Bitdefender

GravityZone

ADMINISTRATOR'S GUIDE

Bitdefender GravityZone
Administrator's Guide

Publication date 2017.07.17

Legal Notice

Table of Contents

Preface vii
1. Conventions Used in This Guide vii
1. About GravityZone 1
1.1. GravityZone Security Services 1
1.2. GravityZone Architecture 3
1.2.1. GravityZone Virtual Appliance 4
1.2.2. GravityZone Database 4
1.2.3. GravityZone Update Server 4
1.2.4. GravityZone Communication Server 4
1.2.5. Web Console (Control Center) 4
1.2.6. Report Builder 5
1.2.7. Security Server 5
1.2.8. HVI Supplemental Pack 5
1.2.9. Security Agents 6
2. Getting Started 13
2.1. Connecting to Control Center 13
2.2. Control Center at a Glance 13
2.2.1. Control Center Overview 14
2.2.2. Table Data 16
2.2.3. Action Toolbars 17
2.2.4. Contextual Menu 17
2.2.5. Views Selector 18
2.3. Managing Your Account 19
2.4. Changing Login Password 20
3. Managing User Accounts 21
3.1. User Roles 22
3.2. User Rights 23
3.3. Creating User Accounts 24
3.4. Editing Accounts 26
3.5. Deleting Accounts 26
3.6. Resetting Login Passwords 26
4. Managing Network Objects 28
4.1. Working with Network Views 30
4.1.1. Computers and Virtual Machines 30
4.1.2. Virtual Machines 31
4.1.3. Mobile Devices 32
4.2. Managing Computers 33
4.2.1. Checking the Computers Status 33
4.2.2. Viewing Computer Details 36
4.2.3. Organizing Computers into Groups 41
4.2.4. Sorting, Filtering and Searching for Computers 43
4.2.5. Running Tasks 47
4.2.6. Creating Quick Reports 70

4.2.7. Assigning Policies . . . 70
4.2.8. Using Recovery Manager for Encrypted Volumes . . . 71
4.2.9. Synchronizing with Active Directory . . . 72
4.3. Managing Virtual Machines . . . 73
4.3.1. Checking the Virtual Machines Status . . . 74
4.3.2. Viewing Virtual Machine Details . . . 77
4.3.3. Organizing Virtual Machines into Groups . . . 83
4.3.4. Sorting, Filtering and Searching for Virtual Machines . . . 85
4.3.5. Running Tasks on Virtual Machines . . . 89
4.3.6. Creating Quick Reports . . . 117
4.3.7. Assigning Policies . . . 118
4.3.8. Using Recovery Manager for Encrypted Volumes . . . 119
4.3.9. Clearing License Seats . . . 120
4.4. Managing Mobile Devices . . . 120
4.4.1. Adding Custom Users . . . 121
4.4.2. Adding Mobile Devices to Users . . . 123
4.4.3. Organizing Custom Users into Groups . . . 125
4.4.4. Checking the Mobile Devices Status . . . 127
4.4.5. Compliant and Not Compliant Mobile Devices . . . 128
4.4.6. Checking User and Mobile Devices Details . . . 129
4.4.7. Sorting, Filtering and Searching for Mobile Devices . . . 132
4.4.8. Running Tasks on Mobile Devices . . . 136
4.4.9. Creating Quick Reports . . . 142
4.4.10. Assigning Policies . . . 142
4.4.11. Synchronizing with Active Directory . . . 143
4.4.12. Deleting Users and Mobile Devices . . . 144
4.5. Application Inventory . . . 145
4.6. Viewing and Managing Tasks . . . 151
4.6.1. Checking Task Status . . . 151
4.6.2. Viewing Task Reports . . . 153
4.6.3. Restarting Tasks . . . 153
4.6.4. Stopping Exchange Scan Tasks . . . 154
4.6.5. Deleting Tasks . . . 154
4.7. Deleting Endpoints from Network Inventory . . . 155
4.8. Credentials Manager . . . 156
4.8.1. Operating System . . . 157
4.8.2. Virtual Environment . . . 158
4.8.3. Deleting Credentials from Credentials Manager . . . 158
5. Security Policies . . . 159
5.1. Managing Policies . . . 160
5.1.1. Creating Policies . . . 161
5.1.2. Assigning Policies . . . 162
5.1.3. Changing Policy Settings . . . 170
5.1.4. Renaming Policies . . . 171
5.1.5. Deleting Policies . . . 171
5.2. Computer and Virtual Machines Policies . . . 172
5.2.1. General . . . 172
5.2.2. HVI . . . 184

5.2.3. Antimalware . . . 190
5.2.4. Firewall . . . 214
5.2.5. Content Control . . . 224
5.2.6. Application Control . . . 236
5.2.7. Device Control . . . 241
5.2.8. Relay . . . 244
5.2.9. Exchange Protection . . . 246
5.2.10. Encryption . . . 274
5.2.11. NSX . . . 276
5.3. Mobile Device Policies . . . 277
5.3.1. General . . . 277
5.3.2. Device Management . . . 278
6. Monitoring Dashboard . . . 298
6.1. Refreshing Portlet Data . . . 299
6.2. Editing Portlet Settings . . . 299
6.3. Adding a New Portlet . . . 299
6.4. Removing a Portlet . . . 300
6.5. Rearranging Portlets . . . 300
7. Using Reports . . . 301
7.1. Report Types . . . 301
7.1.1. Computer and Virtual Machine Reports . . . 302
7.1.2. Exchange Server Reports . . . 308
7.1.3. Mobile Devices Reports . . . 311
7.2. Creating Reports . . . 313
7.3. Viewing and Managing Scheduled Reports . . . 316
7.3.1. Viewing Reports . . . 317
7.3.2. Editing Scheduled Reports . . . 317
7.3.3. Deleting Scheduled Reports . . . 318
7.4. Taking Report-Based Actions . . . 319
7.5. Saving Reports . . . 320
7.5.1. Exporting Reports . . . 320
7.5.2. Downloading Reports . . . 320
7.6. Emailing Reports . . . 321
7.7. Printing Reports . . . 321
7.8. Report Builder . . . 321
7.8.1. Query Types . . . 322
7.8.2. Managing Queries . . . 324
7.8.3. Viewing and Managing Reports . . . 329
8. Quarantine . . . 332
8.1. Exploring the Quarantine . . . 332
8.2. Computers and Virtual Machines Quarantine . . . 333
8.2.1. Viewing the Quarantine Details . . . 333
8.2.2. Managing the Quarantined Files . . . 334
8.3. Exchange Servers Quarantine . . . 338
8.3.1. Viewing the Quarantine Details . . . 338
8.3.2. Managing the Quarantined Objects . . . 340

9. User Activity Log 344
10. Notifications 346
10.1. Notification Types 346
10.2. Viewing Notifications 351
10.3. Deleting Notifications 352
10.4. Configuring Notification Settings 352
11. Getting Help 356
11.1. Bitdefender Support Center 356
11.2. Asking for Assistance 357
11.3. Using Support Tool 358
11.3.1. Using Support Tool on Windows Operating Systems 358
11.3.2. Using Support Tool on Linux Operating Systems 359
11.3.3. Using Support Tool on Mac Operating Systems 360
11.4. Contact Information 361
11.4.1. Web Addresses 361
11.4.2. Local Distributors 362
11.4.3. Bitdefender Offices 362
A. Appendices 365
A.1. Network Object Types and Statuses 365
A.1.1. Network Object Types 365
A.1.2. Network Object Statuses 366
A.2. Application File Types 367
A.3. Attachment Filtering File Types 367
A.4. System Variables 368
A.5. Application Control Tools 369
Glossary 371

Preface

- Create and manage company accounts for your customers.
- Manage the customer's network inventories in Control Center.
- Create and apply policies on managed endpoints.
- Run tasks and view security settings on network endpoints.
- Manage the quarantined items.
- Monitor network protection through the dashboard, reports and notifications.

This guide is intended for network administrators in charge with managing GravityZone protection within their organization's premises.

This document aims to explain how to apply and view security settings on network endpoints under your account using GravityZone Control Center. You will learn how to view your network inventory in Control Center, how to create and apply policies on managed endpoints, how to create reports, how to manage the quarantine items and how to use the dashboard.

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. vii)	This is an internal link, towards some location inside the document.

Appearance	Description
option	All the product options are printed using **bold** characters.
keyword	Interface options, keywords or shortcuts are highlighted using **bold** characters.

Admonitions

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

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

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

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

1. ABOUT GRAVITYZONE

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

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

GravityZone delivers multiple layers of security for endpoints and for Microsoft Exchange mail servers: antimalware with behavioral monitoring, zero day threat protection, application control and sandboxing, firewall, device control, content control, anti-phishing and antispam.

1.1. GravityZone Security Services

GravityZone provides the following security services:

- Security for Endpoints
- Security for Virtualized Environments
- Security for Exchange
- Security for Mobile
- Hypervisor Memory Introspection

Security for Endpoints

Protects unobtrusively any number of Windows, Linux and macOS laptops, desktops and servers by using top-ranked antimalware technologies. Additionally, Windows systems benefit of even more enhanced security with a two-way firewall, intrusion detection, web access control and filtering, sensitive data protection, application and device control. Low system usage ensures performance improvements, while integration with Microsoft Active Directory makes it easy to automatically apply protection to unmanaged desktops and servers. The solution provides an alternative to legacy antimalware systems by combining industry-acclaimed security technologies with simplicity of deployment and management through the powerful GravityZone Control Center. Proactive heuristics is employed to classify malicious processes based on their behavior, detecting new threats in real time.

Security for Virtualized Environments

GravityZone provides the first platform-agnostic security solution for the dynamic datacenters of today. Compliant with any known hypervisor, from VMware ESXi to Citrix Xen or Microsoft Hyper-V, Bitdefender Security for Virtualized Environments leverages the pooled nature of virtualization by offloading major security processes onto a centralized virtual appliance. Powered by cutting-edge caching technologies, the solution drives significant performance gains and boosts server consolidation by up to 30% compared to traditional antimalware.

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.

Hypervisor Memory Introspection (HVI)

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

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

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

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

Security for Mobile

Unifies enterprise-wide security with management and compliance control of iPhone, iPad and Android devices by providing reliable software and update distribution via Apple or Android marketplaces. The solution has been designed to enable controlled adoption of bring-your-own-device (BYOD) initiatives by enforcing usage policies consistently on all portable devices. Security features include screen lock, authentication control, device location, remote wipe, detection of rooted or jailbroken devices and security profiles. On Android devices the security level is enhanced with real-time scanning and removable media encryption. As a result, mobile devices are controlled and sensitive business information residing on them is protected.

1.2. GravityZone Architecture

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

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

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

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

The GravityZone solution includes the following components:

- GravityZone Virtual Appliance with the available roles:
  - Database

  - Update Server
  - Communication Server
  - Web Console (Control Center)
- Report Builder Virtual Appliance with the available roles:
  - Database
  - Processors
- Security Server
- HVI Supplemental Pack
- Security Agents

1.2.1. GravityZone Virtual Appliance

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

1.2.2. GravityZone Database

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

1.2.3. GravityZone Update Server

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

1.2.4. GravityZone Communication Server

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

1.2.5. Web Console (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, servers and mobile devices.

Powered by a Gravity Architecture, Control Center is capable of addressing the needs of even the largest organizations.

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

1.2.6. Report Builder

Report Builder allows to create and manage complex database interrogations named queries, using a high number of filters. The query-based reports can provide all information you need to understand any event or change that occurred in your network, at any time.

1.2.7. Security Server

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

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

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

1.2.8. HVI Supplemental Pack

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

1.2.9. 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
- Bitdefender Tools (vShield)
- GravityZone Mobile Client

Bitdefender Endpoint Security Tools

GravityZone ensures physical and virtual machines protection with Bitdefender Endpoint Security Tools, an intelligent environment-aware security agent capable to automatically self-configure according 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). Bitdefender Endpoint Security Tools is also available for Linux physical endpoints (servers and desktops).

Scanning Engines

The scanning engines are automatically set during Bitdefender Endpoint Security Tools packages creation, letting the endpoint agent detect the machine's configuration and adapt the scanning technology accordingly. 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 all signatures and engines stored locally.
2. **Hybrid Scan with Light Engines (Public Cloud)**, with a medium footprint, using in-the-cloud scanning and, partially, the local signatures. This scanning mode brings the benefit of better resources consumption, while involving off-premise scanning.

3. **Central Scan in Private Cloud**, with a small footprint requiring a Security Server for scanning. In this case, no signature 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 (Private Cloud scanning with Security Server) with fallback* on Local Scan (Full Engines)**
5. **Central Scan (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 be based on used engines.

Protection Modules

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

- Antimalware
- Advanced Threat Control
- Firewall
- Content Control
- Application Control
- Device Control
- Power User
- Volume Encryption

Antimalware

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

Bitdefender's antimalware scanning technology relies on the following protection layers:

- 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 suspected malware in a virtual environment to test its impact on the system and ensure it poses no threat. If a threat is detected, the program is prevented from running.

Advanced Threat Control

For threats that elude even the heuristic engine, a third 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.

Important
This module is available only for supported Windows desktop and server operating systems, except:

- Windows XP (64-bit)
- Windows Server 2003 / Windows Server 2003 R2 (32-bit, 64-bit)

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.

Important
This module is available only for supported Windows workstations, except legacy operating systems. For more information, refer to the GravityZone Installation Guide.

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.

Important
This module is available only for supported Windows workstations, except legacy operating systems. For more information, refer to the GravityZone Installation Guide.

Application Control

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

Important
This module is available only for supported Windows desktop and server operating systems, except:

- Windows Vista
- Windows Server 2008
- Windows legacy operating systems. For more information, refer to the GravityZone Installation Guide.

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.).

Important
This module is available only for supported Windows desktop and server operating systems, except legacy ones. For more information, refer to the GravityZone Installation Guide.

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, except legacy ones. For more information, refer to the GravityZone Installation Guide.

Volume Encryption

The Volume Encryption module allows you to provide full disk encryption by managing BitLocker on Windows machines. You can encrypt and decrypt boot and non-boot volumes, with just one click, while GravityZone handles the entire process, with minimal intervention from the users. Additionally, GravityZone stores the recovery keys needed to unlock volumes when the users forget their passwords.

Note
This module is available on certain Windows operating systems. For the Encryption module requirements, refer to GravityZone Installation Guide.
The Encryption feature may be available for your GravityZone solution with a separate license key.

Endpoint Roles

Relay Role

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:

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

Exchange Protection Role

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.

Endpoint Security for Mac

Endpoint Security for Mac is a powerful antimalware scanner, which can detect and remove all kinds of malware, including viruses, spyware, Trojan horses, keyloggers, worms and adware on Intel-based Macintosh workstations and laptops with OS X Mountain Lion version 10.8.5 or later.

Endpoint Security for Mac includes only the Antimalware and Encryption modules. The scanning technology available is **Local Scan**, with all signatures and engines stored locally. The Encryption module allows you to provide full disk encryption by managing FileVault, with GravityZone handling the entire process.

Note
The Encryption module may be available in your GravityZone solution with a separate license key.

Bitdefender Tools (vShield)

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

- Allows you to run Memory and Process Scan tasks on the machine.

- Informs the user about the detected infections and actions taken on them.
- Adds more options for antimalware scan exclusions.

GravityZone Mobile Client

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

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

2. GETTING STARTED

GravityZone solutions can be configured and managed via a centralized management platform named Control Center. Control Center has a web-based interface, which you can access by means of username and password.

2.1. Connecting to Control Center

Access to Control Center is done via user accounts. You will receive your login information by email once your account has been created.

Prerequisites:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Recommended screen resolution: 1024x768 or higher
- The computer you connect from must have network connectivity to Control Center.

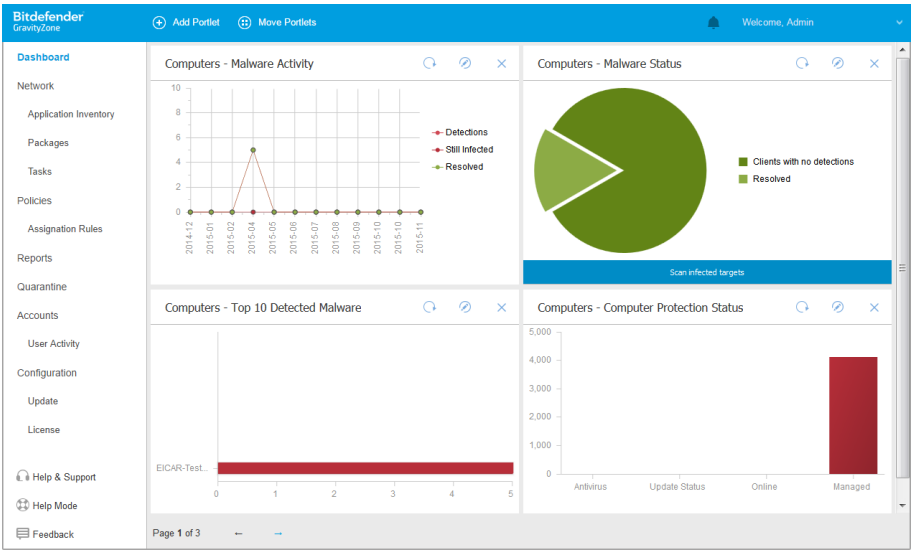
To connect to Control Center:

1. In the address bar of your web browser, enter the IP address or the DNS hostname of the Control Center appliance (using the `https://` prefix).
2. Enter your user name and password.
3. Click **Login**.

Note
If you have forgotten your password, use the password recovery link to receive a new password. You must provide the email address of your account.

2.2. Control Center at a Glance

Control Center is organized so as to allow easy access to all the features. Use the menu bar at the right side to navigate through the console. Available features depend on the type of user accessing the console.



The Dashboard

2.2.1. Control Center Overview

Users with company administrator role have full privileges over the Control Center configuration and network security settings, while users with administrator role have access to network security features, including users management.

According to their role, GravityZone administrators can access the following sections from the menu bar:

Dashboard
View easy-to-read charts providing key security information concerning your network.

Network
Install protection, apply policies to manage security settings, run tasks remotely and create quick reports.

Policies
Create and manage security policies.

Reports
Get security reports concerning the managed clients.

Quarantine

Remotely manage quarantined files.

Accounts

Manage the access to Control Center for other company employees.

Under this menu you can also find the **User Activity** page, which allows accessing the user activity log.

Note
This menu is available only to users with the **Manage Users** right.

Configuration

Configure Control Center settings, such as mail server, integration with Active Directory or virtualization environments and security certificates.

Note
This menu is available only to users with the **Manage Solution** right.

By clicking your username in the upper-right corner of the console, the following options are available:

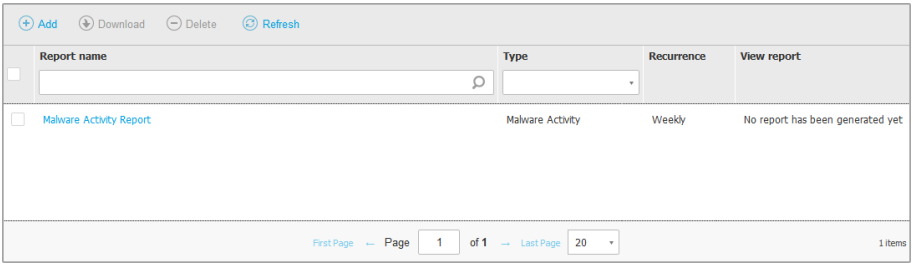
- **My Account**. Click this option to manage your user account details and preferences.
- **Credentials Manager**. Click this option to add and manage the authentication credentials required for remote installation tasks.
- **Help & Support**. Click this option to find help and support information.
- **Feedback**. Click this option to display a form allowing you to edit and send your feedback messages regarding your experience with GravityZone.
- **Logout**. Click this option to log out of your account.

Additionally, in the upper-right corner of the console, you can find:

- The **Help Mode** icon, which enables expandable tooltip boxes placed on Control Center items. You can easily find out useful information regarding the Control Center features.
- The **Notifications** icon, which provides easy access to notification messages and also to the **Notifications** page.

2.2.2. Table Data

Tables are frequently used throughout the console to organize data into an easy-to-use format.



The Reports page

Navigating through Pages

Tables with more than 20 entries span on several pages. By default, only 20 entries are displayed per page. To move through the pages, use the navigation buttons at the bottom of the table. You can change the number of entries displayed on a page by selecting a different option from the menu next to the navigation buttons.

Searching for Specific Entries

To easily find specific entries, use the search boxes available below the column headers.

Enter the search term in the corresponding field. Matching items are displayed in the table as you type. To reset the table contents, clear the search fields.

Sorting Data

To sort data by a specific column, click the column header. Click the column header again to revert the sorting order.

Refreshing Table Data

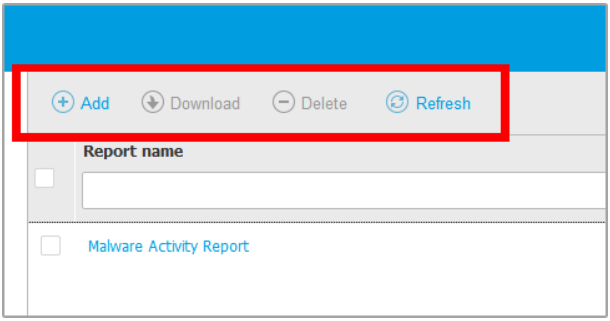
To make sure the console displays the latest information, click the **Refresh** button at the upper side of the table.

This may be needed when you spend more time on the page.

2.2.3. Action Toolbars

In Control Center, action toolbars allow you to perform specific operations pertaining to the section you are in. Each toolbar consists of a set of icons that is usually placed at the upper side of the table. For example, the action toolbar in the **Reports** section allows you to perform the following actions:

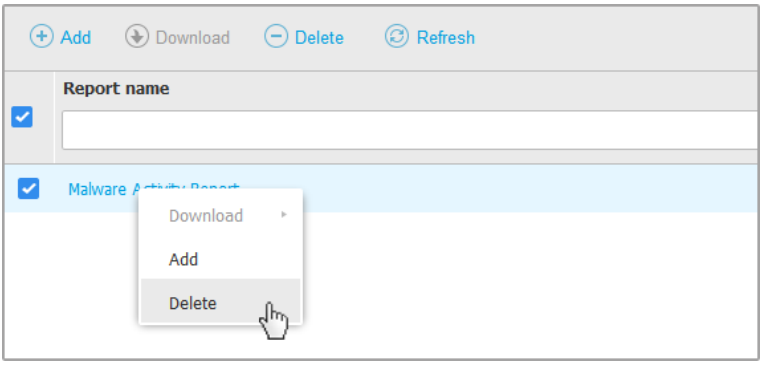
- Create a new report.
- Download a scheduled report.
- Delete a scheduled report.



The Reports page - Action Toolbar

2.2.4. Contextual Menu

The action toolbar commands are also accessible from the contextual menu. Right-click the Control Center section you are currently using and select the command that you need from the available list.



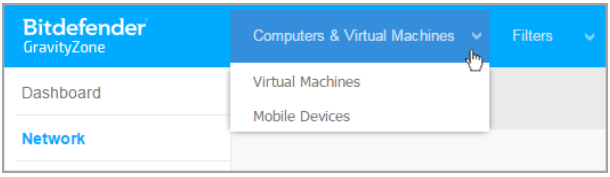
The Reports page - Contextual menu

2.2.5. Views Selector

If you work with different types of endpoints, you can find them organized in the **Network** page by type under several network views:

- **Computers & and Virtual Machines**: displays Active Directory groups and computers and also physical and virtual workstations outside Active Directory that are discovered in the network.
- **Virtual Machines**: displays the infrastructure of the virtual environment integrated with Control Center and all the containing virtual machines.
- **Mobile Devices**: displays users and the mobile devices assigned to them.

To select the network view that you want, click the views menu in the upper-right corner of the page.



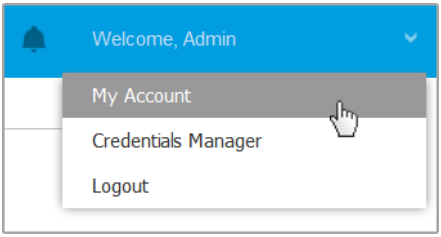
The Views Selector

Note
You will see only the endpoints you have permissions to view, permissions granted to you by the administrator who added your user to Control Center.

2.3. Managing Your Account

To check or change your account details and settings:

1. Click your username in the upper-right corner of the console and choose **My Account**.



The User Account menu

2. Under **Account Details**, correct or update your account details. If you use an Active Directory user account, you cannot change account details.
   - **Username.** The username is the unique identifier of a user account and cannot be changed.
   - **Full name.** Enter your full name.
   - **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
   - A **Change password** link allows you to change your login password.
3. Under **Settings**, configure the account settings according to your preferences.
   - **Timezone.** Choose from the menu the timezone of your account. The console will display time information according to the selected timezone.
   - **Language.** Choose from the menu the console display language.
   - **Session Timeout.** Select the inactivity time interval before your user session will expire.
4. Click **Save** to apply the changes.

Note
You cannot delete your own account.

2.4. Changing Login Password

After your account has been created, you will receive an email with the login credentials.

Unless you use Active Directory credentials to access Control Center, it is recommended to do the following:

- Change the default login password first time you visit Control Center.
- Change your login password periodically.

To change the login password:

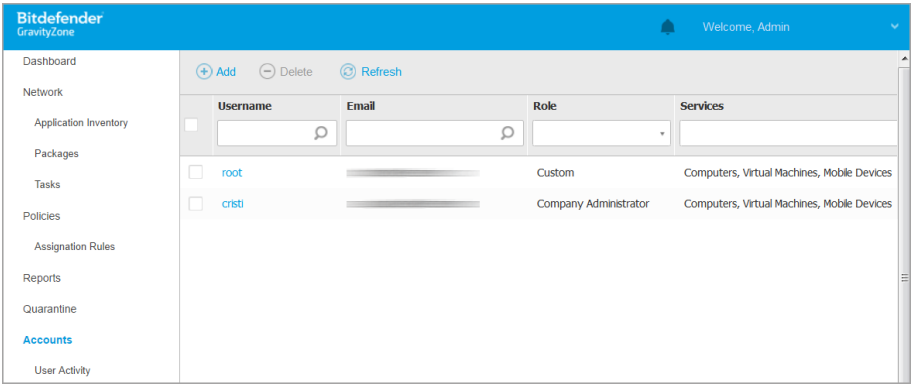
1. Click your username in the upper-right corner of the console and choose **My Account**.
2. Under **Account Details**, click **Change password**.
3. Enter your current password and the new password in the corresponding fields.
4. Click **Save** to apply the changes.

3. MANAGING USER ACCOUNTS

You can create the first GravityZone user account during the initial Control Center setup, after deploying the GravityZone appliance. The initial Control Center user account has company administrator role, with full rights over Control Center configuration and network management. From this account you can create all the other user accounts required for the management of your company's network.

This is what you need to know about GravityZone user accounts:

- To allow other employees of the company to access Control Center, you can create internal user accounts. You can assign user accounts with different roles, according to their access level in the company.
- For each user account, you can customize the access to GravityZone features or to specific parts of the network it belongs to.
- All accounts with the **Manage Users** right can create, edit and delete other user accounts.
- You can only manage accounts with equal privileges as your account, or lesser.
- You can create and manage user accounts in the **Accounts** page.



The Accounts page

Existing accounts are displayed in the table. For each user account, you can view:

– The username of the account (used to log in to Control Center).

- Email address of the account (used as a contact address). Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
- User role (company administrator / network administrator / reporter / custom).
- GravityZone security services the user is allowed to manage (Computers, Virtual Machines, Mobile Devices).

3.1. User Roles

A user role consists in a specific combination of user rights. When creating a user account, you can choose one of the predefined roles or you can create a custom role, by selecting certain user rights only.

Note
You can grant user accounts the same privileges as your account, or lesser.

The following user roles are available:

1. **Company Administrator** - Usually, a unique user account with Company Administrator role is created for each company, with full access to all management features of the GravityZone solutions. A company administrator configures the Control Center settings, manages the security services license keys, manages user accounts while also having administrative privileges over the company's network security settings. Company administrators can share or delegate their operational responsibilities to subordinate administrator and reporter user accounts.
2. **Network Administrator** - Several accounts with Network Administrator role can be created for a company, with administrative privileges over the company's entire security agents deployment or over a specific group of endpoints, including user management. Network Administrators are responsible for actively managing the network security settings.
3. **Reporter** - Reporter accounts are internal read-only accounts. They only allow access to reports and logs. Such accounts can be allocated to personnel with monitoring responsibilities or to other employees who must be kept up-to-date with security status.

4. **Custom** - Predefined user roles include a certain combination of user rights. If a predefined user role does not fit your needs, you can create a custom account by selecting only the rights that you are interested in.

The following table summarizes the relationships between different account roles and their rights. For detailed information, refer to "User Rights" (p. 23).

Account Role	Allowed Child Accounts	User Rights
Company Administrator	Company Administrators, Network Administrators, Reporters	Manage Solution Manage Company Manage Users Manage Networks Manage Reports
Network Administrator	Network Administrators, Reporters	Manage Users Manage Networks Manage Reports
Reporter	-	Manage Reports

3.2. User Rights

You can assign the following user rights to GravityZone user accounts:

- **Manage Solution**. Allows to configure Control Center settings (mail server and proxy settings, integration with Active Directory and virtualization platforms, security certificates and GravityZone updates). This privilege is specific to company administrator accounts.
- **Manage Users**. Create, edit or delete user accounts.
- **Manage Company**. Users can manage their own GravityZone license key and edit their company profile settings. This privilege is specific to company administrator accounts.
- **Manage Networks**. Provides administrative privileges over the network security settings (network inventory, policies, tasks, installation packages, quarantine). This privilege is specific to network administrator accounts.
- **Manage Reports**. Create, edit, delete reports and manage dashboard.

3.3. Creating User Accounts

Before creating a non-Active Directory user account, make sure you have the required email address at hand. The user will receive the GravityZone login details at the supplied email address.

To create a user account:

1. Go to the **Accounts** page.
2. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.
3. Under the **Details** section, fill in the account details.
   - You can either add a user from Active Directory (provided Active Directory integration is configured), or create a custom user.
     - To add a user from Active Directory, select **Import from Active Directory** option. You can then specify the user account in the **Username** field.

       When adding a user from Active Directory, user details are imported from Active Directory. The user will log in to Control Center using the Active Directory user password.

       Note
       - By default, Control Center is automatically synchronized with Active Directory by a specified interval. To make sure the latest Active Directory changes are imported in Control Center, click the **Synchronize** button.
       - Users with Manage Solution right can configure the Active Directory synchronization interval using the options available in the **Configuration > Active Directory** page. For more details, refer to **Installing Protection > GravityZone Installation and Setup >Configure Control Center Center Settings** chapter from the GravityZone Installation Guide.

     - To create a custom user, disable the **Import from Active Directory** option and fill in the user's username, email address, full name and password.

       Note
       - The password must contain at least one upper case character, at least one lower case character and at least one digit or special character.

- The email address must be unique. You cannot create another user account with the same email address.

4. Under the **Settings and Privileges** section, configure the following settings:
   - **Timezone**. Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
   - **Language**. Choose from the menu the console display language.
   - **Role**. Select the user's role. For details regarding the user roles, refer to "User Roles" (p. 22).
   - **Rights**. Each predefined user role has a certain configuration of rights. However, you can select only the rights that you need. In this case, the user role changes to **Custom**. For details regarding the user rights, refer to "User Rights" (p. 23).
   - **Select Targets**. Select the network groups the user will have access to for each available security service. You can restrict the user access to a certain GravityZone security service or to specific areas of the network.

     Note
     The target selection options will not be displayed for users with Manage Solution right, which, by default, have privileges over the entire network and security services.

     Important
     Whenever you make changes to your network structure, or when setting up a new integration with another vCenter Server or XenServer system, remember to also review and update access privileges for existing users.

5. Click **Save** to add the user. The new account will appear in the user accounts list.

   Control Center automatically sends the user an email with the login details, provided the mail server settings have been properly configured. For more details regarding the mail server configuration, refer to **Installing Protection > GravityZone Installation and Setup >Configure Control Center Center Settings** chapter from the GravityZone Installation Guide.

3.4. Editing Accounts

Edit accounts to keep account details up to date or to change account settings.

To edit a user account:

1. Log in to Control Center.
2. Go to the **Accounts** page.
3. Click the user's name.
4. Change account details and settings as needed.
5. Click **Save** to apply the changes.

Note
All accounts with the **Manage Users** right can create, edit and delete other user accounts. You can only manage accounts with equal privileges as your own account, or lesser.

3.5. Deleting Accounts

Delete accounts when they are no longer needed. For example, if the account owner is no longer with the company.

To delete an account:

1. Log in to Control Center.
2. Go to the **Accounts** page.
3. Select the account from the list.
4. Click the ⊖ **Delete** button at the upper side of the table.

   You will have to confirm your action by clicking **Yes**.

3.6. Resetting Login Passwords

Accounts owners who forget their password can reset it by using the password recovery link on the login page. You can also reset a forgotten login password by editing the corresponding account from the console.

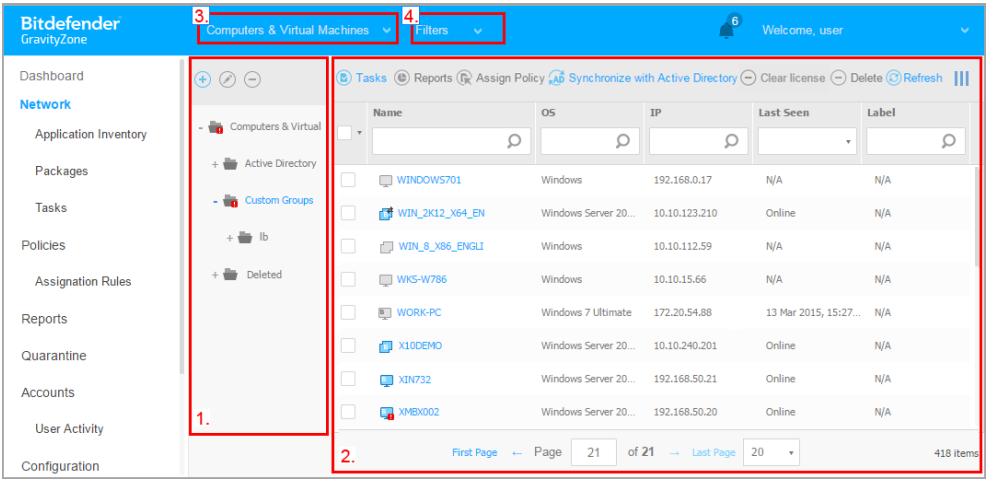
To reset the login password for a user:

1. Log in to Control Center.
2. Go to the **Accounts** page.

3. Click the user's name.
4. Type a new password in the corresponding fields (under **Details**).
5. Click **Save** to apply the changes. The account owner will receive an email with the new password.

4. MANAGING NETWORK OBJECTS

The **Network** page provides several features for exploring and managing each type of network object available in Control Center (computers, virtual machines and mobile devices). The **Network** section consists of a two-pane interface displaying the real-time status of network objects:



The Network Page

1. The left-side pane displays the available network tree. According to the selected network view, this pane displays the network infrastructure integrated with Control Center such as Active Directory, vCenter Server or Xen Server.

   At the same time, all computers and virtual machines detected in your network that do not belong to any integrated infrastructure are displayed under **Custom Groups**.

   All deleted endpoints are stored under the **Deleted** folder. To learn more, refer to "Deleting Endpoints from Network Inventory" (p. 155).

   Note
   You can view and manage only the groups on which you have administrator rights.

2. The right-side pane displays the contents of the group you have selected in the left-side pane. This pane consists of a grid, where the rows contain network objects and the columns display specific information for each type of object.

   From this pane, you can do the following:

   - View detailed information about each network object under your account. You can view the status of each object by checking the icon next to its name. Move the mouse cursor over the icon to view tooltip information. Click the object's name to display a window containing more specific details.

     Each type of object, such as computer, virtual machine or folder is represented by a specific icon. At the same time, each network object may have a certain status, regarding the management state, security issues, connectivity and so on. For details regarding the description of each network object icon and the available statuses, refer to "Network Object Types and Statuses" (p. 365).
   - Use the Action Toolbar at the upper side of the table to carry out specific operations for each network object (such as run tasks, create reports, assign policies and delete) and refresh table data.
3. The views selector on the upper side of the network panes allows switching between different network inventory contents, according to the endpoint type you want to work with.
4. The **Filters** menu available at the upper side of the network panes helps you easily display only specific network objects, providing several filter criteria. The **Filters** menu options are related to the currently selected network view.

From the **Network** section you can also manage the installation packages and the tasks for each type of network object.

Note
To find out more about installation packages, refer to the GravityZone Installation Guide.

For detailed information, refer to:

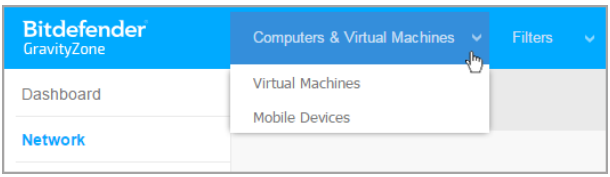
- "Working with Network Views" (p. 30)
- "Managing Computers" (p. 33)
- "Managing Virtual Machines" (p. 73)
- "Managing Mobile Devices" (p. 120)
- "Viewing and Managing Tasks" (p. 151)
- "Deleting Endpoints from Network Inventory" (p. 155)

- "Credentials Manager" (p. 156)

4.1. Working with Network Views

The different types of endpoints available in Control Center are grouped in the **Network** page by different network views. Each network view displays a specific type of network infrastructure, according to the endpoint type you want to manage.

To change the network view, go to the upper-left side of the **Network** page and click the views selector:



The Views Selector

The following network views are available:

- Computers and Virtual Machines
- Virtual Machines
- Mobile Devices

4.1.1. Computers and Virtual Machines

This view is designed for computers and virtual machines integrated in Active Directory, providing specific actions and filtering options for managing the computers in your network. If an Active Directory integration is available, the Active Directory tree is loaded, together with the corresponding endpoints.

While working in the **Computers and Virtual Machines** view, you can anytime synchronize the Control Center contents with your Active Directory using the **Synchronize with Active Directory** button from the Action Toolbar.

At the same time, all computers and virtual machines that are not integrated in Active Directory are grouped under Custom Groups. This folder may contain the following types of endpoints:

- Computers and virtual machines available in your network outside Active Directory.

- Virtual Machines from a virtualized infrastructure available in your network.
- Security Servers already installed and configured on a host in your network.

Note
When a virtualized infrastructure is available, you can deploy and manage Security Servers from the **Virtual Machines** view. Otherwise, Security Servers can only be installed and configured locally on the host.

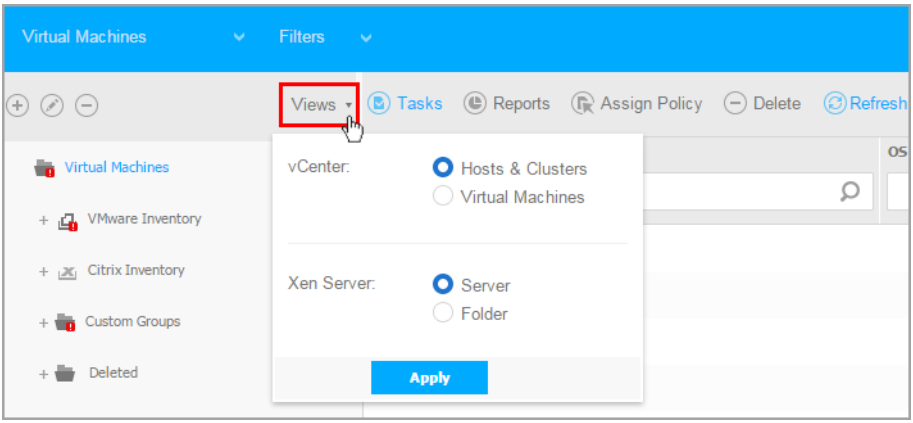
Important
Assigning policies to virtual machines from **Computers and Virtual Machines** view may be restricted by the GravityZone solution manager while configuring the vCenter Server or a Xen Server in the **Configuration > Virtualization** page. To find out more, refer to **Installing Protection > GravityZone Installation and Setup** chapter from the GravityZone Installation Guide.

4.1.2. Virtual Machines

This view is specifically designed to display your virtualized infrastructure integrations. The filter options available in this view allow you to choose special criteria for displaying virtual environment entities.

You can view your VMware or Citrix virtual inventories in the left pane.

On the upper-side of the left pane you can also find the **Views** menu, allowing you to choose the virtual inventories display mode.



The Network page - Virtual Machines Views

All virtual machines in your network that are not integrated in a virtual infrastructure are displayed under **Custom Groups**.

To access the virtualized infrastructure integrated with Control Center, you must provide your user credentials for each vCenter Server system available. Control Center uses your credentials to connect to the virtualized infrastructure, displaying only resources you have access to (as defined in vCenter Server). If you have not specified your authentication credentials, you will be required to enter them when you try to browse the inventory of any vCenter Server. Once you have entered your credentials, they are saved to your Credentials Manager so that you do not need to enter them the next time.

4.1.3. Mobile Devices

This view is exclusively designed for viewing and managing mobile devices available in your network, providing specific actions and filtering options.

In this specific view, you can display network entities by users or by devices.

The network pane displays your Active Directory tree structure, if available. In this case, all Active Directory users will appear in your network inventory, and also the mobile devices assigned to them.

Note
Active Directory user details are automatically loaded and cannot be changed.

Custom Groups contains all mobile device users that you have manually added to Control Center.

4.2. Managing Computers

To view the computers under your account, go to the **Network** page and choose **Computers and Virtual Machines** from the views selector.

You can view the available network structure in the left-side pane and details about each endpoint in the right-side pane.

At first, all computers and virtual machines detected in your network are displayed as unmanaged so that you can remotely install protection on them.

To customize the computer details displayed in the table:

1. Click the **Columns** button at the right side of the Action Toolbar.
2. Select the columns you want to view.
3. Click the **Reset** button to return to the default columns view.

From the **Network** page, you can manage computers as follows:

- Check the computer status
- View computer details
- Organize computers into groups
- Sort, filter and search
- Run tasks
- Create quick reports
- Assign policies
- Synchronize with Active Directory

To view the latest information in the table, click the **Refresh** button in the bottom-left corner of the table. This may be needed when you spend more time on the page.

4.2.1. Checking the Computers Status

Each computer is represented in the network page by an icon specific to its type and status.

Refer to "Network Object Types and Statuses" (p. 365) for a list with all available icon types and statuses.

For detailed status information, refer to:

- Management Status

- Connectivity Status
- Security Status

Management Status

Computers can have the following management statuses:

- **Managed** - computers on which the security agent is installed.
- **Pending restart** - endpoints that require a system restart after installing or updating Bitdefender protection.
- **Unmanaged** - detected computers on which the security agent has not been installed yet.
- **Deleted** - computers that you have deleted from Control Center. For more information, refer to "Deleting Endpoints from Network Inventory" (p. 155).

Connectivity Status

The connectivity status concerns only the managed computers. From this viewpoint, managed computers can be:

- **Online**. A blue icon indicates that the computer is online.
- **Offline**. A grey icon indicates that the computer is offline.

A computer is offline if the security agent is inactive for more than 5 minutes. Possible reasons why computers appear offline:

- The computer is shut down, sleeping or hibernating.

  Note
  Computers appear online even when they are locked or the user is logged off.

- The security agent does not have connectivity with the GravityZone Communication Server:
  - The computer might be disconnected from the network.
  - A network firewall or router might block the communication between the security agent and the GravityZone Communication Server.
  - The computer is behind a proxy server and the proxy settings have not been properly configured in the applied policy.

Warning
For computers behind a proxy server, the proxy settings must be properly configured in the security agent installation package, otherwise the computer will not communicate with GravityZone console and will always appear offline, no matter if a policy with the proper proxy settings is applied after installation.

- The security agent might not be working properly.

To find out for how long computers have been inactive:

1. Display only the managed computers. Click the **Filters** menu located at the upper side of the table, select all the "Managed" options that you need from the **Security** tab, choose **All items recursively** from the **Depth** tab and click **Save**.
2. Click the **Last Seen** column header to sort computers by inactivity period.

You can ignore shorter periods of inactivity (minutes, hours) as they are likely the result of a temporary condition. For example, the computer is currently shut down.

Longer inactivity periods (days, weeks) usually indicate a problem with the computer.

Note
It is recommended to refresh the network table from time to time, to update the endpoints information with the latest changes.

Security Status

The security status concerns only the managed computers. You can identify computers with security issues by checking the status icons displaying a warning symbol:

- Computer managed, with issues, online.
- Computer managed, with issues, offline.

A computer has security issues provided at least one of the following situations applies:

- Antimalware protection is disabled.
- The license has expired.
- The security agent product is outdated.
- Antimalware signatures are outdated.
- Malware is detected.

- The connection with Bitdefender Cloud Services could not be established, due to the following possible reasons:
  - The computer has internet connectivity issues.
  - A network firewall is blocking the connection with Bitdefender Cloud Services.
  - Port 443, required for the communication with Bitdefender Cloud Services, is closed.

  In this case, the antimalware protection relies solely on local engines, while in-the-cloud scanning is off, meaning that the security agent cannot provide full real-time protection.

If you notice a computer with security issues, click its name to display the **Information** window. You can identify the security issues by the ! icon. Make sure to check for security information in all the information page's tabs. Display the icon's tooltip to find out more details. Further local investigations may be needed.

Note
It is recommended to refresh the network table from time to time, to update the endpoints information with the latest changes.

4.2.2. Viewing Computer Details

You can obtain detailed information about each computer from the **Network** page, such as OS, IP and last seen date.

To find out details about a computer:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group that you want from the left-side pane.

   All endpoints available in the selected group are displayed in the right-side pane table.
4. You can easily identify the computer status by checking the corresponding icon. For detailed information, refer to "Checking the Computers Status" (p. 33).
5. Check the information displayed on columns for each computer:
   - **Name**: endpoint name.
   - **FQDN**: fully qualified domain name that includes the hostname and domain name.
   - **OS**: operating system installed on the endpoint.
   - **IP**: endpoint's IP address.

- **Last Seen**: date and time when the endpoint has last been seen online.

  Note
  It is important to monitor the **Last Seen** field as long inactivity periods might indicate a communication issue or a disconnected computer.

- **Label**: a custom string with additional information about the endpoint.

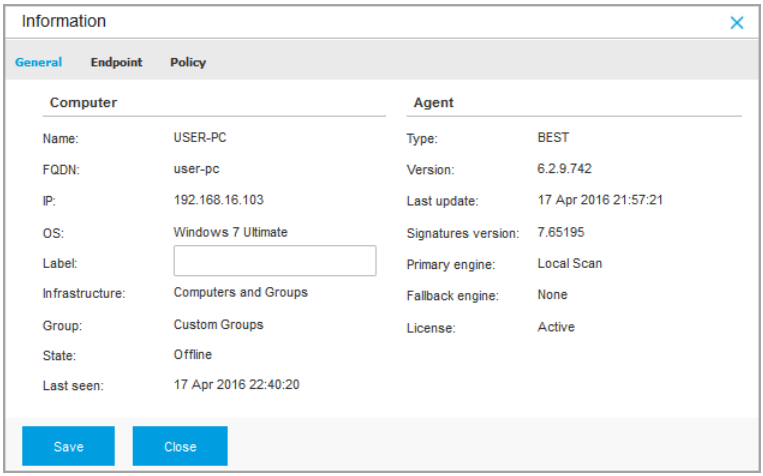
Click the **Columns** button at the upper-right side of the pane and then add or remove columns to customize the displayed information according to your needs.

6. Click the name of the computer you are interested in to view more details in the **Information** window. Details are grouped in tabs as follows:
   - In the **General** tab you can find:
     - General computer information, such as name, FQDN information, IP address, operating system, infrastructure, parent group and current connection status.

       Here you can assign the computer with a label to help you in computer searching.
     - License status for each installed Bitdefender protection layer.

       Note
       Additional information on the protection layers is available in the **Protection** tab.

     - The name, IP and label of the relay to which the endpoint is connected, if the case.



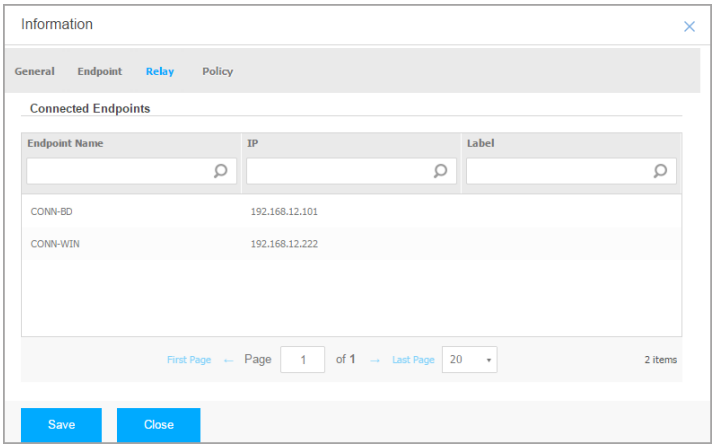
Information window - General tab

- In the **Protection** tab you can find details for each protection layer installed on the endpoint. Details refer to:
  - Security agent information like product name and version, scanning engines configuration and update status. For Exchange Protection, antispam engine and signatures versions are also available.
  - Assigned Security Server. They are displayed in case of agentless deployments or when scanning engines of the security agents are set to use remote scan. Security Server information helps you identify the virtual appliance and get its update status.
  - The protection modules status. You can easily view which protection modules have been installed on the endpoint and also the status of available modules (**On / Off**) set via the applied policy.
  - A quick overview regarding the modules activity and malware reporting in the current day.

    Click the **View** link to access the report options and then generate the report. For more information, refer to "Creating Reports" (p. 313)
  - Additional information regarding the Encryption module, such as:
    - Detected volumes (mentioning the boot drive).

- Encryption status (which may be **Encrypted**, **Encryption in progress**, **Unencrypted**). Click the **Recovery** link to retrieve the recovery key for the associated encrypted volume. For details about retrieving the recovery keys, refer to "Using Recovery Manager for Encrypted Volumes" (p. 71).

- The **Relay** tab is available only for endpoints with relay role. This tab displays information about the endpoints connected to the current relay, such as name, IP and label.



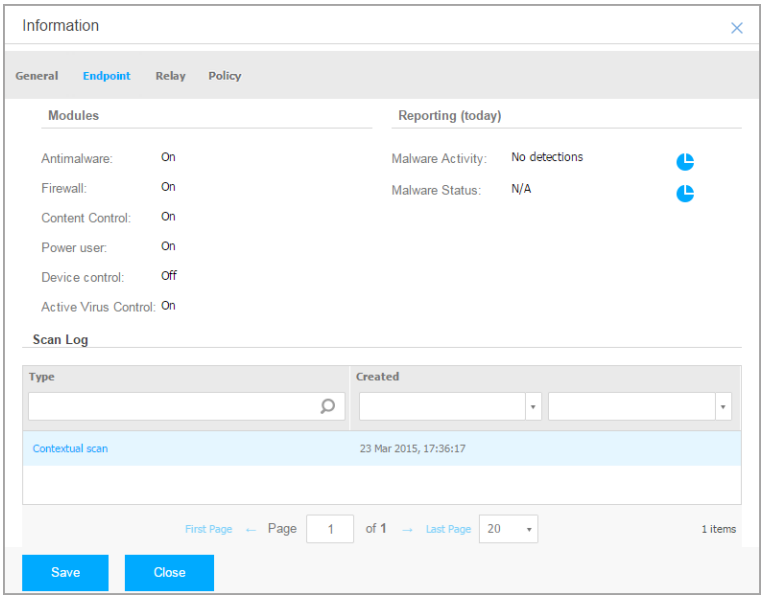
Information window - Relay tab

- The **Scan logs** tab displays detailed information about all scan tasks performed on the endpoint.

