configured as the external MDM address in the configuration interface of the GravityZone appliance console.
- Mobile clients must trust this certificate. For this, you must also add the iOS MDM Trust Chain.

To add or replace the Communication Server 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**.

Apple MDM Push Certificate

Apple requires an MDM Push certificate to ensure secure communication between the Communication Server and the Apple Push Notifications service (APNs) when sending push notifications. Push notifications are used to prompt devices to connect to the Communication Server when new tasks or policy changes are available.

Apple issues this certificate directly to your company, but requires your Certificate Signing Request (CSR) to be signed by Bitdefender. Control Center provides a wizard to help you easily obtain your Apple MDM Push certificate.

Important

- You need an Apple ID to obtain and manage the certificate. If you do not have an Apple ID, you can create one on My Apple ID webpage. Use a generic and not an employee's email address to register for the Apple ID, as you will need it later to renew the certificate.
- Apple website does not work properly on Internet Explorer. We recommend using the latest versions of Safari or Chrome.
- The Apple MDM Push certificate is valid for one year only. When the certificate is about to expire, you must renew it and import the renewed certificate to Control Center. If you allow the certificate to expire, you must create a new one and reactivate all your devices.

Adding an Apple MDM Push Certificate

To obtain the Apple MDM Push certificate and import it in Control Center:

1. Go to the **Configuration** page and click the **Certificates** tab.
2. Click the certificate name and follow the wizard as described below:

Step 1 - Obtain a Certificate Signing Request signed by Bitdefender

Select the appropriate option:

- **I need to generate a certificate signing request signed by Bitdefender** (Recommended)
  a. Enter your company name, your full name and email address in the corresponding fields.
  b. Click **Generate** to download the CSR file signed by Bitdefender.
- **I already have a certificate signing request and I need to get it signed by Bitdefender**
  a. Upload your CSR file and the associated private key by clicking the **Add** button next to their fields.

     The Communication Server needs the private key when authenticating with the APNs servers.
  b. Specify the password protecting the private key, if any.
  c. Click the **Sign** button to download the CSR file signed by Bitdefender.

Step 2 - Request a push certificate from Apple

a. Click the **Apple Push Certificates Portal** link and sign in using your Apple ID and password.
b. Click the **Create a Certificate** button and accept the Terms of Use.
c. Click **Choose file**, select the CSR file and then click **Upload**.

> **Note**
> You may find the **Choose file** button with a different name such as **Choose** or **Browse**, depending on the browser you use.

d. From the confirmation page, click the **Download** button to receive your MDM Push certificate.
e. Go back to the wizard from Control Center.

Step 3 - Import the Apple push certificate

Click the **Add Certificate** button to upload the certificate file from your computer.

You may check the certificate details in the field below.

3. Click **Save**.

Renewing the Apple MDM Push Certificate

To renew the Apple MDM certificate and update it in Control Center:

1. Go to the **Configuration** page and click the **Certificates** tab.

2. Click the certificate name to open the import wizard.
3. Obtain a Certificate Signing Request signed by Bitdefender. The procedure is the same as for obtaining a new certificate.
4. Click the **Apple Push Certificates Portal** link and sign in with the same Apple ID used to create the certificate.
5. Locate the MDM Push certificate for Bitdefender and click the corresponding **Renew** button.
6. Click **Choose file**, select the CSR file and then click **Upload**.
7. Click **Download** to save the certificate to your computer.
8. Go back to Control Center and import the new Apple push certificate.
9. Click **Save**.

iOS MDM Identity and Profile Signing Certificate

The iOS MDM Identity and Profile Signing certificate is used by the Communication Server to sign identity certificates and configuration profiles sent to mobile devices.

Requirements:

- It must be an Intermediate or End-Entity certificate, signed either by your company or by an external Certificate Authority.
- Mobile clients must trust this certificate. For this, you must also add the iOS MDM Trust Chain.

To add or replace the iOS MDM Identity and Profile Signing 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**.

iOS MDM Trust Chain Certificate

The iOS MDM Trust Chain certificates are required on mobile devices to ensure they trust the Communication Server certificate and the iOS MDM Identity and Profile Signing certificate. The Communication Server sends this certificate to mobile devices during activation.

The iOS MDM Trust Chain must include all intermediate certificates up to the root certificate of your company or to the intermediate certificate issued by the external Certificate Authority.

To add or replace the iOS MDM Trust Chain certificates:

1. Go to the **Configuration** page and click the **Certificates** tab.
2. Click the certificate name.
3. Click the **Add** button next to the **Certificate** field and upload the certificate.
4. 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. 111).

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.

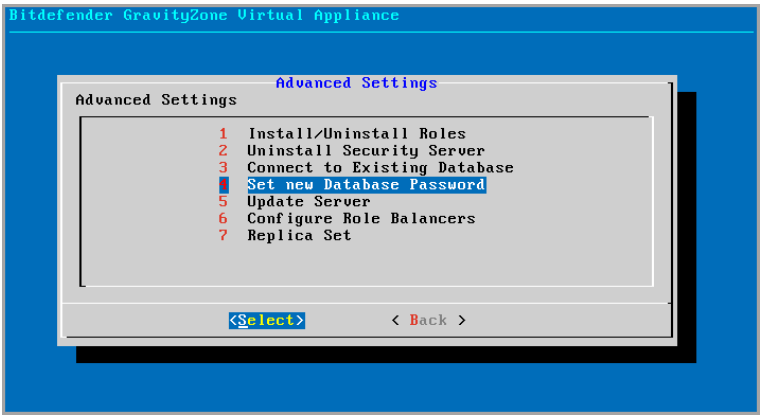
To install the Security Server from the appliance interface:

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 accesing **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 (Communication Server, Web Console).

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.

Each role can have only one 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. 107).
2. Configure the other appliances to connect to the first database instance. For more information, refer to "Connect to Existing Database" (p. 114).
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. 115).

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. 113)
- "Connect to Existing Database (Secure VPN Cluster)" (p. 115)

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**.

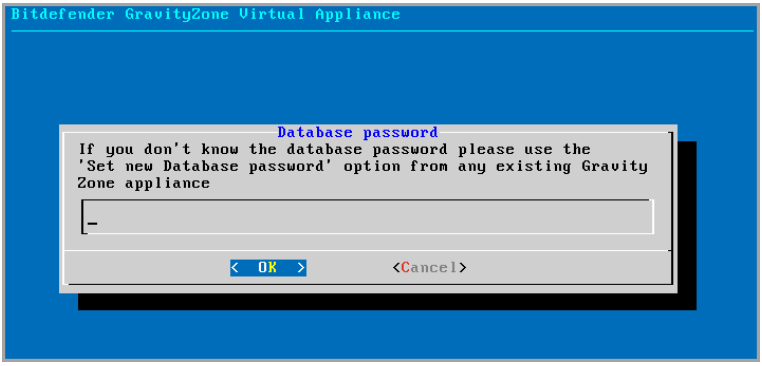
   Note
   Make sure you set a database password before accessing this option. If you don't know the database password, set a new one by accessing **Advanced Settings > Set a new database password** from the main menu.

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. 113).

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 continune.

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

The GravityZone security services are licensed and sold separately. Each GravityZone security service requires a valid basic license key. At least one valid license key must be provided for using GravityZone.

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 evaluation license keys from the registration email in Control Center.

Note
Control Center is provided for free with any GravityZone security service.

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

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

GravityZone license keys can be managed from the **Configuration > 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 **Configuration > 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 each security service you want to use.

For offline registration, you will also need the offline registration code associated to the license key.

You can enter several license keys for the same service, but only the last key that you enter will be active.

To license your GravityZone security services, to change an existing license key, or to enter a separate key for 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.

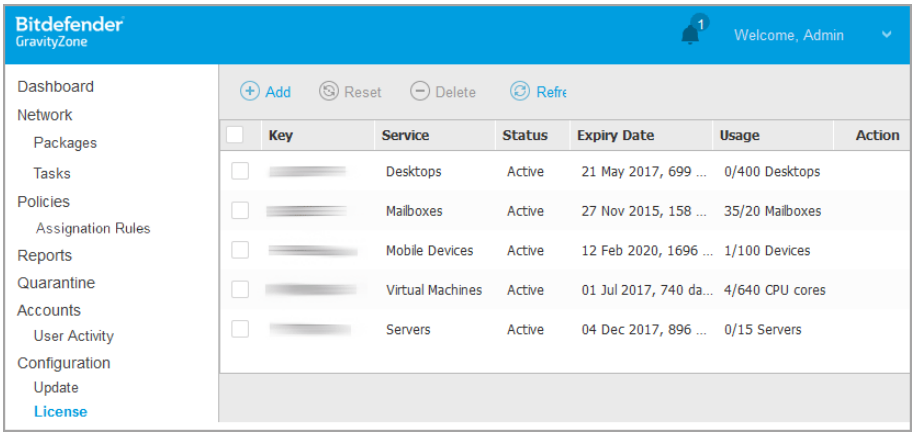
   If the license key is not valid, a validation error is displayed as tooltip over the **License key** field.
5. Click **Add**. The license key will be added to the **License** page, where you can check its details.
6. Click **Save** to apply the changes. Control Center restarts and you need to log in 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.



The License page

3. In the table, you can view details about the existing license keys.
   - License key
   - Security service the license key applies to
   - License key status

     Important
     Only one license key can be active at a time for a specific service.

   - 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 keys' usage count in the **License** page, under the **Usage** column.

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

5.2.5. Deleting License Keys

You can choose to delete invalid or expired license keys from the **License** page.

Warning
Deleting a license key will remove the corresponding security service from Control Center. You will not be able to install and manage protection offered by that service, on the endpoints in your network. Nevertheless, the endpoints remain protected as long as the license key is valid.
If you enter a new valid license key that includes the previously deleted service, it will re-enable all features of that service in Control Center.

To delete a license key:

1. Log in to Control Center using a company administrator account.
2. Go to the **Configuration > License** page.
3. Select the license key you want to remove and click the ⊖ **Delete** button at the upper side of the table.

5.3. Installing Endpoint Protection

Depending on the machines configuration and on the network environment, you can choose to install only the security agents or to also use a Security Server. In the latter case, you need to first install the Security Server and then the security agents.

It is recommended to use the Security Server in virtualized environments such as Nutanix, VMware or Citrix Xen, or if the machines have little hardware resources.

Important
Only Bitdefender Endpoint Security Tools and Bitdefender Tools support connection to a Security Server. For more information, refer to "GravityZone Architecture" (p. 10).

5.3.1. Installing Security Server

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

Security Server deployment is specific to the environment it is installed in. The installation procedures are described herein:

- Security Server for VMware NSX
- Security Server Multi-Platform or for VMware vShield
- Security Server for Amazon EC2
- Security Server for Microsoft Azure

Installing Security Server for VMware NSX

In VMware NSX environments, you must deploy the Bitdefender service in each cluster to be protected. The purpose-built appliance will automatically deploy on all hosts in the cluster. All virtual machines on a host are automatically connected via Guest Introspection to the Security Server instance installed on that host.

Security Server deployment is to be performed exclusively from the vSphere Web Client.

To install the Bitdefender service:

1. Log in to vSphere Web Client.
2. Go to **Network & Security > Installation** and click the **Service Deployments** tab.
3. Click the **New service deployment** button (the plus sign icon). The configuration window opens.
4. Select **Guest Introspection** and click **Next**.
5. Select the datacenter and the clusters on which to deploy the service, then click **Next**.
6. Select storage and management network, click **Next** and then **Finish**.
7. Repeat the steps from 3 to 6, this time choosing **Bitdefender** service.

