Bitdefender

GravityZone

INSTALLATION GUIDE

Bitdefender GravityZone Installation Guide

Publication date 2020.07.02

Copyright© 2020 Bitdefender

Legal Notice

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

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

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

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

Table of Contents

Preface v
1. Conventions Used in This Guide v
1. About GravityZone 1
2. GravityZone Protection Layers 2
2.1. Antimalware 2
2.2. Advanced Threat Control 3
2.3. Advanced Anti-Exploit 4
2.4. Firewall 4
2.5. Content Control 4
2.6. Network Attack Defense 4
2.7. Patch Management 4
2.8. Device Control 5
2.9. Full Disk Encryption 5
2.10. Security for Exchange 5
2.11. Endpoint Risk Analytics (ERA) 6
2.12. Email Security 6
2.13. Security for Storage 6
2.14. GravityZone Protection Layers Availability 7
3. GravityZone Architecture 8
3.1. Web Console (GravityZone Control Center) 8
3.2. Security Server 8
3.3. Security Agents 8
3.3.1. Bitdefender Endpoint Security Tools 8
3.3.2. Endpoint Security for Mac 11
4. Requirements 12
4.1. Control Center 12
4.2. Endpoint Protection 12
4.2.1. Hardware 13
4.2.2. Supported Operating Systems 16
4.2.3. Supported File Systems 21
4.2.4. Supported Browsers 21
4.2.5. Security Server 22
4.2.6. Traffic Usage 24
4.3. Exchange Protection 26
4.3.1. Supported Microsoft Exchange Environments 26
4.3.2. System Requirements 26
4.3.3. Other Software Requirements 26
4.4. Full Disk Encryption 27
4.5. Storage Protection 28
4.6. GravityZone Communication Ports 29
5. Installing Protection 30
5.1. License Management 30

5.1.1. Finding a Reseller . . . 30
5.1.2. Activating Your License . . . 30
5.1.3. Checking Current License Details . . . 31
5.2. Installing Endpoint Protection . . . 32
5.2.1. Installing Security Server . . . 32
5.2.2. Installing Security Agents . . . 35
5.3. Installing Full Disk Encryption . . . 57
5.4. Installing Exchange Protection . . . 58
5.4.1. Preparing for Installation . . . 58
5.4.2. Installing Protection on Exchange Servers . . . 59
5.5. Installing Storage Protection . . . 59
5.6. Credentials Manager . . . 60
5.6.1. Adding Credentials to the Credentials Manager . . . 60
5.6.2. Deleting Credentials from Credentials Manager . . . 61
6. Integrations . . . 63
6.1. Integrating with Amazon EC2 . . . 63
7. Uninstalling Protection . . . 64
7.1. Uninstalling Endpoint Protection . . . 64
7.1.1. Uninstalling Security Agents . . . 64
7.1.2. Uninstalling Security Server . . . 66
7.2. Uninstalling Exchange Protection . . . 66
8. Getting Help . . . 68
8.1. Bitdefender Support Center . . . 68
8.2. Asking for Assistance . . . 69
8.3. Using Support Tool . . . 70
8.3.1. Using Support Tool on Windows Operating Systems . . . 70
8.3.2. Using Support Tool on Linux Operating Systems . . . 71
8.3.3. Using Support Tool on Mac Operating Systems . . . 73
8.4. Contact Information . . . 74
8.4.1. Web Addresses . . . 74
8.4.2. Local Distributors . . . 74
8.4.3. Bitdefender Offices . . . 75
A. Appendices . . . 78
A.1. Supported File Types . . . 78

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 deploy Bitdefender security agents on all types of endpoints in your company, and how to configure the GravityZone solution.