  Logs are grouped by protection layer and you can choose from the drop-down menu for which layer to display logs.

  Click the scan task you are interested in and the log will open in a new page of the browser.

  When many scan logs are available, they may span through several pages. To move through the pages, use the navigation options at the bottom of the table. If there are too many entries, you can use the filter options available at the top of the table.

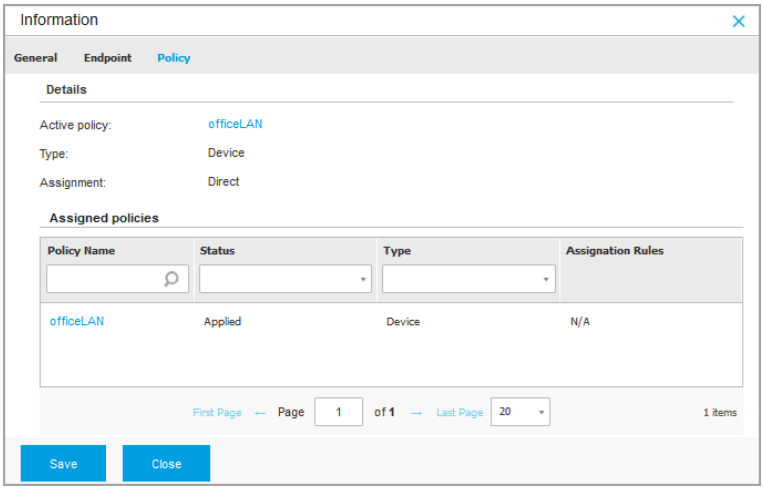


Information window - Scan logs tab

- In the **Policy** tab, you can find:
  - Information regarding the active policy on the endpoint. An active policy is one of the assigned policies, which is effective at that moment.

    For example, a laptop has assigned two location-aware policies: one named `Office`, which is active when it connects to the company's LAN, and `Roaming`, which becomes active when the user works remotely and connects to other networks.

    Click the active policy name to open the policy template and view its settings. When the policy is assigned by a rule, click the assignment to view and/or edit the rule settings.
  - Details about the assigned policies. Click the policy name to view the details. Click the assignment rule to view the settings and/or modify them.



Information window - Policy tab

Each property in this window which is generating security issues is marked with the ! icon. Check the icon's tooltip to find out more details. Further local investigations may be needed.

4.2.3. Organizing Computers into Groups

You can manage computer groups in the left-side pane of the **Network** page.

A major benefit of this feature is that you can use group policies to meet different security requirements.

Computers imported from Active Directory are grouped under the **Active Directory** folder. You cannot edit the Active Directory groups. You can only view and manage the corresponding computers.

All non-Active Directory computers discovered in your network are placed under **Custom Groups**, where you can organize them into groups as you want. Under **Custom Groups** you can create, delete, rename and move computer groups within a custom-defined tree structure.

Note

- A group can contain both computers and other groups.

- When selecting a group in the left-side pane, you can view all computers except for those placed into its sub-groups. To view all computers included in the group and in its sub-groups, click the **Filters** menu located at the upper side of the table and select **All items recursively** in the **Depth** section.

Creating Groups

Before you start creating groups, think of the reasons why you need them and come up with a grouping scheme. For example, you can group endpoints based on one or a mix of the following criteria:

- Organization structure (Sales, Marketing, Quality Assurance, Software Development, Management etc.).
- Security needs (Desktops, Laptops, Servers, etc.).
- Location (Headquarter, Local Offices, Remote Workers, Home Offices etc.).

To organize your network into groups:

1. Select **Custom Groups** in the left-side pane.
2. Click the ⊕ **Add group** button at the upper-side of the left-side pane.
3. Enter a suggestive name for the group and click **OK**. The new group will appear under the **Custom Groups** folder.

Renaming Groups

To rename a group:

1. Select the group in the left-side pane.
2. Click the ✎ **Edit group** button at the upper-side of the left-side pane.
3. Enter the new name in the corresponding field.
4. Click **OK** to confirm.

Moving Groups and Computers

You can move entities to **Custom Groups** anywhere inside the group hierarchy. To move an entity, drag and drop it from the right-side pane to the group that you want in the left-side pane.

Note

The entity that is moved will inherit the policy settings of the new parent group, unless a different policy has been directly assigned to it. For more information about policy inheritance, refer to "Security Policies" (p. 159).

Deleting Groups

Deleting a group is a final action. As a result, the security agent installed on the targeted endpoint will be removed.

To delete a group:

1. Click the empty group in the left-side pane of the **Network page**.
2. Click the **Remove group** button at the upper-side of the left-side pane. You will have to confirm your action by clicking **Yes**.

4.2.4. Sorting, Filtering and Searching for Computers

Depending on the number of endpoints, the right-side pane table can span through several pages (only 20 entries are displayed per page by default). To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

If there are too many entries, you can use the search boxes under the column headers or the **Filters** menu at the upper side of the page to display only the entities you are interested in. For example, you can search for a specific computer or choose to view only the managed computers.

Sorting Computers

To sort data by a specific column, click the column headers. For example, if you want to order computers by name, click the **Name** heading. If you click the heading again, the computers will be displayed in reverse order.

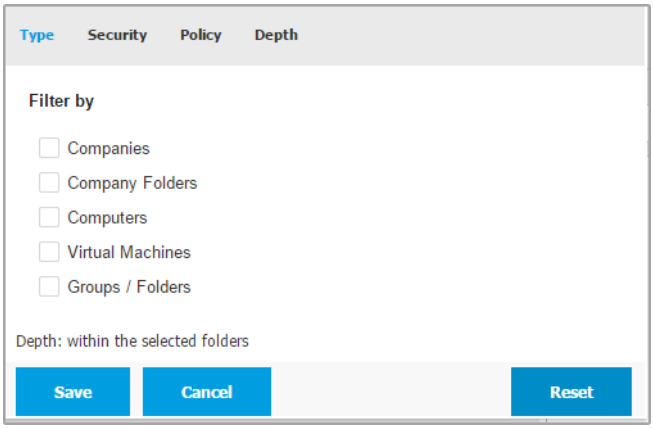
Sorting Computers

Filtering Computers

To filter your network entities, use the **Filters** menu from the upper-side of the network panes area.

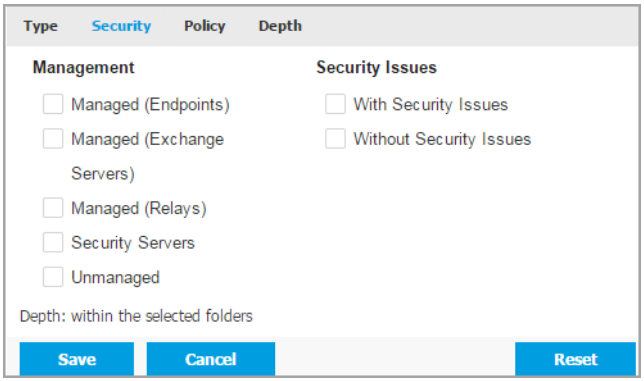
1. Select the group that you want in the left-side pane.
2. Click the **Filters** menu at the upper-side of the network panes area.
3. Use the filter criteria as follows:

- **Type**. Select the type of entities you want to display (computers, virtual machines, folders).



Computers - Filter by Type

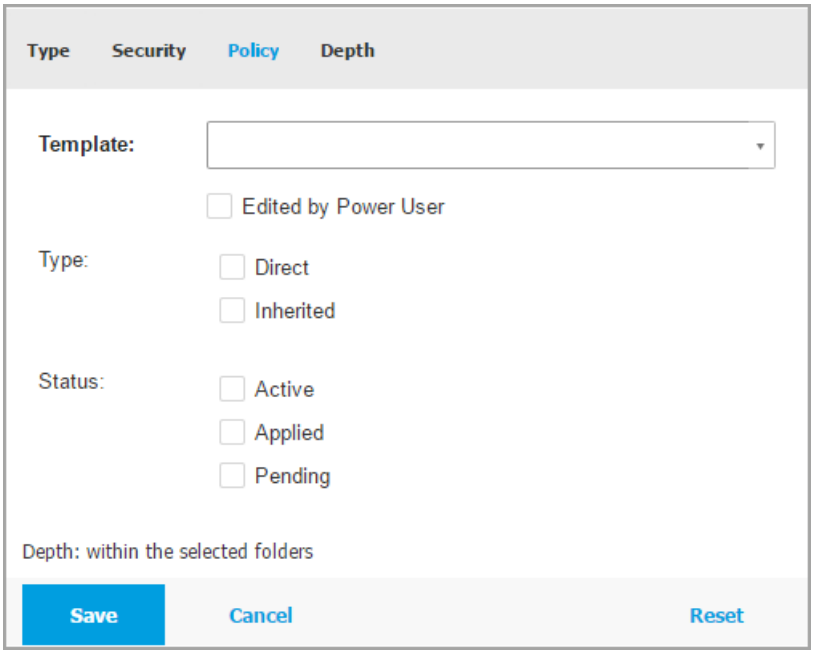
- **Security**. Choose to display computers by protection management and security status.



Computers - Filter by Security

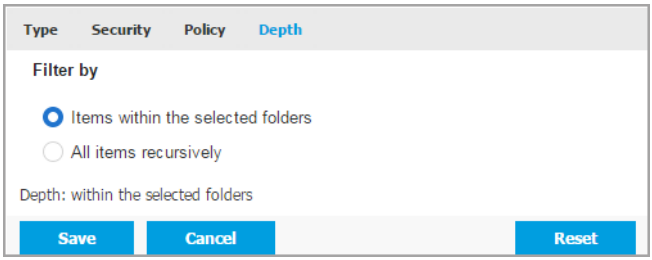
- **Policy**. Select the policy template you want to filter the computers by, the policy assignment type (Direct or Inherited), as well as the policy assignment

status (Active, Applied or Pending). You can also choose to display only entities with policies edited in the Power User mode.



Computers - Filter by Policy

- **Depth**. When managing a tree-structured network, computers placed in sub-groups are not displayed when selecting the root group. Select **All items recursively** to view all the computers included in the current group and all its sub-groups.



Computers - Filter by Depth

When choosing to view all items recursively, Control Center displays them in a plain list. To find the location of an item, select the item you are interested in, and then click the **Go to container** button at the upper side of the table. You will be redirected to the parent container of the selected item.

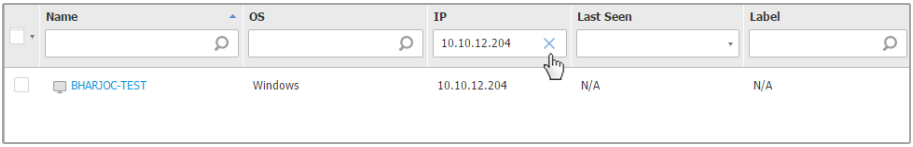
Note
You can view all selected filter criteria in the lower part of the **Filters** window. If you want to clear all filters, click the **Reset** button.

4. Click **Save** to filter the computers by the selected criteria. The filter remains active in the **Network** page until you log out or reset the filter.

Searching for Computers

1. Select the desired group in the left-side pane.
2. Enter the search term in the corresponding box under the column headers from the right-side pane. For example, enter the IP of the computer you are looking for in the **IP** field. Only the matching computer will appear in the table.

   Clear the search box to display the full list of computers.



Search for computers

4.2.5. Running Tasks

From the **Network** page, you can remotely run a number of administrative tasks on computers.

This is what you can do:

- “Scan” (p. 47)
- “Exchange Scan” (p. 56)
- “Install” (p. 59)
- “Uninstall Client” (p. 64)
- “Update Client” (p. 65)
- “Reconfigure Client” (p. 66)
- “Restart Machine” (p. 67)
- “Network Discovery” (p. 68)
- “Applications Discovery” (p. 68)
- “Update Security Server” (p. 69)

You can choose to create tasks individually for each computer or for groups of computers. For example, you can remotely install the security agent on a group of unmanaged computers. At a later time, you can create a scan task for a certain computer from the same group.

For each computer, you can only run compatible tasks. For example, if you select an unmanaged computer, you can only choose to install the security agent, all the other tasks being disabled.

For a group, the selected task will be created only for compatible computers. If none of the computers in the group is compatible with the selected task, you will be notified that the task could not be created.

Once created, the task will start running immediately on the online computers. If a computer is offline, the task will run as soon as it gets back online.

You can view and manage the task in the **Network > Tasks** page. For more information, refer to “Viewing and Managing Tasks” (p. 151).

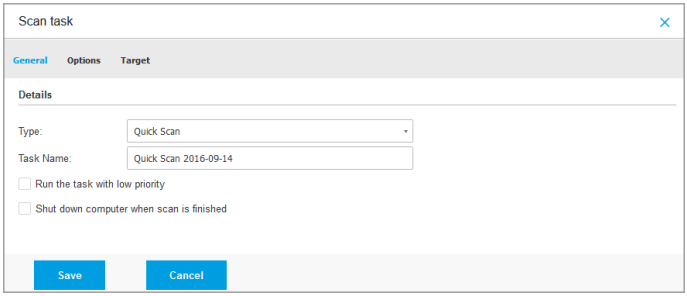
Scan

To remotely run a scan task on one or several computers:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.

3. Select the container that you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
4. Select the check boxes of computers or groups you want to scan.
5. Click the **Tasks** button at the upper side of the table and choose **Scan**.

   A configuration window will appear.
6. Configure the scan options:
   - In the **General** tab, you can choose the type of scan and you can enter a name for the scan task. The scan task name is intended to help you easily identify the current scan in the **Tasks** page.



Computers Scan task - Configuring general settings

Select the type of scan from the **Type** menu:

- **Quick Scan** uses in-the-cloud scanning to detect malware running in the system. This type of scan is preconfigured to allow scanning only critical Windows and Linux system locations. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

  When malware or rootkits are found, Bitdefender automatically proceeds with disinfection. If, for any reason, the file cannot be disinfected, then it is moved to quarantine. This type of scanning ignores suspicious files.
- **Full Scan** checks the entire system for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

  Bitdefender automatically tries to disinfect files detected with malware. In case malware cannot be removed, it is contained in quarantine, where it cannot do any harm. Suspicious files are being ignored. If you want to

take action on suspicious files as well, or if you want other default actions for infected files, then choose to run a Custom Scan.

- **Memory Scan** checks the programs running in the computer's memory.
- **Network Scan** is a type of custom scan, allowing to scan network drives using the Bitdefender security agent installed on the target endpoint.

  For the network scan task to work:

  - You need to assign the task to one single endpoint in your network.
  - You need to enter the credentials of a user account with read/write permissions on the target network drives, for the security agent to be able to access and take actions on these network drives. The required credentials can be configured in the **Target** tab of the tasks window.
- **Custom Scan** allows you to choose the locations to be scanned and to configure the scan options.

For memory, network and custom scans, you have also these options:

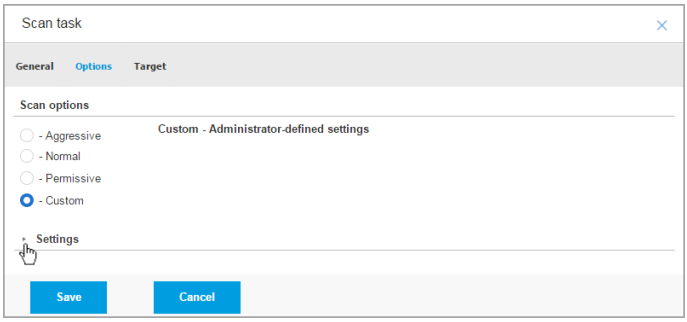
- **Run the task with low priority**. Select this check box to decrease the priority of the scan process and allow other programs to run faster. This will increase the time needed for the scan process to finish.
- **Shut down computer when scan is finished**. Select this check box to turn off your machine if you do not intend to use it for a while.

Note
These two options apply only to Bitdefender Endpoint Security Tools and Endpoint Security (legacy agent).

For custom scans, configure the following settings:

- Go to the **Options** tab to set the scan options. Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right-side of the scale to guide your choice.

  Based on the selected profile, the scan options in the **Settings** section are automatically configured. However, if you want to, you can configure them in detail. To do that, select the **Custom** check box and then expand the **Settings** section.



Computers Scan task - Configuring a Custom Scan

The following options are available:

- **File Types.** Use these options to specify which types of files you want to be scanned. You can set the security agent to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Note

  Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

  If you want only specific extensions to be scanned, choose **Custom extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

  Important

  Bitdefender security agents installed on Windows and Linux operating systems scan most of the .ISO formats, but does not take any action on them.

Computers scan task options - Adding custom extensions

- **Archives.** Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to scan archives in order to detect and remove any potential threat, even if it is not an immediate threat.

  Important
  Scanning archived files increases the overall scanning time and requires more system resources.

  – **Scan inside archives.** Select this option if you want to check archived files for malware. If you decide on using this option, you can configure the following optimization options:

    - **Limit archive size to (MB).** You can set a maximum accepted size limit of archives to be scanned. Select the corresponding check box and type the maximum archive size (in MB).
    - **Maximum archive depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.

  – **Scan email archives.** Select this option if you want to enable scanning of email message files and email databases, including file formats such as .eml, .msg, .pst, .dbx, .mbx, .tbb and others.

    Important
    Email archive scanning is resource intensive and can impact system performance.

- **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.
  - **Scan boot sectors.** Scans the system's boot sector. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
  - **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.
  - **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.
  - **Scan for keyloggers.** Select this option to scan for keylogger software.
  - **Scan network shares.** This option scans mounted network drives.

    For quick scans, this option is deactivated by default. For full scans, it is activated by default. For custom scans, if you set the security level to **Aggressive/Normal**, the **Scan network shares** option is automatically enabled. If you set the security level to **Permissive**, the **Scan network shares** option is automatically disabled.
  - **Scan memory.** Select this option to scan programs running in the system's memory.
  - **Scan cookies.** Select this option to scan the cookies stored by browsers on the computer.
  - **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
  - **Scan for Potentially Unwanted Applications (PUA).** A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express

installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

- **Scan detachable volumes.** Select this option to scan any removable storage drive attached to the computer.

- **Actions.** Depending on the type of detected file, the following actions are taken automatically:
  - **When an infected file is found.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies. The Bitdefender security agent can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

    By default, if an infected file is detected, the Bitdefender security agent will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

    Important
    For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

  - **When a suspect file is found.** Files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but the users must be aware of certain false positives (clean files detected as suspicious) in some cases. Suspect files cannot be disinfected, because no disinfection routine is available.

    Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine. Quarantined files are sent for analysis to Bitdefender Labs on a regular basis. If malware presence is confirmed, a signature is released to allow removing the malware.

- **When a rootkit is found.** Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

  Detected rootkits and hidden files are ignored by default.

Though not recommended, you can change the default actions. You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file. The following actions are available:

Disinfect
Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

Move files to quarantine
Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

Delete
Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Ignore
No action will be taken on detected files. These files will only appear in the scan log.

- Go to **Target** tab to configure the locations you want to be scanned on the target computers.

  In the **Scan target** section you can add a new file or folder to be scanned:

  a. Choose a predefined location from the drop-down menu or enter the **Specific paths** you want to scan.

  b. Specify the path to the object to be scanned in the edit field.

  - If you have chosen a predefined location, complete the path as needed. For example, to scan the entire `Program Files` folder, it suffices to select the corresponding predefined location from

the drop-down menu. To scan a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name.

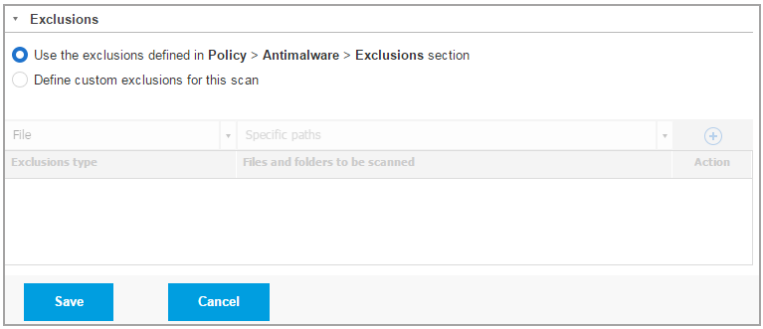
- If you have chosen **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers. For more information regarding system variables, refer to "System Variables" (p. 368).

c. Click the corresponding ⊕ **Add** button.

To edit an existing location, click it. To remove a location from the list, click the corresponding ⊗ **Delete** button.

For network scan tasks, you need to enter the credentials of a user account with read/write permissions on the target network drives, for the security agent to be able to access and take actions on these network drives.

Click the **Exclusions** sections if you want to define target exclusions.



Computers Scan Task - Defining Exclusions

You can either use the exclusions defined by policy or define explicit exclusions for the current scan task. For more details regarding exclusions, refer to "Exclusions" (p. 207).

7. Click **Save** to create the scan task. A confirmation message will appear.

You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Note
To schedule a scan task, go to the **Policies** page, select the policy assigned to the computers you are interested in, and add a scan task in the **Antimalware > On-Demand** section. For more information, refer to "On-Demand" (p. 197).

Exchange Scan

You can remotely scan the database of an Exchange Server by running an **Exchange Scan** task.

To be able to scan the Exchange database, you must enable on-demand scanning by providing the credentials of an Exchange administrator. For more information, refer to " Exchange Store Scanning " (p. 254).

To scan an Exchange Server database:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. From the left-side pane, select the group containing the target Exchange Server. You can find the server displayed in the right-side pane.

   Note
   Optionally, you can apply filters to quickly find the target server:
   - Click the **Filters** menu and select the following options: **Managed (Exchange Servers)** from the **Security** tab and **All items recursively** from the **Depth** tab.
   - Enter the server's hostname or IP in the fields from the corresponding column headers.

4. Select the check box of the Exchange Server whose database you want to scan.
5. Click the **Tasks** button at the upper side of the table and choose **Exchange Scan**. A configuration window will appear.
6. Configure the scan options:
   - **General.** Enter a suggestive name for the task.

     For large databases, the scan task may take a long time and may impact the server performance. In such cases, select the check box **Stop scan if it takes longer than** and choose a convenient time interval from the corresponding menus.
   - **Target.** Select the containers and objects to be scanned. You can choose to scan mailboxes, public folders or both. Beside emails, you can choose to scan other objects such as **Contacts**, **Tasks**, **Appointments** and **Post Items**. You can furthermore set the following restrictions to the content to be scanned:

- Only unread messages
- Only items with attachments
- Only new items, received in a specified time interval

For example, you can choose to scan only emails from user mailboxes, received in the last seven days.

Select the **Exclusions** check box, if you want to define scan exceptions. To create an exception, use the fields from the table header as follows:

a. Select the repository type from the menu.
b. Depending on the repository type, specify the object to be excluded:

Repository type	Object format
Mailbox	Email address
Public Folder	Folder path, starting from the root
Database	The database identity

Note
To obtain the database identity, use the Exchange shell command:
`Get-MailboxDatabase | fl name,identity`

You can enter only one item at a time. If you have several items of the same type, you must define as many rules as the number of items.

c. Click the ⊕ **Add** button at the upper side of the table to save the exception and add it to the list.

To remove an exception rule from the list, click the corresponding ⊖ **Delete** button.

- **Options.** Configure the scan options for emails matching the rule:
  - **Scanned file types.** Use this option to specify which file types you want to be scanned. You can choose to scan all files (regardless of their file extension), application files only, or specific file extensions you consider to be dangerous. Scanning all files provides the best protection, while scanning only applications is recommended for a quicker scan.

    Note
    Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

If you want to scan only files with specific extensions, you have two alternatives:

- **User defined extensions**, where you must provide only the extensions to be scanned.
- **All files, except specific extensions**, where you must enter only the extensions to be skipped from scanning.

– **Attachment / email body maximum size (MB).** Select this check box and enter a value in the corresponding field to set the maximum accepted size of an attached file or of the email body to be scanned.
– **Archive maximum depth (levels).** Select the check box and choose the maximum archive depth from the corresponding field. The lower the depth level is, the higher the performance and the lower the protection grade.
– **Scan for Potentially Unwanted Applications (PUA).** Select this check box to scan for possibly malicious or unwanted applications, such as adware, which may install on systems without user's consent, change the behavior of various software products and lower the system performance.

- **Actions.** You can specify different actions for the security agent to automatically take on files, based on the detection type.

  The detection type separates the files into three categories:
  – **Infected files.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies.
  – **Suspect files.** These files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but the users must be aware of certain false positives (clean files detected as suspicious) in some cases.
  – **Unscannable files.** These files cannot be scanned. Unscannable files include but are not limited to password-protected, encrypted or over-compressed files.

  For each detection type, you have a default or main action and an alternative action in case the main one fails. Though not recommended, you can change these actions from the corresponding menus. Choose the action to be taken:
  – **Disinfect.** Removes the malware code from infected files and reconstructs the original file. For particular types of malware, disinfection is not possible because the detected file is entirely malicious. It is recommended to always keep this as the first action to be taken on

infected files. Suspect files cannot be disinfected, because no disinfection routine is available.
- **Reject / Delete email.** On servers with Edge Transport role, the detected email is rejected with a 550 SMTP error code. In all other cases, the email is deleted without any warning. It is advisable to avoid using this action.
- **Delete file.** Deletes the attachments with issues without any warning. It is advisable to avoid using this action.
- **Replace file.** Deletes the files with issues and inserts a text file that notifies the user of the actions taken.
- **Move file to quarantine.** Moves detected files to the quarantine folder and inserts a text file that notifies the user of the actions taken. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the **Quarantine** page.

  Note
  Please note that 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.

- **Take no action.** No action will be taken on detected files. These files will only appear in the scan log. Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine.
- By default, when an email matches the rule scope, it is processed exclusively in accordance with the rule, without being checked against any other remaining rule. If you want to continue checking against the other rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

7. Click **Save** to create the scan task. A confirmation message will appear.
8. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Install

To protect your computers with the Bitdefender security agent, you must install it on each of them.

Important
In isolated networks that do not have direct connectivity with the GravityZone appliance, you can install the security agent with Relay role. In this case, the communication between the GravityZone appliance and the other security agents will be done through the Relay agent, which will also act as a local update server for security agents protecting the isolated network.
Once you have installed a Relay agent, it will automatically detect unprotected computers in the same network.

Note

- It is recommended that the computer on which you install the Relay agent to be always on.
- If no Relay agent is installed in the network, the detection of unprotected computers can be done manually by sending a **Network Discovery** task to a protected endpoint.

The Bitdefender protection can then be installed on computers remotely from Control Center.

Remote installation is performed in the background, without the user knowing about it.

Warning
Before installation, be sure to uninstall existing antimalware and firewall software from computers. Installing the Bitdefender protection over existing security software may affect their operation and cause major problems with the system. Windows Defender and Windows Firewall will be turned off automatically when installation starts.
When deploying the agent through a Linux relay, the following conditions must be met:

- The relay must have installed the Samba package (`smbclient`) version 4.1.0 or above, so that it can deploy Windows agents.
- Target Windows endpoints must have Administrative Share and Network Share enabled.
- Target Linux and Mac endpoints must have SSH enabled and firewall disabled.

To run a remote installation task:

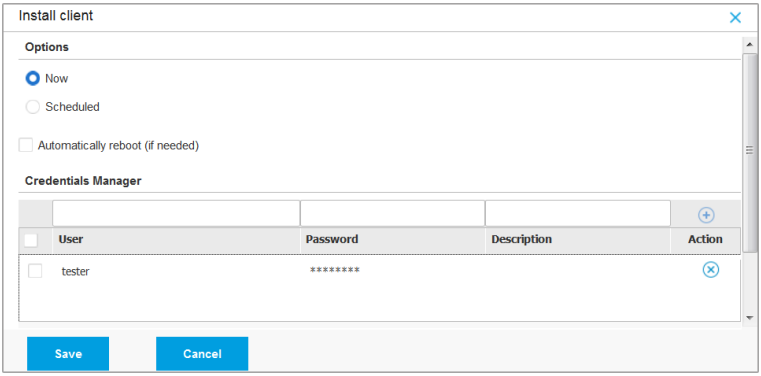
1. Connect and log in to Control Center.

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

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

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

   The **Install Client** wizard is displayed.



Installing Bitdefender Endpoint Security Tools from the Tasks menu

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

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

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

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

   To add the required OS credentials:

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

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

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

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

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

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

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

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

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

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

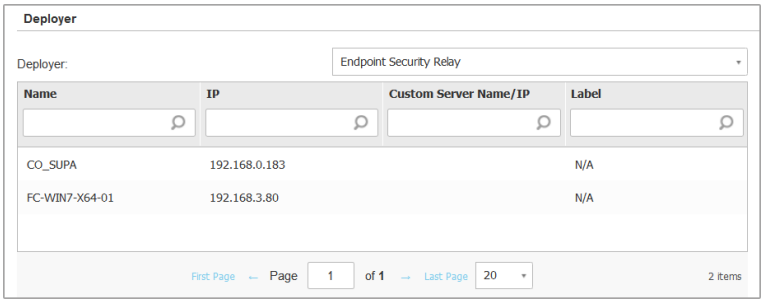
11. Under **Deployer** section, choose the entity to which the target endpoints will connect for installing and updating the client:
    - **GravityZone Appliance**, when endpoints connect directly to GravityZone Appliance.

      In this case, you can also define:

      – A custom Communication Server by entering its IP or Hostname, if required.

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

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



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

    The installation package's settings will appear below and you can make the changes that you need. To find out more about editing installation packages, refer to the GravityZone Installation Guide.

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

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

Uninstall Client

To remotely uninstall the Bitdefender protection:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.

3. Select the container that you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
4. Select the check boxes of computers from which you want uninstall the Bitdefender security agent.
5. Click the **Tasks** button at the upper side of the table and choose **Uninstall client**.
6. A configuration window is displayed, allowing you to make the following settings:
   - You can opt for keeping the quarantined items on the client machine.
   - For vShield integrated environments, you must select the required credentials for each machine, otherwise the uninstallation will fail. Select **Use credentials for vShield integration**, then check all the appropriate credentials in the Credentials Manager table displayed below.
7. Click **Save** to create the task. A confirmation message will appear.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Note
If you want to reinstall protection, be sure to restart the computer first.

Update Client

Check the status of managed computers periodically. If you notice a computer with security issues, click its name to display the **Information** page. For more information, refer to "Security Status" (p. 35).

Outdated clients or outdated signatures represent security issues. In these cases, you should run an update on the corresponding computer. This task can be done locally from the computer, or remotely from Control Center.

To remotely update the client and the signatures on managed computers:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
4. Select the check boxes of computers where you want to run a client update.

5. Click the **Tasks** button at the upper side of the table and choose **Update**. A configuration window will appear.
6. You can choose to update only the product, only the virus signatures or both.
7. For Linux OS and machines integrated with vShield, it is mandatory to also select the required credentials. Check the **Use credentials for Linux and vShield integration** option, then select the appropriate credentials from the Credentials Manager table displayed below.
8. Click **Update** to run the task. A confirmation message will appear.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Reconfigure Client

The security agent's protection modules, roles and scanning modes are initially configured within the installation package. After you have installed the security agent in your network, you can anytime change the initial settings by sending a **Reconfigure Client** remote task to the managed endpoints you are interested in.

Warning
Please note that **Reconfigure Client** task overwrites all installation settings and none of the initial settings is kept. While using this task, make sure to reconfigure all the installation settings for the target endpoints.

To change the installation settings for one or several computers:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group that you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
4. Select the check boxes of computers for which you want to change the installation settings.
5. Click the **Tasks** button at the upper side of the table and choose **Reconfigure client**.
6. Under the **General** section, configure the time when the task will run:
   - **Now**, to launch the task immediately.

- **Scheduled**, to set up the task 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 other important processes are also required to run on the target machine, you can schedule the task to run every 2 hours. The task will start on each target machine every 2 hours until it is successfully done.

7. Configure the modules, roles and scan modes for the target endpoint as you want. For more information, refer to the GravityZone Installation Guide.

   Warning
   - Only the supported modules for each operating system will be installed.

     Please note that the Firewall module is available only for supported Windows workstations.
   - Endpoint Security (legacy agent) supports only Local Scan.

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

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Restart Machine

You can choose to remotely restart managed computers.

Note
Check the **Network > Tasks** page before restarting certain computers. Previously created tasks may still be processing on target computers.

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
4. Select the check boxes of computers you want to restart.
5. Click the **Tasks** button at the upper side of the table and choose **Restart machine**.

6. Choose the restart schedule option:
   - Select **Restart now** to restart computers immediately.
   - Select **Restart on** and use the fields below to schedule the restart at the desired date and time.
7. Click **Save**. A confirmation message will appear.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Network Discovery

Network discovery is done automatically by security agents with Relay role. If you do not have a Relay agent installed in your network, you have to manually send a network discovery task from a protected endpoint.

To run a network discovery task in your network:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.
4. Select the check box of the computer you want to perform network discovery with.
5. Click the **Tasks** button at the upper side of the table and choose **Network Discovery**.
6. A confirmation message will appear. Click **Yes**.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Applications Discovery

To discover applications in your network:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group that you want from the left-side pane. All computers from the selected container are displayed in the right-side pane table.

4. Select the computers on which you want to perform applications discovery.
5. Click the **Tasks** button at the upper side of the table and choose **Applications Discovery**.

> **Note**
> Bitdefender Endpoint Security Tools with Application Control must be installed and activated on the selected computers. Otherwise, the task will be grayed out. When a selected group contains both valid and invalid targets, the task will be sent out only to valid endpoints.

6. Click **Yes** in the confirmation window to proceed.

The discovered applications and processes are displayed on the **Network > Application Inventory** page. For more information, refer to "Application Inventory" (p. 145).

> **Note**
> The **Applications Discovery** task may take a while, depending on the number of applications installed. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Update Security Server

Installed Security Server can be viewed and managed also from **Computers and Virtual Machines**, under the **Custom Groups** folder.

If a Security Server is outdated, you can send it an update task:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group where the Security Server is installed.

   To easily locate the Security Server, you can use the **Filters** menu as follows:

   - Go to **Security** tab and select **Security Servers** only.
   - Go to **Depth** tab and select **All items recursively**.
4. Click the **Tasks** button at the upper side of the table and choose **Update Security Server**.
5. You will have to confirm your action. Click **Yes** to create the task.

You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Important
It is recommended to use this method to update the Security Server for NSX, otherwise you will lose the quarantine saved on the appliance.

4.2.6. Creating Quick Reports

You can choose to create instant reports on managed computers starting from the **Network** page:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group you want from the left-side pane. All computers from the selected group are displayed in the table from the right side pane.

   Optionally, you can filter the contents of the selected group only by managed computers.
4. Select the check boxes of computers you want to include in the report.
5. Click the **Report** button at the upper side of the table and choose the report type from the menu.

   For more information, refer to "Computer and Virtual Machine Reports" (p. 302).
6. Configure the report options. For more information, refer to "Creating Reports" (p. 313).
7. Click **Generate**. The report is immediately displayed.

   The time required for reports to be created may vary according to the number of selected computers.

4.2.7. Assigning Policies

You can manage security settings on computers using policies.

From the **Network** page you can view, change and assign policies for each computer or group of computers.

Note
Security settings are available for managed computers only. To easier view and manage security settings, you can filter the network inventory only by managed computers.

To view the policy assigned to a particular computer:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group that you want from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
4. Click the name of the managed computer you are interested in. An information window will appear.
5. Under **General** tab, in the **Policy** section, click the name of the current policy to view its settings.
6. You can change security settings as needed, provided the policy owner has allowed other users to make changes to that policy. Please note that any change you make will affect all the computers assigned with the same policy.

   For more information about computer policy settings, refer to "Computer and Virtual Machines Policies" (p. 172).

To assign a policy to a computer or a group:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Select the group that you want from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
4. Select the check box of the computer or group that you want. You can select one or several objects of the same type only from the same level.
5. Click the **Assign Policy** button at the upper side of the table.
6. Make the necessary settings in the **Policy assignment** window. For more information, refer to "Assigning Policies" (p. 162).

4.2.8. Using Recovery Manager for Encrypted Volumes

On the Network page, the **Recovery manager** button allows you to retrieve the recovery keys for encrypted volumes.

To retrieve a recovery key:

1. Click the **Recovery manager** button.
2. In a new window, under the **Identifier** section, you are presented with two fillable boxes:
   a. **Recovery Key ID** – this string of number and letters helps GravityZone to determine the encrypted volume. The Recovery Key ID is available in the BitLocker recovery screen, on the endpoint.
   b. **Password** – enter your GravityZone account password to gain access to the recovery key.
3. Click **Reveal**. The window expands.
4. In the **Volume Information**, you are presented with the following data:
   a. **Volume name**.
   b. **Type of volume** – boot or non-boot.
   c. **Endpoint** – the computer name, as listed in the network inventory.
   d. **Recovery key** – the password that helps the user to unlock encrypted volumes. For Mac, the recovery key is actually the user's password.
5. Send the password to the user.

For details about encrypting and decrypting volumes with GravityZone, refer to "Encryption" (p. 274).

4.2.9. Synchronizing with Active Directory

The network inventory is automatically synchronized with Active Directory at a time interval specified in the Control Center configuration section. For more information, refer to the GravityZone Installation and Setup chapter from the GravityZone Installation Guide.

To manually synchronize the currently displayed network inventory with Active Directory:

1. Go to the **Network** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Click the **Synchronize with Active Directory** button at the upper side of the table.

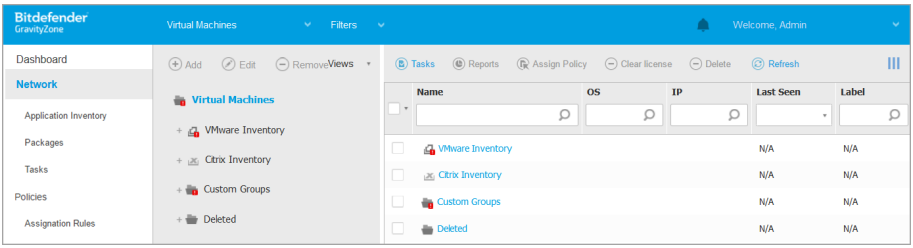
4. You will have to confirm your action by clicking **Yes**.

> **Note**
> For large Active Directory networks, the synchronization may take a longer time to complete.

4.3. Managing Virtual Machines

To view the virtualized infrastructure under your account, go to the **Network** page and choose **Virtual Machines** from the views selector.

> **Note**
> You can manage virtual machines also from the **Computers and Virtual Machines** view, but you can view your virtualized infrastructure and filter its content using specific criteria only from the **Virtual Machines** view.
> For more details about working with network views, refer to "Working with Network Views" (p. 30).



The Network - Virtual Machines view

You can view the available virtual machine networks in the left-side pane and details about each virtual machine in the right-side pane.

To customize the virtual machine details displayed in the table:

1. Click the **Columns** button at the upper-right side of the right pane.
2. Select the columns you want to view.
3. Click the **Reset** button to return to the default columns view.

The left-side pane displays a tree-like view of the virtual infrastructure. The root of the tree is called **Virtual Machines** and the virtual machines are grouped beneath

the root, under the following categories based on the virtualization technology provider:

- **VMware Inventory.** Contains the list of vCenter servers you have access to.
- **Citrix Inventory.** Contains the list of XenServer systems you have access to.
- **Custom Groups.** Contains the security servers and the virtual machines detected in your network outside any vCenter Server or a XenServer system.

The left-side pane also contains a menu called **Views** from which the user can select the view type for each virtualization technology provider.

In order to have access to the virtualized infrastructure integrated with Control Center, you must provide your user credentials for each vCenter Server system available. Once you have entered your credentials, they are saved to your Credentials Manager so that you do not need to enter them the next time. For more information, refer to "Credentials Manager" (p. 156).

From the **Network** section, you can manage virtual machines as follows:

- Check the virtual machines status
- View machine details
- Organize virtual machines into groups
- Sort, filter and search
- Run tasks
- Create quick reports
- Assign policies
- Clearing license seats

4.3.1. Checking the Virtual Machines Status

Each virtual machine is represented in the network page by an icon specific to its type and status.

Refer to "Network Object Types and Statuses" (p. 365) for a list with all available icon types and statuses.

For detailed status information, refer to:

- Management Status
- Connectivity Status
- Security Status

Management Status

Virtual Machines can have the following management statuses:

- **Managed** - virtual machines on which Bitdefender protection is installed.
- **Pending restart** - virtual machines that require a system restart after installing or updating Bitdefender protection.
- **Unmanaged** - detected virtual machines on which Bitdefender protection has not been installed yet.
- **Deleted** - virtual machines that you have deleted from Control Center. For more information, refer to "Deleting Endpoints from Network Inventory" (p. 155).

Connectivity Status

The connectivity status concerns managed virtual machines and Security Servers. From this viewpoint, managed virtual machines can be:

- **Online**. A blue icon indicates that the machine is online.
- **Offline**. A grey icon indicates that the machine is offline.

A virtual machine is offline if the security agent is inactive for more than 5 minutes. Possible reasons why virtual machines appear offline:

- The virtual machine is shut down, sleeping or hibernating.

  Note
  Virtual machines appear online even when they are locked or the user is logged off.

- The security agent does not have connectivity with the GravityZone Communication Server:
  - The virtual machine might be disconnected from the network.
  - A network firewall or router might block the communication between the security agent and Bitdefender Control Center or the assigned Endpoint Security Relay.
  - The virtual machine is behind a proxy server and the proxy settings have not been properly configured in the applied policy.

Warning
For virtual machines behind a proxy server, the proxy settings must be properly configured in the security agent installation package, otherwise the virtual machine will not communicate with GravityZone console and will always appear offline, no matter if a policy with the proper proxy settings is applied after installation.

- The security agent has been manually uninstalled from the virtual machine, while the virtual machine did not have connectivity with Bitdefender Control Center or with the assigned Endpoint Security Relay. Normally, when the security agent is being manually uninstalled from a virtual machine, Control Center is notified of this event, and the virtual machine is flagged as unmanaged.
- The security agent might not be working properly.

To find out for how long virtual machines have been inactive:

1. Display only the managed virtual machines. Click the **Filters** menu located at the upper side of the table, select all the "Managed" options that you need from the **Security** tab, choose **All items recursively** from the **Depth** tab and click **Save**.
2. Click the **Last Seen** column header to sort virtual machines by inactivity period.

You can ignore shorter periods of inactivity (minutes, hours) as they are likely the result of a temporary condition. For example, the virtual machine is currently shut down.

Longer inactivity periods (days, weeks) usually indicate a problem with the virtual machine.

Note
It is recommended to refresh the network table from time to time, to update the endpoints information with the latest changes.

Security Status

The security status concerns managed virtual machines and Security Servers. You can identify virtual machines or Security Servers with security issues by checking the status icons displaying a warning symbol:

- With issues.
- Without issues.

A virtual machine or a Security Server has security issues provided at least one of the following situations applies:

- Antimalware protection is disabled (only for virtual machines).
- The license has expired.
- The Bitdefender product is outdated.
- Antimalware signatures are outdated.
- HVI Supplemental Pack is outdated.
- Malware is detected (only for virtual machines).
- The connection with Bitdefender Cloud Services could not be established, due to the following possible reasons:
  - The virtual machine has internet connectivity issues.
  - A network firewall is blocking the connection with Bitdefender Cloud Services.
  - Port 443, required for the communication with Bitdefender Cloud Services, is closed.

  In this case, the antimalware protection relies solely on local engines, while in-the-cloud scanning is off, meaning that the security agent cannot provide full real-time protection.

If you notice a virtual machine with security issues, click its name to display the **Information** window. You can identify the security issues by the ! icon. Make sure to check for security information in all the information page's tabs. Display the icon's tooltip to find out more details. Further local investigations may be needed.

Note
It is recommended to refresh the network table from time to time, to update the endpoints information with the latest changes.

4.3.2. Viewing Virtual Machine Details

You can obtain detailed information about each virtual machine from the **Network** page, such as IP, OS and last seen date.

To find out details about a virtual machine:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the group that you want from the left-side pane.

   All virtual machines from the selected group are displayed in the right-side pane table.

4. You can easily identify the virtual machine status by checking the corresponding icon. For detailed information, refer to "Checking the Virtual Machines Status" (p. 74).
5. Check the information displayed on table columns for each virtual machine:
   - **Name**: virtual machine name.
   - **FQDN**: fully qualified domain name that includes the hostname and domain name.
   - **OS**: operating system installed on the virtual machine.
   - **IP**: virtual machine's IP address.
   - **Last Seen**: date and time when the virtual machine has last been seen online.

     Note
     It is important to monitor the **Last Seen** field as long inactivity periods might indicate a communication issue or a disconnected virtual machine.

   - **Label**: a custom string with additional information about the virtual machine.

   Click the **Columns** button at the upper-right side of the pane and then add or remove columns to customize the displayed information according to your needs.
6. Click the name of the virtual machine you are interested in to view more details in the **Information** window. The details in this window depend on the management status and on whether the machine is a Security Server instance or not, as follows:

   For Security Servers, details are grouped into the following sections:

   - **Virtual Machine**, containing general appliance information, such as name, FQDN information, IP address, operating system, infrastructure, parent group and current status. You can also assign the Security Server with a label. You can therefore search and filter Security Servers by label using the **Label** column search field from right-side table of the **Network** page.
   - **HVI Prerequisites**, containing information about whether you can use the Security Server to deploy HVI protection or not. Thus, if the host of the Security Server is running on a supported XenServer version and the supplemental pack is installed, you can enable HVI on virtual machines from that host.

- **Product**, containing information, such as product type, license status, product and signatures versions and update status.
- **Policy**, containing information regarding the assigned policy (name, assignment mode and status). Click the policy name to open the policy template and view its settings.

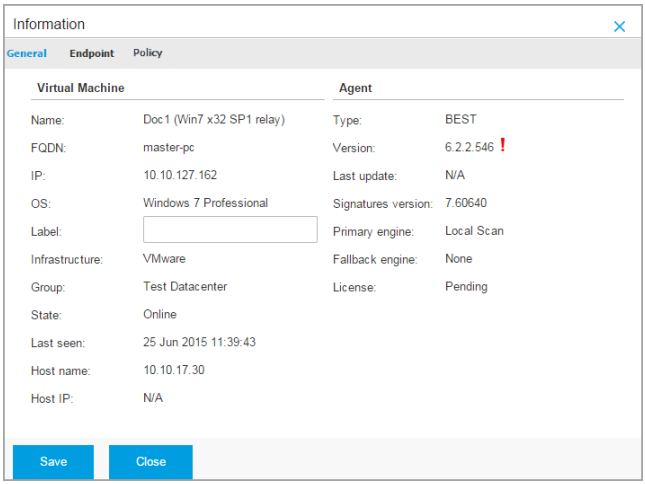
For virtual machines you can find the following details:

- In the **General** tab:
  - General virtual machine information, such as name, FQDN information, IP address, operating system, infrastructure, parent group and current status.

    Here you can assign the virtual machine with a label to help you in machine searching.
  - License status for each installed Bitdefender protection layer.

    Note
    For machines protected by Bitdefender Tools, instead of protection layers you can view security details related to the installed agent, such as agent type, version, last update, product and signature versions, used antimalware engines and license status.
    Additional information on the protection layers is available in the **Protection** tab.

  - The name, IP and label of the relay to which the endpoint is connected, if the case.



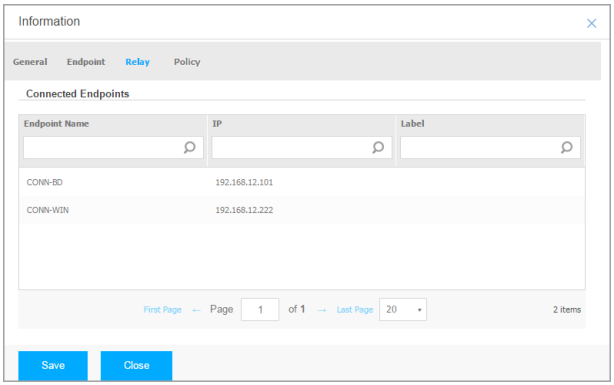
Virtual Machine Information window - General

- In the **Protection** tab you can find details for each protection layer installed on the virtual machine. Details refer to:
  - Security agent information like product name and version, scanning engines configuration and update status. For Exchange Protection, antispam engine and signatures versions are also available.
  - Assigned Security Server. They are displayed in case of agentless deployments or when scanning engines of the security agents are set to use remote scan. Security Server information helps you identify the virtual appliance and get its update status.
  - NSX related information, such as virus tag status and the security group to which the virtual machine belongs. If a security tag has been applied, it informs you that the machine is infected. Otherwise, either the machine is clean or security tags are not being used.
  - The protection modules status. You can easily view which protection modules have been installed on the endpoint and also the status of available modules (On / Off) set via the applied policy.
  - A quick overview regarding the modules activity and malware reporting in the current day.

Click the **View** link to access the report options and then generate the report. For more information, refer to "Creating Reports" (p. 313)

– Additional information regarding the Encryption module, such as:
  - Detected volumes (mentioning the boot drive).
  - Encryption status (which may be **Encrypted**, **Encryption in progress**, **Unencrypted**). Click the **Recovery** link to retrieve the recovery key for the associated encrypted volume. For details about retrieving the recovery keys, refer to "Using Recovery Manager for Encrypted Volumes" (p. 71).

- The **Relay** tab is available only for virtual machines with relay role. This tab displays information about the endpoints connected to the current relay, such as name, IP and label.



Virtual Machine Information window - Relay

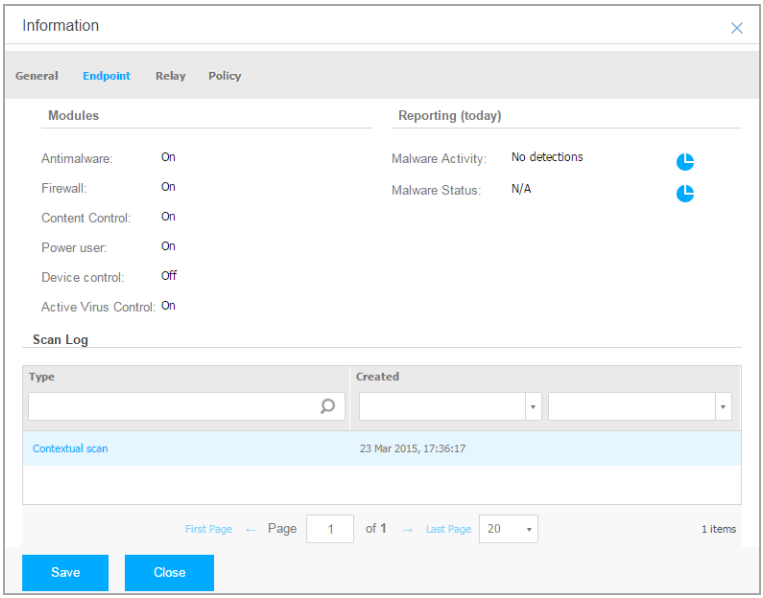
- The **Scan logs** tab displays detailed information about all scan tasks performed on the virtual machine.

  Logs are grouped by protection layer and you can choose from the drop-down menu for which layer to display logs.

  Click the scan task you are interested in and the log will open in a new page of the browser.

  When many scan logs are available, they may span through several pages. To move through the pages, use the navigation options at the bottom of the

table. If there are too many entries, you can use the filter options available at the top of the table.



Information window - Scan logs tab

- In the **Policy** tab, you can find:
  - Information regarding the active policy on the endpoint. An active policy is one of the assigned policies, which is effective at that moment.

    For example, a machine can have assigned two user-aware policies, one for administrators and one for other employees. Each policy becomes active when the user with the apropriate privileges logs in.

    Click the active policy name to open the policy template and view its settings. When the policy is assigned by a rule, click the assignment to view and/or edit the rule settings.
  - Details about other assigned policies. Click the policy name to view the details. Click the assignment rule to view the settings and/or modify them.