   Before you proceed with installation, make sure that you have network connection between the selected network and GravityZone Control Center.

   Once the Bitdefender service is installed, it will automatically deploy the Security Server on all ESXi hosts in the selected clusters.

Warning
For the services to work properly, it is very important you install them in this order, first Guest Introspection and then Bitdefender, and not both at the same time.

Note
For more information on adding partner services to NSX, refer to VMware NSX Documentation Center.
If you choose **Specified on host** for storage and network management, check that Agent VM is set on hosts for both Guest Introspection and Bitdefender services.

Security Server has specific requirements that depend on the number of virtual machines it has to protect. To adjust the default hardware configuration of the Security Server:

1. Log in to VMware vSphere Web Client.
2. Go to **Hosts and Clusters**.
3. Select the cluster where Security Server is deployed and then select **Related Objects > Virtual Machines** tab.
4. Power off the **Bitdefender** appliance.
5. Right-click the appliance name and then choose **Edit Settings...** in the contextual menu.
6. In the **Virtual Hardware** tab, adjust the CPU and RAM values to fit your needs and then click **OK** to save the changes.
7. Power the appliance back on.

Note
To upgrade from VMware vShield to NSX, refer to this KB article.

Installing Security Server Multi-Platform or for VMware vShield

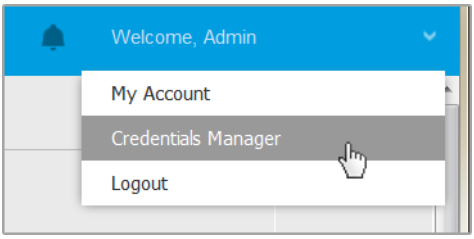
1. Connect to the virtualization platform
2. Install Security Server on hosts

Connecting to the Virtualization Platform

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

To specify the credentials to connect to the virtualization server systems:

1. Click your username in the upper-right corner of the page and choose **Credentials Manager**.



The Network > Packages menu

2. Go to the **Virtual Environment** tab.
3. Specify the necessary authentication credentials.
   a. Select a 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.

   b. Enter your username and password and a suggestive description.
   c. Click the ⊕ **Add** button. The new set of credentials is displayed in the table.

> **Note**
> If you have not specified your authentication credentials, you will be required to enter them when you try to browse the inventory of any vCenter 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.

Installing Security Server on Hosts

You must install Security Server on hosts as follows:

- In VMware environments with vShield Endpoint, you must install the purpose-built appliance on each host to be protected. All virtual machines on a host are automatically connected via vShield Endpoint to the Security Server instance installed on that host.

- In Citrix environments, you must install Security Server on each host you want to protect with HVI, via remote installation task.
- In Nutanix Prism Element environments, you must install Security Server on each host, via remote installation task.
- In all other environments, you must install Security Server on one or more hosts so as to accommodate the number of virtual machines to be protected. You must consider the number of protected virtual machines, resources available for Security Server on hosts, as well as network connectivity between Security Server and protected virtual machines. The security agent installed on virtual machines connects to Security Server over TCP/IP, using details configured at installation or via a policy.

If Control Center is integrated with vCenter Server, XenServer and Nutanix Prism Element, you can automatically deploy Security Server on hosts from Control Center. You can also download Security Server packages for standalone installation from Control Center.

Note
For VMware environments with vShield Endpoint, you can deploy Security Server on hosts exclusively via installation tasks.

Local Installation

In all virtualized environments that are not integrated with Control Center, you must install Security Server on hosts manually, using an installation package. The Security Server package is available for download from Control Center in several different formats, compatible with the main virtualization platforms.

Downloading Security Server Installation Packages

To download Security Server installation packages:

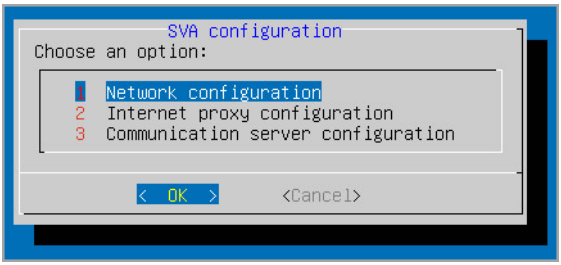
1. Go to the **Network > Packages** page.
2. Select the Default Security Server Package.
3. Click the **Download** button at the upper side of the table and choose the package type from the menu.
4. Save the selected package to the desired location.

Deploying Security Server Installation Packages

Once you have the installation package, deploy it to the host using your preferred virtual machine deployment tool.

After deployment, set up the Security Server as follows:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client). Alternatively, you can connect to the appliance via SSH.
2. Log in using the default credentials.
   - User name: `root`
   - Password: `sve`
3. Run the `sva-setup` command. You will access the appliance configuration interface.



Security Server configuration interface (main menu)

To navigate through menus and options, use the `Tab` and arrow keys. To select a specific option, press `Enter`.

4. Configure the network settings.

   The Security Server uses the TCP/IP protocol to communicate with the other GravityZone components. You can configure the appliance to automatically obtain network settings from the DHCP server or you can manually configure network settings, as described herein:

   a. From the main menu, select **Network configuration**.

   b. Select the network interface.

   c. Select the IP configuration mode:

- **DHCP**, if you want the Security Server to automatically obtain network settings from the DHCP server.
- **Static**, if a DHCP server is absent or an IP reservation for the appliance has been made on the DHCP server. In this case, you must manually configure the network settings.
  i. Enter the hostname, IP address, network mask, gateway and DNS servers in the corresponding fields.
  ii. Select **OK** to save the changes.

Note
If you are connected to the appliance via a SSH client, changing the network settings will immediately terminate your session.

5. Configure the proxy settings.

   If a proxy server is used within the network, you must provide its details so that the Security Server can communicate with GravityZone Control Center.

   Note
   Only proxies with basic authentication are supported.

   a. From the main menu, select **Internet proxy configuration**.
   b. Enter the hostname, username, password and the domain in the corresponding fields.
   c. Select **OK** to save the changes.
6. Configure the Communication Server address.
   a. From the main menu, select **Communication server configuration**.
   b. Enter the address of the Communication Server, including the port number 8443, using the following format:

      `https://Communication-Server-IP:8443`

      Alternatively, you can use the Communication Server hostname instead of the IP address.
   c. Select **OK** to save the changes.

Remote Installation

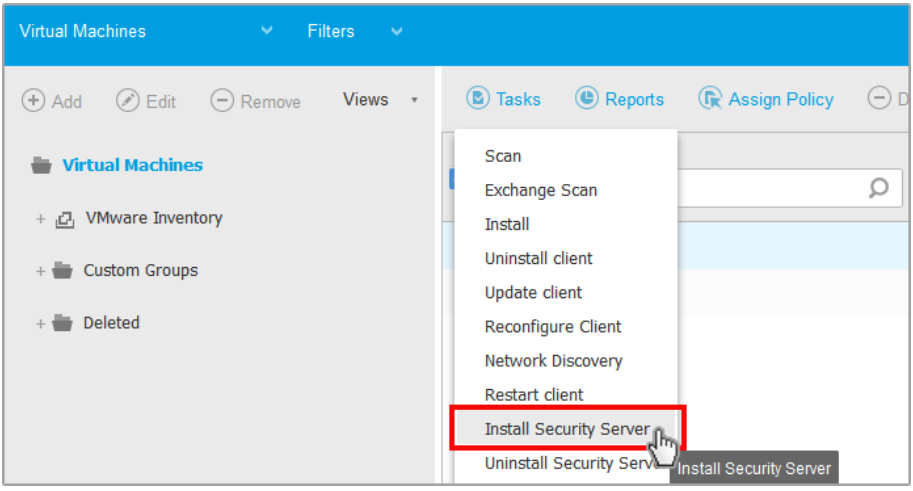
Control Center allows you to remotely install Security Server on visible hosts by using installation tasks.

To install Security Server remotely on one or several hosts:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Browse the VMware, Citrix or Nutanix inventory and select the check boxes corresponding to the desired hosts or containers (Nutanix Prism, vCenter Server, XenServer or datacenter). For a fast selection, you can directly select the root container (Nutanix Inventory, VMware Inventory or Citrix Inventory). You will be able to select hosts individually from the installation wizard.

   Note
   You cannot select hosts from different folders.

4. Click the **Tasks** button at the upper side of the table and choose **Install Security Server** from the menu. The **Security Server Installation** window is displayed.



Installing Security Server the from Tasks menu

5. Select the hosts on which you want to install the Security Server instances.
6. Choose the configuration settings you want to use.

   Important
   Using common settings while deploying multiple Security Server instances simultaneously requires the hosts to share the same storage, have their IP addresses assigned by a DHCP server and be part of the same network.

   When choosing to configure each Security Server differently, you will be able to define the settings that you want for each host at the next step of the wizard. The steps described hereinafter apply for the case when **Configure each Security Server** option is used.
7. Click **Next**.
8. Enter a suggestive name for the Security Server.
9. For VMware environments, select the container in which you want to include the Security Server from the **Deploy Container** menu.
10. Select the destination storage.
11. Choose the disk provisioning type. It is recommended to deploy the appliance using thick disk provisioning.

    Important
    If you use thin disk provisioning and the disk space in the datastore runs out, the Security Server will freeze and, consequently, the host will remain unprotected.

12. Configure the memory and CPU resource allocation based on the VM consolidation ratio on the host. Choose **Low**, **Medium** or **High** to load the recommended resource allocation settings or **Manual** to configure resource allocation manually.
13. You have to set an administrative password for the Security Server console. Setting an administrative password overrides the default root password ("sve").
14. Set the timezone of the appliance.
15. Select the network configuration type for the Bitdefender network. The IP address of the Security Server must not change in time, as it is used by Linux agents for communication.

If you choose DHCP, make sure to configure the DHCP server to reserve an IP address for the appliance.

If you choose static, you must enter the IP address, subnet mask, gateway and DNS information.

16. Select the vShield network and enter the vShield credentials. Default label for the vShield network is `vmservice-vshield-pg`.
17. Click **Save**.

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

Note
To upgrade from VMware vShield to NSX, refer to this KB article.

Important
Installing Security Server on Nutanix through remote task may fail when the Prism Element cluster is registered to Prism Central or because of another reason. In these situations, it is recommended to perform a manual deployment of Security Server. For more details, refer to this KB article.

Installing Security Server for Amazon EC2

You can use Security Server to protect your Amazon EC2 instances as follows:

- Configure the Security Server installed in your local network to communicate with the Amazon EC2 instances. Therefore, you will be able to use your local resources, either physical or virtual, to protect also the Amazon EC2 inventory.
- Install one or several Security Server instances in your Amazon EC2 environment, according to your needs. In this case, follow the procedure described in this KB article.

  Important
  - For the communication between your EC2 machines and the Security Server instances installed in your Amazon EC2 inventory to work, you need to properly configure your Amazon VPC (Virtual Private Cloud) and Amazon VPN connections. For more information, refer to Amazon VPC documentation.
  - We recommend installing the Security Server in the same Amazon EC2 region with the instances you want to protect.

The default scan mode for EC2 instances is Local Scan (security content is stored on the installed security agent, and the scan is run locally on the machine). If you want to scan your EC2 instances with a Security Server, you need to configure the security agent's installation package and the applied policy accordingly.