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. v)	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, 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 blacklisting 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
- Advanced Anti-Exploit
- Firewall
- Content Control
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Endpoint Risk Analytics (ERA)
- Email Security

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. Advanced Anti-Exploit

Powered by machine learning, Advanced Anti-Exploit is a proactive technology that stops zero-day attacks carried out through evasive exploits. Advanced anti-exploit catches the latest exploits in real-time and mitigates memory corruption vulnerabilities that can evade other security solutions. It protects the most commonly used applications, such as browsers, Microsoft Office or Adobe Reader, as well as others that you may think of. It watches over system processes and protects against security breaches and hijacking existing processes.

2.4. Firewall

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

2.5. Content Control

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

2.6. Network Attack Defense

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

2.7. Patch Management

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

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

You can learn more about GravityZone Patch Management supported vendors and products from this KB article.

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

2.8. Device Control

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

2.9. Full Disk Encryption

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

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

2.10. 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.
The Security for Exchange license capacity equals to 150% of the total number of Security for Endpoints license seats. In case the number of active mailboxes in your organization exceeds the number of mailboxes covered by the license, you will receive a notification to extend your license.

2.11. Endpoint Risk Analytics (ERA)

Endpoint Risk Analytics (ERA) identifies, assesses and remediates Windows endpoints weaknesses via security risk scans (on-demand or scheduled via policy), taking into account a vast number of indicators of risk. Once you have scanned your network with certain indicators of risk, you will obtain an overview of your network risk status via **Risk Management** dashboard, available from the main menu. You will be able to resolve certain security risks automatically from GravityZone Control Center, and view recommendations for endpoint exposure mitigation.

2.12. Email Security

Through Email Security you can control email delivery, filter messages, and apply company-wide policies, to stop targeted and sophisticated email threats, including Business Email Compromise (BEC) and CEO fraud. Email Security requires account provisioning to access the console. For more information, refer to the Bitdefender Email Security User Guide.

2.13. 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.

2.14. 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 GravityZone solution includes the following components:

- Web Console (Control Center)
- Security Server
- Security Agents

3.1. Web Console (GravityZone Control Center)

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

Control Center, a web-based interface, integrates with the existing system management and monitoring systems to make it simple to apply protection to unmanaged workstations and servers.

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.

The Security Server must be installed on one or several hosts so as to accommodate the number of protected virtual machines.

3.3. Security Agents

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

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

3.3.1. 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
- Firewall
- Content Control
- Network Attack Defense
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Endpoint Risk Analytics (ERA)

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. 16).

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.

  This functionality is essential for the security agent deployment in a cloud GravityZone environment.
- 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.

3.3.2. 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

4. REQUIREMENTS

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

4.1. 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

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.

4.2. 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. 8).

4.2.1. Hardware

Security Agent Without Roles

CPU

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

Warning
ARM processors are currently not supported.

Free RAM Memory

At Installation (MB)

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

For Daily Usage (MB)*

OS	Antivirus (Single Engine)			Protection Modules				
	Local	Hybrid	Centralized	Behavioral Scan	Firewall	Content Control	Power User	Update Server
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

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

Free Disk Space

At Installation (MB)

OS	SINGLE ENGINE						DUAL ENGINE			
	Local Scanning		Hybrid Scanning		Centralized Scanning		Centralized + Local Scanning		Centralized + Hybrid Scanning	
	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options	AV Only	Full Options
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

For Daily Usage (MB)*

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

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

Security Agent with Relay Role

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

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

Warning

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

Important

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

Security Agent With 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.

4.2.2. Supported Operating Systems

Windows Desktop

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

Warning
Bitdefender does not support Windows Insider Program builds.

Windows Tablet and Embedded

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Windows Server

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

Linux

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

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

- Amazon Linux AMI 2016.09 or higher

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	**Fanotify** (kernel option) must be enabled.

Kernel Versions	Linux Distributions	On-access Requirements
	Debian 9.0 or higher Oracle Linux 6.3 or higher Amazon Linux AMI 2016.09 or higher	
2.6.38 or higher	Debian 8	**Fanotify** must be enabled and set to enforcing mode and then the kernel package must be rebuilt. For details, refer to this KB article.
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender provides support via **DazukoFS** with prebuilt kernel modules.
All other kernels	All other supported systems	The **DazukoFS** module must be manually compiled. For more details, refer to "Manually compile the DazukoFS module" (p. 52).