Note
This section is available only for machines protected by Bitdefender Endpoint Security Tools and Endpoint Security for Mac.

Each property in this window which is generating security issues is marked with the ! icon. Check the icon's tooltip to find out more details. Further local investigations may be needed.

4.3.3. Organizing Virtual Machines into Groups

You can manage virtual machines groups in the left-side pane of the **Network** page, under the **Custom Groups** folder.

Virtual machines imported from VMware vCenter are grouped under the **VMware Inventory** folder. Virtual machines imported from XenServer are grouped under the **Citrix Inventory** folder. You cannot edit the VMware Inventory or the Citrix Inventory. You can only view and manage the corresponding virtual machines.

All virtual machines that are not managed by vCenter or XenServer systems are detected by Network Discovery and placed under **Custom Groups**, where you can organize them into groups as you want. A major benefit is that you can use group policies to meet different security requirements.

Under **Custom Groups** you can create, delete, rename and move virtual machine groups within a custom-defined tree structure.

Note

- A group can contain both virtual machines and other groups.
- When selecting a group in the left-side pane, you can view all virtual machines except for those placed into its sub-groups. To view all virtual machines included in the group and in its sub-groups, click the **Filters** menu located at the upper side of the table and select **All items recursively** in the **Depth** section.

Creating Groups

Before you start creating groups, think of the reasons why you need them and come up with a grouping scheme. For example, you can group virtual machines based on one or a mix of the following criteria:

- Organization structure (Sales, Marketing, Quality Assurance, Software Development, Management etc.).

- Security needs (Desktops, Laptops, Servers, etc.).
- Location (Headquarter, Local Offices, Remote Workers, Home Offices etc.).

To organize your network into groups:

1. Select **Custom Groups** in the left-side pane.
2. Click the **Add group** button at the top of the left-side pane.
3. Enter a suggestive name for the group and click **OK**. The new group is displayed under **Custom Groups** .

Renaming Groups

To rename a group:

1. Select the group in the left-side pane.
2. Click the **Edit group** button at the top of the left-side pane.
3. Enter the new name in the corresponding field.
4. Click **OK** to confirm.

Moving Groups and Virtual Machines

You can move entities anywhere inside the **Custom Groups** hierarchy. To move an entity, drag and drop it from the right-side pane to the group that you want in the left-side pane.

Note

The entity that is moved will inherit the policy settings of the new parent group, unless the policy inheritance has been disabled and a different policy has been assigned to it. For more information about policy inheritance, refer to "Security Policies" (p. 159).

Deleting Groups

A group cannot be deleted if it contains at least one virtual machine. Move all the virtual machines from the group you want to delete to other groups. If the group includes sub-groups, you can choose to move entire sub-groups rather than individual virtual machines.

To delete a group:

1. Select the empty group.

2. Click the ⊗ **Remove group** button at the top of the left-side pane. You will have to confirm your action by clicking **Yes**.

4.3.4. Sorting, Filtering and Searching for Virtual Machines

Depending on the number of virtual machines, the virtual machines table can span several pages (only 20 entries are displayed per page by default). To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

If there are too many entries, you can use the search boxes under the column headers or the **Filters** menu at the upper side of the page to display only the entities you are interested in. For example, you can search for a specific virtual machine or choose to view only the managed virtual machines.

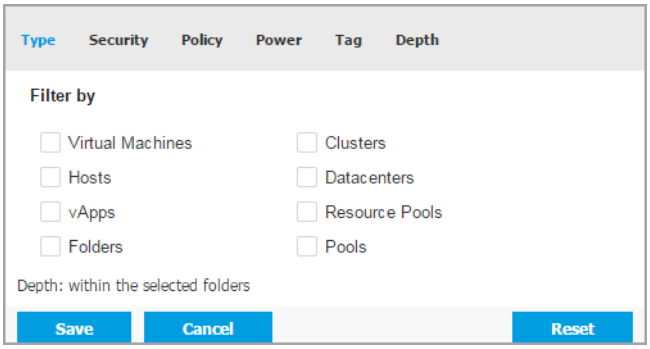
Sorting Virtual Machines

To sort data by a specific column, click column headers. For example, if you want to order virtual machines by name, click the **Name** heading. If you click the heading again, the virtual machines will be displayed in reverse order.

Sorting Computers

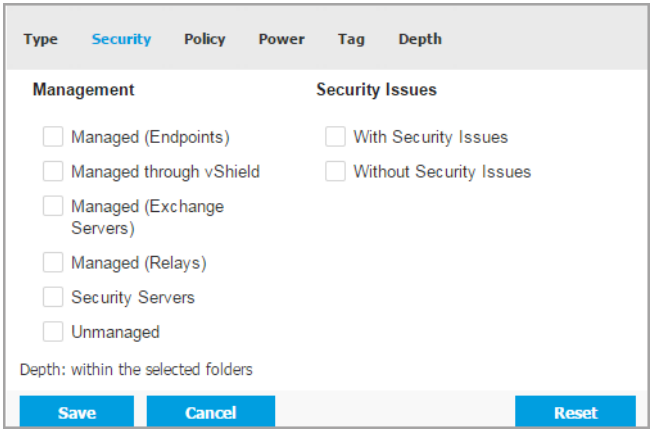
Filtering Virtual Machines

1. Select the group that you want in the left-side pane.
2. Click the **Filters** menu at the upper-side of the network panes area.
3. Use the filter criteria as follows:
   - **Type**. Select the type of virtual entities to be displayed.



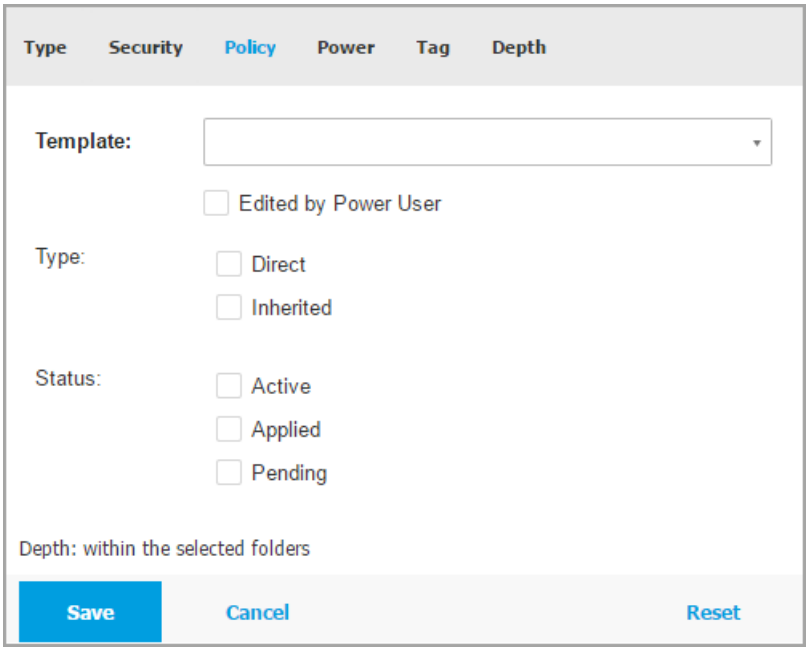
Virtual Machines - Filter by Type

- **Security**. Select the protection management and/or security status to filter network objects by. For example, you can choose to view only the Security Server machines, or you can view only endpoints with security issues.



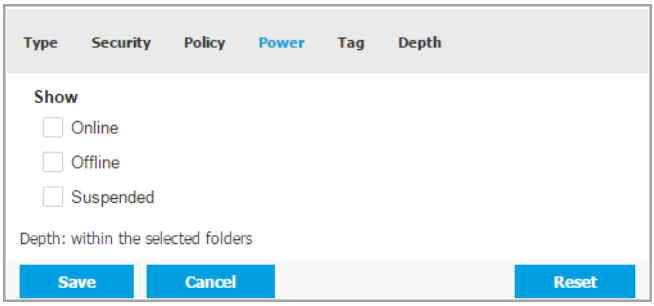
Virtual Machines - Filter by Security

- **Policy**. Select the policy template you want to filter the virtual machines by, the policy assignment type (Direct or Inherited), as well as the policy assignment status (Active, Applied or Pending).



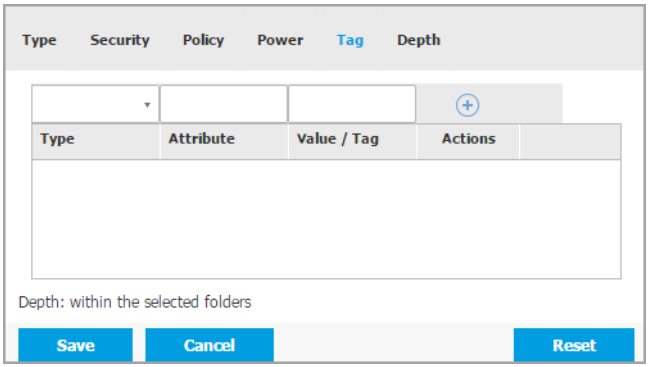
Virtual Machines - Filter by Policy

- **Power**. You can choose to show between online, offline and suspended virtual machines.



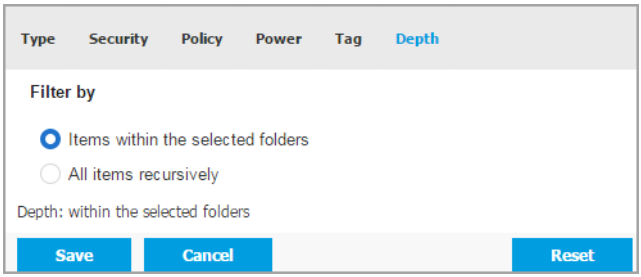
Virtual Machines - Filter by Power

- **Tags**. You can choose to filter the virtual machines by tags and attributes you have defined in your virtualization environment.



Virtual Machines - Filter by Tags

- **Depth**. When managing a tree-structure virtual machines network, virtual machines placed in sub-groups are not displayed by default. Select **All items recursively** to view all virtual machines included in the current group and in its sub-groups.



Virtual Machines - Filter by Depth

Note
Click **Reset** to clear the filter and display all virtual machines.

4. Click **Save** to filter the virtual machines by the selected criteria.

Searching for Virtual Machines

1. Select the desired container in the left-side pane.
2. Enter the search term in the corresponding box under the column headers (Name, OS or IP) from the right-side pane. For example, enter the IP of the virtual machine you are looking for in the **IP** field. Only the matching virtual machine will appear in the table.

   Clear the search box to display the full list of virtual machines.

4.3.5. Running Tasks on Virtual Machines

From the **Network** page, you can remotely run a number of administrative tasks on virtual machines.

This is what you can do:

- "Scan" (p. 90)
- "Exchange Scan" (p. 98)
- "Install" (p. 102)
- "Uninstall Client" (p. 107)
- "Update" (p. 107)
- "Reconfigure Client" (p. 108)
- "Network Discovery" (p. 109)
- "Applications Discovery" (p. 110)
- "Restart Machine" (p. 111)
- "Install Security Server" (p. 111)
- "Uninstall Security Server" (p. 114)
- "Update Security Server" (p. 114)
- "Install HVI Supplemental Pack" (p. 115)
- "Uninstall HVI Supplemental Pack" (p. 116)
- "Update HVI Supplemental Pack" (p. 117)

You can choose to create tasks individually for each virtual machine or for groups of virtual machines. For example, you can remotely install Bitdefender Endpoint Security Tools on a group of unmanaged virtual machines. At a later time, you can create a scan task for a certain virtual machine from the same group.

For each virtual machine, you can only run compatible tasks. For example, if you select an unmanaged virtual machine, you can only choose to install the security agent, all the other tasks being disabled.

For a group, the selected task will be created only for compatible virtual machines. If none of the virtual machines in the group is compatible with the selected task, you will be notified that the task could not be created.

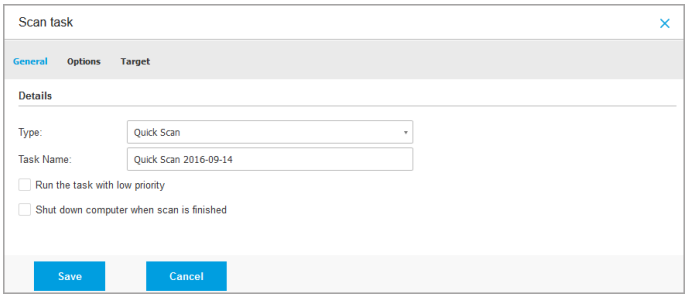
Once created, the task will start running immediately on online virtual machines. If a virtual machine is offline, the task will run as soon as it gets back online.

You can view and manage the task in the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Scan

To remotely run a scan task on one or several virtual machines:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All the entities contained in the selected group are displayed in the right-side pane table.
4. Select the check boxes corresponding to the objects you want to scan.
5. Click the **Tasks** button at the upper side of the table and choose **Scan**. A configuration window will appear.
6. Configure the scan options:
   - In the **General** tab, you can choose the type of scan and you can enter a name for the scan task. The scan task name is intended to help you easily identify the current scan in the **Tasks** page.



Virtual Machines Scan task - Configuring general settings

Select the type of scan from the **Type** menu:

- **Quick Scan** is preconfigured to allow scanning only critical system locations and new files. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

  When malware or rootkits are found, Bitdefender automatically proceeds with disinfection. If, for any reason, the file cannot be disinfected, then it is moved to quarantine. This type of scanning ignores suspicious files.

- **Full Scan** checks the entire system for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

  Bitdefender automatically tries to disinfect files detected with malware. In case malware cannot be removed, it is contained in quarantine, where it cannot do any harm. Suspicious files are being ignored. If you want to take action on suspicious files as well, or if you want other default actions for infected files, then choose to run a Custom Scan.

- **Memory Scan** checks the programs running in the virtual machine's memory.

- **Network Scan** is a type of custom scan, allowing to scan network drives using the Bitdefender security agent installed on the target virtual machine.

  For the network scan task to work:

  - You need to assign the task to one single endpoint in your network.
  - You need to enter the credentials of a user account with read/write permissions on the target network drives, for the security agent to be able to access and take actions on these network drives. The required credentials can be configured in the **Target** tab of the tasks window.

- **Custom Scan** allows you to choose the locations to be scanned and to configure the scan options.

For memory, network and custom scans, you have also these options:

- **Run the task with low priority**. Select this check box to decrease the priority of the scan process and allow other programs to run faster. This will increase the time needed for the scan process to finish.

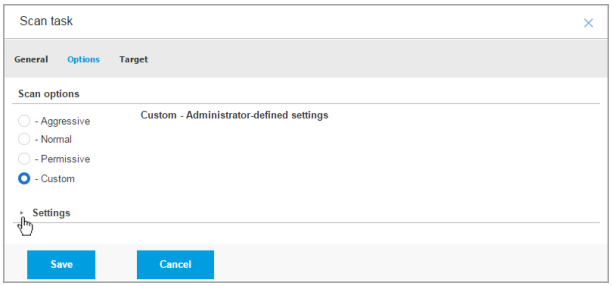
- **Shut down computer when scan is finished**. Select this check box to turn off your machine if you do not intend to use it for a while.

Note
These two options apply only to Bitdefender Endpoint Security Tools and Endpoint Security (legacy agent).

For custom scans, configure the following settings:

– Go to the **Options** tab to set the scan options. Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right-side of the scale to guide your choice.

  Based on the selected profile, the scan options in the **Settings** section are automatically configured. However, if you want to, you can configure them in detail. To do that, select the **Custom** option and then expand the **Settings** section.



Virtual Machines Scan task - Configuring a Custom Scan

The following options are available:

- **File Types.** Use these options to specify which types of files you want to be scanned. You can set the security agent to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Note
  Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

If you want only specific extensions to be scanned, choose **Custom extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

> **Important**
> Bitdefender security agents installed on Windows and Linux operating systems scan most of the .ISO formats, but does not take any action on them.

Virtual Machines scan task options - Adding custom extensions

- **Archives.** Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to scan archives in order to detect and remove any potential threat, even if it is not an immediate threat.

  > **Important**
  > Scanning archived files increases the overall scanning time and requires more system resources.

  – **Scan inside archives.** Select this option if you want to check archived files for malware. If you decide on using this option, you can configure the following optimization options:

    - **Limit archive size to (MB).** You can set a maximum accepted size limit of archives to be scanned. Select the corresponding check box and type the maximum archive size (in MB).
    - **Maximum archive depth (levels).** Select the corresponding check box and choose the maximum archive depth from the

menu. For best performance choose the lowest value, for maximum protection choose the highest value.

- **Scan email archives.** Select this option if you want to enable scanning of email message files and email databases, including file formats such as .eml, .msg, .pst, .dbx, .mbx, .tbb and others.

  Important
  Email archive scanning is resource intensive and can impact system performance.

- **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.
  - **Scan boot sectors.** Scans the system's boot sector. This sector of the hard disk contains the necessary virtual machine code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
  - **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.
  - **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.
  - **Scan for keyloggers.** Select this option to scan for keylogger software. Keyloggers are not malicious applications in nature, but they can be used with malicious intent. The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.
  - **Scan memory.** Select this option to scan programs running in the system's memory.
  - **Scan cookies.** Select this option to scan the cookies stored by browsers on the virtual machine.
  - **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.

- **Scan for Potentially Unwanted Applications (PUA).** A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.
- **Scan detachable volumes.** Select this option to scan any removable storage drive attached to the virtual machine.

- **Actions.** Depending on the type of detected file, the following actions are taken automatically:
  - **When an infected file is found.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies. The Bitdefender security agent can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

    If an infected file is detected, the Bitdefender security agent will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

    Important
    For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

  - **When a suspect file is found.** Files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but the users must be aware of certain false positives (clean files detected as suspicious) in some cases. Suspect files cannot be disinfected, because no disinfection routine is available.

    Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect

files to quarantine. Quarantined files are sent for analysis to Bitdefender Labs on a regular basis. If malware presence is confirmed, a signature is released to allow removing the malware.

– **When a rootkit is found.** Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

  Detected rootkits and hidden files are ignored by default.

When a virus is found on an NSX virtual machine, the Security Server automatically tags the virtual machine with a Security Tag, provided this options has been selected at vCenter Server integration.

For this purpose, the NSX includes three security tags, specific to the threat severity:

– `ANTI_VIRUS.VirusFound.threat=low`, applying on machine when Bitdefender finds low risk malware, which it can delete.

– `ANTI_VIRUS.VirusFound.threat=medium`, applying on the machine if Bitdefender cannot delete the infected files, but instead it disinfects them.

– `ANTI_VIRUS.VirusFound.threat=high`, applying on the machine if Bitdefender can neither delete, nor disinfect the infected files, but blocks access to them.

You can isolate infected machines by creating a security groups with dynamic membership based on the security tags.

Important

– If Bitdefender finds on a machine threats of different severity levels, it will apply all matching tags.

– A security tag is removed from a machine only after a Full Scan is performed and the machine has been disinfected.

Though not recommended, you can change the default actions. You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file. The following actions are available:

Disinfect
Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

Move files to quarantine
Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

Delete
Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Ignore
No action will be taken on detected files. These files will only appear in the scan log.

– Go to **Target** tab to add the locations you want to be scanned on the target virtual machines.

In the **Scan target** section you can add a new file or folder to be scanned:

a. Choose a predefined location from the drop-down menu or enter the **Specific paths** you want to scan.

b. Specify the path to the object to be scanned in the edit field.

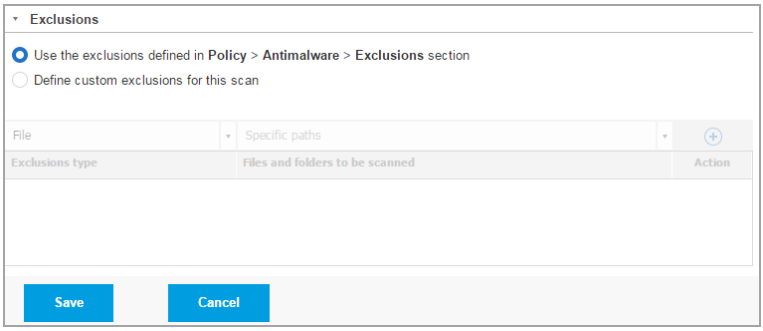
- If you have chosen a predefined location, complete the path as needed. For example, to scan the entire `Program Files` folder, it suffices to select the corresponding predefined location from the drop-down menu. To scan a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name.
- If you have chosen **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target virtual machines. For more information regarding system variables, refer to "System Variables" (p. 368).

c. Click the corresponding ⊕ **Add** button.

To edit an existing location, click it. To remove a location from the list, click the corresponding ⊗ **Delete** button.

For network scan tasks, you need to enter the credentials of a user account with read/write permissions on the target network drives, for the security agent to be able to access and take actions on these network drives.

Click the **Exclusions** sections if you want to define target exclusions.



Virtual Machines Scan Task - Defining Exclusions

You can either use the exclusions defined by policy or define explicit exclusions for the current scan task. For more details regarding exclusions, refer to "Exclusions" (p. 207).

7. Click **Save** to create the scan task. A confirmation message will appear.

You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Note
To schedule a scan task, go to the **Policies** page, select the policy assigned to the virtual machines you are interested in, and add a scan task in the **Antimalware > On-Demand** section. For more information, refer to "On-Demand" (p. 197).

Exchange Scan

You can remotely scan the database of an Exchange Server by running an **Exchange Scan** task.

To be able to scan the Exchange database, you must enable on-demand scanning by providing the credentials of an Exchange administrator. For more information, refer to " Exchange Store Scanning " (p. 254).

To scan an Exchange Server database:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. From the left-side pane, select the group containing the target Exchange Server. You can find the server displayed in the right-side pane.

   Note
   Optionally, you can apply filters to quickly find the target server:
   - Click the **Filters** menu and select the following options: **Managed (Exchange Servers)** from the **Security** tab and **All items recursively** from the **Depth** tab.
   - Enter the server's hostname or IP in the fields from the corresponding column headers.

4. Select the check box of the Exchange Server whose database you want to scan.
5. Click the **Tasks** button at the upper side of the table and choose **Exchange Scan**. A configuration window will appear.
6. Configure the scan options:
   - **General.** Enter a suggestive name for the task.

     For large databases, the scan task may take a long time and may impact the server performance. In such cases, select the check box **Stop scan if it takes longer than** and choose a convenient time interval from the corresponding menus.
   - **Target.** Select the containers and objects to be scanned. You can choose to scan mailboxes, public folders or both. Beside emails, you can choose to scan other objects such as **Contacts**, **Tasks**, **Appointments** and **Post Items**. You can furthermore set the following restrictions to the content to be scanned:
     – Only unread messages
     – Only items with attachments
     – Only new items, received in a specified time interval

     For example, you can choose to scan only emails from user mailboxes, received in the last seven days.

     Select the **Exclusions** check box, if you want to define scan exceptions. To create an exception, use the fields from the table header as follows:

a. Select the repository type from the menu.
b. Depending on the repository type, specify the object to be excluded:

Repository type	Object format
Mailbox	Email address
Public Folder	Folder path, starting from the root
Database	The database identity

Note
To obtain the database identity, use the Exchange shell command:
`Get-MailboxDatabase | fl name,identity`

You can enter only one item at a time. If you have several items of the same type, you must define as many rules as the number of items.
c. Click the ⊕ **Add** button at the upper side of the table to save the exception and add it to the list.

To remove an exception rule from the list, click the corresponding ⊖ **Delete** button.

- **Options.** Configure the scan options for emails matching the rule:
  - **Scanned file types.** Use this option to specify which file types you want to be scanned. You can choose to scan all files (regardless of their file extension), application files only, or specific file extensions you consider to be dangerous. Scanning all files provides the best protection, while scanning only applications is recommended for a quicker scan.

    Note
    Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

    If you want to scan only files with specific extensions, you have two alternatives:
    - **User defined extensions**, where you must provide only the extensions to be scanned.
    - **All files, except specific extensions**, where you must enter only the extensions to be skipped from scanning.

- **Attachment / email body maximum size (MB).** Select this check box and enter a value in the corresponding field to set the maximum accepted size of an attached file or of the email body to be scanned.
- **Archive maximum depth (levels).** Select the check box and choose the maximum archive depth from the corresponding field. The lower the depth level is, the higher the performance and the lower the protection grade.
- **Scan for Potentially Unwanted Applications (PUA).** Select this check box to scan for possibly malicious or unwanted applications, such as adware, which may install on systems without user's consent, change the behavior of various software products and lower the system performance.

- **Actions.** You can specify different actions for the security agent to automatically take on files, based on the detection type.

  The detection type separates the files into three categories:
  - **Infected files.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies.
  - **Suspect files.** These files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but the users must be aware of certain false positives (clean files detected as suspicious) in some cases.
  - **Unscannable files.** These files cannot be scanned. Unscannable files include but are not limited to password-protected, encrypted or over-compressed files.

  For each detection type, you have a default or main action and an alternative action in case the main one fails. Though not recommended, you can change these actions from the corresponding menus. Choose the action to be taken:
  - **Disinfect.** Removes the malware code from infected files and reconstructs the original file. For particular types of malware, disinfection is not possible because the detected file is entirely malicious. It is recommended to always keep this as the first action to be taken on infected files. Suspect files cannot be disinfected, because no disinfection routine is available.
  - **Reject / Delete email.** On servers with Edge Transport role, the detected email is rejected with a 550 SMTP error code. In all other cases, the email is deleted without any warning. It is advisable to avoid using this action.
  - **Delete file.** Deletes the attachments with issues without any warning. It is advisable to avoid using this action.

- **Replace file.** Deletes the files with issues and inserts a text file that notifies the user of the actions taken.
- **Move file to quarantine.** Moves detected files to the quarantine folder and inserts a text file that notifies the user of the actions taken. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the **Quarantine** page.

  Note
  Please note that 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.

- **Take no action.** No action will be taken on detected files. These files will only appear in the scan log. Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine.
- By default, when an email matches the rule scope, it is processed exclusively in accordance with the rule, without being checked against any other remaining rule. If you want to continue checking against the other rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

7. Click **Save** to create the scan task. A confirmation message will appear.
8. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Install

To protect your virtual machines with Security for Virtualized Environments, you must install Bitdefender security agent on each of them. Bitdefender security agent manages protection on the virtual machines. It also communicates with Control Center to receive the administrator's commands and to send the results of its actions. Once you have installed a Bitdefender security agent in a network, it will automatically detect unprotected virtual machines in that network. The Security for Virtualized Environments protection can then be installed on those virtual machines remotely from Control Center. Remote installation is performed in the background, without the user knowing about it.

In isolated networks that do not have direct connectivity with the GravityZone appliance, you can install the security agent with Relay role. In this case, the

communication between the GravityZone appliance and the other security agents will be done through the Relay agent, which will also act as a local update server for security agents protecting the isolated network.

Note
It is recommended that the machine on which you install the Relay agent to be always on.

Warning
Before installation, be sure to uninstall existing antimalware and firewall software from virtual machines. Installing the Bitdefender protection over existing security software may affect their operation and cause major problems with the system. Windows Defender and Windows Firewall will be turned off automatically when installation starts.

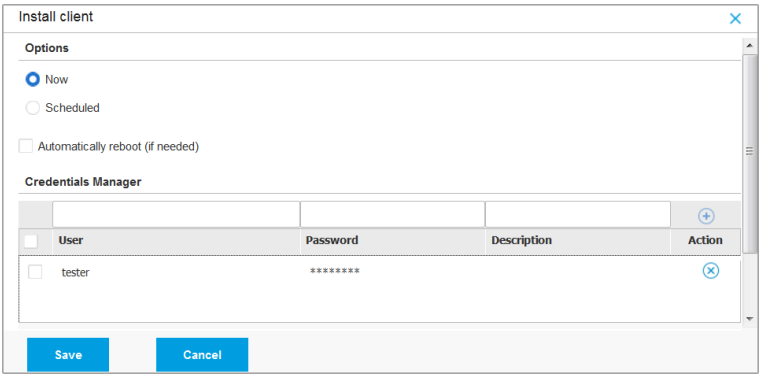
To remotely install the Security for Virtualized Environments protection on one or several virtual machines:

1. Connect and log in to Control Center.
2. Go to the **Network** page.
3. Choose **Virtual Machines** from the views selector.
4. Select the container that you want 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 machines only. Click the **Filters** menu and select the following options: **Unmanaged** from the **Security** tab and **All items recursively** from the **Depth** tab.

5. Select the entities (virtual machines, hosts, clusters or groups) on which you want to install protection.
6. Click the **Tasks** button at the upper side of the table and choose **Install > BEST**.

   The **Install Client** wizard is displayed.



Installing Bitdefender Endpoint Security Tools from the Tasks menu

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

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

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

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

Note
A warning message is displayed as long as you have not selected any credentials. This step is mandatory to remotely install Bitdefender Endpoint Security Tools on endpoints.

To add the required OS credentials:

a. Enter the user name and password of an administrator account for each target operating system in the corresponding fields from the credentials table header. Optionally, you can add a description that will help you identify each account more easily.

   If the machines 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.

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 click 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.

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

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

    - **GravityZone Appliance**, when the machines connect directly to GravityZone Appliance.

For this case, you can also define a custom Communication Server by entering its IP or Hostname, if required.

- **Endpoint Security Relay**, if you want to connect the machines to a relay client installed in your network. All machines with relay role detected in your network will show-up in the table displayed below. Select the relay machine that you want. Connected endpoints will communicate with Control Center only via the specified relay.

  Important
  - Port 7074 must be open, for the deployment through the relay agent to work.
  - When deploying the agent through a Linux relay, the following conditions must be met:
    - The relay must have installed the Samba package (`smbclient`) version 4.1.0 or above, so that it can deploy Windows agents.
    - Target Windows endpoints must have Administrative Share and Network Share enabled.
    - Target Linux and Mac endpoints must have SSH enabled and firewall disabled.

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 company.
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 the GravityZone Installation Guide.

    Warning
    Please note that the Firewall module is available only for supported Windows workstations.

    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.

Uninstall Client

To remotely uninstall the Bitdefender protection:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All entities from the selected container are displayed in the right-side pane table.
4. Select the check boxes of virtual machines from which you want uninstall the Bitdefender security agent.
5. Click the **Tasks** button at the upper side of the table and choose **Uninstall client**.
6. A configuration window is displayed, allowing you to make the following settings:
   - You can opt for keeping the quarantined items on the client machine.
   - For vShield integrated environments, you must select the required credentials for each machine, otherwise the uninstallation will fail. Select **Use credentials for vShield integration**, then check all the appropriate credentials in the Credentials Manager table displayed below.
7. Click **Save** to create the task. A confirmation message will appear.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Note
If you want to reinstall protection, be sure to restart the computer first.

Update

Check the status of managed virtual machines periodically. If you notice a virtual machine with security issues, click its name to display the **Information** page. For more information, refer to "Security Status" (p. 76).

Outdated clients or outdated signatures represent security issues. In these cases, you should run an update on the corresponding virtual machines. This task can be done locally from the virtual machine, or remotely from Control Center.

To remotely update the client and the signatures on managed virtual machines:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All entities from the selected container are displayed in the right-side pane table.
4. Select the check boxes of virtual machines where you want to run a client update.
5. Click the **Tasks** button at the upper side of the table and choose **Update**. A configuration window will appear.
6. You can choose to update only the product, only the virus signatures or both.
7. For Linux OS and machines integrated with vShield, it is mandatory to also select the required credentials. Check the **Use credentials for Linux and vShield integration** option, then select the appropriate credentials from the Credentials Manager table displayed below.
8. Click **Update** to run the task. A confirmation message will appear.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Reconfigure Client

The security agent's protection modules, roles and scanning modes are initially configured within the installation package. After you have installed the security agent in your network, you can anytime change the initial settings by sending a **Reconfigure Client** remote task to the managed endpoints you are interested in.

Warning
Please note that **Reconfigure Client** task overwrites all installation settings and none of the initial settings is kept. While using this task, make sure to reconfigure all the installation settings for the target endpoints.

To change the installation settings for one or several virtual machines:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All entities from the selected container are displayed in the right-side pane table.

4. Select the check boxes of virtual machines for which you want to change the installation settings.
5. Click the **Tasks** button at the upper side of the table and choose **Reconfigure client**.
6. Under the **General** section, configure the time when the task will run:
   - **Now**, to launch the task immediately.
   - **Scheduled**, to set up the task 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 other important processes are also required to run on the target machine, you can schedule the task to run every 2 hours. The task will start on each target machine every 2 hours until it is successfully done.

7. Configure the modules, roles and scan modes for the target endpoint as you want. For more information, refer to the GravityZone Installation Guide.

   Warning
   - Only the supported modules for each operating system will be installed.

     Please note that the Firewall module is available only for supported Windows workstations.
   - Bitdefender Tools (legacy agent) supports only Central Scan.

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

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Network Discovery

Network discovery is done automatically only by security agents with Relay role. If you do not have a Relay agent installed in your network, you have to manually send a network discovery task from a protected endpoint.

To run a network discovery task in your network:

Important
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.

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All entities from the selected container are displayed in the right-side pane table.
4. Select the check box of the machine you want to perform network discovery with.
5. Click the **Tasks** button at the upper side of the table and choose **Network Discovery**.
6. A confirmation message will appear. Click **Yes**.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Applications Discovery

To discover applications in your network:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All virtual machines from the selected container are displayed in the right-side pane table.
4. Select the virtual machines on which you want to perform applications discovery.
5. Click the **Tasks** button at the upper side of the table and choose **Applications Discovery**.

   Note
   Bitdefender Endpoint Security Tools with Application Control must be installed and activated on the selected virtual machines. Otherwise, the task will be grayed out. When a selected group contains both valid and invalid targets, the task will be sent out only to valid endpoints.

6. Click **Yes** in the confirmation window to proceed.

The discovered applications and processes are displayed on the **Network > Application Inventory** page. For more information, refer to "Application Inventory" (p. 145).

Note
The **Applications Discovery** task may take a while, depending on the number of applications installed. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Restart Machine

You can choose to remotely restart managed virtual machines.

Note
Check the **Network > Tasks** page before restarting certain virtual machines. Previously created tasks may still be processing on target machines.

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All entities from the selected container are displayed in the right-side pane table.
4. Select the check boxes of virtual machines you want to restart.
5. Click the **Tasks** button at the upper side of the table and choose **Restart machine**.
6. Choose the restart schedule option:
   - Select **Restart now** to restart virtual machines immediately.
   - Select **Restart on** and use the fields below to schedule the restart at the desired date and time.
7. Click **Save**. A confirmation message will appear.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to Viewing and Managing Tasks.

Install Security Server

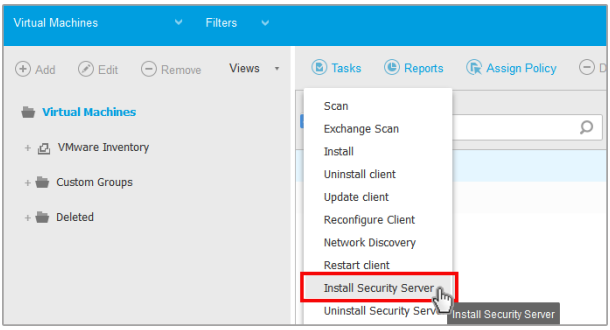
To install a Security Server in your virtual environment:

1. Go to the **Network** page.

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

> **Note**
> You cannot select hosts from different folders.

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



Installing Security Server from Tasks menu

5. All the hosts detected in the selected container will appear in the list. Select the hosts on which you want to install the Security Server instances.
6. Choose the configuration settings you want to use.

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

7. Click **Next**.

8. Provide the corresponding VMware vShield credentials for each vCenter machine.
9. Enter a suggestive name for the Security Server.
10. Select the container in which you want to include the Security Server from the **Deploy Container** menu.
11. Select the destination storage.
12. Choose the disk provisioning type. It is recommended to deploy the appliance using thick disk provisioning.

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

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

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

    If you choose static, you must enter the IP address, subnet mask, gateway and DNS information.
17. Select the vShield network and enter the vShield credentials. Default label for the vShield network is `vmservice-vshield-pg`.
18. Click **Save** to create the task. A confirmation message will appear.

Important
The Security Server packages are not included by default in the GravityZone appliance. Depending on the settings made by the root administrator, the Security Server package necessary for your environment will either be downloaded when a Security Server install task is launched or the administrator will be notified about the missing image and the installation will not proceed. If the package is missing, the root administrator will have to manually download it before the installation is possible.

19. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Uninstall Security Server

To uninstall a Security Server:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the datacenter or folder containing the host on which the Security Server is installed.
4. Select the check box corresponding to the host on which the Security Server is installed.
5. Click the **Tasks** button at the upper side of the table and choose **Uninstall Security Server**.
6. Enter the vShield credentials and click **Yes** to create the task.
7. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Update Security Server

To update a Security Server:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the host on which the Security Server is installed.

   To easily locate the Security Server, you can use the **Filters** menu as follows:

   - Go to **Security** tab and select **Security Servers** only.

- Go to **Depth** tab and select **All items recursively**.

Note
If you are using a virtualization management tool which is not currently integrated with Control Center, the Security Server will be placed under **Custom Groups**. For more information regarding supported virtualization platforms, refer to the GravityZone Installation Guide.

4. Click the **Tasks** button at the upper side of the table and choose **Update Security Server**.
5. You will have to confirm your action by clicking **Yes**.
6. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Important
It is recommended to use this method to update the Security Server for NSX, otherwise you will lose the quarantine saved on the appliance.

Install HVI Supplemental Pack

To protect virtual machines with HVI you must install a supplemental package on the host. The role of this package is to ensure communication between the hypervisor and Security Server installed on the host. Once installed, HVI will protect the virtual machines which have HVI enabled in the policy.

Important
- HVI protects virtual machines exclusively on Citrix Xen hypervisors.
- You do not need to uninstall existing security agent from the virtual machines.

To install the supplemental package on a host:

1. Go to the **Configuration > Update** page.
2. Select the HVI Supplemental Pack in the **Components** list and click the **Download** button at the upper side of the table.
3. Go to the **Network** page and select **Virtual Machines** from the views selector.
4. Select **Server** from the **Views** menu in the left pane.

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

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

Uninstall HVI Supplemental Pack

To uninstall Supplemental Pack from hosts:

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

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

Update HVI Supplemental Pack

To update Supplemental Pack on hosts:

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

   GravityZone will update the Supplemental Pack with the highest version available on the Update Server.

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

4.3.6. Creating Quick Reports

You can choose to create instant reports on managed virtual machines starting from the **Network** page:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container you want from the left-side pane. All virtual machines from the selected container are displayed in the right-side pane table.
4. Filter the contents of the selected group only by managed virtual machines.
5. Select the check boxes corresponding to the virtual machines to be included in the report.

6. Click the **Report** button at the upper side of the table and choose the report type from the menu. For more information, refer to "Computer and Virtual Machine Reports" (p. 302).
7. Configure the report options. For more information, refer to "Creating Reports" (p. 313)
8. Click **Generate**. The report is immediately displayed. The time required for reports to be created may vary depending on the number of selected virtual machines.

4.3.7. Assigning Policies

You can manage security settings on virtual machines using policies.

From the **Network** page you can view, change and assign policies for each virtual machine or group of virtual machines.

Note
Security settings are available for managed virtual machines only. To view and manage security settings easier, you can filter the network inventory only by managed virtual machines.

To view the security settings assigned to a particular virtual machine:

1. Go to the **Network** page.
2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All virtual machines from the selected container are displayed in the right-side pane table.
4. Click the name of the virtual machine you are interested in. An information window will appear.
5. Under **General** tab, in the **Policy** section, click the name of the current policy to view its settings.
6. You can change security settings as needed, provided the policy owner has allowed other users to make changes to that policy. Please note that any change you make will affect all the virtual machines assigned with the same policy.

   For more information about virtual machine policy settings, refer to "Security Policies" (p. 159)

To assign a policy to a virtual machine or a group of virtual machines:

1. Go to the **Network** page.

2. Choose **Virtual Machines** from the views selector.
3. Select the container that you want from the left-side pane. All virtual machines from the selected container are displayed in the right-side pane table.
4. Select the check box of the entity that you want. You can select one or several objects of the same type only from the same level.
5. Click the **Assign Policy** button at the upper side of the table.
6. Make the necessary settings in the **Policy assignment** window.

   For more information, refer to "Assigning Policies" (p. 162).

Warning
For policies with Hypervisor Memory Introspection enabled, target machines may require a reboot right after policy assignment. Machines in this state are marked in the **Network** page with the **Pending restart** icon.

4.3.8. Using Recovery Manager for Encrypted Volumes

On the Network page, the **Recovery manager** button allows you to retrieve the recovery keys for encrypted volumes.

To retrieve a recovery key:

1. Click the **Recovery manager** button.
2. In a new window, under the **Identifier** section, you are presented with two fillable boxes:
   a. **Recovery Key ID** – this string of number and letters helps GravityZone to determine the encrypted volume. The Recovery Key ID is available in the BitLocker recovery screen, on the endpoint.
   b. **Password** – enter your GravityZone account password to gain access to the recovery key.
3. Click **Reveal**. The window expands.
4. In the **Volume Information**, you are presented with the following data:
   a. **Volume name**.
   b. **Type of volume** – boot or non-boot.
   c. **Endpoint** – the computer name, as listed in the network inventory.

d. **Recovery key** – the password that helps the user to unlock encrypted volumes. For Mac, the recovery key is actually the user's password.

5. Send the password to the user.

For details about encrypting and decrypting volumes with GravityZone, refer to "Encryption" (p. 274).

4.3.9. Clearing License Seats

In Active Directory, vCenter Server (without vShield, NSX or HVI) and Xen Server inventories, you can easily free the license seats used by virtual machines where the security agent was removed without running the uninstaller.

After you do this, the target machines become unmanaged in the Network Inventory.

To clear a license seat:

1. Go to the **Network** page.
2. Select **Computers and Virtual Machines** or **Virtual Machines** from the views selector.
3. Select the group you want from the left-side pane. All virtual machines will be displayed in the right-side table.
4. Select the virtual machine you want to delete the license from.
5. Click the ⊖ **Clear license** button at the upper-side of the table.
6. Click **Yes** in the confirmation window to proceed.

4.4. Managing Mobile Devices

To manage the security of mobile devices used in your company, first you have to link them to specific users in Control Center, then install and activate the GravityZone Mobile Client application on each of them.

Mobile devices can be enterprise-owned or personally-owned. You can install and activate GravityZone Mobile Client on each mobile device, then hand it to the corresponding user. Users can also install and activate GravityZone Mobile Client by themselves, following the instructions received by email. For more information, refer to the GravityZone Installation Guide.

To view the mobile devices of users under your account, go to the **Network** section and choose **Mobile Devices** from the service selector. The **Network** page displays

the available user groups in the left-side pane and the corresponding users and devices in the right-side pane.

If integration with Active Directory has been configured, you can add mobile devices to existing Active Directory users. You can also create users under **Custom Groups** and add mobile devices to them.

You can switch the right-side pane view to **Users** or to **Devices** using the **View** tab from the **Filters** menu located at the upper side of the table. The **Users** view allows you to manage users in Control Center, such as adding users and mobile devices and checking the number of devices for each user. Use the **Devices** view to easily manage and check the details of each mobile device in the Control Center.

You can manage users and mobile devices in the Control Center as follows:

- Add custom users
- Add mobile devices to users
- Organize custom users into groups
- Filter and search users and devices
- Check user or device status and details
- Run tasks on mobile devices
- Create quick mobile devices reports
- Check and change device security settings
- Synchronize the Control Center inventory with Active Directory
- Delete users and mobile devices

4.4.1. Adding Custom Users

If integration with Active Directory has been configured, you can add mobile devices to existing Active Directory users.

In non-Active Directory situations, you must first create custom users in order to have a mean to identify the owners of mobile devices.

There are two ways to create custom users. You can either add them one at a time or import a CSV file.

To add a custom user:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the service selector.
3. Click the **Filters** menu at the upper side of the table and go to the **View** tab. Make sure that the **Users** option is selected.

4. In the left-side pane, select **Custom Groups**.
5. Click the **Add User** button at the upper side of the table. A configuration window will appear.
6. Specify the required user details:
   - A suggestive username (for example, the user's full name)
   - User's email address

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

7. Click **OK**.

To import mobile device users:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the service selector.
3. Click the **Filters** menu at the upper side of the table and go to the **View** tab. Make sure that the **Users** option is selected.
4. In the left-side pane, select **Custom Groups**.
5. Click **Import users**. A new window opens.
6. Select the CSV file and click **Import**. The window closes and the table is populated with the imported users.

   Note
   If any errors occur, a message is displayed and the table is populated only with the valid users. Existing users are skipped.

You can afterwards create user groups under **Custom Groups**.

The policy and tasks assigned to a user will apply to all devices owned by the corresponding user.

4.4.2. Adding Mobile Devices to Users

A user may have an unlimited number of mobile devices. You can add devices to one or multiple users, but only one device per user at a time.

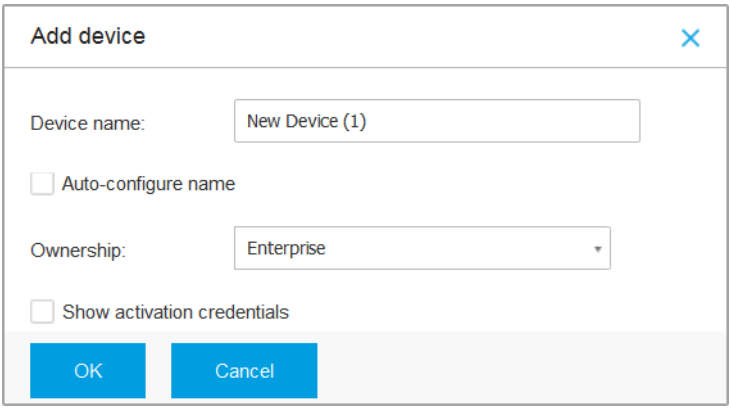
Adding a device to a single user

To add a device to a specific user:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Locate the user in the **Active Directory** group or in **Custom Groups** and select the corresponding check box in the right-side pane.

   Note
   The **Filters** must be set on **Users** in the **View** tab.

4. Click the **Add Device** button at the upper side of the table. A configuration window will appear.



Add mobile device to a user

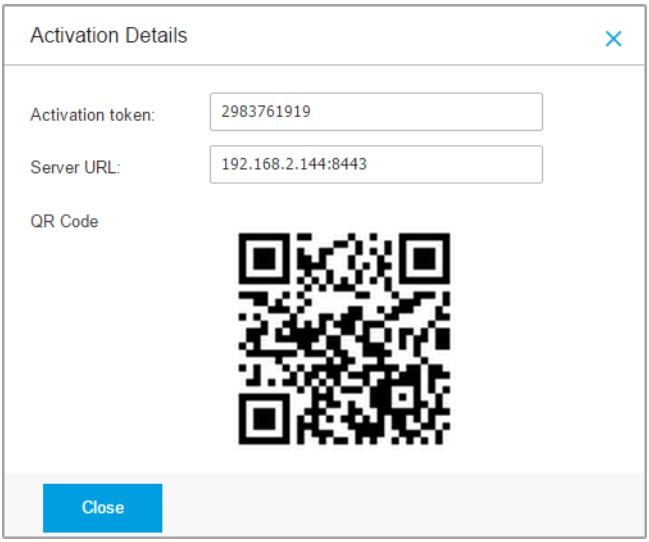
5. Configure the mobile device details:
   a. Enter a suggestive name for the device.
   b. Use the **Auto-configure name** option if you want the device name to be automatically generated. When added, the device has a generic name. Once

the device is activated, it is automatically renamed with the corresponding manufacturer and model information.

c. Select the device ownership type (enterprise or personal). You can anytime filter mobile devices by ownership and manage them according to your needs.

d. Select the **Show activation credentials** option if you are going to install the GravityZone Mobile Client on the user's device.

6. Click **OK** to add the device. The user is immediately sent an email with the installation instructions and the activation details to be configured on the device. The activation details include the activation token and the communication server address (and corresponding QR code).
7. If you have selected the **Show activation credentials** option, the **Activation Details** window appears, displaying the unique activation token, the communication server address and corresponding QR code for the new device.



Mobile devices activation details

After installing the GravityZone Mobile Client, when prompted to activate the device, enter the activation token and the communication server address or scan the provided QR code.

Adding devices to multiple users

To add mobile devices to a selection of users and groups:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Locate the users or groups in the **Active Directory** folders or in **Custom Groups** and select the corresponding check boxes in the right-side pane.

   Note
   The **Filters** must be set on **Users** in the **View** tab.

4. Click the **Add device** button at the right-side of the table. In this case, you have to define in the configuration window the device ownership only.

   If there are users with unspecified email address, you are immediately notified with a message. The list of corresponding users will be available in the **Notification** area of Control Center.

   Mobile devices created by multiple selection have by default a generic name in Control Center. Once a device is activated, it is automatically renamed with the corresponding manufacturer and model information.
5. Click **OK** to add the devices. The users are immediately sent an email with the installation instructions and the activation details to be configured on their devices. The activation details include the activation token and the communication server address (and corresponding QR code).

You can check the number of devices assigned to each user in the right-side pane, under **Devices** column.

4.4.3. Organizing Custom Users into Groups

You can view the available user groups in the left-side pane of the **Network** page.

Active Directory users are grouped under **Active Directory**. You cannot edit the Active Directory groups. You can only view and add devices to the corresponding users.

You can place all non-Active Directory users under **Custom Groups**, where you can create and organize groups as you want. A major benefit is that you can use group policies to meet different security requirements.

Under **Custom Groups** you can create, delete, rename and move user groups within a custom-defined tree structure.

Important
Please note the following:

- A group can contain both users and other groups.
- When selecting a group in the left-side pane, you can view all users except those placed into its sub-groups. To view all users included in the group and in its sub-groups, click the **Filters** menu located at the upper side of the table and select **All items recursively** in the **Depth** section.

Creating Groups

To create a custom group:

1. Select **Custom Groups** in the left-side pane.
2. Click the ⊕ **Add group** button at the top of the left-side pane.
3. Enter a suggestive name for the group and click **OK**. The new group is displayed under **Custom Groups**.

Renaming Groups

To rename a custom group:

1. Select the group in the left-side pane.
2. Click the ✎ **Edit group** button at the top of the left-side pane.
3. Enter the new name in the corresponding field.
4. Click **OK** to confirm.

Moving Groups and Users

You can move groups and users anywhere inside the **Custom Groups** hierarchy. To move a group or a user, drag and drop it from the current location to the new one.

Note
The entity that is moved will inherit the policy settings of the new parent group, unless the policy inheritance has been disabled and a different policy has been assigned to it.

Deleting Groups

A group cannot be deleted if it contains at least one user. Move all users from the group you want to delete to another group. If the group includes sub-groups, you can choose to move all sub-groups rather than individual users.

To delete a group:

1. Select the empty group.
2. Click the ⊗ **Remove group** button at the top of the left-side pane. You will have to confirm your action by clicking **Yes**.

4.4.4. Checking the Mobile Devices Status

Each mobile device is represented in the network page by an icon specific to its type and status.

Refer to "Network Object Types and Statuses" (p. 365) for a list with all available icon types and statuses.

Mobile devices can have the following management statuses:

- **Managed (Active)**, when all the following conditions are satisfied:
  - The GravityZone Mobile Client is activated on the device.
  - The GravityZone Mobile Client has synchronized with the Control Center within the last 48 hours.
- **Managed (Idle)**, when all the following conditions are satisfied:
  - The GravityZone Mobile Client is activated on the device.
  - The GravityZone Mobile Client has not synchronized with the Control Center for more than 48 hours.
- **Unmanaged**, in the following situations:
  - The GravityZone Mobile Client has not yet been installed and activated on the mobile device.
  - The GravityZone Mobile Client has been uninstalled from the mobile device (for Android devices only).
  - The Bitdefender MDM profile has been removed from the device (for iOS devices only).