Installing Security Server for Microsoft Azure

You can use Security Server to protect your Microsoft Azure virtual machines as follows:

- Configure the Security Server installed in your local network to communicate with the Microsoft Azure virtual machines. Therefore, you will be able to use your local resources, either physical or virtual, to protect also the Microsoft Azure inventory.
- Install one or several Security Server instances in your Microsoft Azure environment, according to your needs. In this case, follow the procedure described in this KB article.

  Important

  – For the communication between your Microsoft Azure virtual machines and the Security Server instances installed in your Microsoft Azure inventory to work, you need to properly configure your virtual network/subnet. For details, refer to Microsoft Azure Virtual Network Documentation.

  – We recommend installing the Security Server in the same Microsoft Azure region with the virtual machines you want to protect.

The default scan mode for Microsoft Azure virtual machines is Local Scan (security content is stored on the installed security agent, and the scan is run locally on the machine). If you want to scan your Microsoft Azure virtual machines with a Security Server, you need to configure the security agent's installation package and the applied policy accordingly.

5.3.2. 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.

To learn about the available security agents, refer to "Security Agents" (p. 12).

On Windows and Linux machines, the security agent can have two roles and you can install it as follows:

1. As a simple security agent for your endpoints.
2. As a Relay, acting as a security agent and also as a communication, proxy and update server for other endpoints in the network.

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.

If enabled by the network administrator via installation package and security policy, the security agent can also run in Power User mode on Windows endpoints, letting the endpoint user view and modify policy settings. Nevertheless, the Control Center administrator can always control which policy settings apply, overriding the Power User mode.

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.

On Mac, the display language of the user interface is set at installation time based on the language of the endpoint operating system. On Linux, the security agent does not have a localized user interface.

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. 134).

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. Uninstall (not just disable) any existing antimalware or Internet security software from target endpoints. Running the security agent simultaneously with other security software on an endpoint may affect their operation and cause major problems with the system.

   Many of the incompatible security programs are automatically detected and removed at installation time.

   To learn more and to check the list of the security software detected by Bitdefender Endpoint Security Tools for current Windows operating systems, refer to this KB article.

   Important
   If you want to deploy the security agent on a computer with Bitdefender Antivirus for Mac 5.X, you first must remove the latter manually. For the guiding steps, refer to this KB article.

3. 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.
4. Endpoints must have network connectivity to the GravityZone appliance.
5. 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.
6. When deploying the agent through a Linux Relay, the following additional conditions must be met:

   - The Relay endpoint must have installed the Samba package (`smbclient`) version 4.1.0 or above and the `net` binary/command to deploy Windows agents.

     Note
     The `net` binary/command is usually delivered with the samba-client and / or samba-common packages. On some Linux distributions (such as CentOS 7.4), the `net` command is only being installed when installing the full Samba suite (Common + Client + Server). Make sure that your Relay endpoint has the `net` command available.

- Target Windows endpoints must have Administrative Share and Network Share enabled.
- Target Linux and Mac endpoints must have SSH enabled.

7. Starting with macOS High Sierra (10.13), after installing Endpoint Security for Mac manually or remotely, users are prompted to approve Bitdefender extensions on their computers. Until the users approve the Bitdefender extensions, some Endpoint Security for Mac features will not work. For details, refer to this article.

   With macOS Big Sur (11.x), Endpoint Security for Mac requires additional user approvals following the changes made by Apple to the operating system. For details, refer to this article.

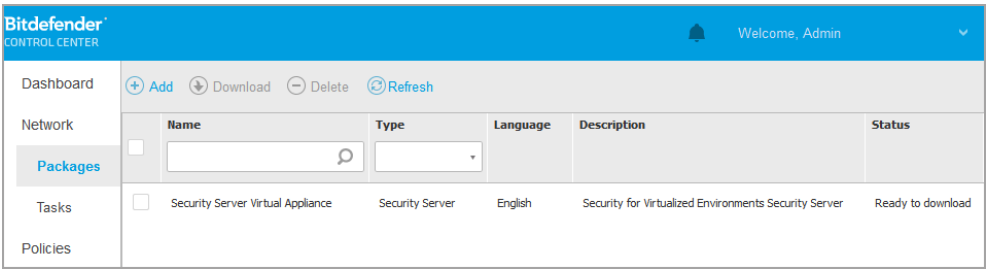
   To eliminate user intervention, you can pre-approve the Bitdefender extensions by whitelisting them using a Mobile Device Management tool like Jamf. For details, refer to this article.
8. When deploying the agent in an Amazon EC2 inventory, configure the security groups associated with the instances you want to protect in the Amazon EC2 **Dashboard > Network & Security** as follows:
   - For remote installation, allow SSH* access from the EC2 instance.
   - For local installation, allow SSH* and RDP (Remote Desktop Protocol) access from the computer you connect from.

   * For remote installation on Linux instances you must allow SSH login using username and password.
9. When deploying the agent in a Microsoft Azure inventory:
   - The target virtual machine must be in the same virtual network with the GravityZone appliance.
   - The target virtual machine must be in the same virtual network with a Relay, which communicates with the GravityZone appliance when the latter is in another network.

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. 151).

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

1. 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.

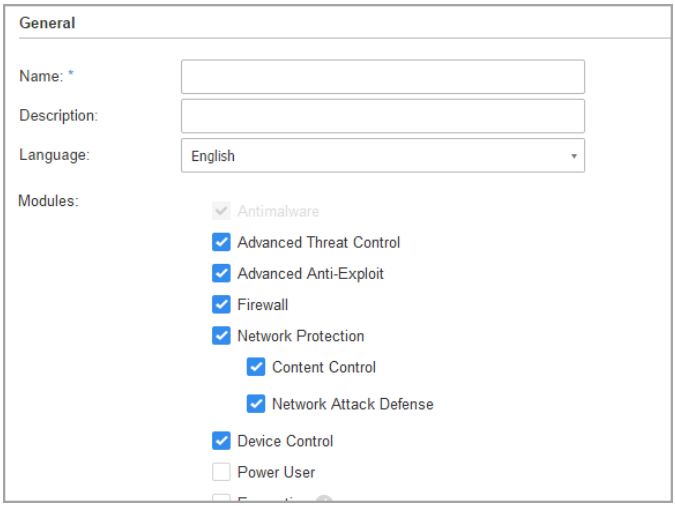
2. Download the installation package on the target endpoint.

   You can alternately send the installation package download links by email to several users in your network.
3. 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.



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.

   Note
   This option is avaiable only for Windows operating systems.

6. Select the protection modules you want to install.

   Note
   Only the supported modules for each operating system will be installed. For more information, refer to "Security Agents" (p. 12).

7. Select the target endpoint role:
   - **Relay**, to create the package for an endpoint with Relay role. For more information, refer to "Relay" (p. 14)
   - **Patch Management Cache Server**, to make the Relay an internal server for distributing software patches. This role is displayed when Relay role is selected. For more information, refer to "Patch Caching Server" (p. 14)

- **Exchange Protection**, to install the protection modules for Microsoft Exchange Servers, including antimalware, antispam, content and attachment filtering for the Exchange email traffic and on-demand antimalware scanning of the Exchange databases. For more information, refer to "Installing Exchange Protection" (p. 162).

8. **Remove Competitors**. It is recommended to keep this check box selected to automatically remove any incompatible security software while the Bitdefender agent installs on endpoint. By deselecting this option, Bitdefender agent will install next to the existing security solution. You can manually remove the previously installed security solution later, at your own risk.

   Important
   Running the Bitdefender agent simultaneously with other security software on an endpoint may affect their operation and cause major problems with the system.

9. **Scan Mode**. Choose the scanning technology that best suits your network environment and your endpoints' resources. You can define the scan mode by choosing one of the following types:

   - **Automatic**. In this case, the security agent will automatically detect the endpoint's configuration and will adapt the scanning technology accordingly:
     - Central Scan in Public or Private Cloud (with Security Server) with fallback on Hybrid Scan (Light Engines), for physical computers with low hardware performance and for virtual machines. This case requires at least one Security Server deployed in the network.
     - Local Scan (with Full Engines) for physical computers with high hardware performance.
     - Local scan for EC2 instances and Microsoft Azure virtual machines.

     Note
     Low performance computers are considered to have the CPU frequency less than 1.5 GHz, or RAM memory less than 1 GB.

   - **Custom**. In this case, you can configure the scan mode by choosing between several scanning technologies for physical and virtual machines:

- Central Scan in Public or Private Cloud (with Security Server), which can fallback* on Local Scan (with Full Engines) or on Hybrid Scan (with Light Engines)
- Hybrid Scan (with Light Engines)
- Local Scan (with Full Engines)

The default scan mode for EC2 instances is Local Scan (security content is stored on the installed security agent, and the scan is run locally on the machine). If you want to scan your EC2 instances with a Security Server, you need to configure the security agent's installation package and the applied policy accordingly.

The default scan mode for Microsoft Azure virtual machines is Local Scan (security content is stored on the installed security agent, and the scan is run locally on the machine). If you want to scan your Microsoft Azure virtual machines with a Security Server, you need to configure the security agent's installation package and the applied policy accordingly.

* When using a dual engines scanning, if the first engine is unavailable, the fallback engine will be used. Resource consumption and network utilization will be based on used engines.

For more information regarding available scanning technologies, refer to "Scanning Engines" (p. 3)

10. **Deploy endpoint with vShield when a VMware environment integrated with vShield is detected**. This option can be used when the installation package is deployed on a virtual machine from a VMware environment integrated with vShield. In this case, VMware vShield Endpoint will be installed on the target machine instead of Bitdefender security agent.

    Important
    This option is only for remote deployments, not local installations. When installing locally in VMware environment integrated with vShield, you have the option to download the vShield-Integrated package.

11. When customizing the scan engines using Public or Private Cloud (Security Server) scanning, you are required to select the locally installed Security Servers you want to use and to configure their priority under **Security Server Assignment** section:

a. Click the Security Server list in the table header. The list of detected Security Servers is displayed.

b. Select an entity.

c. Click the ⊕ **Add** button from the **Actions** column header.

   The Security Server is added to the list.

d. Follow the same steps to add several security servers, if available. In this case, you can configure their priority using the ⌃ up and ⌄ down arrows available at the right side of each entity. When the first Security Server is unavailable, the next one will be used and so on.

e. To delete one entity from the list, click the corresponding ⊗ **Delete** button at the upper side of the table.

You can choose to encrypt the connection to Security Server by selecting the **Use SSL** option.

12. **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.

Note
For information on how these settings interfere with HIPAA regulations, refer to "Bitdefender GravityZone and HIPAA" (p. 179).

13. Select **Scan before installation** if you want to make sure the machines are clean before installing the client on them. An in-the cloud quick scan will be performed on the target machines before starting the installation.

> **Note**
> For information on how this setting interferes with HIPAA regulations, refer to "Bitdefender GravityZone and HIPAA" (p. 179).

14. Bitdefender Endpoint Security Tools is installed in the default installation directory. Select **Use custom installation path** if you want to install the Bitdefender agent in a different location. If the specified folder does not exist, it will be created during the installation.

    - On Windows, the default path is `C:\Program Files\`. To install Bitdefender Endpoint Security Tools in a custom location, use Windows conventions when entering the path. For example, `D:\folder`.
    - On Linux, Bitdefender Endpoint Security Tools is installed by default in the `/opt` folder. To install the Bitdefender agent in a custom location, use Linux conventions when entering the path. For example, `/folder`.