* 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.

Kernel Versions	Linux Distributions	Details
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.

Note
Fanotify and DazukoFS enable third-party applications to control file access on Linux systems. For more information, refer to:

- Fanotify man pages: http://www.xypron.de/projects/fanotify-manpages/man7/fanotify.7.html.
- Dazuko project website: http://dazuko.dnsalias.org/wiki/index.php/About.

macOS

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

4.2.3. 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.

4.2.4. 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+

4.2.5. Security Server

Security Server is a preconfigured virtual machine running on an Ubuntu Server 12.04 LTS (3.2 kernel).

Virtualization Platforms

Bitdefender Security Server can be installed on the following virtualization platforms:

- VMware vSphere 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0 with VMware vCenter Server 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0
- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (including Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 or Windows Server 2008 R2, 2012, 2012 R2 (including Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism with AOS 5.6, 5.11 STS
- Nutanix Prism with AHV 20170830.115, 20170830.301 and 20170830.395 Community Edition

- Nutanix Prism version 2018.01.31 (Community Edition)

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

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

HDD Space

You must provision 8 GB disk space on each host of Security Server.

Security Server Distribution on Hosts

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	Normal	10:30

Storage Protection status	Security Server resources	Security Server load	Transfer time (mm:ss)
	4 GB RAM		
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.

4.2.6. Traffic Usage

- **Product updates traffic between endpoint client and update server**

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

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

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

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

- **Central Scan traffic between endpoint client and Security Server**

Scanned Objects	Traffic Type		Download (MB)	Upload (MB)
Files*	First scan		27	841
	Cached scan		13	382
Websites**	First scan	Web traffic	621	N/A

Scanned Objects	Traffic Type		Download (MB)	Upload (MB)
		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.

Note
The network latency between endpoint client and Bitdefender Cloud Server must be under 1 second.

- **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.

4.3. 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.

4.3.1. 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).

4.3.2. 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. 13).

Recommended server resource availability:

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

4.3.3. 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

4.4. 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 Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Note
On Mac OS X Mountain Lion (10.8), you can install the Bitdefender agent, but the Encryption module will not be available.

4.5. 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 3.6.2

- Citrix® ShareFile

4.6. GravityZone Communication Ports

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

For detailed information regarding GravityZone ports, refer to this KB article.

5. INSTALLING PROTECTION

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

5.1. License Management

GravityZone is licensed with a single key for all security services, except for Full Disk Encryption, which for yearly license comes with a separate key.

You can try GravityZone for free for a period of 30 days. During the trial period all features are fully available and you can use the service on any number of computers. Before the trial period ends, if you want to continue using the services, you must opt for a paid subscription plan and make the purchase.

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

Your subscription is managed by Bitdefender or by the Bitdefender partner who sells you the service. Some Bitdefender partners are security service providers. Depending on your subscription arrangements, GravityZone day-to-day operation may be handled either internally by your company or externally by the security service provider.

5.1.1. 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.

5.1.2. Activating Your License

When you purchase a paid subscription plan for the first time, a license key is issued for you. The GravityZone subscription is enabled by activating this license key.

Warning
Activating a license does NOT append its features to the currently active license. Instead, the new license overrides the old one. For example, activating a 10 endpoints license on top of a 100 endpoints license will NOT result in a subscription for 110 endpoints. On the contrary, it will reduce the number of covered endpoints from 100 to 10.