To check the devices management status:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. In the left-side pane, select the group you are interested in.
4. Click the **Filters** menu located at the upper side of the table and make the following settings:
   a. Go to **View** tab and select **Devices**.
   b. Go to **Security** tab and select the status you are interested in under **Management** section. You can select one or several filter criteria at the same time.
   c. You can also choose to view all devices recursively, by selecting the corresponding option in the **Depth** tab.
   d. Click **Save**.

      All the mobile devices corresponding to the selected criteria are displayed in the table.

You can also generate a Device Synchronization status report on one or several mobile devices. This report provides detailed information regarding the synchronization status of each selected device, including the date and time of the last synchronization. For more information, refer to "Creating Quick Reports" (p. 142)

4.4.5. Compliant and Not Compliant Mobile Devices

Once the GravityZone Mobile Client application has been activated on a mobile device, the Control Center checks if the corresponding device meets all the compliance requirements. Mobile devices can have the following security statuses:

- **Without Security Issues**, when all compliance requirements are satisfied.
- **With Security Issues**, when at least one of the compliance requirements is not satisfied. When a device is declared non-compliant, the user is prompted to fix the non-compliance issue. The user must make the required changes within a certain time period, otherwise the action for non-compliant devices defined in the policy will be applied.

  For more information regarding the non-compliance actions and criteria, refer to "Compliance" (p. 282).

To check the devices compliance status:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. In the left-side pane, select the group you are interested in.
4. Click the **Filters** menu located at the upper side of the table and make the following settings:
   a. Go to **View** tab and select **Devices**.
   b. Go to **Security** tab and select the status you are interested in under **Security Issues** section. You can select one or several filter criteria at the same time.
   c. You can also choose to view all devices recursively, by selecting the corresponding option in the **Depth** tab.
   d. Click **Save**.

      All the mobile devices corresponding to the selected criteria are displayed in the table.
5. You can view the device compliance ratio for each user:
   a. Click the **Filters** menu located at the upper side of the table and select **Users** from the **View** category. All the users in the selected group are displayed in the table.
   b. Check the **Compliance** column to view how many devices are compliant from the total number of devices owned by the user.

You can also generate a Device Compliance report on one or several mobile devices. This report provides detailed information regarding the compliance status of each selected device, including the non-compliance reason. For more information, refer to "Creating Quick Reports" (p. 142)

4.4.6. Checking User and Mobile Devices Details

You can obtain detailed information about each user and mobile device from the **Network** page.

Checking User Details

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the desired group in the left-side pane.

4. Click the **Filters** menu located at the upper side of the table, go to the **View** tab and select **Users**. To display users recursively, go to the **Depth** tab and select **All items recursively**. Click **Save**. All users in the selected group are displayed in the table.
5. Check the information displayed in the table columns for each user:
   - **Name**. The user name.
   - **Devices**. The number of devices attached to user. Click the number to switch to the **Devices** view and display the corresponding devices only.
   - **Compliance**. The ratio of compliant devices to total devices attached to user. Click the first value to switch to the **Devices** view and display the compliant devices only.
6. Click the name of the user you are interested in. A configuration window appears, where you can view and edit the user's name and email address.

Checking Device Details

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the desired group in the left-side pane.
4. Click the **Filters** menu located at the upper side of the table, go to the **View** tab and select **Devices**. Click **Save**. All devices belonging to users in the selected group are displayed in the table.
5. Check the information displayed in the table columns for each device:
   - **Name**. The device name.
   - **User**. The name of the user owning the corresponding device.
   - **OS**. The operating system of the corresponding device.
6. Click the name of a device for more details. The **Mobile Device Details** window appears, where you can check the following information grouped under **Overview** and **Details** tabs:
   - **General**.
     - **Name**. The name specified when adding the device in Control Center.
     - **User**. The device owner's name.

- **Group**. The mobile device's parent group in the network inventory.
- **OS**. The mobile device's operating system.
- **Ownership**. The mobile device ownership type (enterprise or personal).

- **Security**.
  - **Client Version**. The version of GravityZone Mobile Client application installed on the device, only detected after enrollment.
  - **Policy**. The policy currently assigned to the mobile device. Click the policy name to go to the corresponding **Policy** page and check the security settings.

    Important

    By default, only the user who created the policy can modify it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page. The changes made to a policy will affect all devices assigned with the corresponding policy. For more information, refer to "Assigning Policies" (p. 142).

  - **License status**. View license information for the corresponding device.
  - **Compliance status**. The compliance status is available for managed mobile devices. A mobile device can be Compliant or Not compliant.

    Note

    For not compliant mobile devices, a notification icon ! is displayed. Check the icon's tooltip to view the non-compliance reason.
    For more details regarding mobile devices compliance, refer to "Compliance" (p. 282).

  - **Malware Activity (last 24h)**. A quick overview regarding the number of malware detections for the corresponding device in the current day.
  - **Lock Password**. A unique password automatically generated at device enrollment, which is used for remotely locking the device (for Android devices only).
  - **Encryption status**. Some of 3.0 Android devices or newer support the device encryption feature. Check the encryption status in the device details page to find out if the corresponding device supports the

encryption feature. If the encryption has been required by policy on the device, you can also view the encryption activation status.

- **Activation Details**
  - **Activation Code**. The unique activation token assigned to the device.
  - The communication server address.
  - **QR Code**. The unique QR Code containing the activation token and the communication server address.
- **Hardware**. You can view here the device hardware information, available only for managed (activated) devices. Hardware information is checked every 12 hours and updated if changes occur.
- **Network**. You can view here network connectivity information, available only for managed (activated) devices.

4.4.7. Sorting, Filtering and Searching for Mobile Devices

The Mobile Devices inventory table can span several pages, depending on the number of users or devices (only 10 entries are displayed per page by default). To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

If there are too many entries, you can use the filter options to display only the entities you are interested in. For example, you can search for a specific mobile device or choose to view only the managed devices.

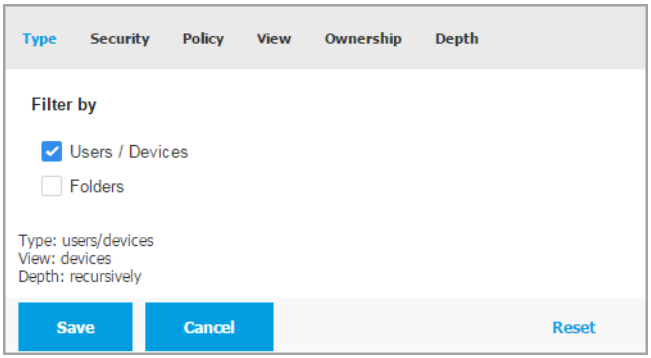
Sorting the Mobile Devices Inventory

To sort data by a specific column, click the column headers. For example, if you want to order devices by name, click the **Name** heading. If you click the heading again, the devices will be displayed in reverse order.

Filtering the Mobile Devices Inventory

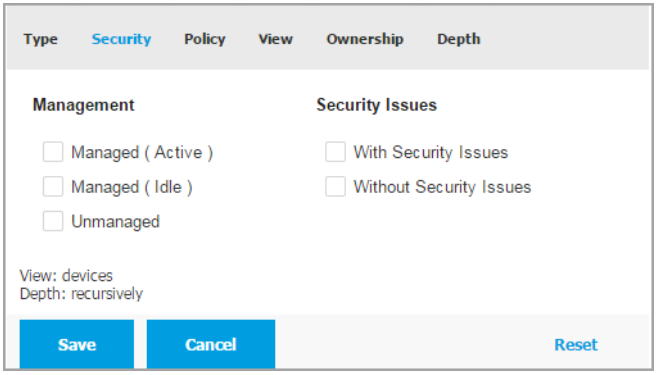
1. Select the group that you want in the left-side pane.
2. Click the **Filters** menu at the upper-side of the network panes area.
3. Use the filter criteria as follows:

- **Type**. Select the type of entities you want to display (Users/Devices and Folders).



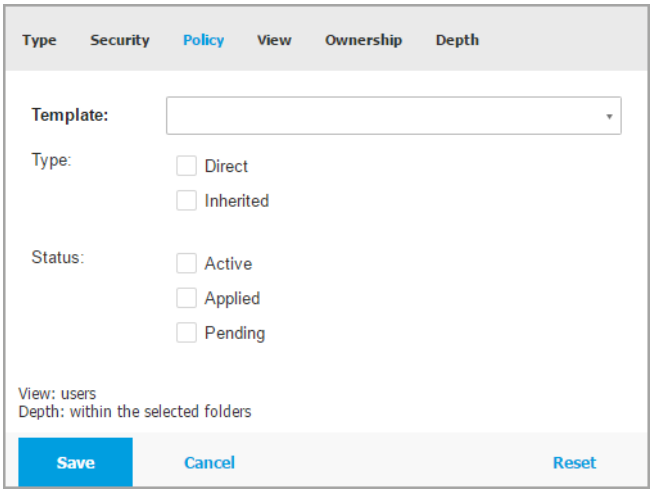
Mobile devices - Filter by Type

- **Security**. Choose to display computers by management and security status.



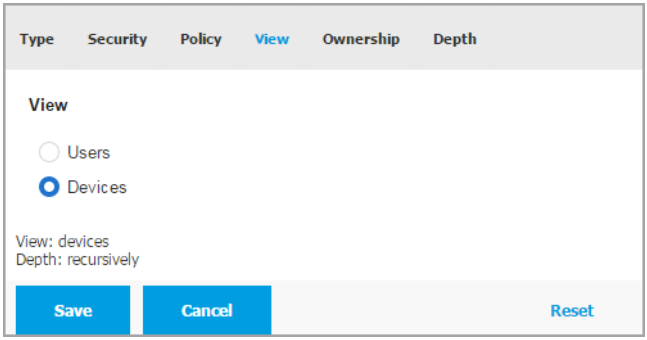
Mobile devices - Filter by Security

- **Policy**. Select the policy template you want to filter the mobile devices by, the policy assignment type (Direct or Inherited), as well as the policy assignment status (Active, Applied or Pending).



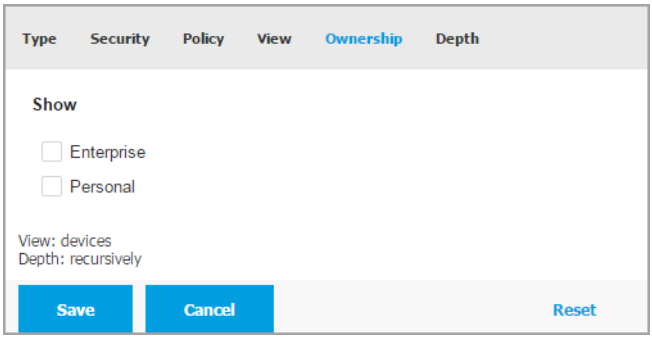
Mobile devices - Filter by Policy

- **View**. Select **Users** to display only users in the selected group. Select **Devices** to display only devices in the selected group.



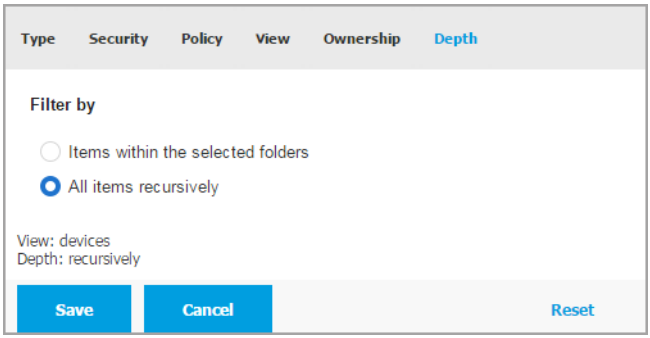
Mobile devices - Filter by View

- **Ownership**. You can filter mobile devices by ownership, choosing to show **Enterprise** devices or **Personal** devices. The ownership attribute is defined in the mobile devices details.



Mobile devices - Filter by Ownership

- **Depth**. When managing a tree-structured network, mobile devices or users placed in sub-groups are not displayed when selecting the root group. Select **All items recursively** to view all entities included in the current group and in its sub-groups.



Mobile devices - Filter by Depth

4. Click **Save** to filter the mobile devices inventory by the selected criteria.

   The filter remains active in the **Network** page until you log out or reset the filter.

Searching for Mobile Devices

The right-side pane table provides specific information of users and mobile devices. You can use the categories available on each column to filter the table contents.

1. Select the desired group in the left-side pane.
2. Switch to the view that you want (Users or Mobile Devices) using the **Filters** menu at the upper-side of the network panes area.
3. Search for the entities that you want using the search fields under each column header from the right-side pane:
   - Enter the search term that you want in the corresponding search field.

     For example, switch to the **Devices** view and enter the name of the user you are looking for in the **User** field. Only the matching mobile devices will appear in the table.
   - Select the attribute that you want to search by in the corresponding drop-down list boxes.

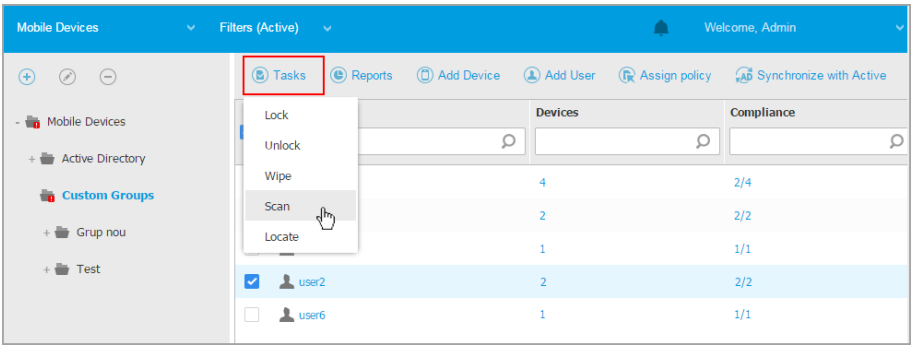
     For example, switch to the **Devices** view, click the **OS** list box and select **Android** to view only Android mobile devices.

   Note
   To clear the search term and show all entities, place the mouse cursor over the corresponding box and click the × icon.

4.4.8. Running Tasks on Mobile Devices

From the **Network** page, you can remotely run a number of administrative tasks on mobile devices. This is what you can do:

- "Lock" (p. 137)
- "Unlock" (p. 138)
- "Wipe" (p. 139)
- "Scan" (p. 140)
- "Locate" (p. 141)



Mobile devices tasks

To run remote tasks on mobile devices, certain prerequisites must be met. For more information, refer to the Installation Requirements chapter from the GravityZone Installation Guide.

You can choose to create tasks individually for each mobile device, for each user or for groups of users. For example, you can remotely scan for malware the mobile devices of a group of users. You can also run a locate task for a specific mobile device.

The network inventory can contain active, idle or unmanaged mobile devices. Once created, tasks will start running immediately on active mobile devices. For idle devices, the tasks will start as soon as they get back online. Tasks will not be created for unmanaged mobile devices. A notification stating that the task could not be created will be displayed in this case.

You can view and manage tasks in the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Lock

The Lock task immediately locks the screen of target mobile devices. The Lock task behavior is operating system dependent:

- On Android, the screen is locked with a password generated by Control Center. If the user already has a lock screen password, this will be automatically changed. The device can be unlocked only by an Unlock task sent from the Control Center.

Note
The lock screen password generated by Control Center is displayed in the Mobile Device Details window.

- On iOS, if the device has a lock screen password, it is asked in order to unlock.

To remotely lock mobile devices:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the group that you want from the left-side pane.
4. Click the **Filters** menu at the upper side of the network panes area and select **Users** from the **View** category. Click **Save**. All users in the selected group are displayed in the table.
5. Select the check boxes corresponding to users you are interested in. You can select one or several users at the same time.
6. Click the **Tasks** button at the upper side of the table and choose **Lock**.
7. You will have to confirm your action by clicking **Yes**. A message will inform you whether the task was created or not.
8. You can view and manage the task in the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Unlock

The **Unlock** task resets the screen locking with password and unlocks the screen on the target mobile devices.

Note
When unlocking a mobile device that is required to have a lock screen password via the policy, GravityZone Mobile Client will notify the user to set a new lock screen password according to policy settings.

To remotely unlock mobile devices:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the group that you want from the left-side pane.

4. Click the **Filters** menu at the upper side of the network panes area and select **Users** from the **View** category. Click **Save**. All users in the selected group are displayed in the table.
5. Select the check boxes corresponding to users you are interested in. You can select one or several users at the same time.
6. Click the **Tasks** button at the upper side of the table and choose **Unlock**.
7. You will have to confirm your action by clicking **Yes**. A message will inform you whether the task was created or not.
8. You can view and manage the task in the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Note
After applying the **Unlock** task to encrypted Android devices, the user is still prompted to provide a blank password.

Wipe

The **Wipe** task restores the target mobile devices to factory settings. Run this task to remotely erase all sensitive information and applications stored on target mobile devices.

Warning
Use the **Wipe** task carefully. Check the ownership of target devices (if you want to avoid wiping personally-owned mobile devices) and make sure that you really want to wipe the selected devices. Once sent, the **Wipe** task cannot be undone.

To remotely wipe a mobile device:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the group that you want from the left-side pane.
4. Click the **Filters** menu at the upper side of the network panes area and select **Devices** from the **View** category. Click **Save**. All devices in the selected group are displayed in the table.

Note
You can also select **All items recursively** under the **Depth** section to view all devices in the current group.

5. Select the check box corresponding to the device you want to wipe.
6. Click the **Tasks** button at the upper side of the table and choose **Wipe**.
7. You will have to confirm your action by clicking **Yes**. A message will inform you whether the task was created or not.
8. You can view and manage the task in the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

Scan

The **Scan** task allows you to check selected mobile devices for malware. The device user is notified about any detected malware and prompted to remove it. The scan is performed in the cloud, therefore the device must have Internet access.

Note
The remote scan does not work on iOS devices (platform limitation).

To remotely scan mobile devices:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the group that you want from the left-side pane.
4. Click the **Filters** menu at the upper side of the network panes area and select **Devices** from the **View** category. Click **Save**. All devices in the selected group are displayed in the table.

   Note
   You can also select **All items recursively** under the **Depth** section to view all devices in the current group.
   To display only Android devices in the selected group, go to the **OS** column header in the right-side pane and choose **Android** from the corresponding list box.

5. Select the check boxes corresponding to devices you want to scan.
6. Click the **Tasks** button at the upper side of the table and choose **Scan**.
7. You will have to confirm your action by clicking **Yes**. A message will inform you whether the task was created or not.

8. You can view and manage the task in the **Network > Tasks** page. A scan report is available when the task completes. Click the corresponding icon in the **Reports** column to generate an instant report.

   For more information, refer to "Viewing and Managing Tasks" (p. 151).

Locate

The Locate task opens a map showing the location of selected devices. You can locate one or several devices at the same time.

For the Locate task to work, the location services must be enabled on the mobile devices.

To locate mobile devices:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the group that you want from the left-side pane.
4. Click the **Filters** menu at the upper side of the network panes area and select **Devices** from the **View** category. Click **Save**. All devices in the selected group are displayed in the table.

   Note
   You can also select **All items recursively** under the **Depth** section to view recursively all devices in the current group.

5. Select the check box corresponding to the device you want to locate.
6. Click the **Tasks** button at the upper side of the table and choose **Locate**.
7. The **Location** window opens, displaying the following information:
   - A map showing the position of the selected mobile devices. If a device is not synchronized, the map will display its last known location.
   - A table displaying the details of selected devices (name, user, last synchronization date and time). To view the map location of a certain device listed in the table, just select its check box. The map will instantly focus on the corresponding device's location.
   - The **Autorefresh** option automatically updates the selected mobile devices locations after each 10 seconds.

8. You can view and manage the task in the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 151).

4.4.9. Creating Quick Reports

You can choose to create instant reports on mobile devices starting from the **Network** page:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Select the group you want from the left-side pane.
4. Click the **Filters** menu at the upper side of the network panes area and select **Devices** from the **View** category. You can also select the Managed options from the **Security** tab, to filter the selected group only by managed devices. Click **Save**. All devices corresponding to the filter criteria from the selected group are displayed in the table.
5. Select the check boxes corresponding to the mobile devices you are interested in. You can select one or several devices at the same time.
6. Click the **Report** button at the upper side of the table and choose the report type from the menu. For more information, refer to "Mobile Devices Reports" (p. 311)
7. Configure the report options. For more information, refer to "Creating Reports" (p. 313)
8. Click **Generate**. The report is immediately displayed. The time required for reports to be created may vary depending on the number of selected mobile devices.

4.4.10. Assigning Policies

You can manage security settings on mobile devices using policies.

From the **Network** section you can view, change and assign policies for mobile devices under your account.

You can assign policies to groups, users or specific mobile devices.

Note

A policy assigned to a user affects all devices owned by the user. For more information, refer to "Assigning Local Policies" (p. 163).

To view the security settings assigned to a mobile device:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Click the **Filters** menu at the upper side of the network panes area and select **Devices** from the **View** category. Click **Save**. All devices belonging to users in the selected group are displayed in the table.
4. Click the name of the mobile device you are interested in. A details window will appear.
5. In the **Security** section from the **Overview** page, click the name of the currently assigned policy to view its settings.
6. You can change security settings as needed. Please note that any change you make will also apply to all other devices on which the policy is active.

   For more information, refer to "Mobile Device Policies" (p. 277)

To assign a policy to a mobile device:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. In the left-side pane, select the group you are interested in.
4. Click the **Filters** menu at the upper side of the network panes area and select **Devices** from the **View** category. Click **Save**. All devices belonging to users in the selected group are displayed in the table.
5. In the right-side pane, select the check box of the mobile device you are interested in.
6. Click the **Assign policy** button at the upper side of the table.
7. Make the necessary settings in the **Policy assignment** window. For more information, refer to "Assigning Local Policies" (p. 163).

4.4.11. Synchronizing with Active Directory

The network inventory is automatically synchronized with Active Directory at a time interval specified in the Control Center configuration section. For more information, refer to the GravityZone Installation and Setup chapter from the GravityZone Installation Guide.

To manually synchronize the currently displayed users with Active Directory:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. Click the **Synchronize with Active Directory** button at the upper side of the table.
4. You will have to confirm your action by clicking **Yes**.

Note
For large Active Directory networks, the synchronization may take a longer time to complete.

4.4.12. Deleting Users and Mobile Devices

When the network inventory contains obsolete users or mobile devices, it is recommended to delete them.

Deleting Mobile Devices from the Network Inventory

When you delete a device from Control Center:

- GravityZone Mobile Client is unlinked, but not removed from the device.
- For iOS devices, the MDM Profile is removed. If the device is not connected to the Internet, the MDM Profile remains installed until a new connection is available.
- All logs related to the deleted device are still available.
- Your personal information and applications are not affected.

Warning
- You cannot restore deleted mobile devices.
- Before deletion, perform an **Unlock** task to make sure the device is not locked.
- If you accidentally delete a locked device, you need to reset the device to the factory settings to unlock it.

To delete a mobile device:

1. Go to the **Network** page.

2. Choose **Mobile Devices** from the views selector.
3. In the left-side pane, select the group you are interested in.
4. Click the **Filters** menu at the upper side of the network panes area and select **Devices** from the **View** category.
5. Click **Save**.
6. Select the check box corresponding to the mobile devices you want to delete.
7. Click the ⊖ **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

Deleting Users from the Network Inventory

Users currently linked to mobile devices cannot be deleted. You will have to delete the corresponding mobile devices first.

Note
You can delete users from the Custom Groups only.

To delete a user:

1. Go to the **Network** page.
2. Choose **Mobile Devices** from the views selector.
3. In the left-side pane, select the group you are interested in.
4. Click the **Filters** menu at the upper side of the network panes area and select **Users** from the **View** category.
5. Click **Save**.
6. Select the check box corresponding to the user you want to delete.
7. Click the ⊖ **Delete** button at the right-side of the table. You will have to confirm your action by clicking **Yes**.

4.5. Application Inventory

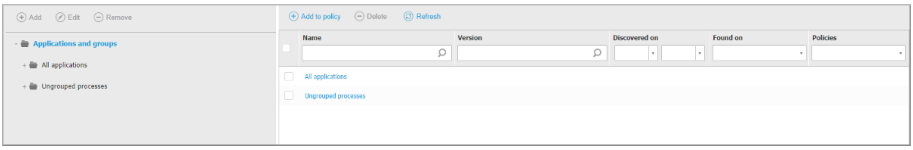
You can view all the applications discovered in your network by the **Applications Discovery** task, in the **Applications and groups** section. For more information, refer to "Applications Discovery" (p. 68).

The applications and processes are automatically added under the **Applications and groups** folder, on the left-side pane.

You can organize applications and processes under custom groups.

All applications/processes under a selected folder are displayed in the right-side pane table. You can search by name, version, publisher/author, updater, location and policy.

To view the latest information in the table, click the **Refresh** button at the upper side of the table. This may be needed when you spend more time on the page.



Application Inventory

Important
New applications discovered each time you run the **Application Discovery** task are automatically placed in the **Ungrouped Applications** folder. The processes that are not related to specific applications, are placed in the **Ungrouped Processes** folder.

Applications and Groups Tree

To add a custom group in the **Applications and groups** tree:

1. Select the **All applications** folder.
2. Click the **Add** button at the upper side of the tree.
3. Enter a name in the new window.
4. Click **OK** to create the new group.
5. Select the **Ungrouped applications** folder. All applications grouped under a selected folder are displayed in the right-side pane table.
6. Select the desired applications from the right-side pane table. Drag and drop the selected items from the right-side pane to move them to the custom group that you want in the left-side pane.

To add a custom application:

1. Select the target folder under **All applications**.

2. Click the ⊕ **Add** button at the upper side of the tree.
3. Enter a name in the new window.
4. Click **OK** to create the custom application.
5. You can add processes related to the new custom application from the **Ungrouped processes** folder, or from other folders displayed in the **Applications and groups** tree. After you select the folder, all processes are displayed in the right-side pane table.
6. Select the desired processes from the right-side pane table. Drag and drop the selected items in the left-side pane, to move them to the custom application.

Note
An application can be part of only one group.

To edit a folder or an application name:

1. Select it in the **Applications and groups** tree.
2. Click the ✎ **Edit** button at the upper side of the tree.
3. Change the name with the one you want.
4. Click **OK**.

You can move groups and applications anywhere inside the **Applications and groups** hierarchy. To move a group or an application, drag and drop it from the current location to the new one.

To remove a custom folder or application, select it in the **Applications and groups** tree and then click the ⊖ **Remove** button at the upper side of the tree.

Adding Applications to Policies

To add an application or a process to a rule directly from Application Inventory:

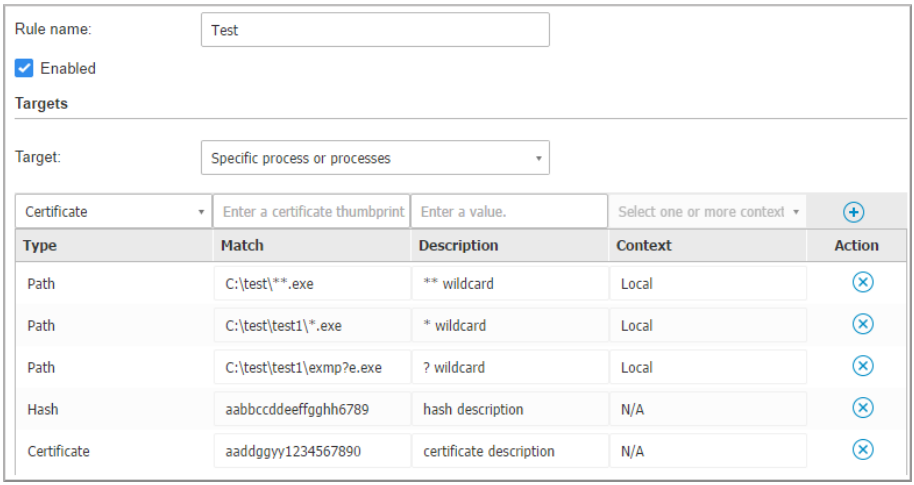
1. Select the desired folder from the **Applications and groups** tree. The folder contents is listed in the right-side pane.
2. Select the processes or applications that you want from the right-side pane.
3. Click the ⊕ **Add to policy** button to open the configuration window.
4. In the **Apply rule to these policies** section, enter an existing policy name. Use the search box to find by policy name or owner.

5. In the **Rule details** section, enter a **Rule name**.
6. Select the **Enabled** check box to activate the rule.
7. The target type is automatically recognized. If needed, edit the existing criteria:
   - **Specific process or processes**, to define a process that is allowed or denied from starting. You can authorize by path, hash or certificate. The conditions inside the rule are matched by logical AND.
     - To authorize an application from a specific path:
       a. Select **Path** in the **Type** column. Specify the path to the object. You can provide an absolute or relative pathname and use wildcard characters. The asterisk symbol (*) matches any file within a directory. A double asterisk (**) matches all files and directories in the defined directory. A question mark (?) matches exactly one character. You can also add a description to help identify the process.
       b. From the **Select one or more contexts** drop-down menu you can choose among local, CD-ROM, removable and network. You can block an application executed from a removable device, or allow it if the application is locally executed.
     - To authorize an application based on hash, select **Hash** in the **Type** column and enter a hash value. You can also add a description to help identify the process.

       Important
       To generate the hash value, download the Fingerprint tool. For more information, refer to "Application Control Tools" (p. 369)

     - To authorize based on a certificate, select **Certificate** in the **Type** column and enter a certificate thumbprint. You can also add a description to help identify the process.

       Important
       To obtain the certificate thumbprint, download the Thumbprint tool. For more information, refer to "Application Control Tools" (p. 369)



Application Rules

Click ⊕ **Add** to add the rule. The newly created rule will have the highest priority in this policy.

- **Inventory applications or groups**, to add a group or an application discovered in your network. You can view the applications running in your network on the **Network > Application Inventory** page.

  Insert the applications or group names in the field, separated by a comma. The auto-fill function displays suggestions as you type.

8. Select the **Include subprocesses** check box to apply the rule to spawned child processes.

   Warning
   When setting rules for browser applications, it is recommended to turn off this option to prevent security risks.

9. Optionally, you can also define exclusions from the process start rule. The adding operation is similar to the one described in the previous steps.
10. In the **Permissions** section, choose whether to allow or deny the rule to run.
11. Click **Save** to apply the changes.

To delete an application or process:

1. Select the desired folder from the **Applications and groups** tree.
2. Select the processes or applications that you want from the right-side pane.
3. Click the **Delete** button.

Updaters

You must define updaters for the applications discovered in your network.

Warning
If you do not assign updaters, the whitelisted applications will not be allowed to update.

To assign an updater:

1. Select the desired folder in the **Applications and groups** tree. The folder content is listed in the right-side pane.
2. In the right side pane, select the file you want to use as updater.
3. Click the **Assign updaters** button.
4. Click **Yes** to confirm the assignment. Updaters are marked with a specific icon:

Updater

To dismiss an updater:

1. Select the desired folder in the **Applications and groups** tree. The folder content is listed in the right-side pane.
2. In the right side pane, select the updater you want to dismiss.
3. Click the **Dismiss updater** button.
4. Click **Yes** to confirm.

4.6. Viewing and Managing Tasks

The **Network > Tasks** page allows you to view and manage all the tasks you have created.

Once you have created a task for one of several network objects, you can view it in the tasks table.

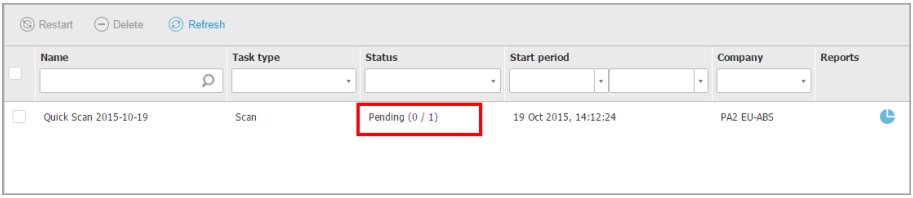
You can do the following from the **Network > Tasks** page:

- Check the task status
- View task reports
- Restart tasks
- Stop Exchange scan tasks
- Delete tasks

4.6.1. Checking Task Status

Each time you create a task for one or several network objects, you will want to check its progress and get notified when errors occur.

Go to the **Network > Tasks** page and check the **Status** column for each task you are interested in. You can check the status of the main task, and you can also obtain detailed information about each sub-task.



The Tasks page

- **Checking the main task status**.

  The main task concerns the action launched on network objects (such as install client or scan) and contains a certain number of sub-tasks, one for each selected network object. For example, a main installation task created for eight computers contains eight sub-tasks. The numbers between brackets represent the sub-tasks completion ratio. For example, (2/8) means that two out of eight sub-tasks are finished.

  The main task status may be:

- **Pending**, when none of the sub-tasks has started yet, or when the number of concurrent deployments is exceeded. The maximum number of concurrent deployments can be set from the **Configuration** menu. For more information, refer to the GravityZone Installation Guide.
- **In Progress**, when all sub-tasks are running. The main task status remains In Progress until the last sub-task is done.
- **Finished**, when all sub-tasks are (successfully or unsuccessfully) finished. In case of unsuccessful sub-tasks, a warning symbol is displayed.

- **Checking the sub-tasks status**.

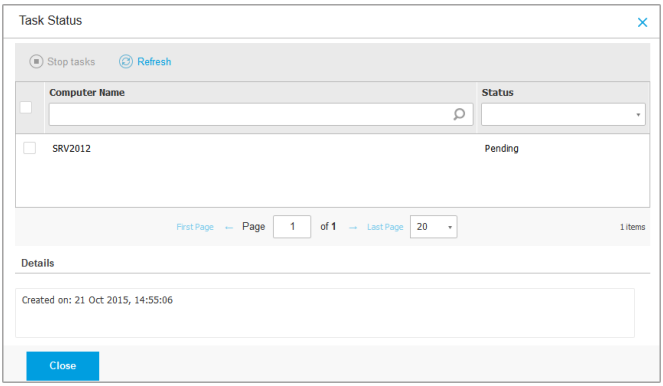
  Go to the task you are interested in and click the link available in the **Status** column to open the **Status** window. You can view the list of network objects assigned with the main task and the status of the corresponding sub-task. The sub-tasks status can be:

  - **In Progress,** when the sub-task is still running.

    Additionally, for Exchange on-demand scan tasks, you can also view the completion status.

  - **Finished**, when the sub-task has finished successfully.
  - **Pending**, when the sub-task has not started yet. This can happen in the following situations:
    - The sub-task is waiting in a queue.
    - There are connectivity issues between Control Center and the target network object.
    - The target device is Idle (offline), in the case of mobile devices. The task will run on target device as soon as it gets back online.
  - **Failed**, when the sub-task could not start or it had stopped due to errors, such as incorrect authentication credentials and low memory space.
  - **Stopping**, when the on-demand scanning is taking too long to complete and you have chosen to stop it.

  To view the details of each sub-task, select it and check the **Details** section at the bottom of the table.



Tasks Status Details

You will obtain information regarding:

- Date and time when the task started.
- Date and time when the task ended.
- Description of encountered errors.

4.6.2. Viewing Task Reports

From the **Network > Tasks** page you have the option to view quick scan tasks reports.

1. Go to the **Network > Tasks** page.
2. Choose the desired network object from the views selector.
3. Select the check box corresponding to the scan task you are interested in.
4. Click the corresponding button from the **Reports** column. Wait until the report is displayed. For more information, refer to "Using Reports" (p. 301).

4.6.3. Restarting Tasks

For various reasons, the client installation, uninstallation or update tasks may fail to complete. You can choose to restart such failed tasks instead of creating new ones, following the next steps:

1. Go to the **Network > Tasks** page.

2. Choose the desired network object from the views selector.
3. Select the check boxes corresponding to the failed tasks.
4. Click the **Restart** button at the upper side of the table. The selected tasks will restart and the tasks status will change to **Retrying**.

Note
For tasks with multiple sub-tasks, **Restart** option is available only when all sub-tasks have finished and it will execute only the failed sub-tasks.

4.6.4. Stopping Exchange Scan Tasks

Scanning the Exchange Store can take a considerable amount of time. If by any reasons you want to stop an on-demand Exchange scan task, follow the steps described herein:

1. Go to the **Network > Tasks** page.
2. Choose the desired network view from the views selector.
3. Click the link in the **Status** column to open the **Task Status** window.
4. Select the check box corresponding to the pending or running sub-tasks you want to stop.
5. Click the **Stop tasks** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

Note
You can also stop an on-demand scan of the Exchange Store from the events area of Bitdefender Endpoint Security Tools.

4.6.5. Deleting Tasks

GravityZone automatically deletes pending tasks after two days, and finished tasks after 30 days. If you still have many tasks, it is recommended to delete the tasks that you no longer need, to prevent the list from getting cluttered.

1. Go to the **Network > Tasks** page.
2. Choose the desired network object from the views selector.
3. Select the check box corresponding to the task you want to delete.

4. Click the ⊖ **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

Warning
Deleting a pending task will also cancel the task.
If a task in progress is being deleted, any pending sub-tasks will be cancelled. In this case, all finished sub-tasks cannot be undone.

4.7. Deleting Endpoints from Network Inventory

The network inventory contains by default the **Deleted** folder, designated for storing endpoints that you do not plan to manage.

By using the **Delete** action on an endpoint, it will be moved to the **Deleted** folder.

Note
You can only delete endpoints displayed under **Custom Groups**, that are detected outside any integrated network infrastructure.

To delete endpoints from the network inventory:

1. Go to the **Network** page.
2. Choose the appropriate network view from the views selector.
3. Select **Custom Groups** from the left-side pane. All endpoints available in this group are displayed in the right-side pane table.
4. In the right-side pane, select the check box corresponding to the endpoint you want to delete.
5. Click the ⊖ **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

   An **Uninstall client** task will be created on the **Tasks** page.

   The endpoint will be moved under the **Deleted** folder. If the deleted endpoint was managed, the security agent will be expired, releasing one license seat.

You can anytime move endpoints from the **Deleted** folder under the **Custom Groups**, by using drag-and-drop.

Furthermore, you can permanently remove deleted endpoints from the network inventory, by also deleting them from the **Deleted** folder. In this case, the endpoints are removed also from the GravityZone database.

To permanently remove endpoints from the Control Center:

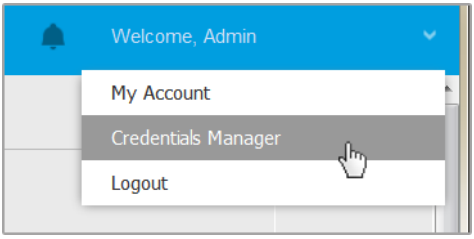
1. Go to the **Network** page.
2. Choose the appropriate network view from the views selector.
3. Select the **Deleted** group from the left-side pane. All endpoints available in this group are displayed in the right-side pane table.
4. Select the check box corresponding to the endpoints you want to permanently remove.
5. Click the ⊖ **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

   The selected endpoints are permanently removed from the GravityZone database.

4.8. Credentials Manager

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

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



The Credentials Manager menu

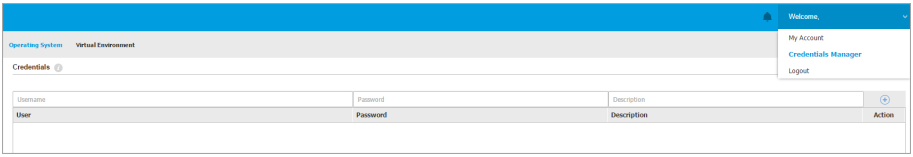
The **Credentials Manager** window contains two tabs:

- Operating System
- Virtual Environment

4.8.1. Operating System

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

To add a set of credentials:



Credentials Manager

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

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

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

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

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

4.8.2. Virtual Environment

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

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

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

1. Select the server from the corresponding menu.

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

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

   Note
   If you do not configure your authentication credentials in Credentials Manager, you will be required to enter them when you try to browse the inventory of any virtualized server system. Once you have entered your credentials, they are saved to your Credentials Manager so that you do not need to enter them the next time.

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

4.8.3. Deleting Credentials from Credentials Manager

To delete obsolete credentials from the Credentials Manager:

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

5. SECURITY POLICIES

Once installed, the Bitdefender protection can be configured and managed from Control Center using security policies. A policy specifies the security settings to be applied on target network inventory objects (computers, virtual machines or mobile devices).

Immediately after installation, network inventory objects are assigned with the default policy, which is preconfigured with the recommended protection settings. Provided the NSX integration is enabled, another three default security policies for NSX are available, one for each security level: permissive, normal and aggressive. These policies are preconfigured with the recommended protection settings. You cannot modify or delete the default policies.

You can create as many policies as you need based on security requirements, for each type of managed network object.

This is what you need to know about policies:

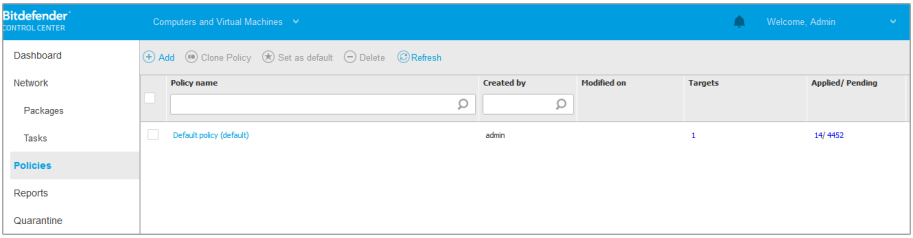
- Policies are created in the **Policies** page and assigned to network objects from the **Network** page.
- Policies can inherit several modules settings from other policies.
- You can configure policy assignment to endpoints so that a policy can apply only in certain conditions, based on location or logged-in user. Therefore, an endpoint can have more policies assigned.
- Endpoints can have one active policy at a time.
- You can assign a policy to individual endpoints or to groups of endpoints. By default,each endpoint inherits the policy of the parent group. At the same time, inheritance options can be defined for each endpoint or group of endpoints. When assigning a policy to a group, the defined policy inheritance settings will be taken into account.
- Policies are pushed to target network objects immediately after creating or modifying them. Settings should be applied to network objects in less than a minute (provided they are online). If a network object is not online, settings will be applied as soon as it gets back online.
- The policy applies only to the installed protection modules.
- The **Policies** page displays only the following types of policies:
  - Policies created by you.
  - Other policies (such as default policy or templates created by other users) which are assigned to endpoints under your account.

- You cannot edit policies created by other users (unless the policy owners allow it from the policy settings), but you can override them by assigning the target objects a different policy.

Warning
Only the supported policy modules will apply to target endpoints.
Please note that only Antimalware module is supported for server operating systems.

5.1. Managing Policies

You can view and manage policies in the **Policies** page.



The Policies page

Each type of endpoint has specific policy settings. To manage policies, you must first select the type of endpoint (**Computers and Virtual Machines** or **Mobile Devices**) from the views selector.

Existing policies are displayed in the table. For each policy, you can view:

- Policy name.
- User who created the policy.
- Date and time when the policy was last modified.
- The number of targets to which the policy was sent.*
- The number of targets for which the policy was applied / is pending.*

For policies with NSX module enabled, additional information is available:

- The NSX policy name, used to identify the Bitdefender policy in VMware vSphere.
- Policy visibility in the management consoles, allowing you to filter the policies for NSX. Thus, while **Local** policies are visible only in Bitdefender Control Center, **Global** policies are also visible in VMware NSX.

These details are hidden by default.

To customize the policy details displayed in the table:

1. Click the **Columns** button at the right side of the Action Toolbar.
2. Select the columns you want to view.
3. Click the **Reset** button to return to the default columns view.

* Clicking the number will redirect you to the **Network** page, where you can view the corresponding endpoints. You will be asked to choose the network view. This action will create a filter using policy criteria.

You can sort the available policies and also search for certain policies using the available criteria.

5.1.1. Creating Policies

You can create policies either by adding a new one or duplicating (cloning) an existing policy.

To create a security policy:

1. Go to the **Policies** page.
2. Choose the type of endpoint that you want from the views selector.
3. Choose the policy creation method:
   - **Add a new policy**.
     - Click the **Add** button at the upper side of the table. This command creates a new policy starting from the default policy template.
   - **Clone an existing policy**.
     a. Select the check box of the policy you want to duplicate.
     b. Click the **Clone** button at the upper side of the table.
4. Configure the policy settings. For detailed information, refer to:
   - "Computer and Virtual Machines Policies" (p. 172)
   - "Mobile Device Policies" (p. 277)
5. Click **Save** to create the policy and return to the policies list.

When defining policies to be used in VMware NSX, besides configuring the antimalware protection settings in GravityZone Control Center, you also need to

create a policy in NSX, instructing it to use the GravityZone policy as a service profile. To create an NSX security policy:

1. Log in to vSphere Web Client.
2. Go to **Network & Security > Service Composer > Security Policies** tab.
3. Click the **Create Security Policy** button in the toolbar at the upper side of the policies table. The configuration window is displayed.
4. Enter the name of the policy and then click **Next**.

   Optionally you can also add a short description.
5. Click the **Add Guest Introspection service** button at the upper side of the table. The Guest Introspection Service configuration window is displayed.
6. Enter the name and description of the service.
7. Leave the default action selected, to allow the Bitdefender service profile to be applied on the security group.
8. From the **Service Name** menu, select **Bitdefender**.
9. From the **Service Profile** menu, select an existing GravityZone security policy.
10. Leave the default values of the **State** and **Enforce** options.

> **Note**
> For more information on the security policy settings, refer to VMware NSX documentation.

11. Click **OK** to add the service.
12. Click **Next** until the last step and then click **Finish**.

5.1.2. Assigning Policies

Endpoints are initially assigned with the default policy. Once you have defined the necessary policies in the **Policies** page, you can assign them to endpoints.

Policy assignment process is bound to the various environments that GravityZone integrates with. For certain integrations, such as VMware NSX, policies are accessible outside GravityZone Control Center. They are also refered to external policies.

Assigning Local Policies

You can assign local policies in two ways:

- Device-based assignment, meaning that you manually select the target endpoints to which you assign the policies. These policies are also known as device policies.
- Rule-based assignment, meaning that a policy is assigned to a managed endpoint if the network settings on the endpoint match the given conditions of an existing assignment rule.

Note

- You can assign only policies created by you. To assign a policy created by another user, you have to clone it first in the **Policies** page.
- On virtual machines protected by HVI alone, you can assign only device policies. When Bitdefender Endpoint Security Tools is also installed on them, you can assign rule-based policies too, the security agent managing policy activation.

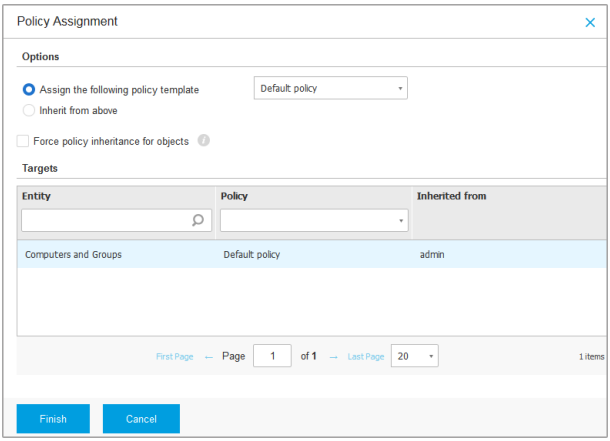
Assigning Device Policies

To assign a device policy:

1. Go to the **Network** page.
2. Choose the type of endpoint that you want from the views selector.
3. Select the check box of the network object that you want. You can select one or several objects only from the same level.
4. Click the **Assign Policy** button at the upper side of the table.

   Note
   You can also right-click on a network tree group and choose **Assign Policy** from the context menu.

   The **Policy Assignment** window is displayed:



Policy Assignment Settings

5. Configure the policy assignment settings for the selected objects:
   - View the current policy assignments for the selected objects in the table under the **Targets** section.
   - **Assign the following policy template**. Select this option to assign the target objects with one policy from the list at the right. Only the policies created from your user account are available in the list.
   - **Inherit from above**. Select the **Inherit from above** option to assign the selected network objects with the parent group's policy.
   - **Force policy inheritance for objects**. By default, each network object inherits the policy of the parent group. If you change the group policy, all the group's children will be affected, excepting the group's members for which you have specifically assigned another policy.

     Select **Force policy inheritance for objects** option to apply the chosen policy to a group, including to the group's children assigned with a different policy. In this case, the table placed below will display the selected group's children that do not inherit the group policy.
6. Click **Finish** to save and apply changes.

Policies are pushed to target network objects immediately after changing the policy assignments or after modifying the policy settings. Settings should be applied on

network objects in less than a minute (provided they are online). If a network objects is not online, settings will be applied as soon as it gets back online.

To check if the policy has been successfully assigned, go to the **Network** page and click the name of the object you are interested in to display the **Information** window. Check the **Policy** section to view the status of the current policy. If in pending state, the policy has not been applied yet to the target object.

You can also easily check the policies assignment status in the **Policies** page, under the **Applied / Pending** column. Click the applied or pending number from the policy you are interested in to display in the **Network** page all the network entities with the selected status.

Assigning Rule-Based Policies

The **Policies > Assignment Rules** page enables you to define user and location-aware policies. For example, you can apply more restrictive firewall rules when users connect to the internet from outside the company or you can enable Web Access Control for users that are not part of the administrators group.

This is what you need to know about assignment rules:

- Endpoints can have only one active policy at a time.
- A policy applied through a rule will overwrite the device policy set on the endpoint.
- If none of the assignment rules is applicable, then the device policy is applied.
- Rules are ordered and processed by priority, with `1` being the highest one. You may have several rules for the same target. In this case, will apply the first rule that matches the active connection settings on the target endpoint.

  For example, if an endpoint matches a user rule with priority 4 and a location rule with priority 3, the location rule will apply.

Warning
Make sure you consider sensitive settings such as exclusions, communication or proxy details when creating rules.
As best practice, it is recommended to use policy inheritance to keep the critical settings from the device policy also in the policy used by assignment rules.

To create a new rule:

1. Go to the **Assignment Rules** page.

2. Click the ⊕ **Add** button at the upper side of the table.
3. Select the rule type:
   - Location Rule
   - User Rule
4. Configure the rule settings as needed.
5. Click **Save** to save the changes and apply the rule to target endpoints of the policy.

To change the settings of an existing rule:

1. In the **Assignment Rules** page, find the rule you are looking for and click its name to edit it.
2. Configure the rule settings as needed.
3. Click **Save** to apply the changes and close the window. To leave the window without saving changes, click **Cancel**.

If you no longer want to use a rule, select the rule and click the ⊖ **Delete** button at the upper side of the table. You will be asked to confirm your action by clicking **Yes**.

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

Configuring Location Rules

A location is a network segment identified by one or several network settings, such as a specific gateway, a specific DNS used to resolve URLs, or a subset of IPs. For example, you can define locations such as the company's LAN, the servers farm or a department.

In the rule configuration window, follow these steps:

1. Enter a suggestive name and a description for the rule you want to create.
2. Set the priority of the rule. The rules are ordered by priority, with the first rule having the highest priority. The same priority cannot be set twice or more.
3. Select the policy for which you create the assignment rule.
4. Define the locations to which the rule applies.

a. Select the type of the network settings from the menu at the upper side of the Locations table. These are the available types:

Type	Value
IP/network prefix	Specific IP addresses in a network or sub-networks. For sub-networks use the CIDR format. For example: `10.10.0.12` or `10.10.0.0/16`
Gateway address	IP address of the gateway
WINS server address	IP address of the WINS server **Important** This option does not apply on Linux and Mac systems.
DNS server address	IP address of the DNS server
DHCP connection DNS suffix	DNS name without the hostname for a specific DHCP connection For example: `hq.company.biz`
Endpoint can resolve host	Hostname. For example: `fileserv.company.biz`
Endpoint can connect to GravityZone	Yes/No
Network type	Wireless/Ethernet When choosing Wireless, you can also add the network SSID. **Important** This option does not apply on Linux and Mac systems.