      Bitdefender Endpoint Security Tools does not support installation to the following custom paths:
      - Any path that does not begin with slash (/). The only exception is the Windows location `%PROGRAMFILES%`, which the security agent interprets as the Linux default folder `/opt`.
      - Any path that is in `/tmp` or `/proc`.
      - Any path that contains the following special characters: `$, !, *, ?, ", ', `, \, (,), [,], {, }`.
      - The `systemd` specifier (%).

      On Linux, installation to custom path requires glibc 2.21 or higher.

> **Important**
> When using custom path, make sure you have the right installation package for each operating system.

15. 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.

16. 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.

17. 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

18. 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
     - **Linux OS:** 32-bit and 64-bit systems
     - **macOS:** 64-bit Intel and Apple M1 systems

       After downloading the macOS kit (Apple M1), you must publish it in the **Update > Components** page of GravityZone Control Center, otherwise the security agent installation will fail.

     Make sure to use the correct version for the system you install on.
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.
  4. Follow the on-screen instructions.

  Note
  On macOS, after installing Endpoint Security for Mac, users are prompted to approve Bitdefender kernel extensions on their computers. Until the users approve the Bitdefender kernel extensions, some features of the security agent will not work. For details, refer to this KB article.

- On Linux operating systems:

1. Connect and log in to Control Center.
2. Download or copy the installation file to the target endpoint.
3. If you have downloaded the full kit, extract the files from the archive.
4. Gain root privileges by running the `sudo su` command.
5. Change permissions to the installation file so that you can execute it:

   ```
   # chmod +x installer
   ```

6. Run the installation file:

   ```
   # ./installer
   ```

7. To check that the agent has been installed on the endpoint, run this command:

   ```
   $ service bd status
   ```

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

Important
If using VMware Horizon View Persona Management, it is recommended to configure Active Directory Group Policy to exclude the following Bitdefender processes (without the full path):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

These exclusions must apply as long as the security agent runs on endpoint. For details, refer to this VMware Horizon documentation page.

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. 151).

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.
  - Disable Windows Firewall or configure it to allow traffic through File and Printer Sharing protocol.

> **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. 28).

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

Running Remote Installation Tasks

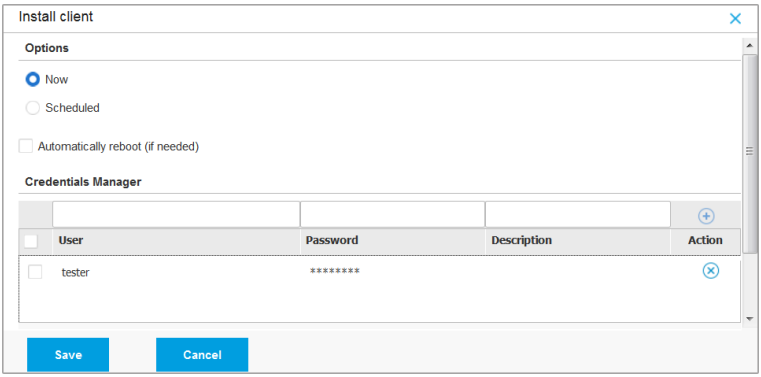
To run a remote installation task:

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.



Installing Bitdefender Endpoint Security Tools from the Tasks menu

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:

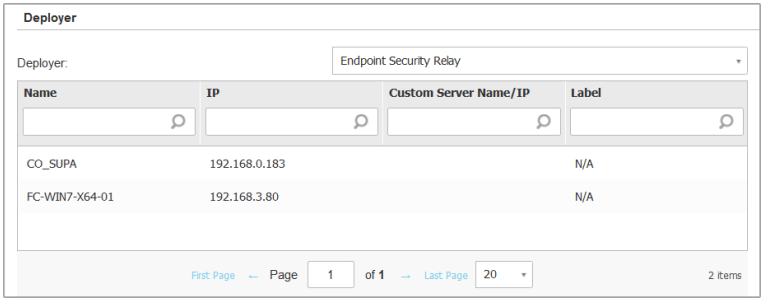
    - **GravityZone Appliance**, when endpoints connect directly to GravityZone Appliance.

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.



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. 134).

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.