The license key is sent to you via email when you purchase it. Depending on your service agreement, once your license key is issued, your service provider may activate it for you. Alternately, you can activate your license manually, by following these steps:

1. Log in to Control Center using your account.
2. Click your username in the upper-right corner of the console and choose **My Company**.
3. Check details about the current license in the **License** section.
4. In the **License** section, select the **License** type.
5. In the **License Key** field, enter your license key.
6. Click the **Check** button and wait until Control Center retrieves information about the entered license key.
7. In the **Add-on key** field, enter the key for a specific add-on, such as Encryption.
8. Click **Add**. The add-on details appear in a table: type, license key and the option to remove the key.
9. Click **Save**.
10. To be able to use the add-on, you must log out from the Control Center and then re-log in. This will make the add-on features visible in GravityZone.

5.1.3. Checking Current License Details

To view your license details:

1. Log in to Control Center using your email and password received by email.
2. Click your username in the upper-right corner of the console and choose **My Company**.
3. Check details about the current license in the **License** section. You can also click the **Check** button and wait until Control Center retrieves the latest information about the current license key.

5.2. 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 if the machines have little hardware resources.

Important
Only Bitdefender Endpoint Security Tools supports connection to a Security Server. For more information, refer to "GravityZone Architecture" (p. 8).

5.2.1. 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.

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.

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:

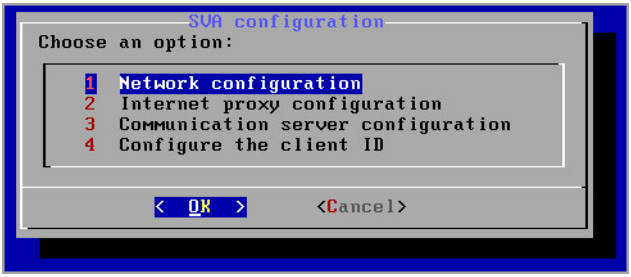
1. Go to the **Network > Packages** page.
2. Select the Default Security Server Package.
3. Click the **Download** button at the upper side of the table and choose the package type from the menu.
4. Save the selected package to the desired location.

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 one of the following addresses for the Communication Server:

   - `https://cloud-ecs.gravityzone.bitdefender.com:443`
   - `https://cloudgz-ecs.gravityzone.bitdefender.com:443`

   Important
   This address must be the same as the one that appears in Control Center policy settings. To check the link, go to the **Policies** page, add or open a

custom policy, navigate to the **General > Communication > Endpoint Communication Assignment** section and enter the Communication Server name in the column header field. The correct server will show in search results.

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

7. Configure the client ID.
   a. From the main menu, select **Configure the client ID**.
   b. Enter the company ID.

      The ID is a string of 32 characters, which you can find by accessing the company details page in Control Center.

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

5.2.2. 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. 8).

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.

Warning

- The first endpoint on which you install protection must have the Relay role, otherwise you will not be able to remotely install the security agent on other endpoints in the same network.
- The Relay endpoint must be powered-on and online in order for the connected agents to communicate with Control Center.

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. 39).

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 connectivity to Control Center.
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.

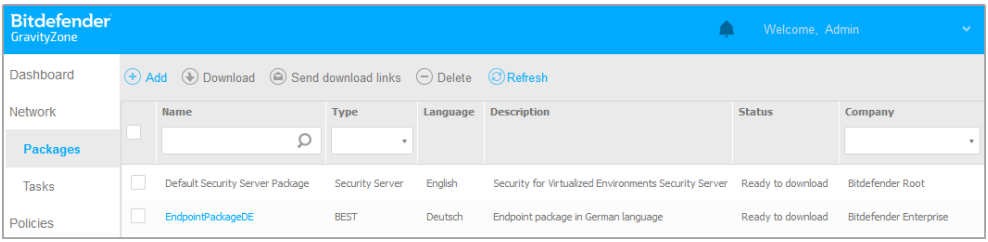
     Note
     The `net` binary/command is usually delivered with the samba-client and / or samba-common packages. On some Linux distributions (such as CentOS 7.4), the `net` command is only being installed when installing the full Samba suite (Common + Client + Server). Make sure that your Relay endpoint 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 kernel extensions on their computers. Until the users approve the Bitdefender kernel extensions, some Endpoint Security for Mac features will not work. To eliminate user intervention, you can pre-approve the Bitdefender kernel extensions by whitelisting them using a Mobile Device Management tool.