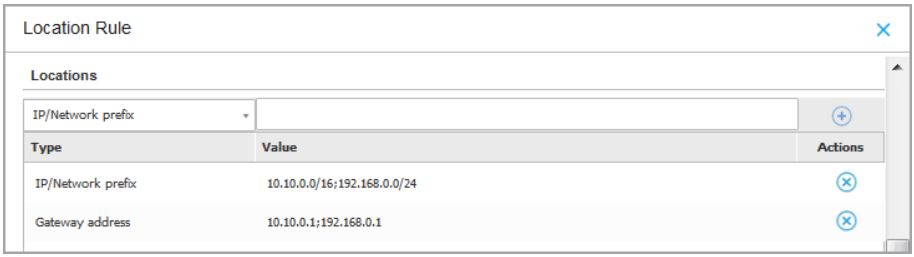
b. Enter the value for the selected type. Where applicable, you can enter multiple values in the dedicated field, separated by semicolon (;) and without

additional spaces. For example, when you enter `10.10.0.0/16;192.168.0.0/24`, the rule applies to target endpoints with the IPs matching ANY of these sub-networks.

Warning
You can use only one network setting type per location rule. For example, if you added a location using the **IP/network prefix**, you cannot use this setting again in the same rule.

c. Click the ⊕ **Add** button at the right side of the table.

The network settings on endpoints must match ALL provided locations, for the rule to apply to them. For example, to identify the office LAN network you can enter the gateway, network type and DNS; furthermore, if you add a sub-network, you identify a department within the company's LAN.



Location rule

Click the **Value** field to edit the existing criteria and then press `Enter` to save changes.

To remove a location, select it and click the ⊗ **Delete** button.

5. You may want to exclude certain locations from the rule. To create an exclusion, define the locations to be excepted from the rule:
   a. Select the **Exclusions** check box under the Locations table.
   b. Select the type of the network settings from the menu at the upper side of the Exclusions table. For more information on the options, refer to the
   c. Enter the value for the selected type. You can enter multiple values in the dedicated field, separated by semicolon (;) and without additional spaces.

d. Click the ⊕ **Add** button at the right side of the table.

The network settings on endpoints must match ALL conditions provided in the Exclusions table, for the exclusion to apply.

Click the **Value** field to edit the existing criteria and then press `Enter` to save changes.

To remove an exclusion, click the ⊗ **Delete** button at the right side of the table.

6. Click **Save** to save the assignment rule and apply it.

   Once created, the location rule automatically applies to all target endpoints that are managed.

Configuring User Rules

Important

- You can create user rules only if an Active Directory integration is available.
- You can define user rules only for Active Directory users and groups. Rules based on Active Directory groups are not supported on Linux systems.

In the rule configuration window, follow these steps:

1. Enter a suggestive name and a description for the rule you want to create.
2. Set the priority. The rules are ordered by priority, with the first rule having the highest priority. The same priority cannot be set twice or more.
3. Select the policy for which you create the assignment rule.
4. In the **Targets** section, select the users and security groups you want the policy rule to apply to. You can view your selection in the table on the right.
5. Click **Save**.

   Once created, the user-aware rule applies to managed target endpoints at user login.

Assigning NSX Policies

In NSX, security policies are assigned to security groups. A security group can contain various vCenter objects, such as datacenters, clusters and virtual machines.

To assign a security policy to a security group:

1. Log in to vSphere Web Client.

2. Go to **Network & Security > Service Composer** and click the **Security Groups** tab.
3. Create as many security groups as needed. For more information, refer to VMware documentation.

   You can create dynamic security groups, based on the security tags. This way, you can group all virtual machines found infected.
4. Right click the security group you are interested in and click **Apply Policy**.
5. Select the policy to apply and click **OK**.

5.1.3. Changing Policy Settings

Policy settings can be initially configured when creating the policy. Later on, you can change them as needed anytime you want.

Note
By default, only the user who created the policy can modify it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page.

To change the settings of an existing policy:

1. Go to the **Policies** page.
2. Choose the type of endpoint that you want from the views selector.
3. Find the policy you are looking for in the list and click its name to edit it.
4. Configure the policy settings as needed. For detailed information, refer to:
   - "Computer and Virtual Machines Policies" (p. 172)
   - "Mobile Device Policies" (p. 277)
5. Click **Save**.

   Policies are pushed to target network objects immediately after changing the policy assignments or after modifying the policy settings. Settings should be applied on network objects in less than a minute (provided they are online). If a network object is not online, settings will be applied as soon as it gets back online.

5.1.4. Renaming Policies

Policies should have suggestive names so that you or other administrator can quickly identify them.

To rename a policy:

1. Go to the **Policies** page.
2. Choose the type of endpoint that you want from the views selector.
3. Click the policy name. This will open the policy page.
4. Enter a new policy's name.
5. Click **Save**.

Note
The policy name is unique. You must enter a different name for each new policy.

5.1.5. Deleting Policies

If you no longer need a policy, delete it. Once the policy is deleted, the network objects to which it used to apply will be assigned the policy of the parent group. If no other policy applies, the default policy will be enforced eventually. When deleting a policy with sections inherited by other policies, the settings of the inherited sections are stored on the child policies.

Note
By default, only the user who created the policy can delete it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page.

To be able to delete an NSX policy from GravityZone Control Center, you must make sure the policy is not in use. Therefore, assign the target security group with another security profile. For more information, refer to "Assigning NSX Policies" (p. 169).

To delete a policy:

1. Go to the **Policies** page.
2. Choose the type of endpoint that you want from the views selector.
3. Select the check box of the policy you want to delete.
4. Click the ⊖ **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

5.2. Computer and Virtual Machines Policies

Policy settings can be initially configured when creating the policy. Later on, you can change them as needed anytime you want.

To configure the settings of a policy:

1. Go to the **Policies** page.
2. Choose **Computers and Virtual Machines** from the views selector.
3. Click the policy name. This will open the policy settings page.
4. Configure the policy settings as needed. Settings are organized under the following categories:
   - General
   - Memory Introspection
   - Antimalware
   - Firewall
   - Content Control
   - Application Control
   - Device Control
   - Relay
   - Exchange Protection
   - NSX

   You can select the settings category using the menu on the left-side of the page.
5. Click **Save** to save changes and apply them to the target computers. To leave the policy page without saving changes, click **Cancel**.

Note
To learn how to work with policies, refer to "Managing Policies" (p. 160).

5.2.1. General

General settings help you manage user interface display options, password protection, proxy settings, power user settings, communication options and update preferences for the target endpoints.

The settings are organized into the following sections:

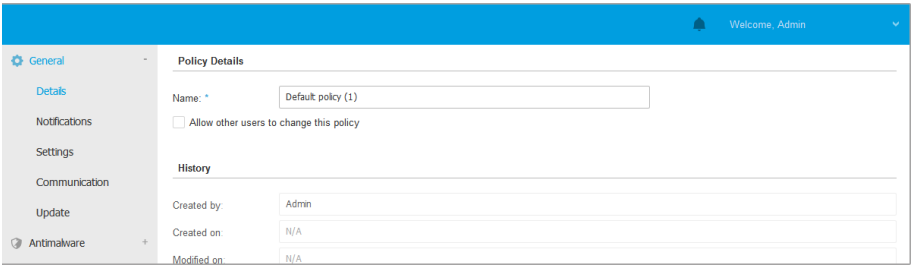
- Details
- Notifications

- Settings
- Communication
- Update

Details

The **Details** page contains general policy details:

- Policy name
- User who created the policy
- Date and time when the policy was created
- Date and time when the policy was last modified



Computers and Virtual Machines Policies

You can rename the policy by entering the new name in the corresponding field and clicking the **Save** button at the lower side of the page. Policies should have suggestive names so that you or other administrator can quickly identify them.

Note
By default, only the user who created the policy can modify it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page.

Inheritance Rules

You can set sections to be inherited from other policies. To do this:

1. Select the module and the section you want the current policy to inherit. All sections are inheritable, except for **General > Details**.
2. Specify the policy you want to inherit the section from.

3. Click the ⊕ **Add** button at the right side of the table.

If a source policy is deleted, the inheritance breaks and the settings of the inherited sections are stored on the child policy.

Inherited sections cannot be further inherited by other policies. Consider the following example:

Policy A inherits the **Antimalware > On-Demand** section from policy B. Policy C cannot inherit the **Antimalware > On-Demand** section from policy A.

Technical Support Information

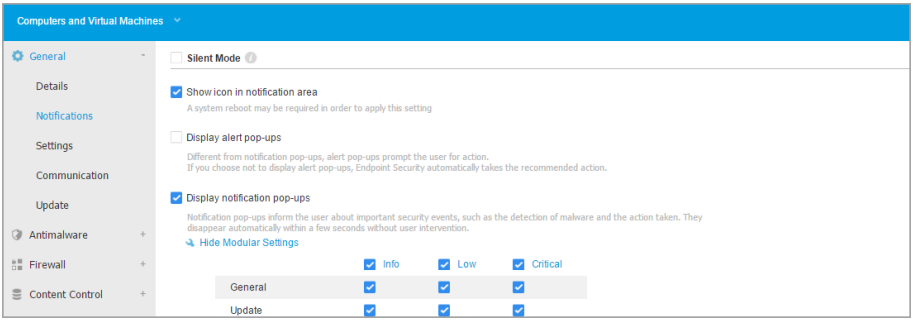
You can customize the technical support and contact information available in the security agent's **About** window by filling in the corresponding fields.

Users can access this information from the security agent console by right-clicking the Bitdefender icon in the system tray and selecting **About**.

Notifications

In this section you can configure the Bitdefender security agent's user interface display options in a comprehensive and intuitive way.

With just one click, you can enable or disable an entire type of notifications, keeping only what truly matters for you. Also, within the same page, you are provided with total control over the endpoint issues visibility.



Policies - Display Settings

- **Silent Mode.** Use the check box to turn Silent Mode on or off. Silent Mode is designed to help you easily disable user interaction in the security agent. When

turning on Silent Mode, the following changes are made to the policy configuration:

- The **Show icon in notification area**, **Display notification pop-ups** and **Display alert pop-ups** options in this section will be disabled.
- If the firewall protection level was set to **Ruleset and ask** or **Ruleset, known files and ask** it will be changed to **Ruleset, known files and allow**. Otherwise, the protection level setting will remain unchanged.

- **Show icon in notification area.** Select this option to show the Bitdefender icon in the notification area (also known as the system tray). The icon informs users on their protection status by changing its appearance and displaying a corresponding notification pop-up. Additionally, users can right-click it to quickly open the security agent main window or the **About** window. Opening the **About** window automatically initiates an on-demand update.
- **Display alert pop-ups.** Users are informed through alert pop-ups about security events that require action. If you choose not to display alert pop-ups, the security agent automatically takes the recommended action. Alert pop-ups are generated in the following situations:
  - If the firewall is set to prompt the user for action whenever unknown applications request network or Internet access.
  - If Advanced Threat Control / Intrusion Detection System is enabled, whenever a potentially dangerous application is detected.
  - If device scanning is enabled, whenever an external storage device is connected to the computer. You can configure this setting in the **Antimalware > On-demand** section.
- **Display notification pop-ups.** Different from alert pop-ups, the notification pop-ups inform users about diverse security events. The pop-ups disappear automatically within a few seconds without user intervention.

  Select **Display notification pop-ups**, then click the **Show Modular Settings** link to choose what events you want the users to be informed about, provided by module. There are three types of notification pop-ups, based on the severity of the events:
  - **Info**. Users are informed about significant but harmless security events. For example, an application that has connected to the Internet.

- **Low**. Users are informed about important security events that may require attention. For example, On-Access scanning has detected a threat and the file has been deleted or quarantined.
- **Critical**. These notification pop-ups inform the users about dangerous situations, such as On-Access scanning that has detected a threat and the default policy action is **Take no action**, thus the malware is still present on the endpoint, or an update process that was unable to complete.

Select the check box associated to the type name to enable that kind of pop-ups for all modules at once. Click the check boxes associated to individual modules to enable or disable specific notifications.

The list of modules may vary according to your license.

- **Endpoint Issues Visibility.** Users determine when their endpoint has security configuration issues or other security risks, based on status alerts. For example, users can view whenever there is a problem related to their antimalware protection, such as: On-Access scanning module is disabled or a full system scan is overdue. Users are informed about their protection status in two ways:
  - Checking the status area of the main window, which displays an appropriate status message and changes its color depending on the severity of the security issues. Users have the possibility to view issues details as well, by clicking the available button.
  - Checking the Bitdefender icon in the system tray, which changes its appearance when issues are detected.

  Bitdefender security agent uses the following color scheme in the notification area:
  - Green: No issues are detected.
  - Yellow: The endpoint has non-critical issues that affect its security. Users don't have to interrupt their current work for resolving these issues.
  - Red: The endpoint has critical issues that require user's immediate action.

  Select **Endpoint Issues Visibility**, then click the **Show Modular Settings** link to customize the status alerts displayed in the Bitdefender's agent user interface.

  For each module, you may choose to show the alert as a warning or a critical issue, or not to display it at all. The options are described herein:

- **General**. The status alert is generated whenever a system restart is required during or after product installation, and also when the security agent could not connect to Bitdefender Cloud Services.
- **Antimalware**. Status alerts are generated in the following situations:
  - On-Access scanning is enabled but many local files are skipped.
  - A certain number of days have passed since the last full system scan has been performed on the machine.

    You may select how to show the alerts and define the number of days from the last full system scan.
  - A restart is required to complete a disinfection process.
- **Firewall**. This status alert is generated when the Firewall module is disabled.
- **Application Control**. This status alert is generated when the Application Control module is modified.
- **Content Control**. This status alert is generated when the Content Control module is disabled.
- **Update**. The status alert is generated whenever a system restart is required to complete an update operation.

Settings

In this section you can configure the following settings:

- **Password configuration.** To prevent users with administrative rights from uninstalling protection, you must set a password.

  The uninstall password can be configured before installation by customizing the installation package. If you have done so, select **Keep installation settings** to keep the current password.

  To set the password, or to change the current password, select **Enable password** and enter the desired password. To remove password protection, select **Disable password**.
- **Proxy Configuration**

  If your network is behind a proxy server, you need to define the proxy settings that will allow your endpoints to communicate with the GravityZone solution components. In this case, you need to enable the **Proxy Configuration** option and fill in the required parameters:

- **Server** - enter the IP of the proxy server
- **Port** - enter the port used to connect to the proxy server.
- **Username** - enter a user name recognized by the proxy.
- **Password** - enter the valid password for the specified user

- **Power User**

  The Power User module enables administration rights at endpoint level, allowing the endpoint user to access and modify policy settings via a local console, through the Bitdefender Endpoint Security Tools interface.

  If you want certain endpoints to have Power User rights, you need at first to include this module in the security agent installed on target endpoints. After that, you need to configure the Power User settings in the policy applied to these endpoints:

  Important
  The Power User module is available only for supported Windows desktop and server operating systems.

  1. Enable the **Power User** option.
  2. Define a Power User password in the fields below.

     Users accessing the Power User mode from the local endpoint will be prompted to enter the defined password.

  To access the Power User module, users must right-click the Bitdefender icon from their system tray and choose **Power User** from the contextual menu. After providing the password in the login window, a console containing the currently applied policy settings will show up, where the endpoint user can view and modify the policy settings.

  Note
  Only certain security features can be accessed locally via the Power User console, concerning the Antimalware, Firewall, Content Control and Device Control modules.

  To revert the changes made in Power User mode:

  - In Control Center, open the policy template assigned to the endpoint with Power User rights and click **Save**. In this way, the original settings will be reapplied to the target endpoint.
  - Assign a new policy to the endpoint with Power User rights.

– Login to the local endpoint, open the Power User console and click **Resync**.

To easily find endpoints with policies modified in Power User mode:

– In the **Network** page, click the **Filters** menu and select the **Edited by Power User** option from the **Policy** tab.

– In the **Network** page, click the endpoint you are interested in to display the **Information** window. If the policy was modified in Power User mode, a notification will be displayed in the **General** tab > **Policy** section.

Important
The Power User module is specifically designed for troubleshooting purposes, allowing the network administrator to easily view and change policy settings on local computers. Assigning Power User rights to other users in the company must be limited to authorized personnel, to ensure that the security policies are being always applied on all endpoints of the company network.

- **Options**

  In this section you can define the following settings:

  – **Remove events older than (days).** Bitdefender security agent keeps a detailed log of events concerning its activity on the computer (also including computer activities monitored by Content Control). By default, events are deleted from the log after 30 days. If you want to change this interval, choose a different option from the menu.

  – **Submit crash reports to Bitdefender.** Select this option so that reports will be sent to Bitdefender Labs for analysis if the security agent crashes. The reports will help our engineers find out what caused the problem and prevent it from occurring again. No personal information will be sent.

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

Communication

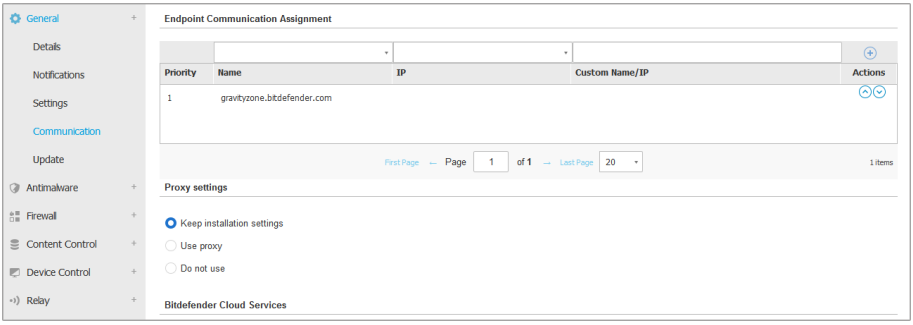
In this section, you can assign one or several relay machines to the target endpoints, then configure the proxy preferences for the communication between the target endpoints and GravityZone.

Endpoint Communication Assignment

When multiple communication servers are installed on the GravityZone appliance, you can assign the target computers with one or several communication servers via policy. Available relay endpoints, which serve as communication servers, are also taken into account.

To assign communication servers to target computers:

1. In the **Endpoint Communication Assignment** table, click the **Name** field. The list of detected communication servers is displayed.
2. Select an entity.



Computers and Virtual Machines Policies - Communication settings

3. Click the ⊕ **Add** button at the right side of the table.

   The communication server is added to the list. All target computers will communicate with Control Center via the specified communication server.
4. Follow the same steps to add several communication servers, if available.
5. You can configure the communication servers priority using the up and down arrows available at the right side of each entity. The communication with target computers will be carried out through the entity placed on top of the list. When the communication with this entity cannot be done, the next one will be taken into account.
6. To delete one entity from the list, click the corresponding ⊗ **Delete** button at the right side of the table.

Communication between Endpoints and Relays / GravityZone

In this section, you can configure the proxy preferences for the communication between the target endpoints and the assigned relay machines, or between target endpoints and the GravityZone appliance (when no relay has been assigned):

- **Keep installation settings**, to use the same proxy settings defined with the installation package.
- **Use proxy defined in the General section**, to use the proxy settings defined in the current policy, under **General > Settings** section.
- **Do not use**, when the target endpoints do not communicate with the specific GravityZone components via proxy.

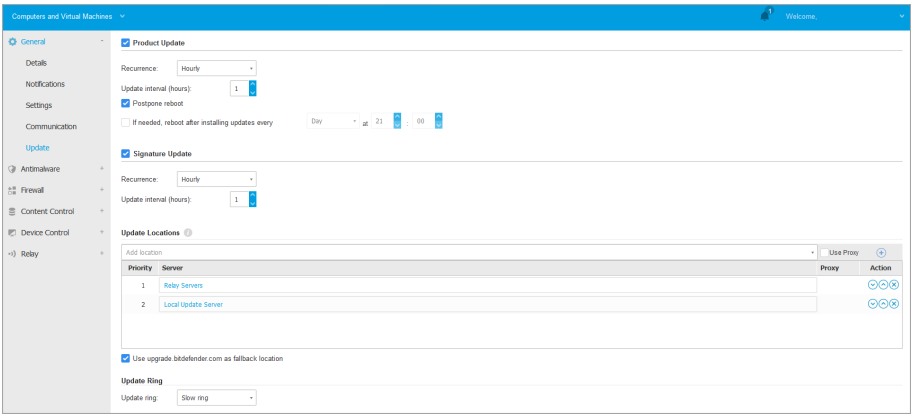
Communication between Endpoints and Cloud Services

In this section, you can configure the proxy preferences for the communication between the target endpoints and Bitdefender Cloud Services (requiring internet connection):

- **Keep installation settings**, to use the same proxy settings defined with the installation package.
- **Use proxy defined in the General section**, to use the proxy settings defined in the current policy, under **General > Settings** section.
- **Do not use**, when the target endpoints do not communicate with the specific GravityZone components via proxy.

Update

Updates are very important as they allow countering the latest threats. Bitdefender publishes all product and signature updates through the Bitdefender servers on the Internet. All updates are encrypted and digitally signed so that they cannot be tampered with. When a new update is available, the Bitdefender security agent checks the digital signature of the update for authenticity, and the contents of the package for integrity. Next, each update file is parsed and its version is checked against the installed one. Newer files are downloaded locally and checked against their MD5 hash to make sure they are not altered. In this section you can configure the Bitdefender security agent and virus signature update settings.



Computers and Virtual Machines Policies - Update options

- **Product Update.** Bitdefender security agent automatically checks for, downloads and installs updates every hour (default setting). Automatic updates are performed silently in the background.
  - **Recurrence**. To change the automatic update recurrence, choose a different option from the menu and configure it according to your needs in the subsequent fields.
  - **Postpone reboot**. Some updates require a system restart to install and work properly. By default, the product will keep working with the old files until the computer is restarted, after which it will apply the latest updates. A notification in the user interface will prompt the user to restart the system whenever an update requires it. It is recommended to leave this option enabled. Otherwise, the system will automatically reboot after installing an update that requires it. Users will be notified to save their work, but the reboot cannot be canceled.
  - If you choose to postpone reboot, you can set a convenient time when computers will reboot automatically if (still) needed. This can be very useful for servers. Select **If needed, reboot after installing updates** and specify when it is convenient to reboot (daily or weekly on a certain day, at a certain time of day).
- **Signature Update.** Bitdefender security agent automatically checks for signature update every hour (default setting). Automatic updates are performed silently

in the background. To change the automatic update recurrence, choose a different option from the menu and configure it according to your needs in the subsequent fields.

- **Update Locations**. Bitdefender security agent's default update location is the local GravityZone update server. Add an update location either by choosing the predefined locations from the drop-down menu or by entering the IP or hostname of one or several update servers in your network. Configure their priority using the up and down buttons displayed on mouse-over. If the first update location is unavailable, the next one is used and so on.

  To set a local update address:

  1. Enter the address of the update server in the **Add location** field. You can:
     - Choose a predefined location:
       - **Relay Servers**. The endpoint will automatically connect to its assigned Relay Server.

         Note
         You can check the assigned Relay Server in the **Information** window. For more details refer to Viewing Computer Details.

       - **Local Update Server**
     - Enter the IP or hostname of one or several update servers in your network. Use one of these syntaxes:
       - `update_server_ip:port`
       - `update_server_name:port`

       The default port is 7074.

       The **Use upgrade.bitdefender.com as fallback location** check box is selected by default. If the update locations are unavailable, the fallback location will be used.

     Warning
     Disabling the fallback location will stop automatic updates, leaving your network vulnerable when the provided locations are unavailable.

2. If client computers connect to the local update server through a proxy server, select **Use Proxy**.
3. Click the ⊕ **Add** button at the right side of the table.
4. Use the ⌃ Up / ⌄ Down arrows in the **Action** column to set priority of defined update locations. If the first update location is not available, the next one is taken into account, and so on.

To remove a location from the list, click the corresponding ⊗ **Delete** button. Although you can remove the default update location, this is not recommended.

- **Update Ring.** You can roll out product updates in phases, using update rings:
  - **Slow Ring**. The machines with a slow ring policy will receive updates at a later date, depending on the response received from the fast ring endpoints. It is a precautionary measure in the update process. This is the default setting.
  - **Fast Ring**. The machines with a fast ring policy will receive the newest available updates. This setting is recommended for the non-critical machines in production.

> **Important**
> In the unlikely event that an issue occurs on the fast ring on machines with a particular configuration, it will be fixed before the slow ring update.

> **Note**
> For details on how the update rings selection affects staging, refer to the **Update GravityZone > Staging** chapter from the GravityZone Installation Guide.

5.2.2. HVI

Hypervisor Memory Introspection protects virtual machines against advanced threats that signature-based engines cannot defeat. It ensures real-time detection of attacks, by monitoring processes from outside the guest operating system. The protection mechanism includes several options to block attacks as they happen and immediately remove the threat.

> **Important**
> HVI provides protection only to virtual machines on Citrix Xen hypervisors.

Following the memory separation principle of the operating systems, HVI also includes two protection modules organized in the related categories:

- User Space, addressing normal processes of the user applications.
- Kernel Space, addressing processes reserved to the core of the operating system.

User Space

In this section you can configure the protection settings for processes running in user space memory.

Use the **User Space Memory Introspection** check box to enable or disable protection.

Functionality of this module relies on rules, allowing you to configure protection separately for different groups of processes. Additionaly, you can choose to collect more forensic information.

- User Space Rules
- Forensic Information

User Space Rules

The module comes with a set of predefined rules that address most vulnerable applications. The table in this section lists existing rules, providing important information on each of them:

- Rule name
- Processes the rule applies to
- Monitoring mode
- Action that blocks the detected attack
- Actions to remove the threat

You can also provide a list of custom rules for the processes you want to monitor. To create a new rule:

1. Click the ⊗ **Add** button at the upper side of the table. This action opens the rule configuration window.
2. Configure the module using the following rule settings:

- **Rule name.** Enter the name under which the rule will be listed in the rules table. For example, for processes such as `firefox.exe` or `chrome.exe`, you can name the rule `Browsers`.
- **Processes.** Enter the name of the processes you intend to monitor, separated by semicolon (;).
- **Monitoring mode.** For a quick configuration, click the security level that best suits your needs (**Aggressive**, **Normal** or **Permissive**). Use the description on the right side of the scale to guide your choice.

  You can configure the module settings in detail by choosing the **Custom** protection level and selecting one or more of the following options:

  - **Hooks being set on critical user mode DLLs.** Detect DLL injections, which load malicious code into the calling process.
  - **Unpacking/decrypting attempts in the main executable.** Detect attempts to decipher the code in the main process executable, and protect the process from being altered with malicious instructions.
  - **Foreign writes inside the target process.** Protect against code injection in the protected process.
  - **Exploits.** Detect unintended process behavior caused by the exploitation of a bug or of a previously undisclosed vulnerability. Use this option if you want to monitor code execution from heap and stack of the protected applications.
  - **Hooking of WinSock.** Block interceptions of network libraries (DLLs) used by the operating system, ensuring a sound TCP/IP communication.
- **Actions.** There are several actions which you can take on detected threats. Each action has, at its turn, several possible options or secondary actions. Find them described herein:
  - **Primary action.** This is the immediate action which you can take when an attack is detected on the guest machine, allowing you to block it. These are the available options:
    - **Log.** Only record the event in the database. In this case you will only receive a notification (if configured) and will be able to view the incident in the **HVI Activity** report.
    - **Deny.** Reject any attempt of the threat to alter the target process.

- **Shut Down Machine.** Power off the virtual machine on which the target process runs.

Important
It is recommended to set the primary action first to **Log**. Then use the policy for a fair amount of time to ensure that everything is running according to expectations. Afterwards, you can select whichever action you want to be taken in case of a memory violation detection.

– **Remediation action.** Depending on the selected option, the Security Server injects a remediation tool on the guest operating system. The tool automatically starts scanning for malware and when a threat is detected, it proceeds with the selected action. These are the available options:

- **Disinfect.** Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.
- **Delete.** Delete detected files from the disk, without any warning. It is advisable to avoid using this action.
- **Ignore.** The remediation tool detects and only reports the detected files.
- **None.** The remediation tool will not be injected in the guest operating system.

Note
Closing the tool will remove it from the system as well, leaving no tracks in the guest operating system.

– **Backup remediation action.** When the remediation action fails, you can choose another remediation action from the available options.

3. Click **Save**.

Once created, you can edit a rule at any time. Clicking the rule name will open the rule configuration window.

GravityZone also allows you to quickly configure Memory Introspection behavior upon detections, by changing several rules at once. To set multiple rules with the same actions:

1. Select the rules you want to change.
2. Click the **Action and Remediation** button at the upper side of the table.
3. Select the option you want for each action.
4. Click **Save**. New actions will become effective once you save the policy, provided the target machines are online.

To remove one or several rules from the list, select them and then click the ⊗ **Delete** button at the upper side of the table.

Forensic Information

Select the **Application crash events** check box below the user space rules table to enable collecting detailed information when applications are being terminated.

You can view this information in the HVI Activity report, and find the reason which caused the application to terminate. If the event is related to an attack, its details will apppear grouped with other events under the corresponding incident that led to the event.

Kernel Space

HVI protects key elements of the operating system, such as:

- Critical kernel drivers and the associated driver objects, involving fast I/O dispatch tables associated with core drivers.
- Network drivers, whose alteration would allow a malware to intercept traffic and to inject malicious components in the traffic stream.
- Kernel image of the operating system, involving the following: code section, data section and read-only section, including the Import Address Table (IAT), Export Address Table (EAT) and resources.

In this section you can configure the protection settings for processes running in the kernel space memory.

Use the **Kernel Space Memory Introspection** check box to enable or disable protection.

For a quick configuration, click the security level that best suits your needs (**Aggressive**, **Normal** or **Permissive**). Use the description on the right side of the scale to guide your choice.

You can configure the module settings in detail by choosing the **Custom** protection level and selecting one or more of the following options:

- **Control registers**. Control Registers (CR) are processor registers that control the general behavior of a processor or other digital device. Select this option to detect loading attempts of invalid values into specific Control Registers.
- **Model specific registers**. These registers refer to any of the various control registers in the x86 instruction set used for debugging, program execution tracing, computer performance monitoring, and toggling certain CPU features. Select this option to detect attempts of changing these registers.
- **IDT/GDT integrity**. The Global or Interrupt Descriptor Tables (IDT/GDT) are used by the processor to determine the correct response to interrupts and exceptions. Select this option to detect any attempts to change these tables.
- **Antimalware drivers protection.** Select this option to detect attempts to alter drivers used by the antimalware software.
- **Xen drivers protection.** Select this option to detect attempts to alter drivers of the Citrix XenServer hypervisor.

There are several actions which you can take on detected threats. Each action has, at its turn, several possible options or secondary actions. Find them described herein:

- **Primary action.**
  - **Log.** Only record the event in the database. In this case you will only receive a notification (if configured) and will be able to view the incident in the **Memory Introspection Activity** report.
  - **Deny.** Reject any attempt of the threat to alter the target process.
  - **Shut Down Machine.** Power off the virtual machine on which the target process runs.

  Important
  It is recommended to set the primary action first to **Log**. Then use the policy for a fair amount of time to ensure that everything is running according to expectations. Afterwards, you can select whichever action you want to be taken in case of a memory violation detection.

- **Remediation action.**

  - **Disinfect.** Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.
  - **Delete.** Delete detected files from the disk, without any warning. It is advisable to avoid using this action.
  - **Ignore.** The remediation tool detects and only reports the detected files.
  - **None.** The remediation tool will not be injected in the guest operating system.
- **Backup remediation action.** When the remediation action fails, you can choose another remediation action from the available options.

Aditionally, you can choose to gather information that will enrich the data provided to forensic teams. Select the **OS failures events** and **Driver events** check boxes to enable collecting information related to guest operating system failures or to events generated by additional modules loaded by the the operating system. These events, preceding an incident, will help forensic investigations to faster zero in on the root-cause of the attack.

These events are aggregated in the HVI Activity report under the incident that led to them.

5.2.3. Antimalware

The Antimalware module protects the system against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on). The protection is divided in two categories:

- On-access scanning: prevents new malware threats from entering the system.
- On-demand scanning: allows detecting and removing malware already residing in the system.

When it detects a virus or other malware, Bitdefender security agent will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to isolate the infection. When a virus is in quarantine, it cannot do any harm because it cannot be executed or read.

Advanced users can configure scan exclusions if they do not want specific files or file types to be scanned.

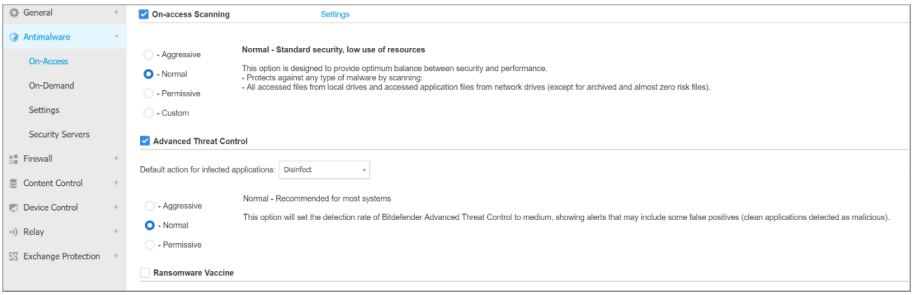
The settings are organized into the following sections:

- On-Access
- On-Demand
- Settings
- Security Servers

On-Access

In this section you can configure the antimalware protection components:

- On-access scanning
- Advanced Threat Control
- Ransomware vaccine



Computers and Virtual Machines Policies - On Access Settings

On-access Scanning

On-access scanning prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA).

To configure on-access scanning:

1. Use the check box to turn on-access scanning on or off.

   Warning
   If you turn off on-access scanning, endpoints will be vulnerable to malware.

2. For a quick configuration, click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.

3. You can configure the scan settings in detail by selecting the **Custom** protection level and clicking the **Settings** link. The **On-access Scanning Settings** window will appear, containing several options organized under two tabs, **General** and **Advanced**.

   The options under the **General** tab are described hereinafter:

   - **File location**. Use these options to specify which types of files you want to be scanned. Scan preferences can be configured separately for local files (stored on the local endpoint) or network files (stored on network shares). If antimalware protection is installed on all computers in the network, you may disable the network files scan to allow a faster network access.

     You can set the security agent to scan all accessed files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all accessed files provides best protection, while scanning applications only can be used for better system performance.

     > **Note**
     > Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

     If you want only specific extensions to be scanned, choose **User defined extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

     For system performance reasons, you can also exclude large files from scanning. Select **Maximum size (MB)** checkbox and specify the size limit of the files which will be scanned. Use this option wisely because malware can affect larger files too.
   - **Scan.** Select the corresponding check boxes to enable the desired scan options.
     - **Only new or changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
     - **Boot sectors.** Scans the system's boot sector. This sector of the hard disk contains the necessary code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
     - **For keyloggers.** Keyloggers record what you type on your keyboard and send reports over the Internet to a malicious person (hacker). The hacker

can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

- **For Potentially Unwanted Applications (PUA).** A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.
- **Archives**. Select this option if you want to enable on-access scanning of archived files. Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having on-access scanning enabled.

  If you decide on using this option, you can configure the following optimization options:
  - **Archive maximum size (MB).** You can set a maximum accepted size limit of archives to be scanned on-access. Select the corresponding check box and type the maximum archive size (in MB).
  - **Archive maximum depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.
- **Deferred Scanning.** Deferred scanning improves system performance when performing file access operations. For example, system resources are not affected when large files are copied. This option is enabled by default.

- **Scan Actions**. Depending on the type of detected file, the following actions are taken automatically:
  - **Default action for infected files.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies. Bitdefender security agent can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

By default, if an infected file is detected, Bitdefender security agent will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine to contain the infection. You can change this recommended flow according to your needs.

> **Important**
> For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

– **Default action for suspect files.** Files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but the users must be aware of certain false positives (clean files detected as suspicious) in some cases. Suspect files cannot be disinfected, because no disinfection routine is available.

  When a suspect file is detected, users will be denied access to that file to prevent a potential infection.

Though not recommended, you can change the default actions. You can define two actions for each type of file. The following actions are available:

Deny access
Deny access to detected files.

> **Important**
> For MAC endpoints, **Move to quarantine** action is taken instead of **Deny access**.

Disinfect
Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

Delete
Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Move to quarantine
Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

Take no action
Only report the infected files detected by Bitdefender.

The **Advanced** tab addresses the on-access scanning for Linux machines. Use the checkbox to turn it on or off.

In the table below, you can configure the Linux directories you want to scan. By default, there are five entries, each one corresponding to a specific location on endpoints: `/home`, `/bin`, `/sbin`, `/usr`, `/etc`.

To add more entries:

- Write down any custom location name in the search field, at the upper side of the table.
- Select the predefined directories from the list displayed when clicking the arrow at the right-end of the search field.

Click the ⊕ **Add** button to save a location to the table and the ⊗ **Delete** button to remove it.

Advanced Threat Control

Bitdefender Advanced Threat Control is an innovative proactive detection technology which uses advanced heuristic methods to detect new potential threats in real time.

Advanced Threat Control continuously monitors the applications running on the endpoint, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful. Advanced Threat Control will automatically try to disinfect the detected file. If the disinfection routine fails, Advanced Threat Control will delete the file. For more information, go to our web site and check out the whitepaper on Advanced Threat Control.

Note
Before applying the disinfect action, a copy of the file is sent to quarantine so as you can restore the file later, in the case of a false positive. This action can be configured using the **Copy files to quarantine before applying the disinfect action** option available in the **Antimalware > Settings** tab of the policy settings. This option is enabled by default in the policy templates.

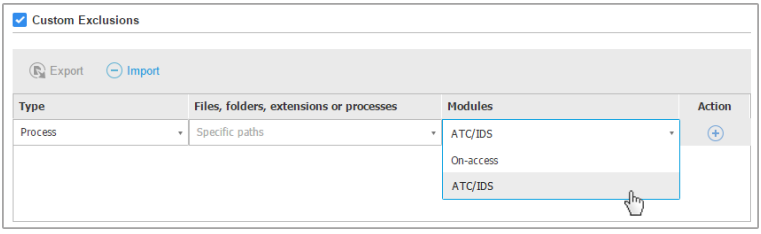
To configure Advanced Threat Control:

1. Use the check box to turn Advanced Threat Control on or off.

Warning
If you turn off Advanced Threat Control, computers will be vulnerable to unknown malware.

2. The default action for infected applications detected by Advanced Threat Control is disinfect. You can set another default action, using the available menu:
   - **Block**, to to deny access to the infected application.
   - **Take no action**, to only report the infected applications detected by Bitdefender.
3. Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.

Note
As you set the protection level higher, Advanced Threat Control will require fewer signs of malware-like behavior to report a process. This will lead to a higher number of applications being reported and, at the same time, to an increased likelihood of false positives (clean applications detected as malicious).
It is highly recommended to create exclusion rules for commonly used or known applications to prevent false positives (incorrect detection of legitimate applications). Go to the Antimalware > Settings tab and configure the ATC/IDS process exclusion rules for trusted applications.



Computers and Virtual Machines Policies - ATC/IDS process exclusion

Ransomware vaccine

Ransomware vaccine immunizes your machines against **known** ransomware blocking the encryption process even if the computer is infected. Use the check box to turn Ransomware vaccine on or off.

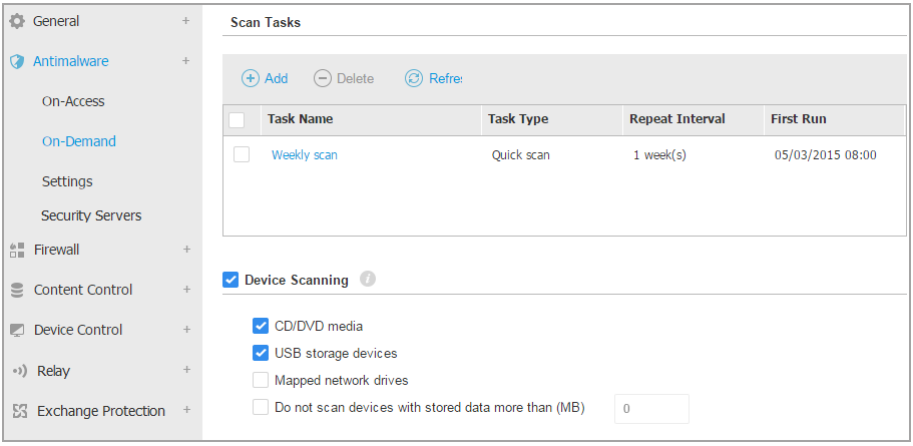
The Ransomware vaccine feature is deactivated by default. Bitdefender Labs analyze the behavior of widespread ransomware, and new signatures are delivered with each malware signature update, to address the latest threats.

Warning
To further increase protection against ransomware infections, be cautious about unsolicited or suspicious attachments and make sure the malware signature database is updated.

Note
Ransomware vaccine is available only if machines are protected by Bitdefender Endpoint Security Tools and Endpoint Security (legacy agent).

On-Demand

In this section you can add and configure antimalware scan tasks that will run regularly on the target computers, according to the specified schedule.



Computers and Virtual Machines Policies - On Demand Scan Tasks

The scanning is performed silently in the background, regardless the user is logged in the system or not. When logged in, the user is informed that a scanning process is running only through an icon that appears in the system tray.

Though not mandatory, it is recommended to schedule a comprehensive system scan to run weekly on all endpoints. Scanning endpoints regularly is a proactive

security measure that can help detect and block malware that might evade real-time protection features.

Besides regular scans, you can also configure the automatic detection and scanning of external storage media.

Managing Scan Tasks

The Scan Tasks table informs you of the existing scan tasks, providing important information on each of them:

- Task name and type.
- Schedule based on which the task runs regularly (recurrence).
- Time when the task was first run.

You can add and configure the following types of scan tasks:

- **Quick Scan** uses in-the-cloud scanning to detect malware running in the system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

  When malware or rootkits are found, Bitdefender automatically proceeds with disinfection. If, for any reason, the file cannot be disinfected, then it is moved to quarantine. This type of scanning ignores suspicious files.

  The Quick Scan is a default scan task with preconfigured options that cannot be changed. You can add only one quick scan task for the same policy.

- **Full Scan** checks the entire endpoint for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

  Bitdefender automatically tries to disinfect files detected with malware. In case malware cannot be removed, it is contained in quarantine, where it cannot do any harm. Suspicious files are being ignored. If you want to take action on suspicious files as well, or if you want other default actions for infected files, then choose to run a Custom Scan.

  The Full Scan is a default scan task with preconfigured options that cannot be changed. You can add only one full scan task for the same policy.

- **Custom Scan** allows you to choose the specific locations to be scanned and to configure the scan options.

- **Network Scan** is a type of custom scan, which allows assigning one single managed endpoint to scan network drives, then configuring the scan options

and the specific locations to be scanned. For network scan tasks, you need to enter the credentials of a user account with read/write permissions on the target network drives, for the security agent to be able to access and take actions on these network drives.

The recurrent network scan task will be sent only to the selected scanner endpoint. If the selected endpoint is unavailable, the local scanning settings will apply.

Note
You can create network scan tasks only within a policy that is already applied to an endpoint which can be used as a scanner.

Besides the default scan tasks (which you cannot delete or duplicate), you can create as many custom and network scan tasks as you want.

To create and configure a new custom or network scan task, click the ⊕ **Add** button at the right side of the table. To change the settings of an existing scan task, click the name of that task. Refer to the following topic to learn how to configure the task settings.

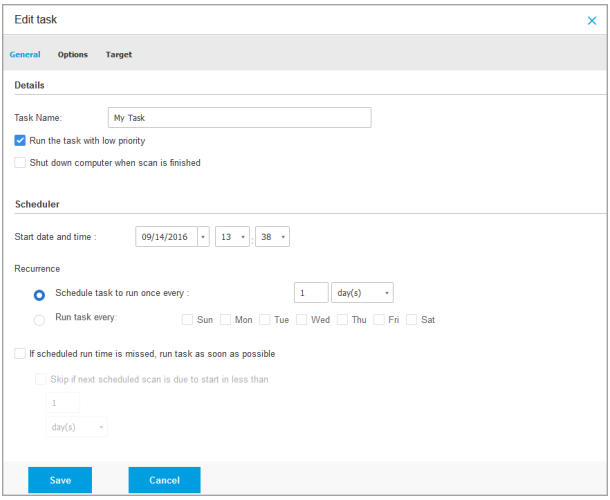
To remove a task from the list, select the task and click the ⊖ **Delete** button at the right side of the table.

Configuring Scan Tasks

The scan task settings are organized under three tabs:

- **General**: set task name and execution schedule.
- **Options**: choose a scan profile for quick configuration of the scan settings and define scan settings for a custom scan.
- **Target**: select the files and folders to be scanned and define scan exclusions.

Options are described hereinafter from the first tab to the last:



Computers and Virtual Machines Policies - Configuring On Demand Scan Tasks General Settings

- **Details.** Choose a suggestive name for the task to help easily identify what it is about. When choosing a name, consider the scan task target and possibly the scan settings.

  By default, scan tasks run with decreased priority. This way, Bitdefender allows other programs to run faster, but increases the time needed for the scan process to finish. Use the **Run the task with low priority** check box to disable or re-enable this feature.

  Select the **Shut down computer when scan is finished** check box to turn off your machine if you do not intend to use it for a while.

  > **Note**
  > These two options apply only to Bitdefender Endpoint Security Tools and Endpoint Security (legacy agent).

- **Scheduler.** Use the scheduling options to configure the scan schedule. You can set the scan to run every few hours, days or weeks, starting with a specified date and time.

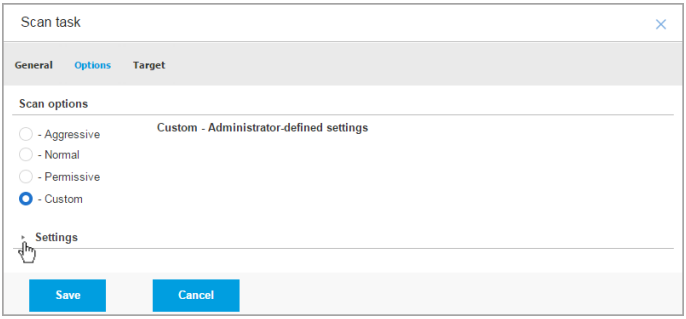
  Please consider that computers must be on when the schedule is due. A scheduled scan will not run when due if the machine is turned off, hibernating

or in sleep mode, or if no user is logged on. In such situations, the scan will be postponed until next time.

Note
The scheduled scan will run at the target endpoint local time. For example, if the scheduled scan is set to start at 6:00 PM and the endpoint is in a different timezone than Control Center, the scanning will start at 6:00 PM (endpoint time).

- **Scan Options.** Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.

  Based on the selected profile, the scan options in the **Settings** section are automatically configured. However, if you want to, you can configure them in detail. To do that, select the **Custom** check box and then go to the **Settings** section.



Computers Scan task - Configuring a Custom Scan

- **File Types.** Use these options to specify which types of files you want to be scanned. You can set the security agent to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

Note
Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

If you want only specific extensions to be scanned, choose **User Defined Extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

- **Archives.** Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

  Note
  Scanning archived files increases the overall scanning time and requires more system resources.

  – **Scan inside archives.** Select this option if you want to check archived files for malware. If you decide on using this option, you can configure the following optimization options:

    - **Limit archive size to (MB).** You can set a maximum accepted size limit of archives to be scanned. Select the corresponding check box and type the maximum archive size (in MB).
    - **Maximum archive depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.

  – **Scan email archives.** Select this option if you want to enable scanning of email message files and email databases, including file formats such as .eml, .msg, .pst, .dbx, .mbx, .tbb and others.

    Note
    Email archive scanning is resource intensive and can impact system performance.

- **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.

  – **Scan boot sectors.** Scans the system's boot sector. This sector of the hard disk contains the necessary code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.

- **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.
- **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.
- **Scan for keyloggers.** Select this option to scan for keylogger software.
- **Scan network shares.** This option scans mounted network drives.

  For quick scans, this option is deactivated by default. For full scans, it is activated by default. For custom scans, if you set the security level to **Aggressive/Normal**, the **Scan network shares** option is automatically enabled. If you set the security level to **Permissive**, the **Scan network shares** option is automatically disabled.
- **Scan memory.** Select this option to scan programs running in the system's memory.
- **Scan cookies.** Select this option to scan the cookies stored by browsers on the endpoint.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan for Potentially Unwanted Applications (PUA).** A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

- **Actions.** Depending on the type of detected file, the following actions are taken automatically:
  - **Default action for infected files.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies. The security agent can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

If an infected file is detected, the security agent will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

Important
For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- **Default action for suspect files.** Files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but the users must be aware of certain false positives (clean files detected as suspicious) in some cases. Suspect files cannot be disinfected, because no disinfection routine is available.

  Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine. Quarantined files are sent for analysis to Bitdefender Labs on a regular basis. If malware presence is confirmed, a signature is released to allow removing the malware.

- **Default action for rootkits.** Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

  Detected rootkits and hidden files are ignored by default.

Though not recommended, you can change the default actions. You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file. The following actions are available:

Take no action
No action will be taken on detected files. These files will only appear in the scan log.

Disinfect
Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

Delete
Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Move to quarantine
Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

- **Scan Target.** Add to the list all the locations you want to be scanned on the target computers.

  To add a new file or folder to be scanned:

  1. Choose a predefined location from the drop-down menu or enter the **Specific paths** you want to scan.
  2. Specify the path to the object to be scanned in the edit field.
     - If you have chosen a predefined location, complete the path as needed. For example, to scan the entire `Program Files` folder, it suffices to select the corresponding predefined location from the drop-down menu. To scan a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name.
     - If you have chosen **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.
  3. Click the corresponding ⊕ **Add** button.

  To edit an existing location, click it. To remove a location from the list, move the cursor over it and click the corresponding ⊖ **Delete** button.

- For network scan tasks, you need to enter the credentials of a user account with read/write permissions on the target network drives, for the security agent to be able to access and take actions on these network drives.

- **Exclusions.** You can either use the exclusions defined in the **Antimalware > Exclusions** section of the current policy, or you can define custom exclusions for the current scan task. For more details regarding exclusions, refer to "Exclusions" (p. 207).

Device Scanning

You can configure the security agent to automatically detect and scan external storage devices when they are connected to the endpoint. Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- Mapped network drives
- Devices with more than a specified amount of stored data.

Device scans automatically attempt to disinfect files detected as infected or to move them to quarantine if disinfection is not possible. Take into account that no action can be taken on infected files detected on CDs/DVDs or on mapped network drives that allow read-only access.

Note
During a device scan, the user can access any data from the device.

If alert pop-ups are enabled in the **General > Display** section, the user is prompted whether or not to scan the detected device instead of the scan starting automatically.

When a device scan is started:

- A notification pop-up informs the user about the device scan, provided that notification pop-ups are enabled in the **General > Display** section.

Once the scan is completed, the user must check detected threats, if any.

Select **Device Scanning** option to enable the automatic detection and scanning of storage devices. To configure device scanning individually for each type of device, use the following options:

- **CD/DVD media**
- **USB storage devices**
- **Mapped network drives**
- **Do not scan devices with stored data more than (MB)**. Use this option to automatically skip scanning of a detected device if the amount of stored data exceeds the specified size. Type the size limit (in megabytes) in the corresponding field. Zero means that no size restriction is imposed.

Note
This option applies only to CDs/DVDs and USB storage devices.

Settings

In this section you can configure the quarantine settings and the scan exclusion rules.

- Configuring quarantine settings
- Configuring scan exclusions

Quarantine

You can configure the following options for the quarantined files from the target endpoints:

- **Delete files older than (days).** By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, choose a different option from the menu.
- **Submit quarantined files to Bitdefender Labs every (hours).** By default, quarantined files are automatically sent to Bitdefender Labs every hour. You can edit the time interval between quarantined files are being sent (one hour by default). The sample files will be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.
- **Rescan quarantine after malware signatures updates.** Keep this option selected to automatically scan quarantined files after each malware signatures update. Cleaned files are automatically moved back to their original location.
- **Copy files to quarantine before applying the disinfect action.** Select this option to prevent data loss in case of false positives and copy each file detected as infected to quarantine before applying the disinfect action. You can afterwards restore legitimate files from the **Quarantine** page.