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 -xzvf 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 smbd start
   ```

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

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.

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. 118).

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:

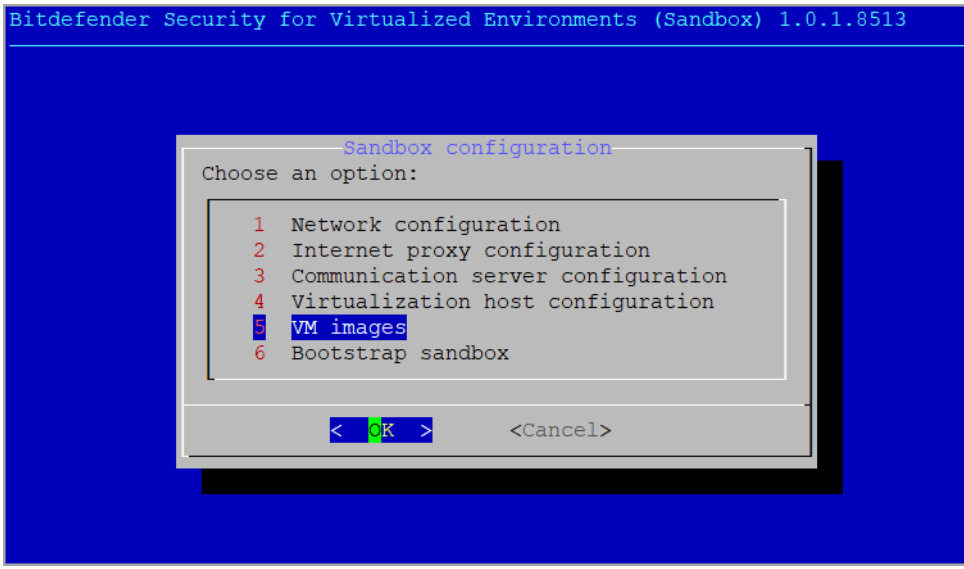
```
/opt/bitdefender/bin/sandbox-setup
```

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.



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`.

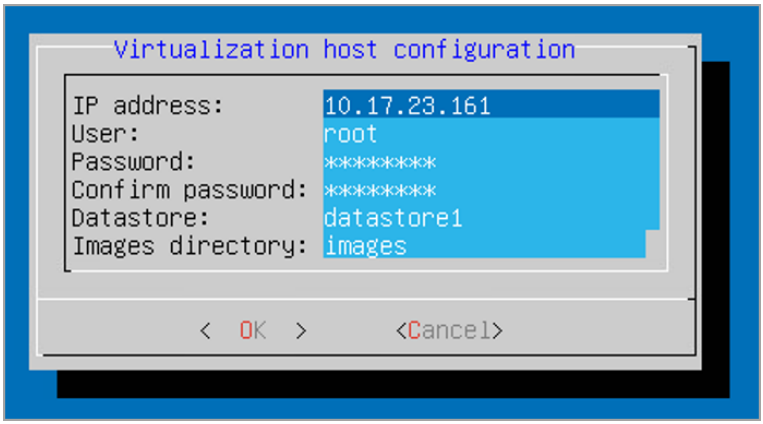
> **Note**
> As soon as IP address or hostname is specified, and configuration is saved, the Sandbox Analyzer instance will become visible in GravityZone Control Center, in the **Sandbox Analyzer > Infrastructure** page.

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. 159).

   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. 160)

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.

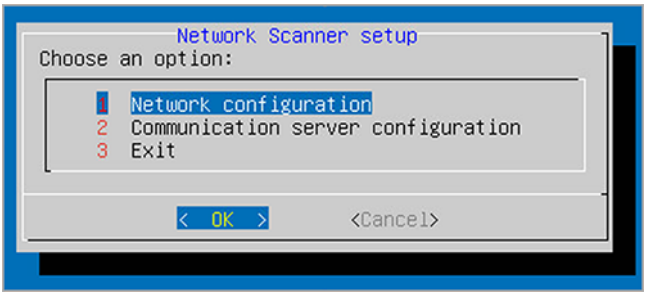
5.4.3. Deploy Network Security Virtual Appliance

This section describes how to deploy Network Security Virtual Appliance, a Sandbox Analyzer component that captures network traffic and submits suspicious samples for behavioral analysis.

To deploy the Network Security Virtual Appliance:

1. Log in to the GravityZone Control Center.
2. Go to the **Network > Packages** page.
3. Select the **Network Security Virtual Appliance** check box from the table.
4. Click the **Download** button at the upper-left side of the page and select the **(VMware OVA)** option.
5. Use your virtualization management tool (for example, vSphere Client) to import the downloaded OVA file into your virtual environment.
6. In the deployment wizard, select the network interface card (NIC) used for communication with GravityZone and the NIC used for capturing traffic.
7. Power on the appliance.
8. From your virtualization management tool, access the console interface of GravityZone SVE SVA Network Security Virtual Appliance.
9. When prompted for credentials, use `root` for username and `sve` for password.
10. Access the configuration menu by running the following command:

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



Network Security appliance console

11. Go to **Communication server configuration** menu option.
12. Specify the IP address or hostname, and the port of a GravityZone Communication Server.

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

Configure Network Sensor to Detonate pcap Files

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

To detonate content from pcap files:

1. Log into Network Security Virtual Appliance.
2. When prompted for credentials, use `root` for username and `sve` for password.
3. Run the following command:

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

   In the above command, `<local pcap path>` represents the location where the pcap file is uploaded in the Network Security Virtual Appliance.

For other details about using the network sensor, refer to the **Policies > Sandbox Analyzer** chapter from the GravityZone Administrator's Guide.

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. 117).

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. Installing Exchange Protection

Security for Exchange automatically integrates with the Exchange Servers, depending on the server role. For each role only the compatible features are installed, as described herein:

Features	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Edge	Mailbox	Edge	Hub	Mailbox
Transport Level					
Antimalware Filtering	x	x	x	x	
Antispam Filtering	x	x	x	x	
Content Filtering	x	x	x	x	
Attachment Filtering	x	x	x	x	
Exchange Store					
On-demand antimalware scanning		x			x

5.6.1. Preparing for Installation

Before installing Security for Exchange, make sure all requirements are met, otherwise Bitdefender Endpoint Security Tools might be installed without the Exchange Protection module.

For the Exchange Protection module to run smoothly and to prevent conflicts and unwanted results, remove any antimalware and email filtering agents.

Bitdefender Endpoint Security Tools automatically detects and removes most of the antimalware products and disables the antimalware agent built in Exchange Server since the 2013 version. For details regarding the detected security software list, refer to this KB article.

You can manually re-enable the built-in Exchange antimalware agent at any time, nevertheless it is not recommended to do so.

5.6.2. Installing Protection on Exchange Servers

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

You have several options to deploy Bitdefender Endpoint Security Tools on Exchange Servers:

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

For detailed installation steps, refer to “Installing Security Agents” (p. 130).

5.7. Installing HVI

To be able to use HVI on virtual machines from your Xen hosts, you have to perform these steps:

1. Check the installation prerequisites
2. Install Security Server
3. Install HVI Supplemental Pack

Prerequisites

- XenServer is integrated with GravityZone.
- XenCenter is installed on your machine.

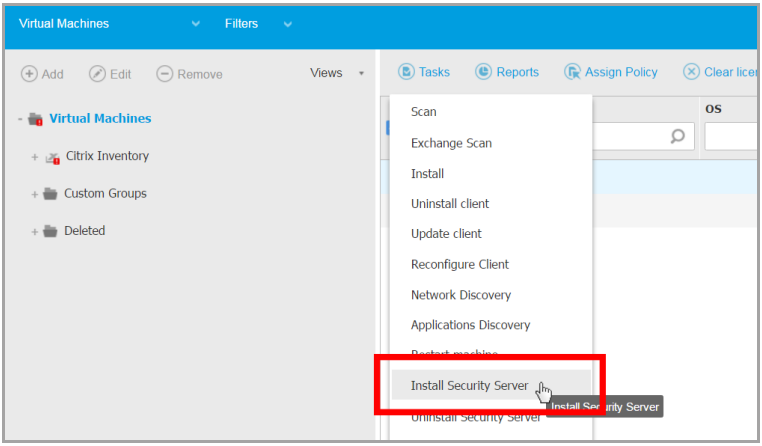
Installing Security Server

To install Security Server on one or several hosts:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Browse the Citrix inventory and select the check boxes corresponding to the desired hosts. For a fast selection, you can directly select the root container (Citrix Inventory). You will be able to select hosts individually from the installation wizard.

   Note
   You cannot select hosts from different folders.

4. Click the **Tasks** button at the upper side of the table and choose **Install Security Server** from the menu. The **Security Server Installation** window is displayed.



Installing Security Server

5. Select the hosts on which you want to install the Security Server instances.
6. Choose the configuration settings you want to use.

   Important
   Using common settings while deploying multiple Security Server instances simultaneously requires the hosts to share the same storage, have their IP addresses assigned by a DHCP server and be part of the same network.

   When choosing to configure each Security Server differently, you will be able to define the settings that you want for each host at the next step of the wizard. The steps described hereinafter apply for the case when **Configure each Security Server** option is used.
7. Click **Next**.

   Note
   Depending on the selection previously made, some options described herein may not apply to your situation.

8. Enter a suggestive name for the Security Server.
9. Select the container in which you want to include the Security Server from the **Container** menu.
10. Select the destination storage.
11. Choose the disk provisioning type. It is recommended to deploy the appliance using thick disk provisioning.

    Important
    If you use thin disk provisioning and the disk space in the datastore runs out, the Security Server will freeze and, consequently, the host will remain unprotected.

12. Configure the memory and CPU resource allocation based on the VM consolidation ratio on the host. Choose **Low**, **Medium** or **High** to load the recommended resource allocation settings or **Manual** to configure resource allocation manually.
13. Set the timezone of the appliance.
14. Set an administrative password for the Security Server console. Setting an administrative password overrides the default root password ("sve").

15. Select the network configuration type for the Bitdefender network. The IP address of the Security Server must not change in time, as it is used by Linux agents for communication.

    If you choose DHCP, make sure to configure the DHCP server to reserve an IP address for the appliance.

    If you choose static, you must enter the IP address, subnet mask, gateway and DNS information.

16. Click **Save**.

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

Installing HVI Supplemental Pack

1. Go to the **Configuration > Update** page.
2. Select the HVI Supplemental Pack in the **Components** list and click the **Download** button at the upper side of the table.
3. Go to the **Network** page and select **Virtual Machines** from the views selector.
4. Select **Server** from the **Views** menu in the left pane.
5. Select one or more Xen hosts from network inventory. You can easily view the available hosts by selecting the option **Type > Hosts** from the **Filters** menu.
6. Click the **Tasks** button in the right pane and choose **Install HVI Supplemental Pack**. The installation window opens.
7. Schedule when the installation task should run. You can choose to run the task immediately after saving the task, or at a specific time. In case installation cannot complete at the specified time, the task automatically repeats according to the recurrence settings. For example, if you select more hosts and one host is not available when the pack is scheduled to install, the task will run again at the specified time.
8. The host must restart to apply the changes and complete installation. If you want the host to restart unattended, select **Automatically reboot host**.
9. Click **Save**. A confirmation message will appear.

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

5.8. Installing Storage Protection

Security for Storage is a Bitdefender service designed to protect Network-Attached Storage (NAS) devices and file-sharing systems compliant with Internet Content Adaptation Protocol (ICAP). For supported file-sharing systems, refer to "Storage Protection" (p. 54).

To use Security for Storage with your GravityZone solution:

1. Install and configure at least two Security Servers in your environment to act as ICAP servers. Bitdefender Security Servers analyze files, send verdicts to the storage systems and take appropriate actions if necessary. In case of overloading, the first Security Server redirects the surplus of data to the second one.

   Note
   As best practices, install dedicated Security Servers for storage protection, separately from the Security Servers used for other roles, such as antimalware scanning.

   For details about the Security Server installing procedure, refer to the **Installing Security Server** section from this guide.

2. Configure the **Storage Protection** module from the GravityZone policy settings.

   For details, refer to **Security Policies > Computer and Virtual Machines Policies > Storage Protection** chapter from the GravityZone Administrator's Guide.

For details about configuring and managing ICAP servers on a certain NAS device or file-sharing system, refer to the documentation for that specific platform.

5.9. Installing Mobile Devices Protection

Security for Mobile is a mobile device management solution designed for iPhone, iPad and Android devices. For a complete list of supported operating system versions, check the system requirements.

To manage Security for Mobile from Control Center, you have to add mobile devices to Active Directory or custom users, then install the GravityZone Mobile Client application on devices. After setting up the service, you can run administrative tasks on mobile devices.

Before you start, make sure to configure a public (external) address for the Communication Server.

To install Security for Mobile:

1. If you do not have integration with Active Directory, you must create users for mobile device owners.
2. Add devices to users.
3. Install GravityZone Mobile Client on devices and activate it.

5.9.1. Configure External Address for Communication Server

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.

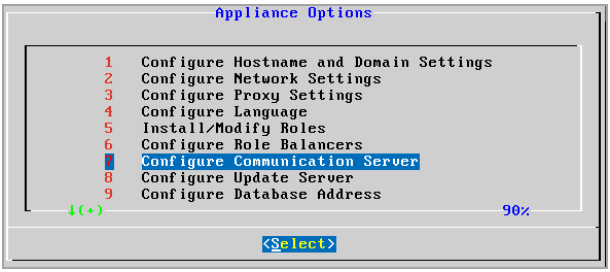
To be able to manage mobile devices over the Internet, no matter where they are located, you must configure the Communication Server with a publicly reachable address.

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.

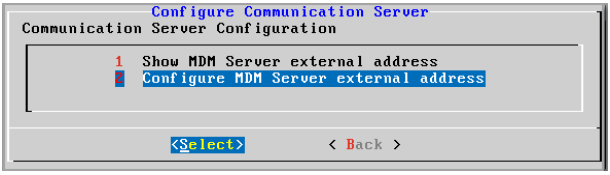
In both cases, you must configure the Communication Server with the external address to be used for mobile device management:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Configure Communication Server**.



Application Options window

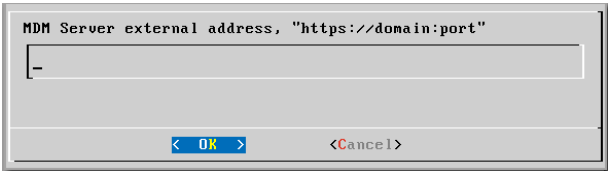
3. Select **Configure MDM Server external address**.



Configure Communication Server window

4. Enter the external address.

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



MDM Server external address input window

- 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.

5.9.2. Create and Organize Custom Users

In non-Active Directory situations, you must first create custom users in order to have a mean to identify the owners of mobile devices. Specified mobile device users are not linked in any way with Active Directory or with other users defined in Control Center.

Creating Custom Users

To create a custom user:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. In the left-side pane, select **Custom Groups**.
4. Click the **Add User** icon on the action toolbar. A configuration window will appear.
5. Specify the required user details:
   - A suggestive username (for example, the user's full name)
   - User's email address

   Important
   - Make sure to provide a valid email address. The user will be sent the installation instructions by email when you add a device.
   - Each email address can only be associated with one user.

6. Click **OK**.

Organizing Custom Users

To organize custom users:

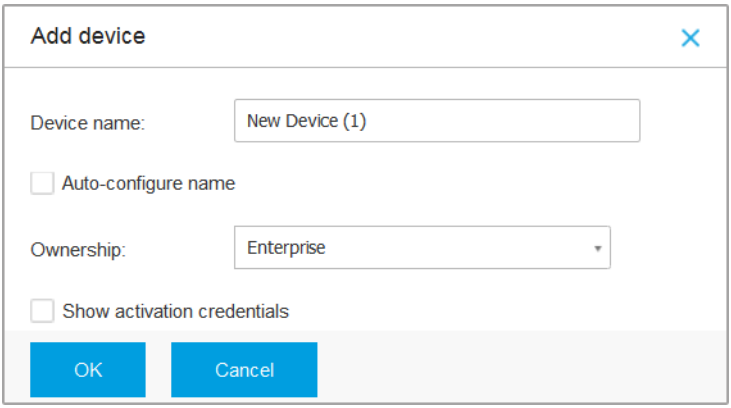
1. Create custom groups.
   a. Select **Custom Groups** in the left-side pane and click the **Add** icon on the action toolbar (above the pane).
   b. Enter a suggestive name for the group and click **OK**. The new group is displayed under **Custom Groups**.

2. Move custom users into appropriate custom groups.
   a. Select users in the right-side pane.
   b. Drag and drop the selection over the desired group in the left-side pane.

5.9.3. Add Devices to Users

To add a device to a user:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Search the user in the Active Directory folders or in Custom Groups.
4. Click the ⊕ **Add Device** icon on the upper side of the network table. A configuration window will appear.



Add mobile device to a user

5. Enter a suggestive name for the device.
6. Use the **Auto-configure name** option if you want the device name to be automatically generated. When added, the device has a generic name. Once the device is activated, it is automatically renamed with the corresponding manufacturer and model information.
7. Select the device ownership type (Enterprise or Personal).

8. Select the **Show activation credentials** option after clicking the **OK** button if you are going to install the GravityZone Mobile Client on the user's device.
9. Click **OK**. The user is immediately sent an email with the installation instructions and the activation details to be configured on the device. The activation details include the activation token and the communication server address (and corresponding QR code).

Note

- You can view the activation details of a device at any time by clicking its name in Control Center.
- You can also add mobile devices to a selection of users and groups. In this case, the configuration window will allow defining the devices ownership only. Mobile devices created by multiple selection will be given by default a generic name. As soon as a device is enrolled, its name will automatically change, including the corresponding manufacturer and model labels.

5.9.4. Install GravityZone Mobile Client on Devices

The GravityZone Mobile Client application is exclusively distributed via Apple App Store and Google Play.

To install GravityZone Mobile Client on a device:

1. Search for the application on the official app store.
   - Google Play link
   - Apple App Store link
2. Download and install the application on the device.
3. Start the application and make the required configuration:
   a. On Android devices, tap **Activate** to enable GravityZone Mobile Client as device administrator. Read carefully the provided information.

Note

- Lock task for Android devices (7.0 or above) will enforce the password set in your GravityZone console only if there is no lock protection configured on the device. Otherwise, the existing screen lock options such as Pattern, PIN, Password, Fingerprint or Smart Lock will be used to protect the device.
- Unlock task is no longer available for Android devices (7.0 or above).

- Due to technical limitations, Lock and Wipe tasks are unavailable on Android 11.

b. Enter the activation token and the communication server address or, alternatively, scan the QR code received by email.

c. Tap **Trust** when prompted to accept the Communication Server's certificate. This way, GravityZone Mobile Client validates the Communication Server and will accept only messages from it, preventing man-in-the-middle attacks.

d. Tap **Activate**.

e. On iOS devices, you are prompted to install the MDM profile. If your device is password protected, you will be asked to provide it. Also, you have to allow GravityZone to access your device settings, otherwise the installation process returns to the previous step. Follow the on-screen instructions to complete profile installation.

Note
Users need to allow on devices background location, not only while using the app, for the Locate feature to work properly.

5.10. Installing Report Builder

Report Builder allow you to create and manage queries and detailed query-based reports in GravityZone.

Report Builder consists of two roles, Database and Processors, that come with the GravityZone Virtual Appliance and must be installed separately from each other and from other GravityZone roles. After installing Report Builder, your GravityZone environment should run at least three instances of the GravityZone Virtual Appliance, as follows:

- One or more instances of GravityZone Appliance Virtual Appliance having all the roles installed, except for Report Builder Database and Report Builder Processors.
- One instance of GravityZone Virtual Appliance having the Report Builder Database role installed.
- One instance of GravityZone Virtual Appliance having the Report Builder Processors role installed.

For a smooth installation, first make sure your virtual environment meets the hardware and software requirements. Then, you must have at hand:

- GravityZone Virtual Appliance image, which you will use to install the Report Builder Database and Report Builder Processors roles.
- DNS name or IP address of the GravityZone Virtual Appliance that has the GravityZone Database role installed.
- Username and password of a domain administrator.
- Password for the GravityZone database. If you forget it, you can create another one in the console interface of the GravityZone appliance.

The Report Builder installation implies two stages:

- Installing Report Builder Database
- Installing Report Builder Processors

As best practice, first install GravityZone and set up Control Center (if needed), then update GravityZone, deploy protection on endpoints, and in the end install the Report Builder roles.

Important
It is rewuired to first install the Report Builder Database role, then the Report Builder Processors role.

5.10.1. Installing Report Builder Database

Report Builder Database is the first role you must install. To install this role:

1. Import the GravityZone Virtual Appliance in your virtualized environment.
2. Power on the appliance.
3. From your virtualization management tool, access the console interface of the GravityZone Virtual Appliance.
4. Configure the password for the built-in `bdadmin` system administrator.
5. Login with the password you have set to 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.

   Initially, the appliance interface is in English.

   To change the interface language:

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

> **Note**
> You may need to scroll down to view your language.

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

6. Go to **Advanced Settings** and select **Connect to Existing Database**.
7. Enter the IP address and the password of the GravityZone database.
8. From the **Advanced Settings** menu, select **Install/Uninstall Roles**.
9. Go to **Add or remove roles** and choose **Report Builder Database**. Press the `Space` bar to select to install this role, then `Enter` to proceed. Press again `Enter` to confirm and wait for installation to complete.

> **Note**
> Report Builder Database installs and runs only as a standalone instance. Replica Set backups are not supported.

5.10.2. Installing Report Builder Processors

Report Builder Processors is the second role you must install. To install this role:

1. Import the GravityZone Virtual Appliance in your virtualized environment.
2. Power on the appliance.
3. From your virtualization management tool, access the interface of the GravityZone Virtual Appliance.
4. Configure the password for the built-in `bdadmin` system administrator.
5. Login with the password you have set. 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.

   Initially, the appliance interface is in English.

   To change the interface language:
   a. Select **Configure Language** from the main menu.

b. Select the language from the available options. A confirmation message will appear.

> **Note**
> You may need to scroll down to view your language.

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

6. Go to **Advanced Settings** and select **Connect to Existing Database**.
7. Enter the IP address and the password of the GravityZone database.
8. From the **Advanced Settings** menu, select **Install/Uninstall Roles**.
9. Go to **Add or remove roles** and choose **Report Builder Processors**. Press the `Space` bar to select to install this role, then `Enter` to proceed. Press again `Enter` to confirm and wait for installation to complete.

> **Note**
> Report Builder Processors installs and runs only as a standalone instance.

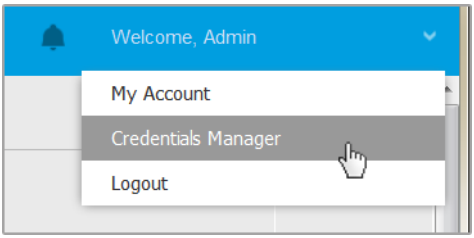
After installing Report Builder, the new menu option **Queries** is displayed under the **Reports** section in Control Center.

The Report Builder Database and Processors roles are displayed in the **Infrastructure** section of the **Configuration > Update** page, along with the other GravityZone roles.

5.11. 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

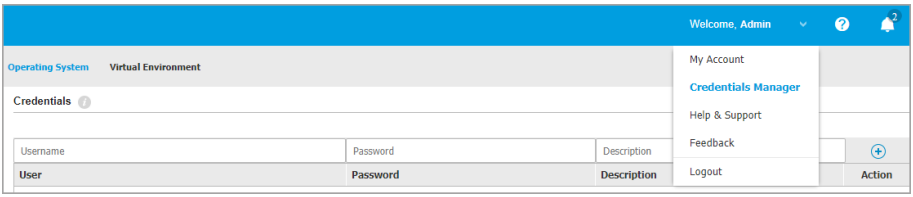
The **Credentials Manager** window contains two tabs:

- Operating System
- Virtual Environment

5.11.1. 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.

5.11.2. 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.

5.11.3. 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.

5.12. Bitdefender GravityZone and HIPAA

One of the Bitdefender's top priorities is to ensure that customers' personal data is safely processed and stored. In this regard, Bitdefender has in place specific privacy policies for home and business solutions. Bitdefender's privacy policies may be found here: https://www.bitdefender.com/site/view/legal-privacy.html.

As part of protecting customers' personal data, Bitdefender aims to help its customers, including health care professionals, comply with regulations of U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

5.12.1. GravityZone Cloud Solution

To ensure protection against threats, GravityZone collects and stores data from managed endpoints on Bitdefender servers. However, health data is neither being accessed nor stored or in any other way processed. All information obtained by GravityZone is anonymized or at least pseudonymized. This technical approach means that using our GravityZone Cloud solution does not warrant your compliance with HIPAA regulations.

5.12.2. GravityZone On-Premises Solution

GravityZone On-Premises solution has been designed to allow keeping your data inside your organization. However, for higher protection, certain GravityZone features require interaction with Bitdefender cloud servers to perform tasks. To be in line

with HIPAA regulations, you need to disable these features in the GravityZone console (Control Center) as described below.

Security Policy Settings

Modify the security policy settings in Control Center as follows:

1. Go to **Policies** and click to edit an existing policy or create a new one.
2. Go to **General > Settings**.
3. Under the **Options** section, deselect the following check boxes:
   - **Submit crash reports to Bitdefender**.
   - **Submit suspicious executable files for analysis**.
   - **Use Bitdefender Global Protective Network to enhance protection**.
4. Go to **Antimalware > Settings**.
5. Under the **Quarantine** section, deselect **Submit quarantined files to Bitdefender Labs every (hours)**.
6. Go to **Sandbox Analyzer**.

   If using Sandbox Analyzer Cloud as detonation environment, you must filter out the submitted file types so that they do not contain medical data or any personally identifiable information (PII). To do this, under the **Content Prefiltering** section, specify in the **Exceptions** box the extensions of the files you do not want automatically submitted.

   If you are not sure about what kind of data you may submit to Sandbox Analyzer, to be on the safe side from a HIPAA perspective, you may disable this feature altogether by deselecting the **Automatic sample submission from managed endpoints** check box.
7. Click **Save** to apply the changes.

Installation Packages

Modify the installation packages in Control Center as follows:

1. Go to **Network > Packages** and click to edit an existing installation package or create a new one.
2. Under the **Miscellaneous** section, deselect these check boxes:
   - **Submit crash dumps**.

- **Submit quarantined files to Bitdefender Labs every (hours)**.
- **Submit suspicious executables to Bitdefender**.
- **Use Bitdefender Global Protective Network to enhance protection**.

3. Under the **Settings** section, deselect **Scan before installation**.
4. Click **Save** to apply the changes.

Sandbox Analyzer Manual Submission

While you can configure automatic submission to Sandbox Analyzer Cloud in the security policy settings, manual submission depends exclusively on the operations you make in the **Sandbox Analyzer > Manual Submission** section of the Control Center main menu. To be in line with HIPAA regulations, make sure you do not submit to Sandbox Analyzer Cloud files that may contain medical data or PII.

Legal Notice

Please be advised that it is entirely your responsibility to check your compliance with any piece of legislation, including HIPAA, and by presenting the above information Bitdefender expressly disclaims any and all liability regarding your compliance with HIPAA and your conduct in relation to HIPAA or any other legal requirements you may be subjected to. For the avoidance of any doubt, by using Bitdefender Solutions, including GravityZone, Bitdefender does not warrant in any way your compliance to any piece of legislation, including HIPAA. The above does not represent legal guidance and you are encouraged to seek legal advice with respect to the above or any other legal related topic.

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, the security agent or the Security Server 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 Security Server and 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.

Important
The GravityZone appliance does not include the Security Server packages by default. You must manually download the Security Server packages necessary for your environment.

6.4. Staging Updates

Staging enables you to test newer kits or product updates in an enclosed and controlled environment before publishing them in your network. The staging environment should mirror production as closely as possible for the purposes of

testing. By doing this, you can maximize your chances of finding any issues that may appear in your environment, before releasing the version in production.

The staging feature also allows you to create a policy for the critical endpoints from production. You can update these endpoints only after the updates have been tested in the staging environment and on the non-critical machines from production. For more details, refer to "Publishing with Update Rings " (p. 193).

Note

- Staging is disabled by default.
- Security Server (VMware with NSX) does not support staging.
- BEST for Windows Legacy does not support staging. The legacy endpoints on staging location must be moved to the production location.

6.4.1. Prerequisites

Staging mode requires the GravityZone infrastructure to meet the following conditions:

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

  If you have the Update Server together with other roles on the appliance, you must follow these steps:

  1. Delete the old Update Server role.
  2. Deploy a new GravityZone appliance.

     Important
     Do not install any roles yet.

  3. Connect the new appliance to the existing GravityZone database.
  4. Install the Update Server role on the new appliance.

  For more information on installing GravityZone roles, refer to "Managing the GravityZone Appliance" (p. 103).
- The Update Server appliance must be of at least 120 GB.
- The Web Console appliance must be of at least 120 GB.

6.4.2. Using Staging

To set up the staging environment and test the latest updates you must:

1. Enable staging and define the update server settings.
2. Define a staging policy for the testing endpoints.
3. Install the packages on the testing endpoint.
4. Assign the staging policy to the testing endpoints.
5. Update the testing endpoints to the latest version and test the update in the staging environment.
6. Run a second test before updating all the endpoints from production. You can first test the update on the non-critical endpoints.

Enabling Staging

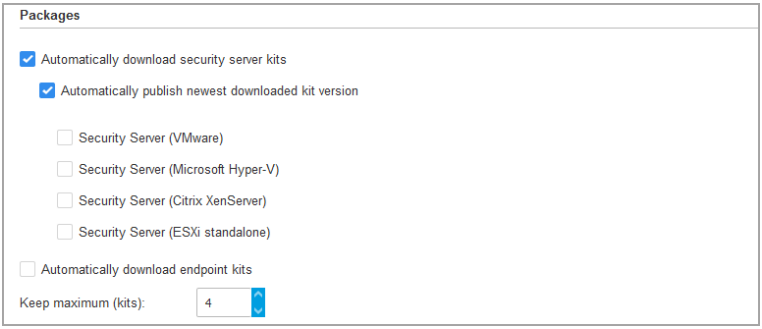
To enable staging mode for GravityZone updates:

1. Go to the **Configuration** > **Update** page 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. Select the **Enable Staging** check box.
4. Under **Production Server Configuration**, configure the main settings:
   - **Packages Address.** The address where packages are downloaded from:`download.bitdefender.com/SMB/Hydra/release`
   - **Update Address.** The address where product updates are downloaded from:`upgrade.bitdefender.com:80`.
   - **Port.** The default port is `7074`. You cannot edit this field.
   - **IP.** The IP address of the Update Server. You cannot edit this field.
   - **Update period (hours).** If you want to change the update period, type a new value in this field. The default value is 1.
5. The production and update server can act as gateways 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.

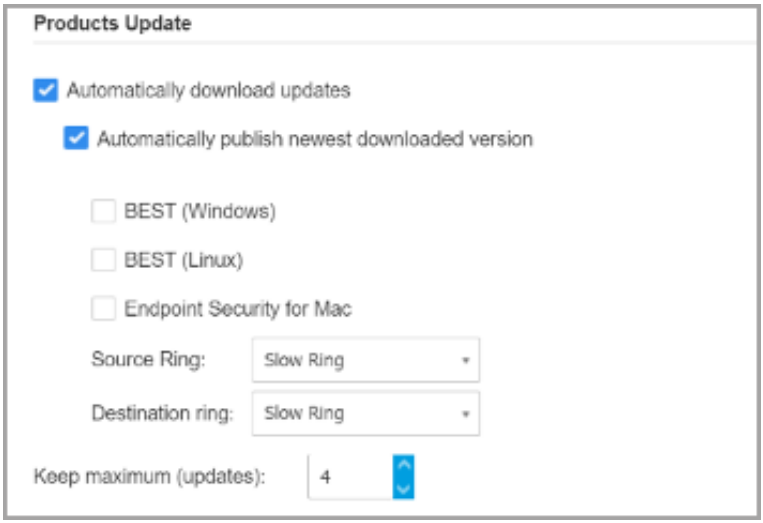
6. Under **Staging Server Configuration**, configure the following options:
   - **Port.** The default port is `7077`.
   - **IP.** The IP address of the Update Server. You cannot edit this field.
7. Under **Packages**, you can configure Update Server to automatically download and publish Security Server and endpoint kits.



Packages - Auto Publish

You can also configure the maximum number of kits that you can store on the GravityZone appliance. Enter a number between 4 and 10 in the **Keep maximum (kits)** menu.

8. Under **Products Update**, you can configure Update Server to automatically download updates for security agents.



Packages - Auto Publish

You can choose to also automatically publish newest downloaded versions:

a. Select at least one security agent from the available list.

b. Define the source and destination rings:

- **Source ring**. The ring used to send the updates in the staging environment. When a version is validated by its early adopters it will be published on the slow ring. This is the default value. The newest available updates will be published on the fast ring.
- **Destination ring**. The ring used to publish the updates in production. You can select between fast and slow.

You can also configure the maximum number of updates that you can store on the GravityZone appliance. Enter a number between 4 and 10 in the **Keep maximum (updates)** menu.

9. Click **Save**.

Once enabled staging, build your staging environment to start testing the available product kits and updates.

Important
Disabling staging will delete all unpublished packages and product updates.

Defining the Staging Policy

You need to define a staging policy:

1. Go to the **Policies** page.
2. Select or create a policy to use in the test environment.
3. Under the **General** > **Update** section, enter the Staging Server address in the **Update Locations** table.
4. Configure the other policy settings as needed. For more details, refer to the **Security Policies** chapter from the GravityZone Administrators Guide.
5. Click **Save**.

Staging Packages

To install the latest package on the testing endpoints:

1. Go to the **Configuration > Update** page and select the **Components** tab.
2. Click **Check for updates** to make sure you view the latest released product version.
3. Click the component you want to update in the **Product** list.
4. Select a package available in the **Packages** table, which you want to test. You can download several kits for every product, up to the limit specified in the **Update Server Settings** window. When this limit is reached, the oldest version is removed from the table.
5. Click **Actions** and select **Download** to get the package to your GravityZone appliance.
6. Having the package selected, click **Save to disk**. The package configuration window is displayed.
7. Configure the package. For more information, refer to “Creating Installation Packages” (p. 134).
8. Install the kit on the testing endpoints.
9. Monitor the behavior of the endpoints.

10. If the package has installed successfully and the endpoints have normal behavior, you can publish the package to the production network.

    To publish a package, select it in the **Packages** table, click **Actions** at the upper side of the table and select **Publish**.

    Important
    You cannot publish packages older than the one already published.

11. If you encountered problems with the package, you can log a support ticket. For more details, refer to "Getting Help" (p. 214).

    To delete a package from the GravityZone appliance, click the **Actions** button and choose **Delete from disk**.

Assigning the Staging Policy

To assign the staging policy to the testing endpoints:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group that you want from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
4. Select the check box of the computer or group that you want. You can select one or several objects of the same type only from the same level.
5. Click the **Assign Policy** button at the upper side of the table.
6. Make the necessary settings in the Policy assignment window. For more information, refer to **Security Policies > Managing Policies > Assigning Policies to Endpoints** chapter from the GravityZone Administrators Guide.

Staging Product Updates

To install the latest updates:

1. Go to the **Configuration > Update** page and select the **Components** tab.
2. Click **Check for updates** to make sure you view the latest released product update.
3. Select the Bitdefender product of your choice in the **Product** list.

Note
You can use staging only with updates for security agents and not for Security Servers.

4. Select an update available in the **Updates** table, which you want to test.
5. Click **Actions** and select **Download** to get the update to your GravityZone appliance.

   You can download several updates for every product, up to the limit specified in the **Update Server Settings** window. When this limit is reached, the oldest version is removed from the table.
6. Having an update selected, click **Actions** and select **Add to staging**. The update will install on the testing endpoints, according to the policy settings. For more details refer to "Defining the Staging Policy" (p. 191).
7. If the update has installed successfully and the endpoints have normal behavior, start to send out the update to the machines in production. First, update the non-critical machines to run another test before updating the critical endpoints. For more details, refer to "Publishing with Update Rings " (p. 193).
8. If you encountered problems with the update, you can log a support ticket. For more details, refer to "Getting Help" (p. 214).

   To delete an unpublished update from the GravityZone appliance, click the **Actions** button and choose **Delete**. You can delete only unpublished updates.

Publishing with Update Rings

To test the update on the non-critical endpoints from production, you must first edit the existing policies and assign them a fast ring policy.

Note
A slow ring policy is automatically assigned for all the policies you create.

1. Go to the **Policies** page.
2. Edit the policy setting for the non-critical endpoints in production. In the **Update Ring** section select **Fast ring**.

Note
The update published on fast ring cannot be older than the one published on the slow ring.

3. Publish the update on the fast ring:
   a. Go to **Configuration** > **Update** page and select the **Components** tab.
   b. Select the update in the Updates table, click the **Actions** button at the upper side of the table and choose **Publish**.
   c. Select the fast ring option.

      Note
      When you first publish an update, it will be available on the fast and slow rings.

      At this point, all endpoints with fast ring policy are being updated to the published version.
4. Monitor the behavior of the fast ring endpoints.
5. If the update has installed successfully and the endpoints have normal behavior, you can publish the update on the slow ring:
   a. Go to **Configuration** > **Update** page and select the **Components** tab.
   b. Select the update in the Updates table, click the **Actions** button at the upper side of the table and choose **Publish**.
   c. Select the slow ring option.

      Every endpoint from production is now updated to the version you published.
6. If you encountered problems with the package, you can log a support ticket. For more details, refer to "Getting Help" (p. 214).

6.5. 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.

6.5.1. 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

6.5.2. 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
```