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

Warning

- The first machine on which you install protection must have Relay role, otherwise you will not be able to deploy the security agent on other endpoints in the network.
- The Relay machine must be powered-on and online in order for the clients to communicate with Control Center.

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. 54).

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.

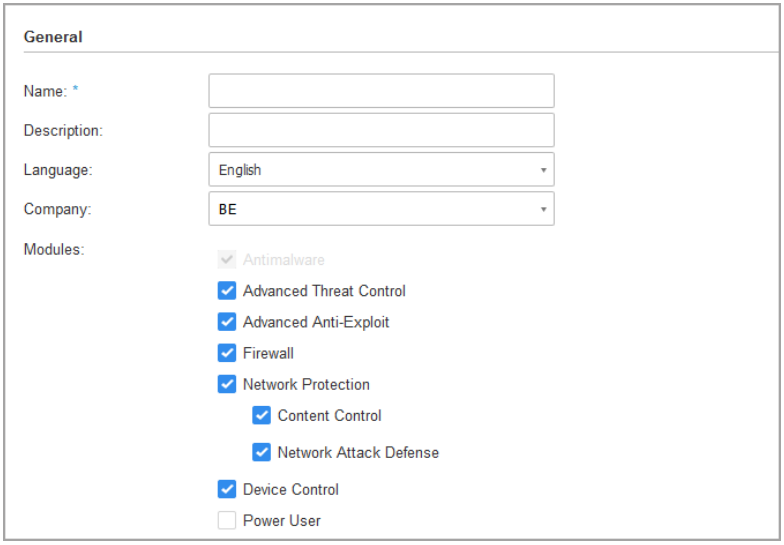
2. Download the installation package on the target endpoint.

   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. 8).

7. Select the target endpoint role:
   - **Relay**, to create the package for an endpoint with Relay role. For more information, refer to "Relay" (p. 10)
   - **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. 10)
   - **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. 58).
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.

> **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. 2)

10. 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.

11. 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.

12. 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.

13. 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.
14. 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.
15. Under **Deployer** section, choose the entity to which the target endpoints will connect for installing and updating the client:
    - **Bitdefender Cloud**, if you want to update the clients directly from the Internet.

      In this case, you can also define the proxy settings, if target endpoints connect to the Internet via proxy. 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 Bitdefender Endpoint Security Tools Relay to work.
16. 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:** only 64-bit systems

     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 detected in the network by using installation tasks.

Once you have locally installed the first client with Relay role, it may take a few minutes for the rest of the network endpoints to become visible in the Control Center. From this point, you can remotely install the security agent on endpoints under your management by using installation tasks from Control Center.

Bitdefender Endpoint Security Tools includes an automatic network discovery mechanism that allows detecting other endpoints in the same network. Detected endpoints are displayed as **unmanaged** in the **Network** page.

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. 54).

Remote Installation Requirements

For remote installation to work:

- Bitdefender Endpoint Security Tools Relay must be installed in your network.
- 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. 16).

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

Running Remote Installation Tasks

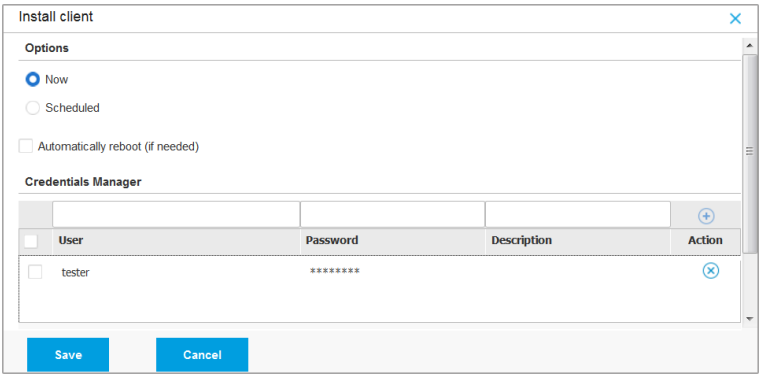
To run a remote installation task:

1. Connect and log in to Control Center.
2. Go to the **Network** page.
3. 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.