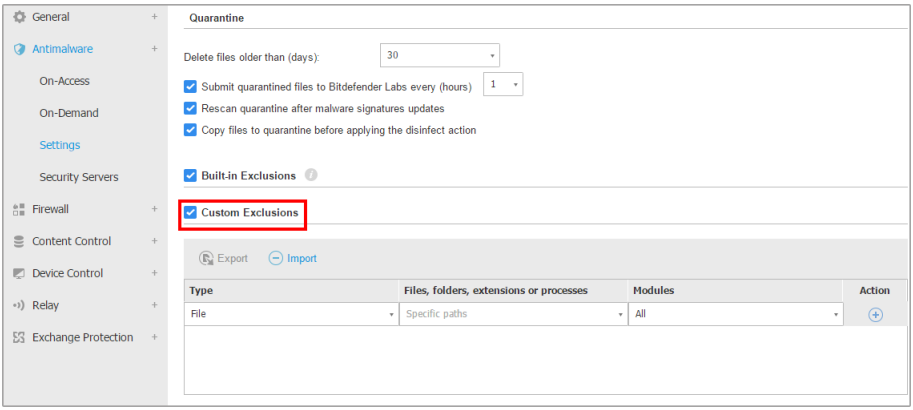
Exclusions

Bitdefender security agent can exclude from scanning certain object types. You can also define custom exclusions, according to your specific needs. In this section, you can configure the use of different types of exclusions available with the Bitdefender security agent.

- The **Built-in Exclusions** are by default enabled and included in Bitdefender security agent.

  You can choose to disable built-in exclusions, if you want to scan all types of objects, but this option will considerably impact the machine performance and will increase the scan time.

- If you want specific objects to be excluded from scanning, you can enable the **Custom Exclusions** option and configure the exclusions according to your needs.



Computers and Virtual Machines Policies - Custom Exclusions

Exclusions can apply to on-access scanning or on-demand scanning, or to both. Based on the object of the exclusion, there are four types of exclusions:

- **File exclusions:** the specified file only is excluded from scanning.
- **Folder exclusions:** all files inside the specified folder and all of its subfolders are excluded from scanning.
- **Extension exclusions:** all files having the specified extension are excluded from scanning.
- **Process exclusions:** any object accessed by the excluded process is also excluded from scanning. You can also configure process exclusions for the Advanced Threat Control and Intrusion Detection System technologies.

Warning
In agentless VMware environments integrated with vShield, you can exclude only folders and extensions. By installing Bitdefender Tools on the virtual machines, you can also exclude files and processes. During installation process, when configuring the package, you must select the check box **Deploy endpoint with vShield when a VMware environment integrated with vShield is detected**. For more information, refer to **Creating Installation Packages** section of the Installation Guide.

Important

- Scan exclusions are to be used in special circumstances or following Microsoft or Bitdefender recommendations. For an updated list of exclusions recommended by Microsoft, please refer to this article. If you have an EICAR test file that you use periodically to test antimalware protection, you should exclude it from on-access scanning.
- If using VMware Horizon View Persona management, it is recommended to exclude the following Bitdefender processes (without the full path):
  - `epsecurityservice.exe`
  - `epconsole.exe`
  - `epintegrationservice.exe`
  - `epag.exe`
- If using VMware Horizon View 7 and App Volumes AppStacks, refer to this VMware document.

Configuring Custom Exclusions

To add a custom exclusion rule:

1. Select the exclusion type from the menu.
2. Depending on the exclusion type, specify the object to be excluded as follows:
   - **File, folder and process exclusions.** You must specify the path to the excluded object on the target computers.
     a. Choose from the menu either a predefined location or enter a specific path.
     b. If you have chosen a predefined location, complete the path as needed. For example, to exclude the entire `Program Files` folder, it suffices to

select the corresponding predefined location from the menu. To exclude a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name. For process exclusions, you must also add the name of the application's executable file.

c. If you want to add a specific path, enter the full path to the object to be excluded. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

- **Extension exclusions.** Specify one or more file extensions to be excluded from scanning, separating them with a semicolon ";". You can enter extensions with or without the preceding dot. For example, enter `txt` to exclude text files.

  Note
  Before you exclude extensions, document yourself to see which are commonly targeted by malware and which are not.

3. Select the scanning modules the rule will apply to. Some exclusions may be relevant for on-access scanning only, some for on-demand scanning only, while others may be recommended for both.

   Process exclusions can be configured for on-access scanning and for the Advanced Threat Control and Intrusion Detection System technologies.

   Important
   Please note that on-demand scanning exclusions will NOT apply to contextual scanning. Contextual scanning is initiated by right-clicking a file or folder and selecting **Scan with Bitdefender Endpoint Security Tools**.

4. Click the ⊕ **Add** button. The new rule will be added to the list.

To remove a rule from the list, click the corresponding ⊗ **Delete** button.

Importing and Exporting Exclusions

If you intend to reuse the exclusion rules in more policies, you can choose to export and import them.

To export custom exclusions:

1. Click the **Export** at the upper side of the exclusions table.

2. Save the CSV file to your computer. Depending on your browser settings, the file may download automatically, or you will be asked to save it to a location.

Each row in the CSV file corresponds to a single rule, having the fields in the following order:

```
<exclusion type>, <object to be excluded>, <modules>
```

These are the available values for the CSV fields:

Exclusion type:

`1`, for file exclusions

`2`, for folder exclusions

`3`, for extension exclusions

`4`, for process exclusions

Object to be excluded:

A path or a file extension

Modules:

`1`, for on-demand scanning

`2`, for on-access scanning

`3`, for all modules

`4`, for ATC/IDS

For example, a CSV file containing antimalware exclusions may look like this:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Note

- While file, folder and extension exclusions are only for on-demand and on-access scanning, process exclusions are only for on-demand scanning and ATC/IDS.
- The Windows paths must have the backslash (\) character doubled. For example, `%WinDir%\\System32\\LogFiles`.

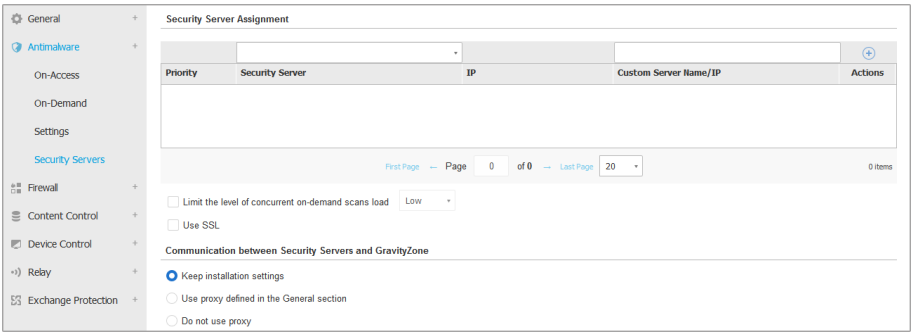
To import custom exclusions:

1. Click **Import**. The **Import Policy Exclusions** window opens.
2. Click **Add** and then select the CSV file.
3. Click **Save**. The table is populated with the valid rules. If the CSV file contains invalid rules, a warning informs you of the corresponding row numbers.

Security Servers

In this section you can configure the target endpoints to communicate with GravityZone via one or several Security Server machines installed in your network. You can also configure the communication settings between the selected Security Server machines and GravityZone.

- Security Server Assignment
- Security Server Configuration



Computers and Virtual Machines Policies - Security Servers

Security Server Assignment

You can select several Security Server appliances and configure their priority. In this case, the target endpoints will be scanned with the Security Server with the first priority. When this Security Server is unavailable, the scan traffic will be redirected to the second Security Server and so on.

To configure the Security Server assignment for the target endpoints:

1. Click the **Security Server** field. The list of detected Security Servers is displayed.
2. Select a Security Server.

3. Click the ⊕ **Add** button at the right side of the table. The Security Server is added to the list. All the target endpoints will be scanned with the specified Security Server.
4. Follow the same steps to add several Security Server appliances, if available.
5. You can configure the Security Server appliances priority using the up and down arrows available at the right side of each entity.
6. To delete a Security Server from the list, click the corresponding ⊗ **Delete** button at the right side of the table.

You can also configure the following settings for the selected Security Server machines:

- You can specify the first Security Server taken into account to be from the same host as the target virtual machines, by selecting the option **First connect to the Security Server installed on the same physical host, if available, regardless the assigned priority**. When the Security Server from the same host with the target virtual machines is unavailable, the specified list of Security Servers will be taken into account, according to the defined priority.
- **Limit the number of concurrent on-demand scans**. Running multiple on-demand scan tasks on virtual machines sharing the same datastore can create antivirus storms. To prevent this:
  1. Enable the **Limit the number of concurrent on-demand scans** option, to allow only a defined number of scan tasks to run at the same time.
  2. Select the option defining the maximum allowed number of concurrent on-demand scan tasks. You can choose one of the following options:
     - **Low**, where N = MAX(a;b)
     - **Medium**, where N = 2 x MAX(a;b)
     - **High**, where N = 4 x MAX(a;b)
     - **Custom**. In this case, you must enter the value for the maximum allowed number of concurrent on-demand scan tasks in the corresponding field.

     Note
     - **N** = maximum allowed number of concurrent on-demand scan tasks
     - Function **MAX(a;b)** returns the maximum number of scan slots available on the Security Server, where:

- **a** = 4 and represents the default number of on-demand scan slots
- **b** = vCPUs - 1

– **vCPUs** = number of virtual CPUs assigned to the Security Server

E.g. For a Security Server with 12 CPUs and a **High** limit of concurrent scans, we have:

N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44 concurrent on-demand scan tasks.

- **Use SSL** - enable this option if you want to encrypt the connection between the target endpoints and the specified Security Server appliances.

Communication between Security Servers and GravityZone

In this section you can define your proxy preferences for the communication between the selected Security Server machines and GravityZone.

- **Keep installation settings**, to use the same proxy settings defined with the installation package.
- **Use proxy defined in the General section**, to use the proxy settings defined in the current policy, under **General > Settings** section.
- **Do not use**, when the target endpoints do not communicate with the specific Bitdefender components via proxy.

5.2.4. Firewall

The Firewall protects the endpoint from inbound and outbound unauthorized connection attempts.

The Firewall's functionality relies on network profiles. The profiles are based on trust levels, which have to be defined for each network.

The Firewall detects each new connection, compares the adapter information for that connection with the information from the existing profiles and applies the correct profile. For detailed information on how the profiles are applied, refer to "Networks Settings" (p. 217).

Important
The Firewall module is available only for supported Windows workstations.

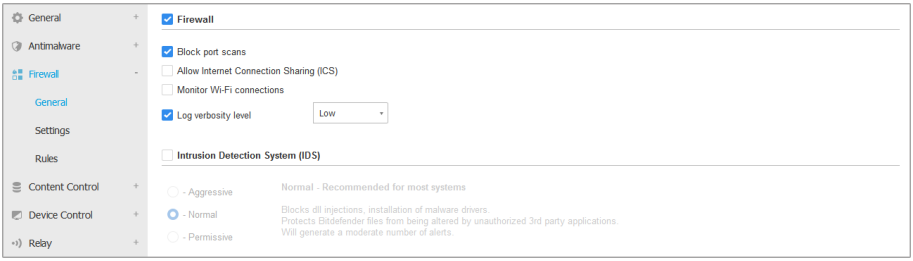
The settings are organized into the following sections:

- General

- Settings
- Rules

General

In this section you can enable or disable the Bitdefender Firewall and configure the general settings.



Computers and Virtual Machines Policies - Firewall General Settings

- **Firewall.** Use the check box to turn Firewall on or off.

  Warning
  If you turn off firewall protection, computers will be vulnerable to network and Internet attacks.

- **Block port scans.** Port scans are frequently used by hackers to find out which ports are open on a computer. They might then break into the computer if they find a less secure or vulnerable port.
- **Allow Internet Connection Sharing (ICS).** Select this option to set the firewall to allow Internet Connection Sharing traffic.

  Note
  This option does not automatically enable ICS on the user's system.

- **Monitor Wi-Fi connections.** Bitdefender security agent can inform users connected to a Wi-Fi network when a new computer joins the network. To display such notifications on the user's screen, select this option.
- **Log verbosity level.** Bitdefender security agent maintains a log of events regarding the Firewall module usage (enabling/disabling firewall, traffic blocking,

modifying settings) or generated by the activities detected by this module (scanning ports, blocking connection attempts or traffic according to the rules). Choose an option from the **Log verbosity level** to specify how much information the log should include.

- **Intrusion Detection System.** Intrusion Detection System monitors the system for suspicious activities (for example, unauthorized attempts to alter the Bitdefender files, DLL injections, keylogging attempts etc.).

  To configure Intrusion Detection System:

  1. Use the check box to turn Intrusion Detection System on or off.
  2. Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.

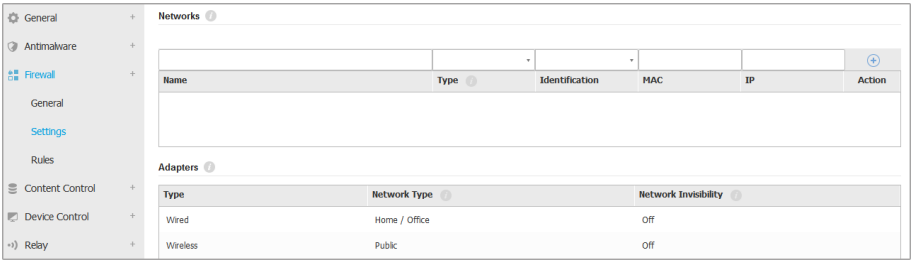
  To prevent a legitimate application from being detected by Intrusion Detection System, add an **ATC/IDS process exclusion rule** for that application in the **Antimalware > Settings > Custom Exclusions** section.

Settings

The firewall automatically applies a profile based on the trust level. You can have different trust levels for network connections, depending on the network architecture or on the type of the adapter used to establish the network connection. For example, if you have sub-networks within your company's network, you can set a trust level to each sub-network.

The settings are organized under the following tables:

- Networks
- Adapters



Policies - Firewall Settings

Networks Settings

If you want the Firewall to apply different profiles to several network segments within your company, you must specify the managed networks in the **Networks** table. Fill in the fields from the **Networks** table as described herein:

- **Name.** Enter the name by which you can recognize the network in the list.
- **Type.** Select from the menu the profile type assigned to the network.

  Bitdefender security agent automatically applies one of the four network profiles to each detected network connection on the endpoint, to define the basic traffic filtering options. The profile types are:

  - **Trusted** network. Disables the firewall for the respective adapters.
  - **Home/Office** network. Allows all traffic to and from computers in the local network while the other traffic is being filtered.
  - **Public** network. All traffic is filtered.
  - **Untrusted** network. Completely blocks network and Internet traffic through the respective adapters.
- **Identification.** Select from the menu the method through which the network will be identified by the Bitdefender security agent. The networks can be identified by three methods: **DNS**, **Gateway** and **Network**.
  - **DNS**: identifies all endpoints using the specified DNS.
  - **Gateway**: identifies all endpoints communicating through the specified gateway.
  - **Network**: identifies all endpoints from the specified network segment, defined by its network address.
- **MAC**. Use this field to specify the MAC address of a DNS server or of a gateway that delimits the network, depending on the selected identification method.

  You must enter the MAC address in the hexadecimal format, separated by hyphens (-) or colons (:). For example, both `00-50-56-84-32-2b` and `00:50:56:84:32:2b` are valid addresses.
- **IP.** Use this field to define specific IP addresses in a network. The IP format depends on the identification method as follows:

- **Network.** Enter the network number in the CIDR format. For example, `192.168.1.0/24`, where `192.168.1.0` is the network address and `/24` is the network mask.
- **Gateway.** Enter the IP address of the gateway.
- **DNS.** Enter the IP address of the DNS server.

After you have defined a network, click the **Add** button at the right side of the table to add it to the list.

Adapters Settings

If a network which is not defined in the **Networks** table is detected, the Bitdefender security agent detects the network adapter type and applies a corresponding profile to the connection.

The fields from the **Adapters** table are described as follows:

- **Type.** Displays the type of the network adapters. Bitdefender security agent can detect three predefined adapter types: **Wired**, **Wireless** and **Virtual** (Virtual Private Network).
- **Network Type.** Describes the network profile assigned to a specific adapter type. The network profiles are described in the network settings section. Clicking the network type field allows you to change the setting.

  If you select **Let Windows decide**, for any new network connection detected after the policy is applied, Bitdefender security agent applies a profile for the firewall based on the network classification in Windows, ignoring the settings from the **Adapters** table.

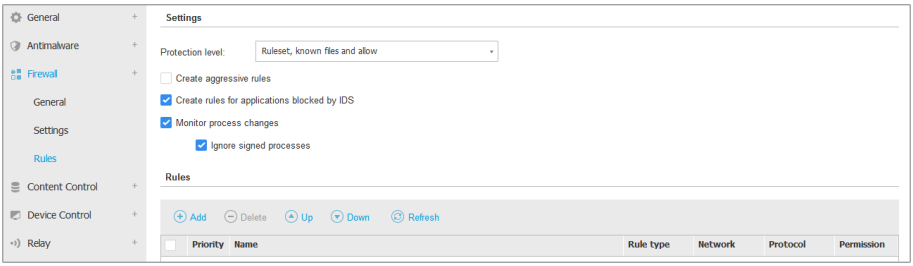
  If the detection based on Windows Network Manager fails, a basic detection is attempted. A generic profile is used, where the network profile is considered **Public** and the stealth settings are set to **On**.

  If the IP address of the domain the computer is found in is in one of the networks associated with the adapter, then the trust level is considered **Home/Office** and the stealth settings are set to **Remote**. If the computer is not in a domain, this condition is not applicable.
- **Network Invisibility.** Hides the computer from malicious software and hackers in the network or the Internet. Configure the network invisibility as needed for each adapter type by selecting one of the following options:
  - **On.** The computer is invisible from both the local network and the Internet.

- **Off.** Anyone from the local network or the Internet can ping and detect the computer.
- **Remote.** The computer cannot be detected from the Internet. Anyone from the local network can ping and detect the computer.

Rules

In this section you can configure the application network access and data traffic rules enforced by the firewall. Note that available settings apply only to the **Home/Office** and **Public** profiles.



Computers and Virtual Machines Policies - Firewall rules settings

Settings

You can configure the following settings:

- **Protection level.** The selected protection level defines the firewall decision-making logic used when applications request access to network and Internet services. The following options are available:

  Ruleset and allow

  Apply existing firewall rules and automatically allow all other connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

  Ruleset and ask

  Apply existing firewall rules and prompt the user for action for all other connection attempts. An alert window with detailed information about the unknown connection attempt is displayed on the user's screen. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset and deny
Apply existing firewall rules and automatically deny all other connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset, known files and allow
Apply existing firewall rules, automatically allow connection attempts made by known applications and automatically allow all other unknown connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset, known files and ask
Apply existing firewall rules, automatically allow connection attempts made by known applications and prompt the user for action for all other unknown connection attempts. An alert window with detailed information about the unknown connection attempt is displayed on the user's screen. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset, known files and deny
Apply existing firewall rules, automatically allow connection attempts made by known applications and automatically deny all other unknown connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

Note
Known files represent a large collection of safe, trustworthy applications, which is compiled and continuously maintained by Bitdefender.

- **Create aggressive rules.** With this option selected, the firewall will create rules for each different process that opens the application requesting network or Internet access.
- **Create rules for applications blocked by IDS.** With this option selected, the firewall will automatically create a **Deny** rule each time the Intrusion Detection System blocks an application.
- **Monitor process changes.** Select this option if you want each application attempting to connect to the Internet to be checked whether it has been changed since the addition of the rule controlling its Internet access. If the application has been changed, a new rule will be created according to the existing protection level.

Note

Usually, applications are changed by updates. But there is a risk that they might be changed by malware applications, with the purpose of infecting the local computer and other computers in the network.

Signed applications are supposed to be trusted and have a higher degree of security. You can select **Ignore signed processes** to automatically allow changed signed applications to connect to the Internet.

Rules

The Rules table lists the existing firewall rules, providing important information on each of them:

- Rule name or application it refers to.
- Protocol the rule applies to.
- Rule action (allow or deny packets).
- Actions you can take on the rule.
- Rule priority.

Note

These are the firewall rules explicitly enforced by the policy. Additional rules may be configured on computers as a result of applying firewall settings.

A number of default firewall rules help you easily allow or deny popular traffic types. Choose the desired option from the **Permission** menu.

Incoming ICMP / ICMPv6

Allow or deny ICMP / ICMPv6 messages. ICMP messages are often used by hackers to carry out attacks against computer networks. By default, this type of traffic is denied.

Incoming Remote Desktop Connections

Allow or deny other computers' access over Remote Desktop Connections. By default, this type of traffic is allowed.

Sending Emails

Allow or deny sending emails over SMTP. By default, this type of traffic is allowed.

Web Browsing HTTP
Allow or deny HTTP web browsing. By default, this type of traffic is allowed.

Printing in Another Network
Allow or deny access to printers in another local area network. By default, this type of traffic is denied.

Windows Explorer traffic on HTTP / FTP
Allow or deny HTTP and FTP traffic from Windows Explorer. By default, this type of traffic is denied.

Besides the default rules, you can create additional firewall rules for other applications installed on endpoints. This configuration however is reserved for administrators with strong networking skills.

To create and configure a new rule, click the ⊕ **Add** button at the upper side of the table. Refer to the following topic for more information.

To remove a rule from the list, select it and click the ⊖ **Delete** button at the upper side of the table.

Note
You can neither delete nor modify the default firewall rules.

Configuring Custom Rules

You can configure two types of firewall rules:

- **Application-based rules.** Such rules apply to specific software found on the client computers.
- **Connection-based rules.** Such rules apply to any application or service that uses a specific connection.

To create and configure a new rule, click the ⊕ **Add** button at the upper side of the table and select the desired rule type from the menu. To edit an existing rule, click the rule name.

The following settings can be configured:

- **Rule name.** Enter the name under which the rule will be listed in the rules table (for example, the name of the application the rule applies to).
- **Application path** (only for application-based rules). You must specify the path to the application executable file on the target computers.

- Choose from the menu a predefined location and complete the path as needed. For example, for an application installed in the `Program Files` folder, select `%ProgramFiles%` and complete the path by adding a backslash (\) and the name of the application folder.
- Enter the full path in the edit field. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

- **Command line** (only for application-based rules). If you want the rule to apply only when the specified application is opened with a specific command in the Windows command line interface, type the respective command in the edit field. Otherwise, leave it blank.
- **Application MD5** (only for application-based rules). If you want the rule to check the application's file data integrity based on its MD5 hash code, enter it in the edit field. Otherwise, leave the field blank.
- **Local Address.** Specify the local IP address and port the rule applies to. If you have more than one network adapter, you can clear the **Any** check box and type a specific IP address. Likewise, to filter connections on a specific port or port range, clear the **Any** check box and enter the desired port or port range in the corresponding field.
- **Remote Address.** Specify the remote IP address and port the rule applies to. To filter the traffic to and from a specific computer, clear the **Any** check box and type its IP address.
- **Apply rule only for directly connected computers.** You can filter access based on Mac address.
- **Protocol.** Select the IP protocol the rule applies to.
  - If you want the rule to apply to all protocols, select **Any**.
  - If you want the rule to apply to TCP, select **TCP**.
  - If you want the rule to apply to UDP, select **UDP**.
  - If you want the rule to apply to a specific protocol, select that protocol from the **Other** menu.

> **Note**
> IP protocol numbers are assigned by the Internet Assigned Numbers Authority (IANA). You can find the complete list of assigned IP protocol numbers at http://www.iana.org/assignments/protocol-numbers.

- **Direction.** Select the traffic direction the rule applies to.

Direction	Description
Outbound	The rule applies only for the outgoing traffic.
Inbound	The rule applies only for the incoming traffic.
Both	The rule applies in both directions.

- **IP version.** Select the IP version (IPv4, IPv6 or any) the rule applies to.
- **Network.** Select the type of network the rule applies to.
- **Permission.** Select one of the available permissions:

Permission	Description
Allow	The specified application will be allowed network / Internet access under the specified circumstances.
Deny	The specified application will be denied network / Internet access under the specified circumstances.

Click **Save** to add the rule.

For the rules you created, use the arrows at the right side of the table to set each rule priority. The rule with higher priority is closer to the top of the list.

5.2.5. Content Control

Use the Content Control module to configure your preferences regarding content filtering and data protection for user activity including web browsing, email and software applications. You can restrict or allow web access and application usage, configure traffic scan, antiphishing and data protection rules. Please note that the configured Content Control settings will apply to all users who log on to the target computers.

Important
The Content Control module is available only for supported Windows workstations.

The settings are organized into the following sections:

- Traffic

- Web
- Data Protection
- Applications

Traffic

Configure the traffic security preferences using the settings under the following sections:

- Options
- Traffic Scan
- Traffic Scan Exclusions

Computers and Virtual Machines Policies - Content Control - Traffic

Options

- **Scan SSL**. Select this option if you want the Secure Sockets Layer (SSL) web traffic to be inspected by the Bitdefender security agent's protection modules.
- **Show browser toolbar**. The Bitdefender toolbar informs users about the rating of the web pages they are viewing. The Bitdefender toolbar is not your typical browser toolbar. The only thing it ads to the browser is a small dragger at the top of every web page. Clicking the dragger opens the toolbar.

  Depending on how Bitdefender classifies the web page, one of the following ratings is displayed on the left side of the toolbar:

  - The message "This page is not safe" appears on a red background.
  - The message "Caution is advised" appears on an orange background.
  - The message "This page is safe" appears on a green background.

- **Browser Search Advisor.** Search advisor rates the results of Google, Bing and Yahoo! searches, as well as links from Facebook and Twitter, by placing an icon in front of every result. Icons used and their meaning:

  You should not visit this web page.
  This web page may contain dangerous content. Exercise caution if you decide to visit it.
  This is a safe page to visit.

Traffic Scan

Incoming emails (POP3) and web traffic are scanned in real time to prevent malware from being downloaded to the endpoint. Outgoing emails (SMTP) are scanned to prevent malware from infecting other endpoints. Scanning the web traffic may slow down web browsing a little, but it will block malware coming from the Internet, including drive-by downloads.

When an email is found infected, it is replaced automatically with a standard email informing the receiver of the original infected email. If a web page contains or distributes malware, it is automatically blocked. A special warning page is displayed instead to inform the user that the requested web page is dangerous.

Though not recommended, you can disable email and web traffic scan to increase system performance. This is not a major threat as long as on-access scanning of local files remains enabled.

Traffic Scan Exclusions

You can choose to skip certain traffic of being scanned for malware while the traffic scan options are enabled.

To define a traffic scan exclusion:

1. Select the exclusion type from the menu.
2. Depending on the exclusion type, define the traffic entity to be excluded from scanning as follows:
   - **IP**. Enter the IP address for which you do not want to scan the incoming and outgoing traffic.
   - **URL**. Excludes from scanning the specified web addresses. To define an URL scan exclusion:
     - Enter a specific URL, such as `www.example.com/example.html`
     - Use wildcards to define web address patterns:

- Asterisk (*) substitutes for zero or more characters.
- Question mark (?) substitutes for exactly one character. You can use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters.

In the following table, you can find several sample syntaxes for specifying web addresses.

Syntax	Exception Applicability
`www.example*`	Any website or web page starting with `www.example` (regardless of the domain extension). The exclusion will not apply to the subdomains of the specified website, such as `subdomain.example.com`.
`*example.com`	Any website ending in `example.com`, including pages and subdomains thereof.
`*string*`	Any website or web page whose address contains the specified string.
`*.com`	Any website having the `.com` domain extension, including pages and subdomains thereof. Use this syntax to exclude from scanning the entire top-level domains.
`www.example?.com`	Any web address starting with `www.example?.com`, where ? can be replaced with any single character. Such websites might include: `www.example1.com` or `www.exampleA.com`.

- **Application**. Excludes from scanning the specified process or application. To define an application scan exclusion:
  - Enter the full application path. For example, `C:\Program Files\Internet Explorer\iexplore.exe`

- Use environment variables to specify the application path. For example: `%programfiles%\Internet Explorer\iexplore.exe`
- Use wildcards to specify any applications matching a certain name pattern. For example:
  - `c*.exe` matches all applications starting with "c" (chrome.exe).
  - `??????.exe` matches all applications with a name that contains six characters (chrome.exe, safari.exe, etc.).
  - `[^c]*.exe` matches all application except for those starting with "c".
  - `[^ci]*.exe` matches all application except for those starting with "c" or "i".

3. Click the ⊕ **Add** button at the right side of the table.

To remove an entity from the list, click the corresponding ⊗ **Delete** button.

Web

In this section you can configure the web browsing security preferences.

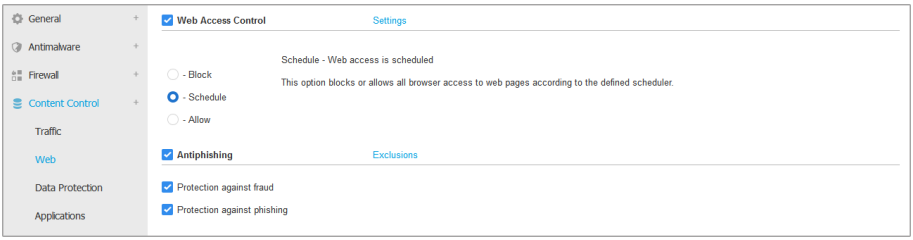
The settings are organized under the following sections:

- Web Access Control
- Antiphishing

Web Access Control

Web Access Control helps you allow or block web access for users or applications during specified time intervals.

The web pages blocked by Web Access Control are not displayed in the browser. Instead, a default web page is displayed informing the user that the requested web page has been blocked by Web Access Control.



Computers and Virtual Machines Policies - Content Control - Web

Use the switch to turn **Web Access Control** on or off.

You have three configuration options:

- Select **Allow** to always grant web access.
- Select **Block** to always deny web access.
- Select **Schedule** to enable time restrictions on web access upon a detailed schedule.

Either you choose to allow or block the web access, you can define exceptions to these actions for entire web categories or only for specific web addresses. Click **Settings** to configure your web access schedule and exceptions as follows:

Scheduler

To restrict the Internet access to certain times of the day on a weekly basis:

1. Select from the grid the time intervals during which you want Internet access to be blocked.

   You can click individual cells, or you can click and drag to cover longer periods. Click again in the cell to reverse the selection.

   To start a new selection, click **Allow All** or **Block all**, depending on the type of restriction you wish to implement.

2. Click **Save**.

Note
Bitdefender security agent will perform updates every hour, no matter if web access is blocked.

Categories

Web Categories Filter dynamically filters access to websites based on their content. You can use the Web Categories Filter for defining exceptions to the selected Web Access Control action (Allow or Block) for entire web categories (such as Games, Mature Content or Online Networks).

To configure Web Categories Filter:

1. Enable **Web Categories Filter**.
2. For a quick configuration, click one of the predefined profiles (**Aggressive**, **Normal** or **Permissive**). Use the description on the right side of the scale to guide your choice. You can view the predefined actions for available web categories by expanding the **Web Rules** section placed below.
3. If you are not satisfied with the default settings, you can define a custom filter:
   a. Select **Custom**.
   b. Click **Web Rules** to expand the corresponding section.
   c. Find the category that you want in the list and choose the desired action from the menu.
4. The default message displayed to the user accessing restricted websites contains also the category that the website's content has matched. Deselect the option **Show matched Web category in user's browser** if you want to hide this information from the user.
5. Select the option **Treat Web Categories as exceptions for Web Access** if you want to ignore the existing Web access settings and apply only the Web Categories Filter.
6. Click **Save**.

Note

- The **Allow** permission for specific web categories is also taken into account during time intervals when web access is blocked by Web Access Control.
- The **Allow** permissions work only when web access is blocked by Web Access Control, while the **Block** permissions work only when web access is allowed by Web Access Control.
- You can override the category permission for individual web addresses by adding them with opposite permission in **Web Access Control > Settings >**

Exclusions. For example, if a web address is blocked by Web Categories Filter, add a web rule for that address with permission set to **Allow**.

Exclusions

You can also define web rules to explicitly block or allow certain web addresses, overriding the existing Web Access Control settings. Users will be able, for example, to access a specific webpage also when the web browsing is blocked by Web Access Control.

To create a web rule:

1. Enable the **Use Exceptions** option.
2. Enter the address you want to allow or block in the **Web Address** field.
3. Select **Allow** or **Block** from the **Permission** menu.
4. Click the ⊕ **Add** button at the right side of the table to add the address to the exceptions list.
5. Click **Save**.

To edit a web rule:

1. Click the web address you want to edit.
2. Modify the existing URL.
3. Click **Save**.

To remove a web rule, click the corresponding ⊗ **Delete** button.

Antiphishing

Antiphishing protection automatically blocks known phishing web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters. Instead of the phishing web page, a special warning page is displayed in the browser to inform the user that the requested web page is dangerous.

Select **Antiphishing** to activate antiphishing protection. You can further tune Antiphishing by configuring the following settings:

- **Protection against fraud**. Select this option if you want to extend protection to other types of scams besides phishing. For example, websites representing fake companies, which do not directly request private information, but instead try to pose as legitimate businesses and make a profit by tricking people into doing business with them.

- **Protection against phishing**. Keep this option selected to protect users against phishing attempts.

If a legitimate web page is incorrectly detected as phishing and blocked, you can add it to the whitelist to allow users to access it. The list should contain only websites you fully trust.

To manage antiphishing exceptions:

1. Click **Exclusions**.
2. Enter the web address and click the ⊕ **Add** button.

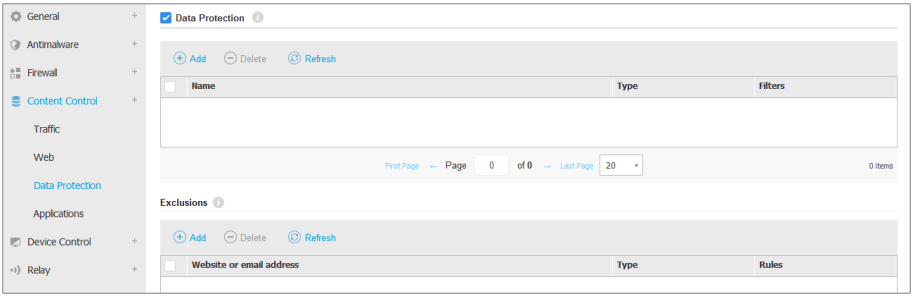
   If you want to exclude an entire website, write the domain name, such as `http://www.website.com`, and if you want to exclude only a webpage, write the exact web address of that page.

   Note
   Wildcards are not accepted for building URLs.

3. To remove an exception from the list, click the corresponding ⊗ **Delete** button.
4. Click **Save**.

Data Protection

Data Protection prevents unauthorized disclosure of sensitive data based on administrator-defined rules.



Computers and Virtual Machines Policies - Content Control - Data Protection

You can create rules to protect any piece of personal or confidential information, such as:

- Customer personal information
- Names and key details of in-development products and technologies
- Contact information of company executives

Protected information might include names, phone numbers, credit card and bank account information, email addresses and so on.

Based on the data protection rules you create, Bitdefender Endpoint Security Tools scans the web and outgoing email traffic for specific character strings (for example, a credit card number). If there is a match, the respective web page or email message is blocked in order to prevent protected data from being sent. The user is immediately informed about the action taken by Bitdefender Endpoint Security Tools through an alert web page or email.

To configure Data Protection:

1. Use the checkbox to turn on Data Protection.
2. Create data protection rules for all of the sensitive data you want to protect. To create a rule:
   a. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.
   b. Enter the name under which the rule will be listed in the rules table. Choose a suggestive name so that you or other administrator can easily identify what the rule is about.
   c. Select the type of data you want to protect.
   d. Enter the data you want to protect (for example, the phone number of a company executive or the internal name of a new product the company is working on). Any combination of words, numbers or strings consisting of alphanumerical and special characters (such as @, # or $) is accepted.

      Make sure to enter at least five characters in order to avoid the mistaken blocking of email messages and web pages.

      Important

      Provided data is stored in encrypted form on protected endpoints, but it can be seen on your Control Center account. For extra safety, do not enter all of the data you want to protect. In this case, you must clear the **Match whole words** option.

e. Configure the traffic scan options as needed.

- **Scan web (HTTP traffic)** - scans the HTTP (web) traffic and blocks the outgoing data that matches the rule data.
- **Scan email (SMTP traffic)** - scans the SMTP (mail) traffic and blocks the outgoing email messages that contain the rule data.

You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.

f. Click **Save**. The new rule will be added to the list.

3. Configure exclusions to data protection rules so that users can still send protected data to authorized websites and recipients. Exclusions can be applied globally (to all rules) or to specific rules only. To add an exclusion:
   a. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.
   b. Enter the web or email address that users are authorized to disclose protected data to.
   c. Select the type of exclusion (web or email address).
   d. From the **Rules** table, select the data protection rules(s) on which this exclusion should be applied.
   e. Click **Save**. The new exclusion rule will be added to the list.

Note
If an email containing blocked data is addressed to multiple recipients, those for which exclusions have been defined will receive it.

To remove a rule or an exclusion from the list, click the corresponding ⊗ **Delete** button at the right side of the table.

Applications

In this section you can configure Application Blacklisting, which helps you completely block or restrict users' access to applications on their computers. Games, media and messaging software, as well as other categories of software and malware can be blocked in this way.

Computers and Virtual Machines Policies - Content Control - Applications

To configure Application Blacklisting:

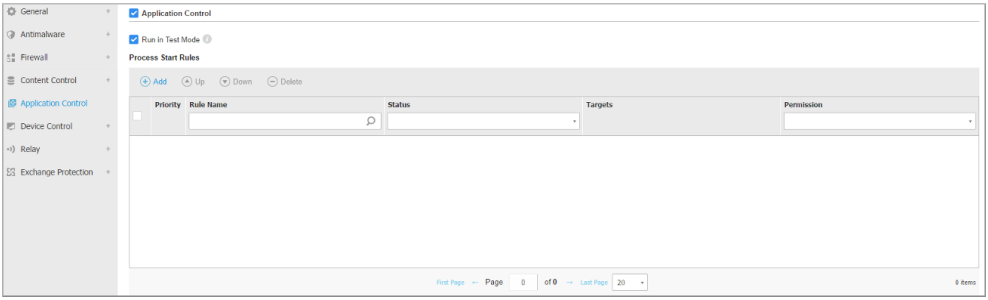
1. Enable the **Application Blacklisting** option.
2. Specify the applications you want to restrict access to. To restrict access to an application:
   a. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.
   b. You must specify the path to the application executable file on the target computers. There are two ways to do this:
      - Choose from the menu a predefined location and complete the path as needed in the edit field. For example, for an application installed in the `Program Files` folder, select `%ProgramFiles` and complete the path by adding a backslash (\) and the name of the application folder.
      - Enter the full path in the edit field. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.
   c. **Access Scheduler**. Schedule the applications access during certain times of day on a weekly basis:
      - Select from the grid the time intervals during which you want to block access to the application. You can click individual cells, or you can click and drag to cover longer periods. Click again in the cell to reverse the selection.
      - To start a new selection, click **Allow All** or **Block All**, depending on the type of restriction you wish to implement.
      - Click **Save**. The new rule will be added to the list.

To remove a rule from the list, select it and click the ⊗ **Delete** button at the upper side of the table. To edit an existing rule, click it to open its configuration window.

5.2.6. Application Control

The Application Control module adds another layer of protection against all kinds of malware threats (ransomware, zero-day attacks, exploits on third party applications, trojans, spyware, rootkits, adware and so on) by blocking unauthorized applications and processes from running. Application Control reduces the attack surface that malware threats can leverage on the endpoint and prevents the installation and execution of any unwanted, untrusted or malicious applications.

Application Control enforces flexible policies that allow you to whitelist applications and manage the update permissions.



Application Control

Important

- To enable **Application Control** for your current installed clients, run the **Reconfigure Client** task. After installing the module, you can view its status in **Information** window.
- Application Control highly affects Power User mode after application updates. For example, when a whitelisted application is updated, the endpoint submits the new information. GravityZone updates the rule with the new values and resends the policy.

You must run the **Applications Discovery** task to view the running applications and processes in your network. For more information, refer to "Applications Discovery" (p. 68). Then, you can define Application Control rules.

Application Control runs in two modes:

- **Test Mode**. Application Control only detects and reports the applications in Control Center, leaving them to run as usual. You can configure and test your whitelisting rules and policies, but applications will not be blocked.
- **Production Mode**. Application Control blocks all unknown applications. Microsoft operating system processes and Bitdefender processes are whitelisted by default. Defined whitelisted applications will be allowed to run. To update whitelisted applications, you must define updaters. These are specific processes that are allowed to change existing applications. For more information, refer to "Application Inventory" (p. 145).

Warning

- To make sure legitimate applications are not restricted by Application Control, you must run Application Control in test mode first. This way you can make sure that the whitelisting rules and policies are properly defined.
- Processes that are already running when the Application Control is set to **Production Mode** will be blocked after the next process restart.

To manage applications' permission to run:

1. Select the **Application Control** check box, to enable this module.
2. Use the **Run in Test Mode** check box to turn Test Mode on or off.

Note

- In test mode, you are notified if Application Control would have blocked a specific application. For more information, refer to "Notification Types" (p. 346).
- **Blocked Application** notifications will be displayed in the Notification Area when new applications are detected and when blacklisted applications are blocked.

3. Define process start rules.

Process Start Rules

Application Control allows you to manually authorize specific applications and processes, based on the hash of the executable, signing certificate thumbprint, and path of the application. You can also define rule exclusions.

Note
To obtain the custom values for the hash of the executable and thumbprint of the certificate use "Application Control Tools" (p. 369)

The **Process Start Rules** table informs you of the existing rules, providing important information:

- Rule priority. The rule with higher priority is closer to the top of the list.
- Rule name and status.
- Target applications and their permission to run. The target represents the number of conditions that must be matched in order for the rule to apply, or the number of applications or groups to which the rule applies.

To create a process start rule:

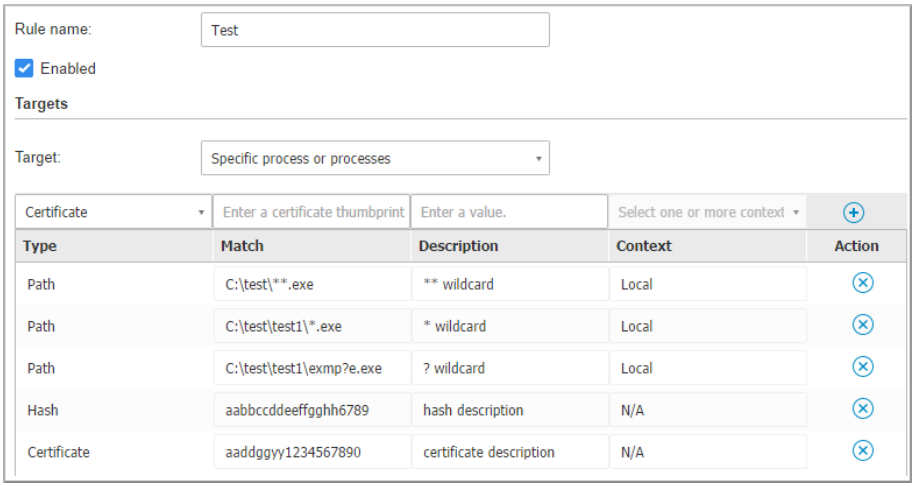
1. Click the ⊕ **Add** button at the upper side of the table to open the configuration window.
2. In the **General** section, enter a **Rule name**.
3. Select the **Enabled** check box to activate the rule.
4. In the **Targets** section, specify the rule destination:
   - **Specific process or processes**, to define a process that is allowed or denied from starting. You can authorize by path, hash or certificate. The conditions inside the rule are matched by logical AND.
     - To authorize an application from a specific path:
       a. Select **Path** in the **Type** column. Specify the path to the object. You can provide an absolute or relative pathname and use wildcard characters. The asterisk symbol (*) matches any file within a directory. A double asterisk (**) matches all files and directories in the defined directory. A question mark (?) matches exactly one character. You can also add a description to help identify the process.
       b. From the **Select one or more context** drop-down menu you can choose among local, CD-ROM, removable and network. You can block an application executed from a removable device, or allow it if the application is locally executed.

– To authorize an application based on hash, select **Hash** in the **Type** column and enter a hash value. You can also add a description to help identify the process.

> **Important**
> To generate the hash value, download the Fingerprint tool. For more information, refer to "Application Control Tools" (p. 369)

– To authorize based on a certificate, select **Certificate** in the **Type** column and enter a certificate thumbprint. You can also add a description to help identify the process.

> **Important**
> To obtain the certificate thumbprint, download the Thumbprint tool. For more information, refer to "Application Control Tools" (p. 369)



Application Rules

Click ⊕ **Add** to add the rule.

- **Inventory applications or groups**, to add a group or an application discovered in your network. You can view the applications running in your network on

the **Network > Application Inventory** page. For more information, refer to "Application Inventory" (p. 145).

Insert the applications or group names in the field, separated by a comma. The auto-fill function displays suggestions as you type.

5. Select the **Include subprocesses** check box to apply the rule to spawned child processes.

   Warning
   When setting rules for browser applications, it is recommended to turn off this option to prevent security risks.

6. Optionally, you can also define exclusions from the process start rule. The adding operation is similar to the one described in the previous steps.
7. In the **Permissions** section, choose whether to allow or deny the rule to run.
8. Click **Save** to apply the changes.

To edit an existing rule:

1. Click the rule name to open the configuration window.
2. Enter the new values for the options you want to modify.
3. Click **Save** to apply the changes.

To set the rule priority:

1. Select the check box of the desired rule.
2. Use the priority buttons at the right side of the table:
   - Click the **Up** button to promote the selected rule.
   - Click the **Down** button to demote it.

You can delete one or several rules at once. All you need to do is:

1. Select the rules you want to delete.
2. Click the **Delete** button at the upper side of the table. Once a rule is deleted, you cannot recover it.

5.2.7. 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 exclusions via policy to a vast range of device types.

Important
The Device Control module is available only for supported Windows desktop and server operating systems (not available for Linux and macOS systems).

To use the Device Control module, you need at first to include it in the security agent installed on target endpoints, then to enable the **Device Control** option in the policy applied to these endpoints. After that, each time a device is connected to a managed endpoint, the security agent will send information regarding this event to Control Center, including the device name, class, ID and the connection date and time.

With Device Control, you can manage permissions for the following types of devices:

- Bluetooth Devices
- CDROM Devices
- Floppy Disk Drives
- IEEE 1284.4
- IEEE 1394
- Imaging Devices
- Modems
- Tape Drives
- Windows Portable
- COM/LPT Ports
- SCSI Raid
- Printers
- Network Adapters
- Wireless Network Adapters
- Internal and External Storage

Device Control allows managing device permissions as follows:

- Define permission rules
- Define permission exclusions

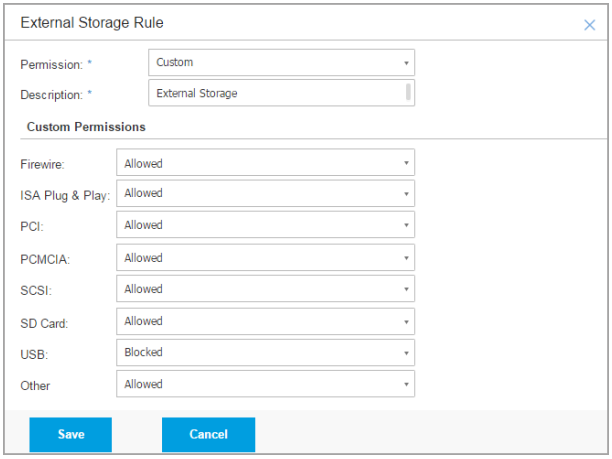
Rules

The **Rules** section allows defining the permissions for devices connected to the target endpoints.

To set permissions for the type of device that you want:

1. Go to **Device Control > Rules**.
2. Click the device name in the available table.
3. Select one permission type from the available options. Please note that the available set of permissions may vary according to the device type:
   - **Allowed**: the device can be used on the target endpoint.
   - **Blocked**: the device cannot be used on the target endpoint. In this case, each time the device is connected to the endpoint, the security agent will prompt a notification stating that the device has been blocked.
   - **Read-Only**: only the read functions can be used with the device.
   - **Custom**: define different permissions for each type of port from the same device, such as Firewire, ISA Plug & Play, PCI, PCMCIA, USB, etc. In this case, the list of components available for the selected device is displayed, and you can set the permissions that you want for each component.

     For example, for External Storage, you can block only USB, and allow all the other ports to be used.



Computer and Virtual Machines Policies - Device Control - Rules

Exclusions

After setting the permission rules for different types of devices, you may want to exclude certain devices or product types from these rules.

You can define device exclusions:

- By Device ID (or Hardware ID), to designate individual devices that you want to exclude.
- By Product ID (or PID), to designate a range of devices produced by the same manufacturer.

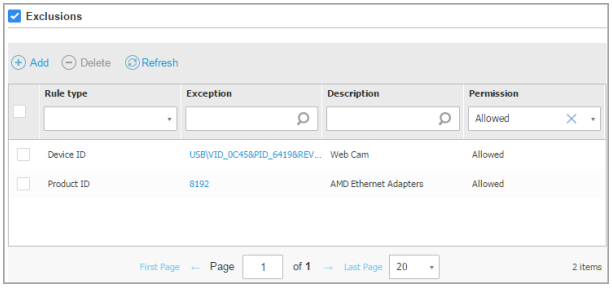
To define device rule exclusions:

1. Go to **Device Control > Exclusions**.
2. Enable the **Exclusions** option.
3. Click the ⊕ **Add** button at the upper side of the table.
4. Select the method you want to use for adding exclusions:
   - **Manually**. In this case, you need to enter each Device ID or Product ID that you want to exclude, provided you have at hand the list of appropriate IDs:
     a. Select the exclusion type (by Product ID or by Device ID).
     b. In the **Exceptions** field, enter the ID's that you want to exclude.
     c. In the **Description** field, enter a name that will help you identify the device or the range of devices.
     d. Select the permission type for specified devices (Allowed or Blocked).
     e. Click **Save**.
   - **From Discovered Devices**. In this case, you can select the Devices IDs or Product IDs to exclude from a list of all discovered devices in your network (concerning the managed endpoints only):
     a. Select the exclusion type (by Product ID or by Device ID).
     b. In the **Exclusions** table, select the ID's that you want to exclude:
        – For Device IDs, select each device to exclude from the list.
        – For Product IDs, by selecting one device, you will exclude all the devices having the same Product ID.
     c. In the **Description** field, enter a name that will help you identify the device or the range of devices.
     d. Select the permission type for specified devices (Allowed or Blocked).
     e. Click **Save**.

Important
Devices already connected to endpoints at the Bitdefender Endpoint Security Tools installation will be discovered only after restarting the corresponding endpoints.

All device exclusions will appear in the **Exclusions** table.

To remove an exclusion:
a. Select it in the table.
b. Click the ⊕ **Delete** button at the upper side of the table.



Computers and Virtual Machines Policies - Device Control - Exclusions

5.2.8. Relay

This section allows you to define communication and update settings for target endpoints assigned with relay role.

The settings are organized into the following sections:

- Communication
- Update

Communication

The **Communication** tab contains proxy preferences for the communication between relay endpoints and the GravityZone components.

If needed, you can configure independently the communication between target relay endpoints and Bitdefender Cloud Services / GravityZone, using the following settings:

- **Keep installation settings**, to use the same proxy settings defined with the installation package.
- **Use proxy defined in the General section**, to use the proxy settings defined in the current policy, under **General > Settings** section.
- **Do not use**, when the target endpoints do not communicate with the specific Bitdefender components via proxy.