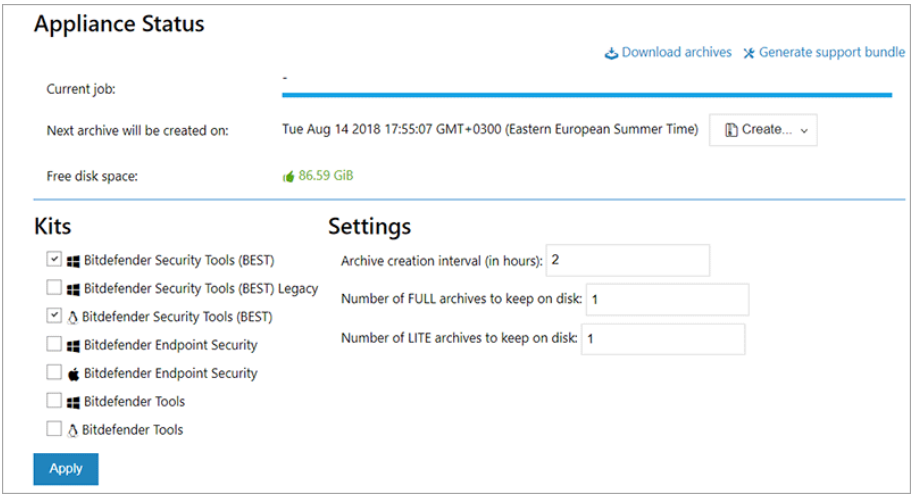
The `gzou-mirror` has the following roles:

- 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.

6.5.3. 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.



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:

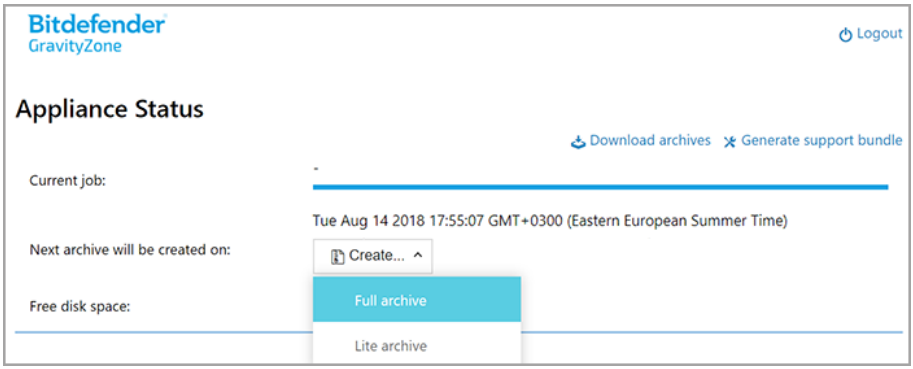
     – **Full archive (product + security content)**, when new update files are available

     – **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`

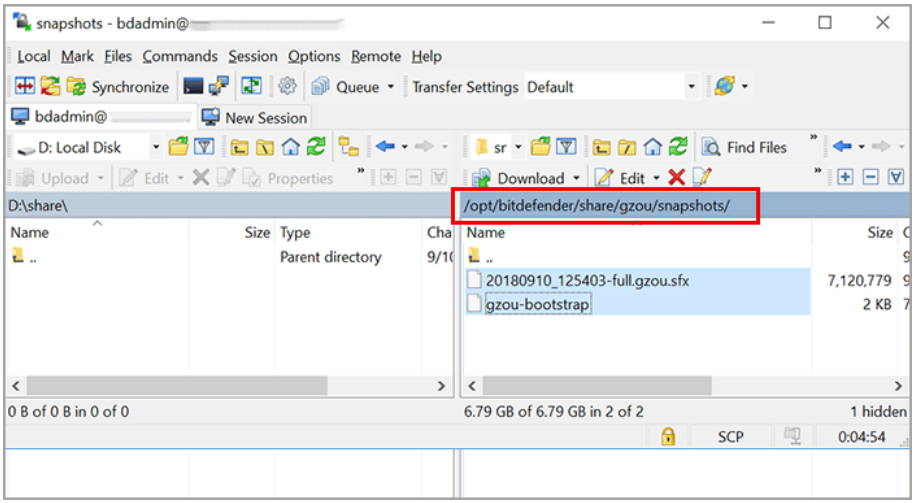
3. Click **Create > Full** archive to create the first full archive. Wait until the archive is created.