4. Select the entities (endpoints or groups of endpoints) on which you want to install protection.
5. 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

6. 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.

7. If you want target endpoints to automatically restart for completing the installation, select **Automatically reboot (if needed)**.
8. 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.

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

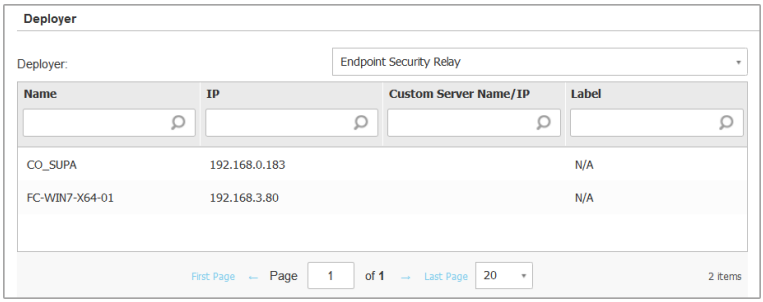
   Note
   A warning message is displayed as long as you have not selected any credentials. This step is mandatory to remotely install the security agent on endpoints.

10. Under **Deployer** section, configure the Relay to which the target endpoints will connect for installing and updating the client:

    - All machines with Relay role detected in your network will show-up in the table available under the **Deployer** section. Each new client must be

connected to at least one Relay client from the same network, that will serve as communication and update server. Select the Relay that you want to link with the target endpoints. 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.



- If target endpoints communicate with the Relay agent via proxy, you also need to define the proxy settings. In this case, select **Use proxy for communication** and enter the required proxy settings in the fields below.

11. 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.
12. 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. 39).

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

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

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.

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.

To enable automatic network discovery, you must have Bitdefender Endpoint Security Tools Relay already installed on at least one computer in the network. This computer will be used to scan the network.

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 is not actively involved in the Computer Browser service operation. Bitdefender Endpoint Security Tools only queries the Computer Browser service for the list of workstations and servers currently visible in the network (known as the browse list) and then sends it to Control Center. 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.

The initial query for the browse list is carried out by the first Bitdefender Endpoint Security Tools installed in 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.

For full network visibility, the Relay must be installed on at least one computer in each workgroup or domain in your network. Ideally, Bitdefender Endpoint Security Tools should be installed on at least one computer in each subnetwork.

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.

Computers from which Bitdefender Endpoint Security Tools queries the Computer Browser service must be able to resolve NetBIOS names.

Note
The network discovery mechanism works for all supported operating systems, including Windows Embedded versions, provided the requirements are met.

5.3. Installing Full Disk Encryption

Full Disk Encryption requires activation based on license key.

For detailed information about license keys, refer to "License Management" (p. 30).

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.

5.4. 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 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

5.4.1. 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.

5.4.2. 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. 35).

5.5. 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. 28).

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.

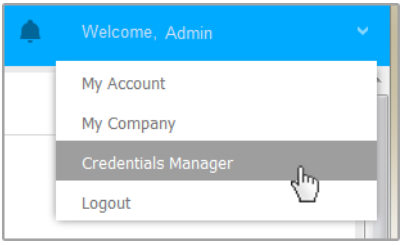
   For details, refer to **Security Policies > Computer and Virtual Machines Policies > Storage Protection** chapter from the GravityZone Administrator's Guide.

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.

5.6. Credentials Manager

The Credentials Manager helps you define the credentials required 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**.