Update

This section allows you to define the update settings for target endpoints with relay role:

- Under **Update** section, you can configure the following settings:
  - The time interval when the relay endpoints check for updates.
  - The folder located on the relay endpoint where product and signature updates are downloaded and also mirrored . If you want to define a specific download folder, enter its full path in the corresponding field.

    Important
    It is recommended to define a dedicated folder for product and signature updates. Avoid choosing a folder containing system or personal files.

- **Define custom update locations**. The default update location for relay agents is the local GravityZone update server. You can specify other update locations by entering the IP or the local hostname of one or several update servers in your network, then configure their priority using the up and down buttons displayed on mouse-over. If the first update location is unavailable, the next one is used and so on.

  To define a custom update location:

  1. Enable the **Define custom update locations** option.
  2. Enter the address of the new update server in the **Add location** field. Use one of these syntaxes:
     - `update_server_ip:port`
     - `update_server_name:port`

     The default port is 7074.

3. If the relay endpoint communicates with the local update server through a proxy server, select **Use Proxy**. The proxy settings defined in the **General > Settings** section will be taken into account.
4. Click the ⊕ **Add** button at the right side of the table.
5. Use the ⌃ Up / ⌄ Down arrows in the **Action** column to set priority of defined update locations. If the first update location is not available, the next one is taken into account, and so on.

To remove a location from the list, click the corresponding ⊗ **Delete** button. Although you can remove the default update location, this is not recommended.

5.2.9. Exchange Protection

Security for Exchange comes with highly configurable settings, securing the Microsoft Exchange Servers against threats such as malware, spam and phishing. With Exchange Protection installed on your mail server, you can also filter emails containing attachments or content considered dangerous according to your company's security policies.

To keep the server's performance at normal levels, the email traffic is processed by the Security for Exchange filters in the following order:

1. Antispam filtering
2. Content Control > Content filtering
3. Content Control > Attachment filtering
4. Antimalware filtering

The Security for Exchange settings are organized into the following sections:

- General
- Antimalware
- Antispam
- Content Control

General

In this section you can create and manage groups of email accounts, define the age of the quarantined items and ban specific senders.

User Groups

Control Center allows creating user groups to apply different scanning and filtering policies to different user categories. For example, you can create appropriate

policies for the IT department, for the sales team or for the managers of your company.

The user groups are globally available, regardless of the policy or the user that created them.

For an easier group management, Control Center automatically imports the user groups from Windows Active Directory.

To create a user group:

1. Click the ⊕ **Add** button at the upper side of the table. The details windows is displayed.
2. Enter the group name, description and the users' email addresses.

   Note
   - For a large list of email addresses, you can copy and paste the list from a text file.
   - Accepted list separators: space, comma, semicolon and enter.

3. Click **Save**.

Custom groups are editable. Click the group name to open the configuration window where and you can change the group details or edit the users list.

To remove a custom group from the list, select the group and click the ⊖ **Delete** button at the upper side of the table.

Note
You cannot edit or delete Active Directory groups.

Settings

- **Delete quarantined files older than (days).** By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, enter a different value in the corresponding field.
- **Connection Blacklist.** With this option enabled, Exchange Server rejects all emails from the blacklisted senders.

  To build a blacklist:
  1. Click the **Edit blacklisted items** link.
  2. Enter the email addresses you want to block. When editing the list, you can also use the following wildcards to define an entire email domain or a pattern for email addresses:

- Asterisk (*), replacing zero, one or more characters.
- Question mark (?), replacing any single character.

For example, if you enter `*@boohouse.com`, all email addresses from `boohouse.com` will be blocked.

3. Click **Save**.

Domain IP Check (Antispoofing)

Use this filter to prevent spammers from spoofing the sender's email address and making the email appear as being sent by someone trusted. You can specify the IP addresses authorized to send email for your email domains and, if needed, for other known email domains. If an email appears to be from a listed domain, but the sender's IP address does not match one of the specified IP addresses, the email is rejected.

Warning
Do not use this filter if you are using a smart host, a hosted email filtering service or gateway email filtering solution in front of your Exchange servers.

Important

- The filter only checks unauthenticated email connections.
- Best practices:
  - It is recommended to use this filter only on Exchange Servers that are directly facing the Internet. For example, if you have both Edge Transport and Hub Transport servers, configure this filter only on the Edge servers.
  - Add to your domains list all internal IP addresses allowed to send email over unauthenticated SMTP connections. These might include automated notification systems, network equipment such as printers, etc.
  - In an Exchange setup using Database Availability Groups, also add to your domains list the IP addresses of all your Hub Transport and Mailbox servers.
  - Use caution if you want to configure authorized IP addresses for specific external email domains that are not under your management. If you do not manage to keep the IP address list up-to-date, email messages from those domains will be rejected. If you are using an MX backup, you must add to all external email domains configured the IP addresses from which MX backup forwards email messages to your primary mail server.

To configure antispoofing filtering, follow the steps described herein:

1. Select the **Domain IP Check (Antispoofing)** check box to enable the filter.
2. Click the ⊕ **Add** button at the upper side of the table. The configuration window appears.
3. Enter the email domain in the corresponding field.
4. Provide the range of authorized IP addresses to be used with the previously specified domain, using the CIDR format (IP/Network mask).
5. Click the ⊕ **Add** button at the right side of the table. The IP addresses are added to the table.
6. To delete an IP range from the list, click the corresponding ⊗ **Delete** button at the right side of the table.
7. Click **Save**. The domain is added to the filter.

To delete an email domain from the filter, select it in the Antispoofing table and click the ⊖ **Delete** button at the upper side of the table.

Antimalware

The Antimalware module protects Exchange mail servers against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware, etc.), by detecting infected or suspect items and attempting to disinfect them or isolating the infection, according to the specified actions.

Antimalware scanning is performed at two levels:

- Transport Level
- Exchange Store

Transport Level Scanning

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

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

Use the **Antimalware filtering** check box to disable or re-enable this feature.

To configure the notification text, click the **Settings** link. The following options are available:

- **Add footer to scanned emails.** Select this check box to add a sentence at the bottom of the scanned emails. To change the default text, enter your message in the text box below.
- **Replacement text.** For emails whose attachments have been deleted or quarantined, a notification file can be attached. To modify the default notification texts, enter your message in the corresponding text boxes.

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

Managing Filtering Rules

You can view all existing rules listed in the table, together with information on their priority, status and scope. The rules are ordered by priority with the first rule having the highest priority.

Any antimalware policy has a default rule that becomes active once the antimalware filtering is enabled. What you need to know about the default rule:

- You cannot copy, disable or delete the rule.
- You can modify only the scanning settings and actions.
- The default rule priority is always the lowest.

Creating Rules

You have two alternatives for creating filtering rules:

- Start from the default settings, by following these steps:
  1. Click the ⊕ **Add** button at the upper side of the table to open the configuration window.
  2. Configure the rule settings. For details regarding the options, refer to Rule Options.
  3. Click **Save**. The rule is listed first in the table.
- Use a clone of a custom rule as a template, by following these steps:
  1. Select the rule that you want from the table.
  2. Click the ⊙ **Clone** button at the upper side of the table to open the configuration window.
  3. Adjust the rule options according to your needs.
  4. Click **Save**. The rule is listed first in the table.

Editing Rules

To edit an existing rule:

1. Click the rule name to open the configuration window.

2. Enter the new values for the options you want to modify.
3. Click **Save**. The changes take effect after the policy is saved.

Setting Rule Priority

To change a rule's priority:

1. Select the rule to be moved.
2. Use the **Up** or **Down** buttons at the upper side of the table to increase or decrease the rule priority.

Removing Rules

You can delete one or several custom rules at once. All you need to do is:

1. Select the check box of the rules to be deleted.
2. Click the **Delete** button at the upper side of the table. Once a rule is deleted, you cannot recover it.

Rule Options

The following options are available:

- **General.** In this section you must set a name for the rule, otherwise you cannot save it. Select the **Active** check box if you want the rule to be effective after the policy is saved.
- **Rule Scope.** You can restrict the rule to apply only to a subset of emails, by setting the following cumulative scope options:
  - **Apply to (direction).** Select the email traffic direction to which the rule applies.
  - **Senders.** You can decide whether the rule applies for any sender or only for specific senders. To narrow the senders range, click the **Specific** button and select the desired groups from the table on the left. View the selected groups in the table on the right.
  - **Recipients.** You can decide whether the rule applies for any recipient or only for specific recipients. To narrow the recipients range, click the **Specific** button and select the desired groups from the table on the left. You can view the selected groups in the table on the right.

    The rule applies if any of the recipients matches your selection. If you want to apply the rule only if all recipients are in the selected groups, select **Match all recipients**.

    Note
    The addresses in the **Cc** and **Bcc** fields also count as recipients.

> **Important**
> The rules based on user groups apply only to Hub Transport and Mailbox roles.

- **Options.** Configure the scan options for emails matching the rule:
  - **Scanned file types.** Use this option to specify which file types you want to be scanned. You can choose to scan all files (regardless of their file extension), application files only, or specific file extensions you consider to be dangerous. Scanning all files provides the best protection, while scanning only applications is recommended for a quicker scan.

    > **Note**
    > Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

    If you want to scan only files with specific extensions, you have two alternatives:
    - **User defined extensions**, where you must provide only the extensions to be scanned.
    - **All files, except specific extensions**, where you must enter only the extensions to be skipped from scanning.
  - **Attachment / email body maximum size (MB).** Select this check box and enter a value in the corresponding field to set the maximum accepted size of an attached file or of the email body to be scanned.
  - **Archive maximum depth (levels).** Select the check box and choose the maximum archive depth from the corresponding field. The lower the depth level is, the higher the performance and the lower the protection grade.
  - **Scan for Potentially Unwanted Applications (PUA).** Select this check box to scan for possibly malicious or unwanted applications, such as adware, which may install on systems without user's consent, change the behavior of various software products and lower the system performance.
- **Actions.** You can specify different actions for the security agent to automatically take on files, based on the detection type.

  The detection type separates the files into three categories:
  - **Infected files.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies.
  - **Suspect files.** These files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but

the users must be aware of certain false positives (clean files detected as suspicious) in some cases.

– **Unscannable files.** These files cannot be scanned. Unscannable files include but are not limited to password-protected, encrypted or over-compressed files.

For each detection type, you have a default or main action and an alternative action in case the main one fails. Though not recommended, you can change these actions from the corresponding menus. Choose the action to be taken:

– **Disinfect.** Removes the malware code from infected files and reconstructs the original file. For particular types of malware, disinfection is not possible because the detected file is entirely malicious. It is recommended to always keep this as the first action to be taken on infected files. Suspect files cannot be disinfected, because no disinfection routine is available.
– **Reject / Delete email.** On servers with Edge Transport role, the detected email is rejected with a 550 SMTP error code. In all other cases, the email is deleted without any warning. It is advisable to avoid using this action.
– **Delete file.** Deletes the attachments with issues without any warning. It is advisable to avoid using this action.
– **Replace file.** Deletes the files with issues and inserts a text file that notifies the user of the actions taken.
– **Move file to quarantine.** Moves detected files to the quarantine folder and inserts a text file that notifies the user of the actions taken. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the **Quarantine** page.

> **Note**
> Please note that 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.

– **Take no action.** No action will be taken on detected files. These files will only appear in the scan log. Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine.
– By default, when an email matches the rule scope, it is processed exclusively in accordance with the rule, without being checked against any other remaining rule. If you want to continue checking against the other rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

Exclusions

If you want certain email traffic to be ignored by any filtering rule, you can define scan exclusions. To create an exclusion:

1. Expand the **Exclusions for Antimalware Rules** section.
2. Click the ⊖ **Add** button from this section toolbar, which opens the configuration window.
3. Configure the exclusion settings. For details on the options, refer to Rule Options.
4. Click **Save**.

Exchange Store Scanning

Exchange Protection uses Exchange Web Services (EWS) from Microsoft to allow scanning the Exchange mailbox and public folder databases. You can configure the antimalware module to run on-demand scan tasks regularly on the target databases, according to the schedule you specify.

Note

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

On-demand scanning requires an Exchange administrator account (service account) to impersonate Exchange users and to retrieve the target objects to be scanned from the user mailboxes and public folders. It is recommended to create a dedicated account for this purpose.

The Exchange administrator account must meet the following requirements:

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

Enabling On-Demand Scanning

1. In the **Scan Tasks** section, click the **Add credentials** link.
2. Enter the service account username and password.

3. If the email differ from the username, you need to also provide the email address of the service account.
4. Enter the Exchange Web Services (EWS) URL, necessary when the Exchange Autodiscovery does not work.

Note

- The username must include the domain name, as in `user@domain` or `domain\user`.
- Do not forget to update the credentials in Control Center, whenever they have changed.

Managing Scan Tasks

The scan tasks table shows all scheduled tasks and provides information on their targets and recurrence.

To create tasks for scanning the Exchange Store:

1. In the **Scan Tasks** section, click the ⊕ **Add** button at the upper side of the table to open the configuration window.
2. Configure the task settings as described in the following section.
3. Click **Save**. The task is added in the list and it becomes effective once the policy is saved.

You can edit a task at any time by clicking the task name.

To remove tasks from the list, select them and click the ⊖ **Delete** button at the upper side of the table.

Scan Task Settings

Tasks have a series of settings which you can find described herein:

- **General.** Enter a suggestive name for the task.

  Note
  You can view the task name in Bitdefender Endpoint Security Tools timeline.

- **Scheduler.** Use the scheduling options to configure the scan schedule. You can set the scan to run every few hours, days or weeks, starting with a specified date and time. For large databases, the scan task may take a long time and may impact the server performance. In such cases, you can configure the task to stop after a specified time.

- **Target.** Select the containers and objects to be scanned. You can choose to scan mailboxes, public folders or both. Beside emails, you can choose to scan other objects such as **Contacts**, **Tasks**, **Appointments** and **Post Items**. You can furthermore set the following restrictions to the content to be scanned:
  - Only unread messages
  - Only items with attachments
  - Only new items, received in a specified time interval

  For example, you can choose to scan only emails from user mailboxes, received in the last seven days.

  Select the **Exclusions** check box, if you want to define scan exceptions. To create an exception, use the fields from the table header as follows:
  1. Select the repository type from the menu.
  2. Depending on the repository type, specify the object to be excluded:

Repository type	Object format
Mailbox	Email address
Public Folder	Folder path, starting from the root
Database	The database identity

     Note
     To obtain the database identity, use the Exchange shell command:
     `Get-MailboxDatabase | fl name,identity`

     You can enter only one item at a time. If you have several items of the same type, you must define as many rules as the number of items.
  3. Click the ⊕ **Add** button at the upper side of the table to save the exception and add it to the list.

  To remove an exception rule from the list, click the corresponding ⊖ **Delete** button.
- **Options.** Configure the scan options for emails matching the rule:
  - **Scanned file types.** Use this option to specify which file types you want to be scanned. You can choose to scan all files (regardless of their file extension), application files only, or specific file extensions you consider to be dangerous. Scanning all files provides the best protection, while scanning only applications is recommended for a quicker scan.

> **Note**
> Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "Application File Types" (p. 367).

If you want to scan only files with specific extensions, you have two alternatives:

- **User defined extensions**, where you must provide only the extensions to be scanned.
- **All files, except specific extensions**, where you must enter only the extensions to be skipped from scanning.

– **Attachment / email body maximum size (MB).** Select this check box and enter a value in the corresponding field to set the maximum accepted size of an attached file or of the email body to be scanned.
– **Archive maximum depth (levels).** Select the check box and choose the maximum archive depth from the corresponding field. The lower the depth level is, the higher the performance and the lower the protection grade.
– **Scan for Potentially Unwanted Applications (PUA).** Select this check box to scan for possibly malicious or unwanted applications, such as adware, which may install on systems without user's consent, change the behavior of various software products and lower the system performance.

- **Actions.** You can specify different actions for the security agent to automatically take on files, based on the detection type.

  The detection type separates the files into three categories:
  – **Infected files.** Bitdefender detects files as infected through various advanced mechanisms, which include malware signatures, machine learning and artificial intelligence (AI) based technologies.
  – **Suspect files.** These files are detected as suspicious by the heuristic analysis and other Bitdefender technologies. These provide a high detection rate, but the users must be aware of certain false positives (clean files detected as suspicious) in some cases.
  – **Unscannable files.** These files cannot be scanned. Unscannable files include but are not limited to password-protected, encrypted or over-compressed files.

  For each detection type, you have a default or main action and an alternative action in case the main one fails. Though not recommended, you can change these actions from the corresponding menus. Choose the action to be taken:
  – **Disinfect.** Removes the malware code from infected files and reconstructs the original file. For particular types of malware, disinfection is not possible

because the detected file is entirely malicious. It is recommended to always keep this as the first action to be taken on infected files. Suspect files cannot be disinfected, because no disinfection routine is available.
- **Reject / Delete email.** The email is deleted without any warning. It is advisable to avoid using this action.
- **Delete file.** Deletes the attachments with issues without any warning. It is advisable to avoid using this action.
- **Replace file.** Deletes the files with issues and inserts a text file that notifies the user of the actions taken.
- **Move file to quarantine.** Moves detected files to the quarantine folder and inserts a text file that notifies the user of the actions taken. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the **Quarantine** page.

  Note
  Please note that 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 and size of the emails stored.

- **Take no action.** No action will be taken on detected files. These files will only appear in the scan log. Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine.
- By default, when an email matches the rule scope, it is processed exclusively in accordance with the rule, without being checked against any other remaining rule. If you want to continue checking against the other rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

Antispam

The Antispam module offers multiple layer protection against spam and phishing by using a combination of various filters and engines to determine whether emails are spam or not.

Note
- Antispam filtering is available for:
  - Exchange Server 2016/2013 with the Edge Transport or Mailbox role
  - Exchange Server 2010/2007 with the Edge Transport or Hub Transport role

- If you have both Edge and Hub roles in your Exchange organization, it is recommended to enable the antispam filtering on the server with the Edge Transport role.

Spam filtering is automatically enabled for incoming emails. Use the **Antispam filtering** check box to disable or re-enable this feature.

Antispam Filters

An email is checked against the antispam filtering rules based on the sender and recipients groups, by order of priority, until it matches a rule. The email is then processed according to the rule options, and actions are taken on the detected spam.

Certain antispam filters are configurable and you can control whether to use them or not. This is the list of the optional filters:

- **Charset Filter.** Many spam emails are written in Cyrillic or Asian charsets. The Charset Filter detects this kind of emails and tags them as SPAM.
- **Sexually Explicit Tagged Content.** Spam that contains sexually oriented material must include the warning SEXUALLY-EXPLICIT: in the subject line. This filter detects emails marked as SEXUALLY-EXPLICIT: in the subject line and tags them as spam.
- **URL Filter.** Almost all spam emails include links to various web locations. Usually, these locations contain more advertising and offer the possibility to buy things. Sometimes, they are also used for phishing.

  Bitdefender maintains a database of such links. The URL filter checks every URL link in an email against its database. If a match is made, the email is tagged as spam.
- **Realtime Blackhole List (RBL).** This is a filter that allows checking the sender's mail server against third party RBL servers. The filter uses the DNSBL protocol and RBL servers to filter spam based on mail servers' reputation as spam senders.

  The mail server address is extracted from the email header and its validity is checked. If the address belongs to a private class (`10.0.0.0`, `172.16.0.0` to `172.31.0.0` or `192.168.0.0` to `192.168.255.0`), it is ignored.

  A DNS check is performed on the domain `d.c.b.a.rbl.example.com`, where `d.c.b.a` is the reversed IP address of the server and `rbl.example.com` is the RBL server. If the DNS replies that the domain is valid, it means that the IP

is listed in the RBL server and a certain server score is provided. This score ranges between 0 and 100, according to the confidence level you granted to the server.

The query is performed for every RBL server in the list and the score returned by each one is added to the intermediate score. When the score has reached 100, no more queries are performed.

If the RBL filter score is 100 or higher, the email is considered spam and the specified action is taken. Otherwise, a spam score is computed from the RBL filter score and added to the global spam score of the email.

- **Heuristic Filter.** Developed by Bitdefender, the Heuristic filter detects new and unknown spam. The filter is automatically trained on large volumes of spam emails inside the Bitdefender Antispam Lab. During training, it learns to distinguish between spam and legitimate emails and to recognize new spam by perceiving its similarities, often very subtle, with the emails it has already examined. This filter is designed to improve signature-based detection, while keeping the number of false positives very low.
- **Bitdefender Cloud Query.** Bitdefender maintains a constantly evolving database of spam mail "fingerprints" in the cloud. A query containing the email fingerprint is sent to the servers in the cloud to verify on the fly if the email is spam. Even if the fingerprint is not found in the database, it is checked against other recent queries and, provided certain conditions are met, the email is marked as spam.

Managing Antispam Rules

You can view all existing rules listed in the table, together with information on their priority, status and scope. The rules are ordered by priority with the first rule having the highest priority.

Any antispam policy has a default rule that becomes active once the module is enabled. What you need to know about the default rule:

- You cannot copy, disable or delete the rule.
- You can modify only the scanning settings and the actions.
- The default rule priority is always the lowest.

Creating Rules

To create a rule:

1. Click the ⊕ **Add** button at the upper side of the table to open the configuration window.

2. Configure the rule settings. For details regarding the options, refer to " Rule options " (p. 261).
3. Click **Save**. The rule is listed first in the table.

Editing Rules

To edit an existing rule:

1. Click the rule name to open the configuration window.
2. Enter the new values for the options you want to modify.
3. Click **Save**. If the rule is active, changes take effect after the policy is saved.

Setting Rule Priority

To change a rule priority, select the rule that you want and use the **Up** and **Down** arrows at the upper side of the table. You can move only one rule at a time.

Removing Rules

If you do not want to use a rule anymore, select the rule and click the **Delete** button at the upper side of the table.

Rule options

The following options are available:

- **General.** In this section you must set a name for the rule, otherwise you cannot save it. Select the **Active** check box if you want the rule to be effective after the policy is saved.
- **Rule Scope.** You can restrict the rule to apply only to a subset of emails, by setting the following cumulative scope options:
  - **Apply to (direction).** Select the email traffic direction to which the rule applies.
  - **Senders.** You can decide whether the rule applies for any sender or only for specific senders. To narrow the senders range, click the **Specific** button and select the desired groups from the table on the left. View the selected groups in the table on the right.
  - **Recipients.** You can decide whether the rule applies for any recipient or only for specific recipients. To narrow the recipients range, click the **Specific** button and select the desired groups from the table on the left. You can view the selected groups in the table on the right.

    The rule applies if any of the recipients matches your selection. If you want to apply the rule only if all recipients are in the selected groups, select **Match all recipients**.

Note
The addresses in the **Cc** and **Bcc** fields also count as recipients.

Important
The rules based on user groups apply only to Hub Transport and Mailbox roles.

- **Settings.** Click the security level that best suits your needs (**Aggressive**, **Normal** or **Permissive**). Use the description on the right side of the scale to guide your choice.

  Additionally, you can enable various filters. For detailed information regarding these filters, refer to "Antispam Filters " (p. 259).

  Important
  The RBL filter requires additional configuration. You can configure the filter after you have created or edited the rule. For more information, refer to " Configuring the RBL Filter " (p. 263)

  For the authenticated connections you can choose whether to bypass or not the antispam scanning.
- **Actions.** There are several actions which you can take on detected emails. Each action has, at its turn, several possible options or secondary actions. Find them described herein:

  Main actions:
  - **Deliver email.** The spam email reaches the recipients mailboxes.
  - **Quarantine email.** The email is encrypted and saved in the quarantine folder from the Exchange Server, without being delivered to recipients. You can manage the quarantined emails in the **Quarantine** page.
  - **Redirect email to.** The email is not delivered to the original recipients, but to a mailbox you specify in the corresponding field.
  - **Reject / Delete email.** On servers with Edge Transport role, the detected email is rejected with a 550 SMTP error code. In all other cases, the email is deleted without any warning. It is advisable to avoid using this action.

  Secondary actions:
  - **Integrate with Exchange SCL.** Adds a header to the spam email, allowing Exchange Server or Microsoft Outlook to take action according to the Spam Confidence Level (SCL) mechanism.

- **Tag the email subject as.** You can add a label to the email subject to help users filter detected emails in the email client.
- **Add an email header.** A header is added to emails detected as spam. You can modify the header name and value by entering the desired values in the corresponding fields. Further on, you can use this email header to create additional filters.
- **Save email to disk.** A copy of the spam email is saved as a file to the specified folder. Provide the absolute path of the folder in the corresponding field.

  Note
  This option supports only emails in MIME format.

- **Archive to account.** A copy of the detected email is delivered to the specified email address. This action adds the specified email address to the email Bcc list.

- By default, when an email matches the rule scope, it is processed exclusively in accordance with the rule, without being checked against any other remaining rule. If you want to continue checking against the other rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

Configuring the RBL Filter

If you want to use the RBL filter, you must provide a list of RBL servers.

To configure the filter:

1. In the **Antispam** page, click the **Settings** link to open the configuration window.
2. Provide the IP address of the DNS server to query and the query timeout interval in the corresponding fields.
3. For each RBL server:
   a. Enter the server hostname or IP address and the confidence level you have assigned to the server, in the fields from the table header.
   b. Click the ⊕ **Add** button at the upper side of the table.
4. Click **Save**.

Configuring Sender Whitelist

For known email senders, you can prevent unnecessary server resource consumption, by including them into lists for trusted or untrusted senders. Thus, the mail server will always accept or reject emails coming from these senders. For

example, you have an intense email communication with a business partner and to make sure you receive all emails, you can add the partner to the whitelist.

To build a whitelist of trusted senders:

1. Click the **Whitelist** link to open the configuration window.
2. Select the **Sender Whitelist** check box.
3. Enter the email addresses in the corresponding field. When editing the list, you can also use the following wildcards to define an entire email domain or a pattern for email addresses:
   - Asterisk (*), replacing zero, one or more characters.
   - Question mark (?), replacing any single character.

   For example, if you enter `*.gov`, all emails coming from the `.gov` domain will be accepted.
4. Click **Save**.

Note
To blacklist known spam senders, use the **Connection Blacklist** option from the **Exchange Protection > General > Settings** section.

Content Control

Use Content Control to enhance email protection by filtering all email traffic that is non-compliant with your company policies (unwanted or potentially sensitive content).

For an overall control of the email content, this module comprises two email filtering options:

- Content filtering
- Attachment filtering

Note
Content Filtering and Attachment Filtering are available for:
- Exchange Server 2016/2013 with the Edge Transport or Mailbox role
- Exchange Server 2010/2007 with the Edge Transport or Hub Transport role

Managing Filtering Rules

Content Control filters rely on rules. You can define various rules for different users and user groups. Each email that reaches the mail server is checked against the

filtering rules, by order of priority, until it matches a rule. The email is then processed according to the options specified by that rule.

The content filtering rules precede the attachment filtering rules.

Content and attachment filtering rules are listed in the corresponding tables ordered by priority, with the first rule having the highest priority. For each rule, the following information is provided:

- Priority
- Name
- Traffic direction
- Senders and recipients groups

Creating Rules

You have two alternatives for creating filtering rules:

- Start from the default settings, by following these steps:
  1. Click the ⊕ **Add** button at the upper side of the table to open the configuration window.
  2. Configure the rule settings. For details about specific content and attachment filtering options, refer to:
     - Content Filtering Rule Options
     - Attachment Filtering Rule Options.
  3. Click **Save**. The rule is listed first in the table.
- Use a clone of a custom rule as a template, by following these steps:
  1. Select the desired rule from the table.
  2. Click the ⧉ **Clone** button at the upper side of the table to open the configuration window.
  3. Adjust the rule options to your needs.
  4. Click **Save**. The rule is listed first in the table.

Editing Rules

To edit an existing rule:

1. Click the rule name to open the configuration window.
2. Enter the new values for the options you want to modify.
3. Click **Save**. The changes take effect after the policy is saved.

Setting Rule Priority

To change a rule's priority:

1. Select the rule to be moved.

2. Use the **Up** or **Down** buttons at the upper side of the table to increase or decrease the rule priority.

Removing Rules

You can delete one or several custom rules. All you need to do is:

1. Select the rules to be deleted.
2. Click the **Delete** button at the upper side of the table. Once a rule is deleted, you cannot recover it.

Content Filtering

Content Filtering helps you filter email traffic based on the character strings you have previously defined. These strings are compared with the email subject or with the text content of the email body. By using Content Filtering, you can achieve the following goals:

- Prevent unwanted email content from entering the Exchange Server mailboxes.
- Block outgoing emails containing confidential data.
- Archive emails that meet specific conditions to a different email account or on the disk. For example, you can save the emails sent to your company's support email address to a folder on the local disk.

Enabling Content Filtering

If you want to use content filtering, select the **Content filtering** check box.

For creating and managing content filtering rules, refer to "Managing Filtering Rules" (p. 264).

Rule Options

- **General.** In this section you must set a name for the rule, otherwise you cannot save it. Select the **Active** check box if you want the rule to be effective after the policy is saved.
- **Rule Scope.** You can restrict the rule to apply only to a subset of emails, by setting the following cumulative scope options:
  - **Apply to (direction).** Select the email traffic direction to which the rule applies.
  - **Senders.** You can decide whether the rule applies for any sender or only for specific senders. To narrow the senders range, click the **Specific** button and select the desired groups from the table on the left. View the selected groups in the table on the right.

- **Recipients.** You can decide whether the rule applies for any recipient or only for specific recipients. To narrow the recipients range, click the **Specific** button and select the desired groups from the table on the left. You can view the selected groups in the table on the right.

  The rule applies if any of the recipients matches your selection. If you want to apply the rule only if all recipients are in the selected groups, select **Match all recipients**.

  Note
  The addresses in the **Cc** and **Bcc** fields also count as recipients.

  Important
  The rules based on user groups apply only to Hub Transport and Mailbox roles.

- **Settings.** Configure the expressions to be searched for in emails as described herein:
  1. Choose the part of the email to be checked:
     - The email subject, by selecting the **Filter by subject** check box. All emails whose subject contains any of the expressions entered in the corresponding table are being filtered.
     - The body content, by selecting the **Filter by body content** check box. All emails that contain in their body any of the defined expressions are being filtered.
     - Both the subject and the body content, by selecting both check boxes. All emails whose subject matches any rule from the first table AND their body contains any expression from the second table, are being filtered. For example:

       The first table contains the expressions: `newsletter` and `weekly`. The second table contains the expressions: `shopping`, `price` and `offer`.

       An email with the subject "Monthly **newsletter** from your favorite watch vendor" and the body containing the phrase "We have the pleasure to present you our latest **offer** containing sensational watches at irresistible **prices**." will make a match on the rule and will be filtered. If the subject is "News from your watch vendor", the email is not filtered.
  2. Build the lists of conditions, using the fields from the table headers. For each condition, follow these steps:

a. Select the expression type used in searches. You can choose to enter the exact text expression or to build text patterns with the use of regular expressions.

> **Note**
> The syntax of regular expressions is validated against the ECMAScript grammar.

b. Enter the search string in the **Expression** field.

For example:

i. The expression `5[1-5]\d{2}([\s\-]?\d{4}){3}` matches the bank cards with numbers that start with fifty-one through fifty-five, have sixteen digits in groups of four, and the groups may be separated by space or hyphen. Therefore, any email containing the card number in one of the formats: `5257-4938-3957-3948`, `5257 4938 3957 3948` or `5257493839573948`, will be filtered.

ii. This expression detects emails with the words `lottery`, `cash` and `prize`, found in this exact order:

```
(lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
```

To detect emails that contain each of the three words regardless of their order, add three regular expressions with different word order.

iii. This expression detects emails that include three or more occurrences of the word `prize`:

```
(prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
```

c. If you want to differentiate the capital letters from the small letters in text comparisons, select the **Match case** check box. For example, with the check box selected, `Newsletter` is not the same with `newsletter`.

d. If you do not want the expression to be a part of other words, select the **Whole word** check box. For example, with the check box selected, the expression `Anne's salary` does not make a match with `MariAnne's salary`.

e. Click the ⊕ **Add** button from the **Action** column header to add the condition to the list.

- **Actions.** There are several actions which you can take on emails. Each action has, at its turn, several possible options or secondary actions. Find them described herein:

  Main actions:
  - **Deliver email.** The detected email reaches the recipients mailboxes.
  - **Quarantine.** The email is encrypted and saved in the quarantine folder from the Exchange Server, without being delivered to recipients. You can manage the quarantined emails in the **Quarantine** page.
  - **Redirect to.** The email is not delivered to the original recipients, but to a mailbox you specify in the corresponding field.
  - **Reject / Delete email.** On servers with Edge Transport role, the detected email is rejected with a 550 SMTP error code. In all other cases, the email is deleted without any warning. It is advisable to avoid using this action.

  Secondary actions:
  - **Tag the email subject as.** You can add a label to the detected email subject to help users filter emails in the email client.
  - **Add a header to the email messages.**You can add a header name and a value to the headers of the detected email, by entering the desired values in the corresponding fields.
  - **Save mail to disk.** A copy of the detected email is saved as a file to the specified folder on the Exchange Server. If the folder does not exist, it will be created. You must provide the absolute path of the folder in the corresponding field.

    Note
    This option supports only emails in MIME format.

  - **Archive to account.** A copy of the detected email is delivered to the specified email address. This action adds the specified email address to the email Bcc list.
- By default, when an email matches the conditions of a rule, it is no longer checked against any other rules. If you want to continue processing rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

Exclusions

If you want the email traffic for specific senders or recipients to be delivered regardless of any content filtering rule, you can define filtering exclusions.

To create an exclusion:

1. Click the **Exclusions** link next to the **Content filtering** check box. This action opens the configuration window.
2. Enter the email addresses of the trusted senders and/or recipients in the corresponding fields. Any email coming from a trusted sender or going to a trusted recipient is excluded from filtering. When editing the list, you can also use the following wildcards to define an entire email domain or a pattern for email addresses:
   - Asterisk (*), replacing zero, one or more characters.
   - Question mark (?), replacing any single character.

   For example, if you enter `*.gov`, all emails coming from the `.gov` domain will be accepted.
3. For emails with multiple recipients, you can select the check box **Exclude email from filtering only if all recipients are trusted** to apply the exclusion only if all email recipients are present in the trusted recipients list.
4. Click **Save**.

Attachment Filtering

The Attachment Filtering module provides filtering features for mail attachments. It can detect attachments with certain name patterns or of a certain type. By using Attachment Filtering, you can:

- Block potentially dangerous attachments, such as `.vbs` or `.exe` files, or the emails containing them.
- Block attachments having offensive names or the emails containing them.

Enabling Attachment Filtering

If you want to use attachment filtering, select the **Attachment filtering** check box.

For creating and managing attachment filtering rules, refer to "Managing Filtering Rules" (p. 264).

Rule Options

- **General.** In this section you must set a name for the rule, otherwise you cannot save it. Select the **Active** check box if you want the rule to be effective after the policy is saved.

- **Rule Scope.** You can restrict the rule to apply only to a subset of emails, by setting the following cumulative scope options:
  - **Apply to (direction).** Select the email traffic direction to which the rule applies.
  - **Senders.** You can decide whether the rule applies for any sender or only for specific senders. To narrow the senders range, click the **Specific** button and select the desired groups from the table on the left. View the selected groups in the table on the right.
  - **Recipients.** You can decide whether the rule applies for any recipient or only for specific recipients. To narrow the recipients range, click the **Specific** button and select the desired groups from the table on the left. You can view the selected groups in the table on the right.

    The rule applies if any of the recipients matches your selection. If you want to apply the rule only if all recipients are in the selected groups, select **Match all recipients**.

    Note
    The addresses in the **Cc** and **Bcc** fields also count as recipients.

    Important
    The rules based on user groups apply only to Hub Transport and Mailbox roles.

- **Settings.** Specify the files that are allowed or denied in email attachments.

  You can filter email attachments by file type or by file name.

  To filter attachments by file type, follow these steps:
  1. Select the **Detect by Content Type** check box.
  2. Select the detection option that is more suitable for your needs:
     - **Only the following categories**, when you have a limited list of forbidden file type categories.
     - **All except the following categories**, when you have a limited list of allowed file type categories.
  3. Select the file type categories of your interest from the available list. For details on the extensions of each category, refer to "Attachment Filtering File Types" (p. 367).

If you are interested in some specific file types only, select the **Custom extensions** check box and enter the list of extensions in the corresponding field.

4. Select the **Enable true type detection** check box to check file headers and correctly identify the attachment file type when scanning for restricted extensions. This means an extension cannot be simply renamed to bypass attachment filtering policies.

> **Note**
> True type detection can be resource intensive.

To filter attachments by their name, select the **Detect by Filename** check box and enter the filenames you want to filter, in the corresponding field. When editing the list, you can also use the following wildcards to define patterns:

- Asterisk (*), replacing zero, one or more characters.
- Question mark (?), replacing any single character.

For example, if you enter `database.*`, all files named `database`, regardless of their extension, will be detected.

> **Note**
> If you enable both content type and filename detections (without true type detection), the file must simultaneously meet the conditions for both detection types. For example, you have selected the **Multimedia** category and entered the filename `test.pdf`. In this case any email passes the rule because the PDF file is not a multimedia file.

Select the **Scan inside archives** check box to prevent blocked files from being hidden in apparently inoffensive archives and thus by-passing the filtering rule.

The scan is recursive inside archives and by default it goes until the fourth archive depth level. You can optimize the scan as described herein:

1. Select the **Archive maximum depth (levels)** check box.
2. Choose a different value from the corresponding menu. For best performance choose the lowest value, for maximum protection choose the highest value.

> **Note**
> If you have selected to scan archives, **Scan inside archives** is disabled and all archives are scanned.

- **Actions.** There are several actions which you can take on detected attachments or on the emails containing them. Each action has, at its turn, several possible options or secondary actions. Find them described herein:

  Main actions:

  - **Replace file.** Deletes the detected files and inserts a text file that notifies the user of the actions taken.

    To configure the notification text:
    1. Click the **Settings** link next to the **Attachment filtering** check box.
    2. Enter the notification text in the corresponding field.
    3. Click **Save**.
  - **Delete file.** Deletes the detected files without any warning. It is advisable to avoid using this action.
  - **Reject/Delete email.** On servers with Edge Transport role, the detected email is rejected with a 550 SMTP error code. In all other cases, the email is deleted without any warning. It is advisable to avoid using this action.
  - **Quarantine email.** The email is encrypted and saved in the quarantine folder from the Exchange Server, without being delivered to recipients. You can manage the quarantined emails in the **Quarantine** page.
  - **Redirect email to.** The email is not delivered to the original recipients, but to an email address you specify in the corresponding field.
  - **Deliver email.** Lets the email pass through.

  Secondary actions:

  - **Tag the email subject as.** You can add a label to the detected email subject to help users filter emails in the email client.
  - **Add an email header.** You can add a header name and a value to the headers of the detected email, by entering the desired values in the corresponding fields.
  - **Save email to disk.** A copy of the detected email is saved as a file to the specified folder on the Exchange Server. If the folder does not exist, it will be created. You must provide the absolute path of the folder in the corresponding field.

    Note
    This option supports only emails in MIME format.

- **Archive to account.** A copy of the detected email is delivered to the specified email address. This action adds the specified email address to the email Bcc list.

- By default, when an email matches the rule scope, it is processed exclusively in accordance with the rule, without being checked against any other remaining rule. If you want to continue checking against the other rules, clear the check box **If the rule conditions are matched, stop processing more rules**.

Exclusions

If you want the email traffic for specific senders or recipients to be delivered regardless of any attachment filtering rule, you can define filtering exclusions.

To create an exclusion:

1. Click the **Exclusions** link next to the **Attachment filtering** check box. This action opens the configuration window.
2. Enter the email addresses of the trusted senders and/or recipients in the corresponding fields. Any email coming from a trusted sender or going to a trusted recipient is excluded from filtering. When editing the list, you can also use the following wildcards to define an entire email domain or a pattern for email addresses:
   - Asterisk (*), replacing zero, one or more characters.
   - Question mark (?), replacing any single character.

   For example, if you enter `*.gov`, all emails coming from the `.gov` domain will be accepted.
3. For emails with multiple recipients, you can select the check box **Exclude email from filtering only if all recipients are trusted** to apply the exclusion only if all email recipients are present in the trusted recipients list.
4. Click **Save**.

5.2.10. Encryption

From the policy settings page, you are able to operate BitLocker Drive Encryption on Windows endpoints and FileVault on Mac endpoints.

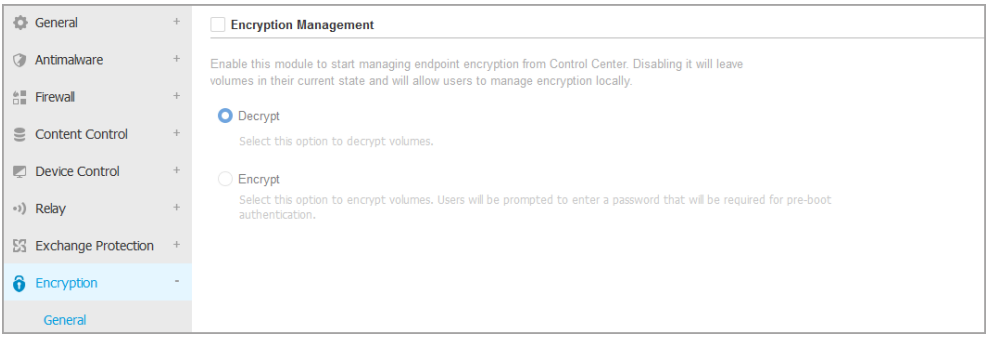
With this approach, GravityZone is able to provide some consistent benefits:

- Secured data in the case of lost and stolen devices.
- Extended protection for most popular computer platforms in the world, Windows and macOS.

- Use of recommended encryption standards with full support from Microsoft and Apple.
- Minimal impact on endpoints' performance due to optimized native encryption tools.

The Encryption module provides full disk encryption for boot and non-boot volumes on fixed storage devices. Also, GravityZone stores the recovery keys needed to unlock volumes, in case the users forget their passwords.

The Encryption module supports BitLocker on Windows machines with a Trusted Module Platform (TMP), starting with version 1.2, and on non-TPM machines. It also supports FileVault on macOS machines starting with OS X Mountain Lion (10.8) operating system. For full list of Encryption requirements, refer to GravityZone Installation Guide.



The Encryption page

To manage encryption on the endpoints, you must select the **Encryption Management** check box. Once the module is active, any policy applied within your network either encrypts or decrypts the detected volumes, depending on the option. When encrypting, the users are required to enter a password to start the process. For decrypting, only the Mac users must enter their password.

An encryption policy overrides any action taken by the users with BitLocker or FileVault, on the endpoints.

When the Encryption module is disabled, the volumes remain in their current state, encrypted or unencrypted. In this case, the user can manage BitLocker and FileVault on his own.

The **Encryption** module has two options:

- **Decrypt** – it decrypts volumes and it keeps them unencrypted when the policy is active on the endpoints.
- **Encrypt** – it encrypts volumes and it keeps them encrypted when the policy is active on the endpoints.

On Windows, GravityZone uses the encryption algorithm AES-256, while on the Mac it suppports XTS-AES-128 encryption with a 256-bit key.

Note

- GravityZone does not support encryption for volumes already encrypted with BitLocker, FileVault and other third-party tools. The volumes must be unencrypted when applying a GravityZone policy to encrypt them.
- GravityZone Encryption does not support multiple users. Only the user who encrypted the computer can log in to the system with the password he configured during the encryption process.

Encrypting Volumes

To encrypt volumes:

1. Select the **Encryption Management** check box, to enable this module.
2. Choose the **Encrypt** option.

Decrypting Volumes

To decrypt volumes on the endpoints:

1. Select the **Encryption Management** check box, to enable this module.
2. Choose the **Decrypt** option.

For details about retrieving the recovery keys, refer to “Using Recovery Manager for Encrypted Volumes” (p. 71).

5.2.11. NSX

In this section you can establish the policy to be used as a security profile in NSX. To do so:

1. Select the **NSX** check box to set its visibility also in vSphere Web Client.
2. Enter the name under which you will be able to identify the policy in NSX. This name may be different from the policy name in [Console]. In vSphere it will

appear preceeded by the `Bitdefender_` prefix. Choose this name wisely as it will become read-only after the policy is saved.

5.3. Mobile Device Policies

Policy settings can be initially configured when creating the policy. Later on, you can change them as needed anytime you want.

To configure the settings of a policy:

1. Go to the **Policies** page.
2. Choose **Mobile Devices** from the views selector.
3. Click the policy name. This will open the policy settings page.
4. Configure the policy settings as needed. Settings are organized under the following categories:
   - General
     - Details
   - Device Management
     - Security
     - Password
     - Profiles

   You can select the settings category using the menu from the left-side of the page.
5. Click **Save** to save changes and apply them to the target mobile devices. To leave the policy page without saving changes, click **Cancel**.

5.3.1. General

The **General** category contains descriptive information regarding the selected policy.

Details

The Details page shows general policy details:

- Policy name
- User who created the policy
- Date and time when the policy was created

- Date and time when the policy was last modified

You can rename the policy by entering the new name in the corresponding field. Policies should have suggestive names so that you or other administrator can quickly identify them.

Note
By default, only the user who created the policy can modify it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page.

5.3.2. Device Management

Device management settings allows defining the security options for mobile devices, the screen locking with password and also several profiles for each mobile device policy.

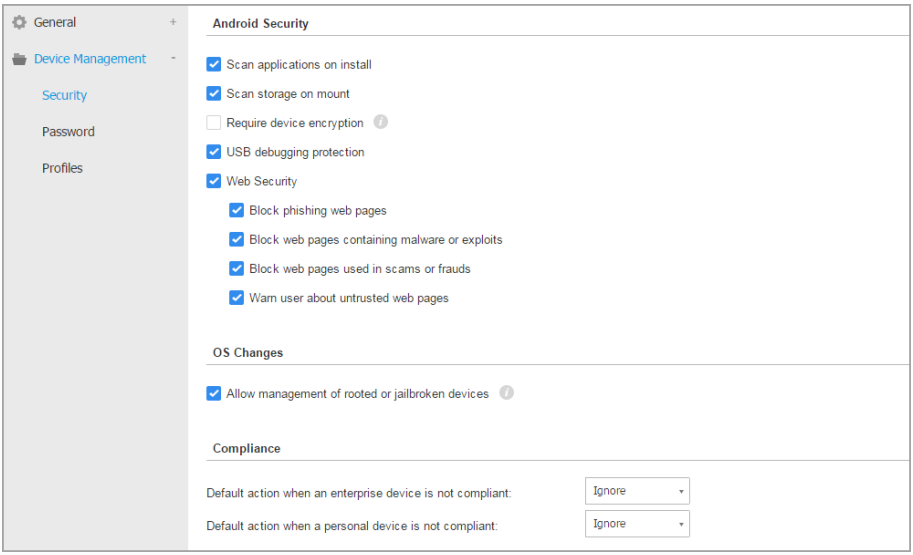
The settings are organized into the following sections:

- Security
- Password
- Profiles

Security

In this section you can configure various security settings for mobile devices, including antimalware scans for Android devices, management of rooted or jailbroken devices or the action to be taken on non-compliant devices.

Important
The antimalware scanning is performed in the cloud, therefore the mobile devices must have Internet access.



Mobile Devices Policies - Security settings

Android Security

- Select **Scan applications on install** if you want to perform a scanning when new applications are installed on the managed mobile devices.
- Select **Scan storage on mount** if you want to perform a scanning of each storage device when it's mounted.

  Warning

  If malware is found, the user is prompted to remove it. If the user does not remove detected malware within one hour after detection, the mobile device is declared non-compliant and the selected non-compliance action is automatically applied (Ignore, Deny Access, Lock, Wipe or Unlink).

- Select **Require device encryption** to prompt the user to activate the encryption feature available in the Android OS. Encryption protects the data stored on Android devices, including accounts, settings, downloaded applications, media and other files, from unauthorized access. Encrypted data can be accessed from external devices only by providing the unlock password.

Important

- Device encryption is available for Android 3.0 or later. Not all device models support encryption. Check the **Mobile Device Details** window for encryption support information.
- Encryption might impact device performance.

Warning

- Device encryption is irreversible and the only way to revert to the unencrypted state is to wipe the device.
- Users should back up their data before activating device encryption.
- Users must not interrupt the encryption process or they will lose some or all of their data.

If you enable this option, GravityZone Mobile Client displays a persistent issue informing the user to activate encryption. The user must tap the **Resolve** button to proceed to the encryption screen and start the process. If encryption is not activated within seven days after the notification, the device will become non-compliant.

To enable encryption on an Android device:

- The battery must be above 80% charged.
- The device must be plugged-in until encryption is completed.
- The user must set an unlock password meeting the complexity requirements.

Note

- Android devices use the same password for unlocking the screen and for unlocking encrypted content.
- Encryption requires password, PIN or FACE to unlock the device, disabling the other screen lock settings.

The encryption process can take an hour or more, during which the device may restart several times.

You can check the storage encryption status for each mobile device in the **Mobile Device Details** window.

- Android devices in USB debugging mode can be connected to a PC through a USB cable, allowing advanced control over their apps and operating system. In

this case, the mobile devices' security may be at risk. Enabled by default, the **USB debugging protection** option prevents using devices in the USB debugging mode. If the user activates USB debugging, the device automatically becomes non-compliant and the non-compliance action is taken. If the non-compliance action is **Ignore**, the user is notified about the unsafe setting.

Nevertheless, you can disable this option for mobile devices that require working in USB debugging mode (such as mobile devices used for developing and testing mobile apps).

- Select **Web Security** to enable web security features on Android devices.

  Web Security scans in-the-cloud each accessed URL, then returns a security status to GravityZone Mobile Client. The URL security status can be: clean, fraud, malware, phishing or untrusted.

  GravityZone Mobile Client can take a specific action based on the URL security status:

  – **Block phishing web pages**. When the user tries to access a phishing website, GravityZone Mobile Client blocks the corresponding URL, displaying instead a warning page.

  – **Block web pages containing malware or exploits**. When the user tries to access a website spreading malware or web exploits, GravityZone Mobile Client blocks the corresponding URL, displaying instead a warning page.

  – **Block web pages used in scams or frauds**. Extends protection to other types of scams besides phishing (for example fake escrows, fake donations, social media threats and so on). When the user tries to access a fraudulent web page, GravityZone Mobile Client blocks the corresponding URL, displaying instead a warning page.

  – **Warn user about untrusted web pages**. When the user is accessing a website that was previously hacked for phishing purposes or recently promoted through spam or phishing emails, a warning pop-up message will be displayed, without blocking the web page.

  Important
  Web Security features work only with Chrome and the built-in Android browser.

OS Changes

Considered a security risk for corporate networks, rooted or jailbroken devices are automatically declared non-compliant.

- Select **Allow management of rooted or jailbroken devices** if you want to manage rooted or jailbroken devices from Control Center. Note that because such devices are by default non-compliant, they are automatically applied the selected non-compliance action as soon as they are detected. Therefore, to be able to apply them the policy security settings or to run tasks on them, you must set the non-compliance action to Ignore.
- If you clear the **Allow management of rooted or jailbroken devices** check box, you automatically unlink rooted or jailbroken devices from the GravityZone network. In this case, the GravityZone Mobile Client application prompts a message stating the device is rooted / jailbroken. The user can tap the OK button, which redirects to the registration screen. As soon as the device is unrooted / unjailbroken, or the policy is set to allow the management of rooted / jailbroken devices, it can be re-enrolled (with the same token for Android devices / with a new token for iOS devices).

Compliance

You can configure specific actions to be taken automatically on devices detected as non-compliant based on device ownership (enterprise or personal).

Note
When adding a new device in Control Center, you are prompted to specify the device ownership (enterprise or personal). This will allow GravityZone to manage personal and enterprise mobile devices separately.