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).

6.5.4. 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).

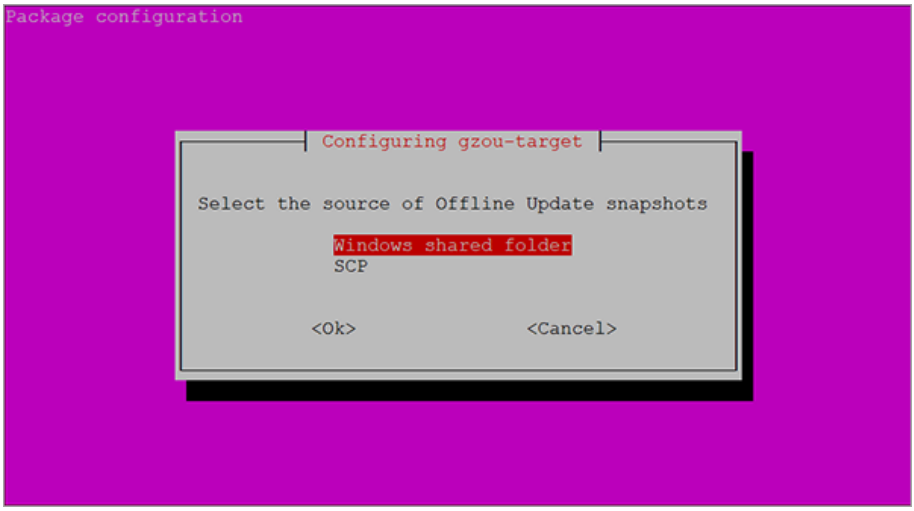
Important
For the offline update to work, make sure that:

- 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:

a. Access the offline instance's TTY terminal in your virtual environment (or connect to it via SSH).

b. Log in with the `bdadmin` user and the password you have set.

c. Run the command `sudo su` to gain root privileges.

d. 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.

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

6.5.5. 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. 195).
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. 198).

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

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

6.5.6. 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 HVI
- Uninstalling Exchange Protection
- Uninstalling Mobile Devices Protection
- Uninstalling Sandbox Analyzer On-Premises
- Uninstalling Report Builder
- Uninstalling GravityZone Server Roles

7.1. Uninstalling Endpoint Protection

To safely remove Bitdefender protection, you have first to uninstall security agents, then Security Server, if needed. If you want to uninstall only the Security Server, make sure to connect its agents to another Security Server first.

- Uninstalling Security Agents
- Uninstalling Security Server

7.1.1. Uninstalling Security Agents

You have two options to uninstall the security agents:

- Remotely in Control Center
- Manually on the target machine

Warning
The security agents and Security Servers are essential for keeping the endpoints safe from any kind of threats, thus uninstalling them may put the entire network in danger.

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 Endpoint Protection" (p. 120).

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 Endpoint Protection" (p. 120).

7.1.2. Uninstalling Security Server

You can uninstall Security Server the same way it was installed, either from Control Center or from the menu-based interface of the GravityZone virtual appliance.

To uninstall Security Server in Control Center:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the datacenter or folder containing the host on which the Security Server is installed. The endpoints are displayed in the right-side pane.

4. Select the check box corresponding to the host on which the Security Server is installed.
5. In the **Tasks** menu, select **Uninstall Security Server**.
6. Enter the vShield credentials (if applicable) and click **Yes** to create the task.

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

When Security Server is installed on the same virtual appliance as the other GravityZone roles, you can remove it using the command-line interface of the appliance. Follow these steps:

1. Access the appliance console 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. In the **Appliance Options** menu, go to **Advanced Settings**.
3. Select **Uninstall Security Server**. A confirmation window is displayed.
4. Press the `Y` key, or press `Enter` while having the **Yes** option selected to continue. Wait until the uninstallation finishes.

7.2. Uninstalling HVI

To remove HVI from a host, it suffices to uninstall the HVI Supplemental Pack. You can further use the Security Server as a scan server, provided you have a valid license key for Security for Virtualized Environments.

If you want to completely remove Bitdefender, you need to uninstall both the HVI Supplemental Pack and the Security Server.

Uninstalling HVI Supplemental Pack

You have two options to remove the Supplemental Pack:

- Remotely from Control Center, by running an uninstallation task.
- Remotely from XenCenter, by running a couple of commands on the target host.

To remove the HVI pack using Control Center:

1. Log in to Control Center.
2. Go to the **Network** page and select **Virtual Machines** from the views selector.

3. Select **Server** from the **Views** menu in the left pane.
4. Select one or more Xen hosts from network inventory. You can easily view the available hosts by selecting the option **Type > Hosts** in the **Filters** menu.
5. Click the **Tasks** button in the right pane and choose **Uninstall HVI Supplemental Pack**. The configuration window opens.
6. Schedule when to remove the pack. You can choose to run the task immediately after saving the task, or at a specific time. In case removal cannot complete at the specified time, the task automatically repeats according to the recurrence settings. For example, if you select more hosts and one host is not available when the pack is scheduled for removal, the task will run again at the specified time.
7. The host must restart to complete the removal. If you want the host to restart unattended, select **Automatically reboot (if needed)**.
8. Click **Save**. A confirmation message will appear.

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

To remove the HVI pack using XenCenter:

1. Log in to XenCenter.
2. Open the console of the Xen host.
3. Enter the password for the XenServer host.
4. Run the following commands:

```
# rpm -e bitdefender-xen-dom0
# rm -rf /etc//xensource/installed-repos\
  /bitdefender\:bitdefender-hvi/
# rm -rf /opt/bitdef*
# service xapi restart
```

Uninstalling Security Server

To uninstall Security Server from one or several hosts:

1. Log in to Control Center.
2. Go to the **Network** page.
3. Choose **Virtual Machines** from the views selector.

4. Browse the Citrix inventory and select the check boxes corresponding to the desired hosts. For a fast selection, you can filter the network inventory to view only the Security Servers.
5. Click the **Tasks** button at the upper side of the table and choose **Uninstall Security Server** from the menu. A confirmation message will appear. Click **Yes** to continue.

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

7.3. Uninstalling Exchange Protection

You can remove Exchange Protection from any Microsoft Exchange Server having Bitdefender Endpoint Security Tools with this role installed. You can perform the uninstallation in Control Center.

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the container you want from the left-side pane. The entities will be displayed in the right-side pane table.
4. Select the endpoint you want to uninstall the Exchange Protection from.
5. Click **Reconfigure Client** in the **Tasks** menu, in the upper-side pane of the table. A configuration window is displayed.
6. Under the **General** section, clear the **Exchange Protection** check box.

   Warning
   In the configuration window, make sure you have selected all the other roles which are active on the endpoint. Otherwise, they will be uninstalled as well.

7. Click **Save** to create the task.

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

If you want to reinstall Exchange Protection, refer to "Installing Exchange Protection" (p. 162).

7.4. Uninstalling Sandbox Analyzer On-Premises

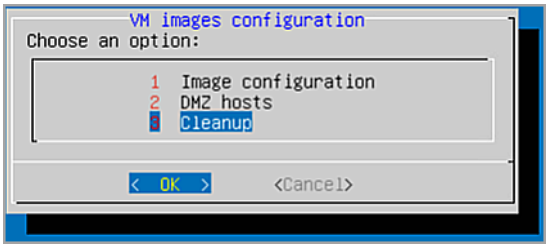
To uninstall Sandbox Analyzer On-Premises:

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.

7.5. Uninstalling Mobile Devices Protection

When removing Bitdefender protection from a mobile device, you need to do this from both Control Center and the device.

When you delete a device from Control Center:

- GravityZone Mobile Client is unlinked, but not removed from the device.
- All logs related to the deleted device are still available.
- Your personal information and applications are not affected.

- For iOS devices, the MDM Profile is removed. If the device is not connected to the Internet, the MDM Profile remains installed until a new connection is available.

Warning

- You cannot restore deleted mobile devices.
- Make sure the target device is not locked before deletion. If you accidentally delete a locked device, you need to reset the device to the factory settings to unlock it.

1. Go to the **Network** page.
2. Select **Mobile Devices** from the views selector.
3. Click **Filters** at the upper-side of network pane and select **Devices** from the **View** category. Click **Save**.
4. Select the container that you want from the left-side pane. All devices are displayed in the right-side pane table.
5. Select the check box of the device you want to remove protection from.
6. Click ⊖ **Delete** at the upper-side of the table.

Next, you have to uninstall the software from the device.

To uninstall Bitdefender protection from an Android device:

1. Go to **Security > Device Administrators**.
2. Deselect the GravityZone check box. A confirmation window appears.
3. Tap **Deactivate**. A warning message is displayed, informing you that the anti-theft features will no longer work and you will lose access to corporate networks and data.
4. Uninstall GravityZone Mobile Client as any other application.

To uninstall Bitdefender protection from an iOS device:

1. Go to Bitdefender GravityZone Mobile Client icon and hold it for a few seconds.
2. Tap the attached ⊗ circle when it appears. The application is deleted.

If you want to reinstall mobile protection, refer to "Installing Mobile Devices Protection" (p. 167)

7.6. Uninstalling Report Builder

To correctly remove Report Builder from your GravityZone solution, you must first uninstall the Report Builder Processors role, then the Report Builder Database role.

To uninstall Report Builder Processors:

1. Log in to Report Builder Processors 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. From the main menu, select **Advanced Settings**.
3. Go to **Install/Uninstall Roles**, then **Add or remove roles**.
4. Using the `Space` bar, deselect **Report Builder Processors** role and press `Enter`. A confirmation window will appear.
5. Select **Yes** and press `Enter` to continue and wait for the uninstallation to complete.

To uninstall Report Builder Database:

1. Log in to Report Builder Database 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. From the main menu, select **Advanced Settings**.
3. Go to **Install/Uninstall Roles**, then **Add or remove roles**.
4. Using the `Space` bar, deselect **Report Builder Database** role and press `Enter`. A confirmation window will appear.
5. Select **Yes** and press `Enter` to continue and wait for the uninstallation to complete.

Warning
If you power off the Report Builder appliances in the virtualization environment without uninstalling the Database and Processors roles, you will be unable to connect to GravityZone Control Center.

7.7. 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. 107).

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 sumbitting 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.com
Web: 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.fr
Website: 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; xlsm; 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