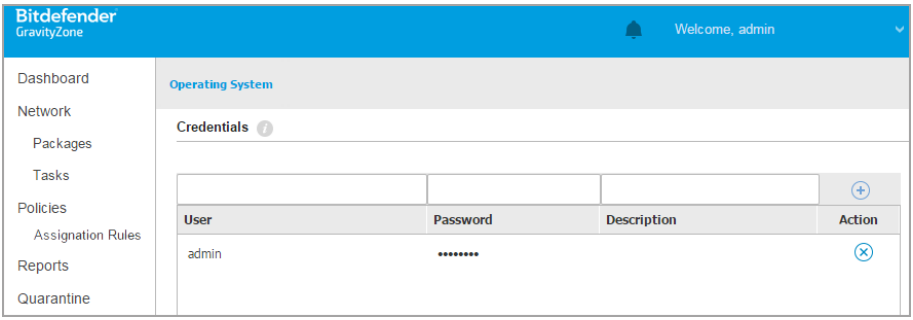


The Credentials Manager menu

5.6.1. Adding Credentials to the Credentials Manager

With the Credentials Manager you can manage the administrator credentials required for remote authentication during installation tasks sent to computers and virtual machines in your network.

To add a set of credentials:



Credentials Manager

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

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

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

2. Click the ⊕ **Add** button at the right side of the table. The new set of credentials is added to the table.

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

5.6.2. Deleting Credentials from Credentials Manager

To delete obsolete credentials from the Credentials Manager:

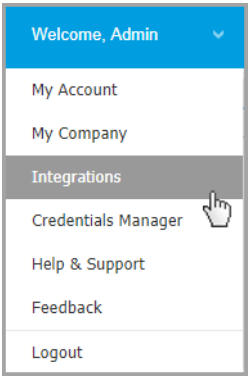
1. Point to the row in the table containing the credentials you want to delete.

2. Click the ⊗ **Delete** button at the right side of the corresponding table row. The selected account will be deleted.

6. INTEGRATIONS

GravityZone provides the possibility to integrate Control Center with third party solutions.

You can configure your third-party solutions integration in the **Integrations** page, which you can access by pointing to your username in the upper-right corner of the console and choosing **Integrations**.



From this page, you can add, edit or remove the integrations according to your needs.

6.1. Integrating with Amazon EC2

If your company has a Bitdefender Security for AWS service license, or you are running a trial Bitdefender Security for AWS subscription, you can configure the integration with this service from GravityZone Control Center and centrally deploy, manage and monitor Bitdefender security on their instance inventory. Proprietary scanning servers are hosted by Bitdefender in the AWS Cloud to ensure an optimal footprint on the protected instances and to eliminate the scanning overhead occurring with traditional security software.

For complete information about the Bitdefender Security for AWS architecture, prerequisites, subscription mode, creating and managing the integration with Amazon EC2, refer to the Amazon EC2 integration guide.

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 Exchange Protection

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. Select the container you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
3. Select the endpoints from which you want to uninstall the Bitdefender security agent.

4. Click **Tasks** at the upper-side of the table and choose **Uninstall client**. A configuration window is displayed.
5. In the **Uninstall agent** task window you can choose whether to keep the quarantined files on the endpoint or to delete them.
6. 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. 32).

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. 32).

7.1.2. Uninstalling Security Server

To remove Security Server:

1. Power off and delete the Security Server virtual machine from your virtualization environment.
2. Log in to GravityZone Control Center.
3. Go to **Network** and look for Security Server in the inventory. After a while from the moment you delete the virtual machine, Security Server will be reported as offline.
4. Select the check box corresponding to Security Server.
5. Click the ⊖ **Delete** button in the action toolbar.

   Security Server will be moved to the **Deleted** folder, where you can completely remove it by clicking again the ⊖ **Delete** button in the action toolbar.

7.2. 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. Select the container you want from the left-side pane. The entities will be displayed in the right-side pane table.

3. Select the endpoint you want to uninstall the Exchange Protection from.
4. Click **Reconfigure Client** in the **Tasks** menu, in the upper-side pane of the table. A configuration window is displayed.
5. 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.

6. 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. 58).

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
rsOrhideea Towe
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
```