- Non-compliance criteria
- Non-compliance actions

Non-compliance criteria

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

- **Android devices**
  - Device is rooted.
  - GravityZone Mobile Client is not Device Administrator.

- Malware is not removed within one hour after detection.
- Policy not satisfied:
  - The user does not set the lock screen password within 24 hours after the first notification.
  - The user does not change the lock screen password at the specified time.
  - The user does not activate device encryption within seven days after the first notification.
  - USB debugging mode is activated on the device while USB debugging protection policy option is enabled.

- **iOS devices**
  - Device is jailbroken.
  - GravityZone Mobile Client is uninstalled from the mobile device.
  - Policy not satisfied:
    - The user does not set the lock screen password within 24 hours after the first notification.
    - The user does not change the lock screen password at the specified time.

Default action when the device is non-compliant

When a device is declared non-compliant, the user is prompted to fix the non-compliance issue. The user must make the required changes within a specific time period, otherwise the selected action for non-compliant devices will be applied (Ignore, Deny access, Lock, Wipe or Unlink).

You can change the action for non-compliant devices in the policy at any time. The new action is applied to non-compliant devices once the policy is saved.

Select from the menu corresponding to each device ownership type the action to be taken when a device is declared non-compliant:

- **Ignore**. Only notifies the user that the device does not comply with the mobile device usage policy.

- **Deny Access**. Blocks the device access to corporate networks by deleting the Wi-Fi and VPN settings, but keeping all the other settings defined in policy. Blocked settings are restored as soon as the device becomes compliant.

  Important
  When Device Administrator is disabled for GravityZone Mobile Client, the device becomes non-compliant and is automatically applied the **Deny Access** action.

- **Lock**. Immediately locks the device screen.
  - On Android, the screen is locked with a password generated by GravityZone. If the user already has a lock screen password, this will be automatically changed.
  - On iOS, if the device has a lock screen password, it is asked in order to unlock.
- **Wipe**. Restores the factory settings of the mobile device, permanently erasing all user data.

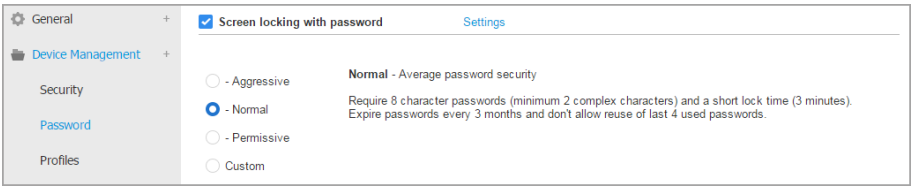
  Note
  Wipe does not currently erase data from mounted devices (SD cards).

- **Unlink**. The device is immediately removed from the network.

  Note
  To re-enroll a mobile device to which the Unlink action has been applied, you must add the device again in Control Center. The device must then be re-registered with the new activation token. Before re-enrolling the device, make sure the conditions that lead to the device being unlinked are no longer present or change the policy settings so as to allow the management of the device.

Password

In this section you can choose to activate the screen locking with password feature available in the mobile devices OS.



Mobile Devices Policies - Password protection settings

Once this feature has been enabled, an on-screen notification prompts the user to define a lock screen password. The user must enter a password that complies with the password criteria defined in the policy. Once the password has been set by the user, all notifications regarding this issue are cleared. A message prompting to enter the password is displayed at each attempt to unlock the screen.

Note

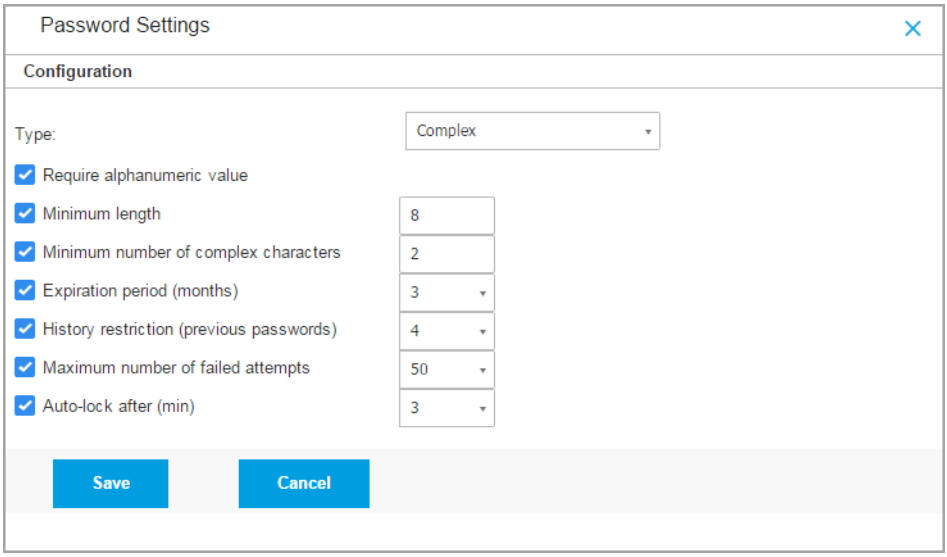
If the user does not set a password when prompted, the device can be used without a lock screen password up to 24 hours after the first notification. During this time, a message asking the user to enter a lock screen password is prompted every 15 minutes on the screen.

Warning

If the user does not set a password within 24 hours after the first notification, the mobile device becomes non-compliant and the selected action for non-compliant devices will be applied.

To configure the lock screen password settings:

1. Select the **Screen locking with password** check box.
2. Click the password security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.
3. For advanced configuration, select the **Custom** protection level and then click the **Settings** link.



Mobile Devices Policies - Password protection advanced settings

Note

To view the password configuration requirements of a predefined security level, select that level and click the **Settings** link. If you modify any option, the password security level will automatically change to **Custom**.

Custom options.

- **Type**. You can require the password to be Simple or Complex. Password complexity criteria are defined within the mobile device OS.
  - On Android devices, complex passwords must contain at least one letter, one digit and one special character.

    Note

    Complex passwords are supported on Android 3.0 or later.

  - On iOS devices, complex passwords do not allow sequential or repeated characters (such as abcdef, 12345 or aaaaa, 11111).

Depending on the selected option, when the user sets the lock screen password, the operating system checks and prompts the user if the required criteria are not met.

- **Require alphanumeric value**. Require the password to contain both letters and numbers.
- **Minimum length**. Require the password to contain a minimum number of characters, which you specify in the corresponding field.
- **Minimum number of complex characters**. Require the password to contain a minimum number of non-alphanumerical characters (such as @, # or $), which you specify in the corresponding field.
- **Expiration period (months)**. Force the user to change the lock screen password at a specified interval (in months). For example, if you enter 3, the user will be prompted to change the lock screen password every three months.

  Note
  On Android, this feature is supported in version 3.0 or later.

- **History restriction (previous passwords)**. Select or enter a value in the corresponding field to specify the number of last passwords that cannot be reused. For example, if you enter 4, the user cannot reuse a password that matches one of the last four used passwords.

  Note
  On Android, this feature is supported in version 3.0 or later.

- **Maximum number of failed attempts**. Specify how many times the user is allowed to enter an incorrect password.

  Note
  On iOS devices, when this number is greater than 6: after six failed attempts, a time delay is imposed before the user can enter the password again. The time delay increases with each failed attempt.

  Warning
  If the user exceeds the maximum number of failed attempts to unlock the screen, the device will be wiped (all data and settings will be erased).

- **Auto-lock after (min)**. Set the period of inactivity (in minutes) after which the device is automatically locked.

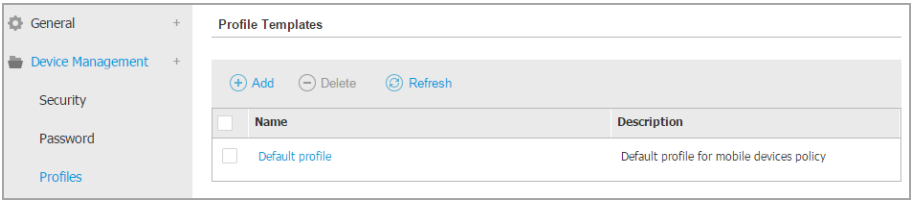
> **Note**
> The iOS devices have a predefined list for auto-lock time and do not allow custom values. When assigning a policy with an incompatible auto-lock value, the device enforces the next more restrictive time period available in the list. For example, if the policy has auto-lock set at three minutes, the device will automatically lock after two minutes of inactivity.

When you modify the policy, if you choose a higher security level for the lock screen password, users will be prompted to change the password according to the new criteria.

If you clear the **Screen locking with password** option, users will regain full access to the lock screen settings on their mobile device. The existing password remains active until the user decides to change or remove it.

Profiles

In this section you can create, modify and delete usage profiles for mobile devices. Usage profiles help you push Wi-Fi and VPN settings and enforce web access control on managed mobile devices.



Mobile Devices Policies - Profile Templates

You can configure one or several profiles, but only one can be active at a time on a device.

- If you configure only one profile, that profile is automatically applied to all devices the policy is assigned to.
- If you configure several profiles, the first in the list is automatically applied to all devices the policy is assigned to.

Mobile device users can view the assigned profiles and the settings configured for each profile in the GravityZone Mobile Client application. Users cannot modify existing settings in a profile, but they can switch between profiles if several are available.

Note
Profile switching requires Internet connectivity.

To create a new profile:

1. Click the ⊕ **Add** button at the right side of the table. The profile configuration page is displayed.
2. Configure the profile settings as needed. For detailed information, refer to:
   - "Details" (p. 289)
   - "Networks" (p. 289)
   - "Web Access" (p. 293)
3. Click **Save**. The new profile is added to the list.

To delete one or several profiles, select their corresponding check boxes and click the ⊖ **Delete** button at the right side of the table.

To modify a profile, click its name, change settings as needed and click **Save**.

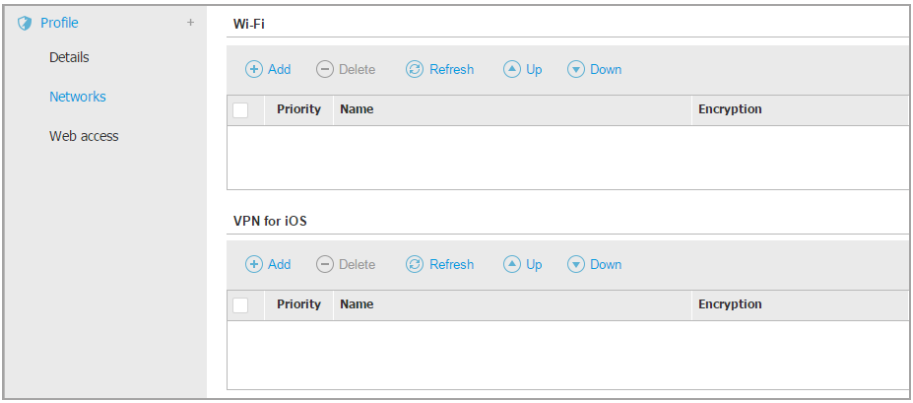
Details

The **Details** page contains general information regarding the profile:

- **Name**. Enter the desired profile name. Profiles should have suggestive names so that you or other administrator can quickly identify them.
- **Description**. Enter a detailed profile description. This option may help administrators easily identify a profile from several others.

Networks

In this section you can specify the settings of one or several Wi-Fi and VPN networks. The VPN settings are available only for iOS devices.



Mobile Devices Policies - Profile's networks connection settings

Important
Before defining the Wi-Fi and VPN connections, make sure you have all the necessary information at hand (passwords, proxy settings etc.).

The mobile devices assigned with the corresponding profile will automatically connect to the defined network, when it is in range. You can set the priority when several networks are created, taking into account that only one network can be used at a time. When the first network is not available, the mobile device will connect to the second one, and so on.

To set the networks priority:

1. Select the check box of the desired network.
2. Use the priority buttons at the right side of the table:
   - Click the **Up** button to promote the selected network.
   - Click the **Down** button to demote it.

- **Wi-Fi**

  You can add as many Wi-Fi networks as you need. To add a Wi-Fi network:

  1. In the **Wi-Fi** section, click the **Add** button at the right side of the table. A configuration window is displayed.
  2. Under the **General** tab, you can configure the details of the Wi-Fi connection:
     – **Name (SSID)**. Enter the name of the new Wi-Fi network.

- **Security**. Select the option corresponding to the Wi-Fi network security level:
  - **None**. Choose this option when the Wi-Fi connection is public (no credentials required).
  - **WEP**. Choose this option to set a Wireless Encryption Protocol (WEP) connection. Enter the required password for this type of connection in the corresponding field displayed below.
  - **WPA/WPA2 Personal**. Choose this option if the Wi-Fi network is secured using Wi-Fi Protected Access (WPA). Enter the required password for this type of connection in the corresponding field displayed below.

3. Under the **TCP/IP** you can configure the TCP/IP settings for the Wi-Fi connection. Each Wi-Fi connection can use IPv4 or IPv6 or both.
   - **Configure IPv4**. If you want to use the IPv4 method, select the IP assignment method from the corresponding menu:

     DHCP: if the IP address is assigned automatically by a DHCP server. If needed, provide the DHCP Client ID in the subsequent field.

     Disabled: select this option if you do not want to use the IPv4 protocol.
   - **Configure IPv6**. If you want to use the IPv6 method, select the IP assignment method from the corresponding menu:

     DHCP: if the IP address is assigned automatically by a DHCP server.

     Disabled: select this option if you do not want to use the IPv6 protocol.
   - **DNS Servers**. Enter the address of at least one DNS server for the network.
4. Under the **Proxy** tab, configure the proxy settings for the Wi-Fi connection. Select the desired proxy configuration method from the **Type** menu:
   - **Off**. Choose this option if the Wi-Fi network has no proxy settings.
   - **Manual**. Choose this option to manually specify the proxy settings. Enter the hostname of the proxy server and the port on which it listens for connections. If the proxy server requires authentication, select the **Authentication** check box and provide the user name and the password in the subsequent fields.

- **Automatic**. Choose this option to retrieve the proxy settings from a Proxy Auto-Configuration (PAC) file published in the local network. Enter the PAC file address in the **URL** field.

5. Click **Save**. The new Wi-Fi connection is added to the list.

- **VPN for iOS**

  You can add as many VPNs as you need. To add a VPN:

  1. In the **VPN for iOS** section, click the ⊕ **Add** button at the right side of the table. A configuration window is displayed.
  2. Define the VPN settings in the **VPN Connection** window:

     General:

     - **Name**. Enter the name of the VPN connection.
     - **Encryption**. The available authentication protocol for this connection type is **IPSec**, which requires user authentication by password and machine authentication by shared secret.
     - **Server**. Enter the VPN server address.
     - **User**. Enter the VPN user name.
     - **Password**. Enter the VPN password.
     - **Group Name**. Enter the group name.
     - **Secret**. Enter the pre-shared key.

     Proxy:

     In this section you can configure the proxy settings for the VPN connection. Select the desired proxy configuration method from the **Type** menu:

     - **Off**. Choose this option if the VPN connection has no proxy settings.
     - **Manual**. This option allows you to manually specify the proxy settings:
       - **Server**: enter the proxy host name.
       - **Port**: enter the proxy port number.
       - If the proxy server requires authentication, select the **Authentication** check box and provide the user name and the password in the subsequent fields.

– **Automatic**. Select this option to retrieve the proxy settings from a Proxy Auto-Configuration (PAC) file published in the local network. Enter the PAC file address in the **URL** field.

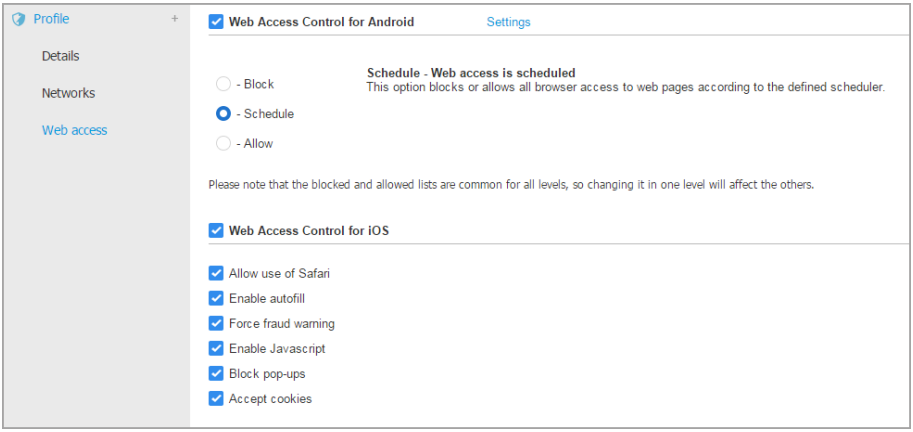
3. Click **Save**. The new VPN connection will be added to the list.

To delete one or several networks, select their corresponding check boxes and click the ⊖ **Delete** button at the right side of the table.

To modify a network, click its name, change settings as needed and click **Save**.

Web Access

In this section you can configure the web access control for Android and iOS devices.



Mobile Devices Policies - Profile's web access settings

- **Web Access Control for Android.** Enable this option to filter web access for the built-in Android browser. You can set time restrictions on web access and also explicitly allow or block access to specific web pages. The web pages blocked by Web Access Control are not displayed in the browser. Instead, a default web page is displayed informing the user that the requested web page has been blocked by Web Access Control.

  You have three configuration options:

  – Select **Allow** to always grant web access.

- Select **Block** to always deny web access.
- Select **Schedule** to enable time restrictions on web access upon a detailed schedule.

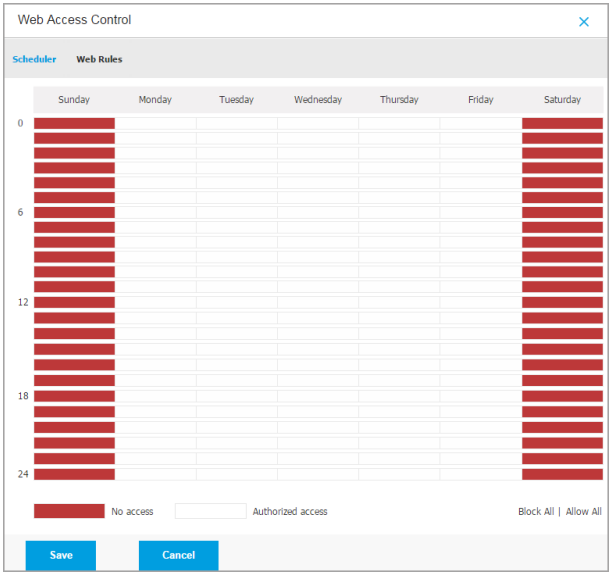
Either if you choose to allow or block the web access, you can define exceptions to these actions for entire web categories or only for specific web addresses. Click **Settings** to configure your web access schedule and exceptions as follows:

Scheduler

To restrict Internet access to certain times of day on a weekly basis:

1. Select from the grid the time intervals during which you want Internet access to be blocked.

   You can click individual cells, or you can click and drag to cover longer periods. Click again in the cell to reverse the selection.



Mobile Devices Policies - Scheduler for web access

   To start a new selection, click **Allow All** or **Block all**, depending on the type of restriction you wish to implement.

2. Click **Save**.

Web Rules

You can also define web rules to explicitly block or allow certain web addresses, overriding the existing Web Access Control settings. Users will be able, for example, to access a specific webpage also when the web browsing is blocked by Web Access Control.

To create a web rule:

1. Select **Use Exceptions** to enable web exceptions.
2. Enter the address you want to allow or block in the **Web Address** field.
3. Select **Allow** or **Block** from the **Permission** menu.
4. Click the ⊕ **Add** button at the right side of the table to add the address to the exceptions list.
5. Click **Save**.

To edit a web rule:

1. Click the web address you want to edit.
2. Modify the existing URL.
3. Click **Save**.

To remove a web rule:

1. Move the cursor over the web address you want to remove.
2. Click the ⊗ **Delete** button.
3. Click **Save**.

Use wildcards to define web address patterns:

– Asterisk (*) substitutes for zero or more characters.

– Question mark (?) substitutes for exactly one character. You can use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters.

In the following table, you can find several sample syntaxes for specifying web addresses.

Syntax	Applicability
`www.example*`	Any website or web page starting with `www.example` (regardless of the domain extension). The rule will not apply to the subdomains of the specified website, such as `subdomain.example.com`.
`*example.com`	Any website ending in `example.com`, including pages and subdomains thereof.
`*string*`	Any website or web page whose address contains the specified string.
`*.com`	Any website having the `.com` domain extension, including pages and subdomains thereof. Use this syntax to exclude from scanning the entire top-level domains.
`www.example?.com`	Any web address starting with `www.example?.com`, where ? can be replaced with any single character. Such websites might include: `www.example1.com` or `www.exampleA.com`.

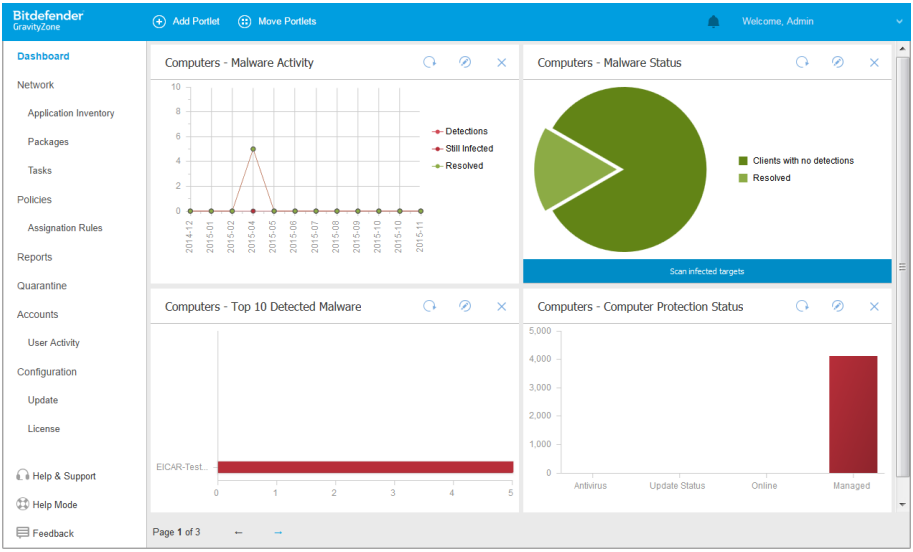
- **Web Access Control for iOS.** Enable this option to centrally manage the settings of the built-in iOS browser (Safari). Mobile device users will no longer be able to change the corresponding settings on their device.
  - **Allow use of Safari**. This option helps you control the use of Safari browser on mobile devices. Disabling the option removes the Safari shortcut from the iOS interface, thus preventing users from accessing the Internet via Safari.
  - **Enable auto-fill**. Disable this option if you want to prevent the browser from storing form entries, which may include sensitive information.
  - **Force fraud warning**. Select this option to ensure that users are warned when accessing fraudulent web pages.
  - **Enable Javascript**. Disable this option if you want Safari to ignore javascript on websites.

- **Block pop-ups**. Select this option to prevent pop-up windows from opening automatically.
- **Accept cookies**. Safari allows cookies by default. Disable this option if you want to prevent websites from storing browsing information.

6. MONITORING DASHBOARD

The Control Center dashboard is a customizable visual display providing a quick security overview of all protected endpoints.

Dashboard portlets display various real-time security information using easy-to-read charts, thus allowing you to quickly identify any issues that might require your attention.



The Dashboard

This is what you need to know about dashboard portlets:

- Control Center comes with several predefined dashboard portlets.
- Each dashboard portlet includes a detailed report in the background, accessible with just one click on the chart.
- There are several types of portlets that include various information about your endpoint protection, such as update status, malware status, firewall activity.

Note
By default, the portlets retrieve data for the current day and, unlike reports, cannot be set for longer intervals than one month.

- The information displayed via portlets refers to endpoints under your account only. You can customize each portlet's target and preferences using the **Edit Portlet** command.
- Click the chart legend entries, when available, to hide or display the corresponding variable on the graph.
- The portlets are displayed in groups of four. Use the arrows at the bottom of the page to navigate between portlet groups.
- For several report types, you have the option to instantly run specific tasks on target endpoints, without having to go to the **Network** page to run the task (for example, scan infected endpoints or update endpoints). Use the button at the lower side of the portlet to take the available action.

The dashboard is easy to configure, based on individual preferences. You can edit portlet settings, add additional portlets, remove or rearrange existing portlets.

6.1. Refreshing Portlet Data

To make sure the portlet displays the latest information, click the **Refresh** icon on its title bar.

6.2. Editing Portlet Settings

Some portlets offer status information, while other report on security events in the last period. You can check and configure the reporting period of a portlet by clicking the **Edit Portlet** icon on its title bar.

6.3. Adding a New Portlet

You can add other portlets to obtain the information you need.

To add a new portlet:

1. Go to the **Dashboard** page.
2. Click the **Add Portlet** button at the upper side of the console. The configuration window is displayed.
3. Under the **Details** tab, configure the portlet details:
   - Endpoint type (**Computers**, **Virtual Machines** or **Mobile Devices**)
   - Type of background report
   - Suggestive portlet name
   - The time interval for the events to be reported

   For more information on available report types, refer to "Report Types" (p. 301).

4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

6.4. Removing a Portlet

You can easily remove any portlet by clicking the **Remove** icon on its title bar. Once you remove a portlet, you can no longer recover it. However, you can create another portlet with the exact same settings.

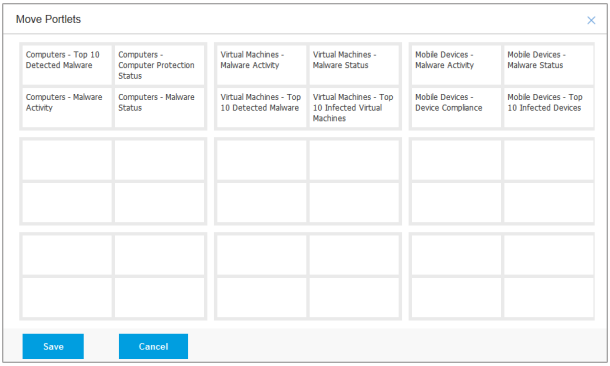
6.5. Rearranging Portlets

You can rearrange dashboard portlets to better suit your needs. To rearrange portlets:

1. Go to the **Dashboard** page.
2. Click the **Move Portlets** button at the upper side of the console. The portlet map window is displayed.
3. Drag and drop each portlet to the desired position. All other portlets between the new and old positions are moved preserving their order.

> **Note**
> You can move portlets only within the positions already taken.

4. Click **Save**.



Move Portlets window

7. USING REPORTS

Control Center allows you to create and view centralized reports on the security status of the managed network objects. The reports can be used for multiple purposes, such as:

- Monitoring and ensuring compliance with the organization's security policies.
- Checking and assessing the network security status.
- Identifying network security issues, threats and vulnerabilities.
- Monitoring security incidents and malware activity.
- Providing upper management with easy-to-interpret data on network security.

Several different report types are available so that you can easily get the information you need. The information is presented as easy-to-read interactive charts and tables, allowing you to quickly check the network security status and identify security issues.

Reports can consolidate data from the entire network of managed network objects or from specific groups only. In this way, from a single report, you can find out:

- Statistical data regarding all or groups of managed network objects.
- Detailed information for each managed network object.
- The list of computers that meet specific criteria (for example, those that have antimalware protection disabled).

Some reports also allow you to quickly fix the issues found in your network. For example, you can effortless update all target network objects right from the report, without having to go and run an update task from the **Network** page.

All scheduled reports are available in Control Center but you can save them to your computer or email them.

Available formats include Portable Document Format (PDF) and comma-separated values (CSV).

7.1. Report Types

Different report types are available for each endpoint type:

- Computer and Virtual Machine Reports
- Exchange Reports
- Mobile Device Reports

7.1.1. Computer and Virtual Machine Reports

These are the available report types for physical and virtual machines:

Antiphishing Activity

Informs you about the activity of the Antiphishing module of Bitdefender Endpoint Security Tools. You can view the number of blocked phishing websites on the selected endpoints and the user that was logged in at the time of the last detection. By clicking the links from the **Blocked Websites** column, you can also view the website URLs, how many times they were blocked and when was the last block event.

Blocked Applications

Informs you about the activity of the following modules: Antimalware, Firewall, Content Control, Application Control, ATC/IDS and HVI. You can see the number of blocked applications on the selected endpoints and the user that was logged in at the time of the last detection.

Click the number associated to a target to view additional information on the blocked applications, the number of events occurred, and the date and time of the last block event.

In this report, you can quickly instruct the protection modules to allow the selected application to run on the target endpoint:

- Click the **Add Exception** button to define exceptions in the following modules: Antimalware, ATC, Content Control, Firewall and HVI. A confirmation window will show up, informing you of the new rule that will modify the existing policy for that specific endpoint.
- Click the **Add Rule** button to define a rule for an application or a process in Application Control. In the configuration window, apply the rule to an existing policy. A message will inform you of the new rule that will modify the policy assigned to that specific endpoint. The report also displays the number of access attempts and if the module ran in Test Mode or in Production Mode.

Blocked Websites

Informs you about the activity of the Web Control module of Bitdefender Endpoint Security Tools. For each target, you can view the number of blocked websites. By clicking this number, you can view additional information, such as:

- Website URL and category

- Number of access attempts per website
- Date and time of the last attempt, as well as the user that was logged in at the time of the detection.
- Reason for blocking, which includes scheduled access, malware detection, category filtering and blacklisting.

Data Protection

Informs you about the activity of the Data Protection module of Bitdefender Endpoint Security Tools. You can see the number of blocked emails and websites on the selected endpoints, as well as the user that was logged in at the time of the last detection.

Device Control Activity

Informs you about the events occurred when accessing the endpoints through the monitored devices. For each target endpoint, you can view the number of allowed / blocked access and read-only events. If events occurred, additional information is available by clicking the corresponding numbers. Details refer to:

- User logged on the machine
- Device type and ID
- Device vendor and product ID
- Date and time of the event.

Endpoint Modules Status

Provides an overview of the protection modules coverage over the selected targets. In the report details, for each target endpoint you can view which modules are active, disabled or not installed, and also the scanning engine in use. Clicking the endpoint name will show up the **Information** window with details about the endpoint and installed protection layers.

Endpoint Protection Status

Provides you with various status information concerning selected endpoints from your network.

- Antimalware protection status
- Bitdefender Endpoint Security Tools update status
- Network activity status (online/offline)
- Management status

You can apply filters by security aspect and status to find the information you are looking for.

Firewall Activity

Informs you about the activity of the Firewall module of Bitdefender Endpoint Security Tools. You can see the number of blocked traffic attempts and blocked port scans on the selected endpoints, as well as the user that was logged in at the time of the last detection.

Malware Activity

Provides you with overall information about the malware threats detected over a specific time period on selected endpoints. You can view:

- Number of detections (files that have been found infected with malware)
- Number of resolved infections (files that have been successfully disinfected or moved to quarantine)
- Number of unresolved infections (files that could not be disinfected, but to which access has been denied; for example, an infected file stored in some proprietary archive format)
- The user that was logged in at the time of the last detection.

For each detected threat, by clicking the links available in the disinfection result columns, you can view the list of the affected endpoints and file paths. For example, if you click the number from the **Resolved** column, you will view the files and endpoints from where the threat has been removed.

Malware Status

Helps you find out how many and which of the selected endpoints have been affected by malware over a specific time period and how the threats have been dealt with. You can also see the user that was logged in at the time of the last detection.

Endpoints are grouped based on these criteria:

- Endpoints with no detections (no malware threat has been detected over the specified time period)
- Endpoints with resolved malware (all detected files have been successfully disinfected or moved to quarantine)
- Endpoints still infected with malware (some of the detected files have been denied access to)

For each endpoint, by clicking the links available in the disinfection result columns, you can view the list of threats and paths to the affected files.

In this report, you can quickly run a Full Scan task on the targets showing still infected, by clicking the **Scan infected targets** button from the Action Toolbar above the data table.

Network Status

Provides you with detailed information on the overall security status of selected endpoints. Endpoints are grouped based on these criteria:

- Overall security status
- Management status
- Infection status
- Installed protection layers
- Licensing status
- Product and signatures update status
- Connection status. If the endpoint is offline when the report is generated, you will see the date and time when it was last seen online by Control Center.

On-demand Scanning

Provides information regarding on-demand scans performed on the selected targets. A pie chart displays the statistics of successful and failed scans. The table below the chart provides details regarding the scan type, occurrence and last successful scan for each endpoint.

Policy Compliance

Provides information regarding the security policies applied on the selected targets. A pie chart displays the status of the policy. In the table below the chart, you can see the assigned policy on each endpoint and the policy type, as well as the date and the user that assigned it.

Security Audit

Provides information about the security events that occurred on a selected target. The information refers to the following events:

- Malware Detection
- Blocked Application
- Blocked Scan Port
- Blocked Traffic
- Blocked Website

- Blocked Device
- Blocked Email
- Blocked Process
- HVI events

Security Server Status

Helps you evaluate the status of the target Security Servers. You can identify the issues each Security Server might have, with the help of various status indicators, such as:

- **Status**: shows the overall Security Server status.
- **Machine status**: informs which Security Server appliances are stopped.
- **AV status**: points out whether the Antimalware module is enabled or disabled.
- **Update status**: shows if the Security Server appliances are updated or whether the updates have been disabled.
- **Load status**: indicates the scan load level of a Security Server as described herein:
  - **Underloaded**, when less than 5% of its scanning capacity is used.
  - **Normal**, when the scan load is balanced.
  - **Overloaded**, when the scan load exceeds 90% of its capacity. In such case, check the security policies. If all the Security Servers allocated within a policy are overloaded, you need to add another Security Server to the list. Otherwise, check the network connection between the clients and the Security Servers without load issues.
- **HVI protected VMs**: informs you of the virtual machines that are monitored and protected by HVI module.
- **HVI status**: points out whether the HVI module is enabled or disabled. HVI is enabled if both Security Server and Supplemental Pack are installed on host.

You can also view how many agents are connected to the Security Server. Further on, clicking the number of connected clients will display the list of endpoints. These endpoints may be vulnerable if the Security Server has issues.

Top 10 Detected Malware

Shows you the top 10 malware threats detected over a specific time period on selected endpoints.

> **Note**
> The details table displays all endpoints which were infected by the top 10 detected malware.

Top 10 Infected Endpoints

Shows you the top 10 most infected endpoints by the number of total detections over a specific time period out of the selected endpoints.

> **Note**
> The details table displays all malware detected on the top 10 infected endpoints.

Update Status

Shows you the update status of the security agent or Security Server installed on selected targets. The update status refers to product version and engines (signatures) version.

Using the available filters, you can easily find out which clients have updated and which have not in the last 24 hours.

In this report, you can quickly bring the agents to the latest version. To do this, click the **Update** button from the Action Toolbar above the data table.

Upgrade Status

Shows you the security agents installed on the selected targets and whether a more recent solution is available.

For endpoints with old security agents installed, you can quickly install the latest supported security agent by clicking the **Upgrade** button.

> **Note**
> This report is available only when a GravityZone solution upgrade has been made.

Virtual Machines Network Protection Status

Informs you of the Bitdefender protection coverage in your virtualized environment. For each of the selected machines, you can view which component resolves security issues:

- Security Server, for agentless deployments in VMware NSX and vShield environments, and for HVI
- A security agent, in any other situation

HVI Activity

Informs you about all attacks that HVI modules detected on the selected machines within a specific period of time.

The report also includes information about the date and time of the last detected incident that involved the monitored process, final status of the action taken against the attack, the user under which the process has started and the target machine.

Depending on the action taken, same process may be reported several times. For example, if a process once was killed and another time access was denied, you will see two entries in the report table.

For each process, when you click the last detection date, a separate log with all incidents detected since the process started will be displayed. The log reveals important information, such as the incident type and description, the source and target of the attack, and actions taken to remediate the problem.

In this report, you can quickly instruct the protection module to ignore certain events, which you consider are legitimate. To do this, click the **Add exception** button from the Action Toolbar above the data table.

7.1.2. Exchange Server Reports

These are the available report types for Exchange Servers:

Exchange - Blocked Content and Attachments

Provides you with information about emails or attachments that Content Control deleted from the selected servers over a specific time interval. The information includes:

- Email addresses of the sender and of the recipients.

  When the email has more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.

- Email subject.
- Detection type, indicating which Content Control filter detected the threat.
- The action taken on the detection.

- The server where the threat was detected.

Exchange - Blocked Unscannable Attachments

Provides you with information about emails containing unscannable attachments (over-compressed, password-protected, etc.), blocked on the selected Exchange mail servers over a specific time period. The information refers to:

- Email addresses of the sender and of the recipients.

  When the email is sent to more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.

- Email subject.
- The actions taken to remove the unscannable attachments:
  - **Deleted Email**, indicating that the entire email has been removed.
  - **Deleted Attachments**, a generic name for all actions that remove attachments from the email message, such as deleting the attachment, moving to quarantine or replacing it with a notice.

  By clicking the link in the **Action** column, you can view details about each blocked attachment and the corresponding action taken.
- Detection date and time.
- The server where the email was detected.

Exchange - Email Scan Activity

Shows statistics on the actions taken by the Exchange Protection module over a specific time interval.

The actions are grouped by detection type (malware, spam, forbidden attachment and forbidden content) and by server.

The statistics refer to the following email statuses:

- **Quarantined.** These emails were moved to the Quarantine folder.
- **Deleted/Rejected.** These emails were deleted or rejected by the server.
- **Redirected.** These emails were redirected to the email address supplied in the policy.
- **Cleaned and delivered.** These emails had the threats removed and passed through the filters.

An email is considered cleaned when all detected attachments have been disinfected, quarantined, deleted or replaced with text.

- **Modified and delivered.** Scan information was added to the emails headers and the emails passed through the filters.
- **Delivered without any other action.** These emails were ignored by Exchange Protection and passed through the filters.

Exchange - Malware Activity

Provides you with information about emails with malware threats, detected on the selected Exchange mail servers over a specific time period. The information refers to:

- Email addresses of the sender and of the recipients.

  When the email is sent to more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.
- Email subject.
- Email status after antimalware scan.

  By clicking the status link, you can view details about the detected malware and the action taken.
- Detection date and time.
- The server where the threat was detected.

Exchange - Top 10 Detected Malware

Informs you about the top 10 most detected malware threats in email attachments. You can generate two views containing different statistics. One view shows the number of detections by affected recipients and one by senders.

For example, GravityZone has detected one email with an infected attachment sent to five recipients.

- In the recipients view:
  - The report shows five detections.
  - The report details shows only the recipients, not the senders.
- In the senders view:
  - The report shows one detection.

- The report details shows only the sender, not the recipients.

Besides the sender/recipients and the malware name, the report provides you with the following details:

- The malware type (virus, spyware, PUA, etc.)
- The server where the threat was detected.
- Measures that the antimalware module has taken.
- Date and time of the last detection.

Exchange - Top 10 Malware Recipients

Shows you the top 10 email recipients most targeted by malware over a specific time interval.

The report details provide you with the entire malware list that affected these recipients, together with the actions taken.

Exchange - Top 10 Spam Recipients

Shows you the top 10 email recipients by the number of spam or phishing emails detected over a specific time interval. The report provides information also on the actions applied to the respective emails.

7.1.3. Mobile Devices Reports

Note
Malware protection and related reports are only available for Android devices.

This is the list of available report types for mobile devices:

Malware Status

Helps you find out how many and which of the target mobile devices have been affected by malware over a specific time period and how the threats have been dealt with. Mobile devices are grouped based on these criteria:

- Mobile devices with no detections (no malware threat has been detected over the specified time period)
- Mobile devices with resolved malware (all detected files have been removed)
- Mobile devices with existing malware (some of the detected files have not been deleted)

Malware Activity

Provides you with details about the malware threats detected over a specific time period on target mobile devices. You can see:

- Number of detections (files that have been found infected with malware)
- Number of resolved infections (files that have been successfully removed from the device)
- Number of unresolved infections (files that have not been removed from the device)

Top 10 Infected Devices

Shows you the top 10 most infected mobile devices over a specific time period out of the target mobile devices.

> **Note**
> The details table displays all malware detected on the top 10 infected mobile devices.

Top 10 Detected Malware

Shows you the top 10 malware threats detected over a specific time period on the target mobile devices.

> **Note**
> The details table displays all mobile devices which were infected by the top 10 detected malware.

Device Compliance

Informs you of the compliance status of the target mobile devices. You can see the device name, status, operating system and the non-compliance reason.

For more information regarding compliance requirements, please check “Non-compliance criteria” (p. 282).

Device Synchronization

Informs you of the synchronization status of the target mobile devices. You can view the device name, the user it is assigned to, as well as the synchronization status, the operating system and the time when the device was last seen online.

For more information, refer to “Checking the Mobile Devices Status” (p. 127).

Blocked Websites

Informs you about the number of attempts of the target devices to access websites which are blocked by **Web Access** rules, over a certain time interval.

For each device with detections, click the number provided in the **Blocked Websites** column to view detailed information of each blocked web page, such as:

- Website URL
- Policy component that performed the action
- Number of blocked attempts
- Last time when the website was blocked

For more information about the web access policy settings, refer to "Profiles" (p. 288).

Web Security Activity

Informs you about the number of attempts of the target mobile devices to access websites with security threats (phishing, fraud, malware or untrusted websites), over a certain time interval. For each device with detections, click the number provided in the Blocked Websites column to view detailed information of each blocked web page, such as:

- Website URL
- Type of threat (phishing, malware, fraud, untrusted)
- Number of blocked attempts
- Last time when the website was blocked

Web Security is the policy component which detects and blocks websites with security issues. For more information about the web security policy settings, refer to "Security" (p. 278).

7.2. Creating Reports

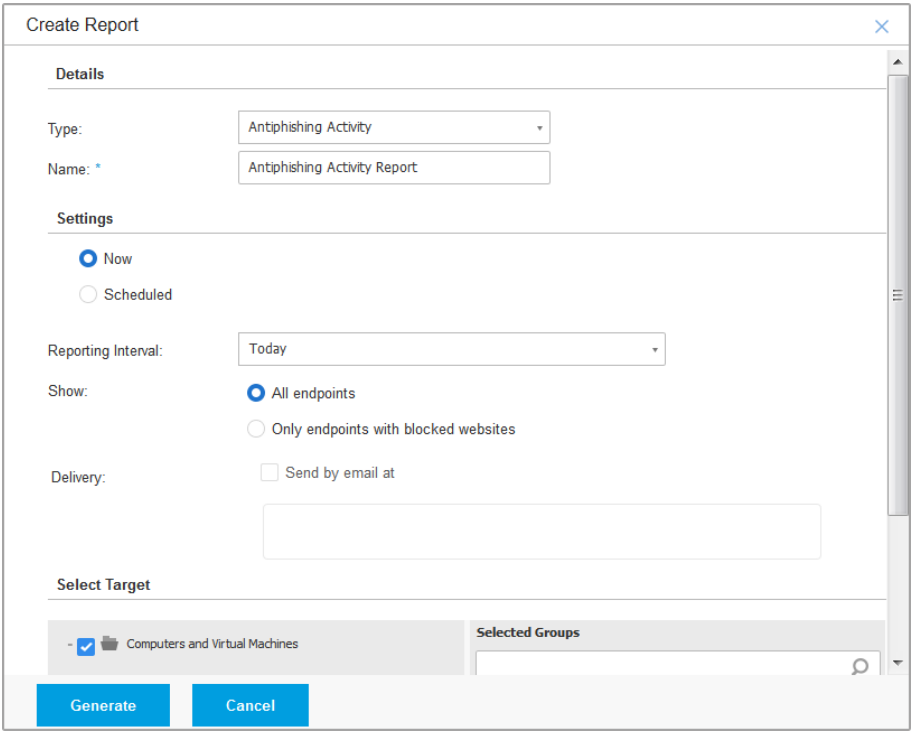
You can create two categories of reports:

- **Instant reports.** Instant reports are automatically displayed after you generate them.
- **Scheduled reports.** Scheduled reports can be configured to run periodically, at a specified time and date. A list of all the scheduled reports is displayed in the **Reports** page.

Important
Instant reports are automatically deleted when you close the report page. Scheduled reports are saved and displayed in the **Reports** page.

To create a report:

1. Go to the **Reports** page.
2. Choose the network objects type from the views selector.
3. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.



Computers and Virtual Machines Report Options

4. Select the desired report type from the menu. For more information, refer to "Report Types" (p. 301)

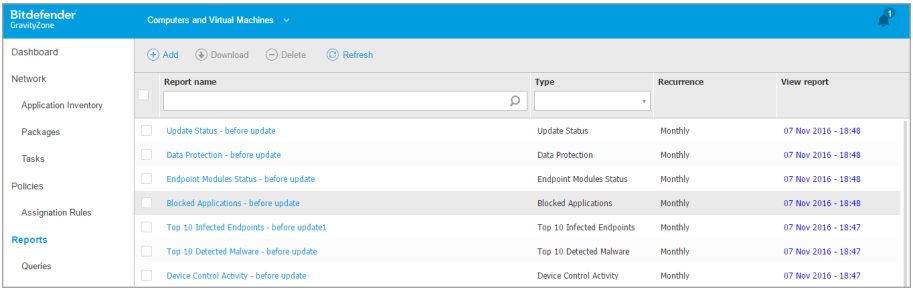
5. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
6. Configure the report recurrence:
   - Select **Now** to create an instant report.
   - Select **Scheduled** to configure the report to be automatically generated at the time interval that you want:
     - Hourly, at the specified interval between hours.
     - Daily. In this case, you can also set the start time (hour and minutes).
     - Weekly, in the specified days of the week and at the selected start time (hour and minutes).
     - Monthly, at each specified day on the month and at the selected start time (hour and minutes).
7. For most report types you must specify the time interval to which the contained data is referring. The report will only display data from the selected time period.
8. Several report types provide filtering options to help you easily find the information you are interested in. Use the filtering options under **Show** section to obtain only the desired information.

   For example, for an **Update Status** report you can choose to view only the list of network objects that have not updated, or the ones that need to be restarted to complete the update.
9. **Delivery**. To receive a scheduled report by email, select the corresponding check box. Enter the email addresses that you want in the field below. By default, the email contains an archive with both report files (PDF and CSV). Use the check boxes in the **Attach files** section to customize what files and how to send them by email.
10. **Select Target**. Scroll down to configure the report target. Select one or several groups of endpoints you want to include in the report.
11. Depending on the selected recurrence, click **Generate** to create an instant report or **Save** to create a scheduled report.
    - The instant report will be displayed immediately after clicking **Generate**. The time required for reports to be created may vary depending on the number of managed network objects. Please wait for the requested report to be created.

- The scheduled report will be displayed in the list on the **Reports** page. Once a report instance has been generated, you can view the report by clicking the corresponding link in the **View report** column on the **Reports** page.

7.3. Viewing and Managing Scheduled Reports

To view and manage scheduled reports, go to the **Reports** page.



The Reports page

All scheduled reports are displayed in a table together with useful information about them:

- Report name and type
- Report reccurence
- Last generated instance.

Note
Scheduled reports are available only for the user who has created them.

To sort reports by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

To easily find what you are looking for, use the search boxes or the filtering options below the column headers.

To clear a search box, place the cursor over it and click the × **Delete** icon.

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

7.3.1. Viewing Reports

To view a report:

1. Go to the **Reports** page.
2. Sort reports by name, type or recurrence to easily find the report you are looking for.
3. Click the corresponding link in the **View report** column to display the report. The most recent report instance will be displayed.

   To view all instances of a report, refer to "Saving Reports" (p. 320)

All reports consist of a summary section (the upper half of the report page) and a details section (the lower half of the report page).

- The summary section provides you with statistical data (pie charts and graphics) for all target network objects, as well as general information about the report, such as the reporting period (if applicable), report target etc.
- The details section provides you with information on each target network object.

Note

- To configure the information displayed by the chart, click the legend entries to show or hide the selected data.
- Click the graphic area (pie section, bar) you are interested in to view related details in the table.

7.3.2. Editing Scheduled Reports

Note
When editing a scheduled report, any updates will be applied starting with the report's next recurrence. Previously generated reports will not be impacted by the editing.

To change the settings of a scheduled report:

1. Go to the **Reports** page.
2. Click the report name.
3. Change report settings as needed. You can change the following:
   - **Report name.** Choose a suggestive name for the report to help easily identify what it is about. When choosing a name, consider the report type and target,

and possibly the report options. Reports generated by a scheduled report are named after it.

- **Report recurrence (schedule).** You can schedule the report to be automatically generated hourly (by a certain hour interval), daily (at a certain start time), weekly (on a specific day of the week andf start time) or monthly (on a specific day of the month and start time). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.
- **Settings.**
  - You can schedule the report to be automatically generated hourly (by a certain hour interval), daily (at a certain start time), weekly (on a specific day of the week andf start time) or monthly (on a specific day of the month and start time). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.
  - The report will only include data from the selected time interval. You can change the interval starting with the next recurrence.
  - Most reports provide filtering options to help you easily find the information you are interested in. When you view the report in the console, all information will be available, regardless of the selected options. If you download or email the report however, only the report summary and the selected information will be included in the PDF file. Report details will only be available in CSV format.
  - You can choose to receive the report by email.
- **Select target.** The selected option indicates the type of the current report target (either groups or individual network objects). Click the corresponding link to view the current report target. To change it, select the groups or network objects to be included in the report.

4. Click **Save** to apply changes.

7.3.3. Deleting Scheduled Reports

When a scheduled report is no longer needed, it is best to delete it. Deleting a scheduled report will delete all the instances it has generated automatically to that point.

To delete a scheduled report:

1. Go to the **Reports** page.
2. Select the report you want to delete.
3. Click the ⊖ **Delete** button at the upper side of the table.

7.4. Taking Report-Based Actions

While most reports only highlight the issues in your network, some of them also offer you several options to fix the issues found with just one click of a button.

To fix the issues displayed in the report, click the appropriate button from the Action Toolbar above the data table.

Note
You need **Manage Network** rights to perform these actions.

These are the available options for each report:

Blocked Applications

- **Add Exception**. Adds an exclusion in the policy to prevent the protection modules from blocking the application again.
- **Add Rule**. Defines a rule for an application or a process in Application Control.

HVI Activity

- **Add exception**. Adds an exclusion in the policy to prevent the protection module from reporting the incident again.

Malware Status

- **Scan infected targets**. Runs a preconfigured Full Scan task on the targets showing as still infected.

Update Status

- **Update**. Updates the target clients to their latest available versions.

Upgrade Status

- **Upgrade**. Replaces old endpoint clients with the latest generation of products available.

7.5. Saving Reports

By default, scheduled reports are automatically saved in Control Center.

If you need reports to be available for longer time periods, you can save them to your computer. The report summary will be available in PDF format, whereas report details will be available just in CSV format.

You have two ways of saving reports:

- Export
- Download

7.5.1. Exporting Reports

To export the report to your computer:

1. Click the **Export** button in the lower-left corner of the report page.
2. Select the desired format of the report:
   - Portable Document Format (PDF) or
   - Comma Separated Values (CSV)
3. Depending on your browser settings, the file may be downloaded automatically to a default download location, or a download window will appear, where you must specify the destination folder.

7.5.2. Downloading Reports

A report archive contains both the report summary and the report details.

To download a report archive:

1. Go to the **Reports** page.
2. Select the report you want to save.
3. Click the **Download** button and select either **Last Instance** to download the last generated instance of the report or **Full Archive** to download an archive containing all the instances.

   Depending on your browser settings, the file may be downloaded automatically to a default download location, or a download window will appear, where you must specify the destination folder.

7.6. Emailing Reports

You can send reports by email using the following options:

1. To email the report you are viewing, click the **Email** button in the lower-left corner of the report page. The report will be sent to the email address associated with your account.
2. To configure the desired scheduled reports delivery by email:
   a. Go to the **Reports** page.
   b. Click the desired report name.
   c. Under **Settings > Delivery**, select **Send by email at**.
   d. Provide the desired email address in the field below. You can add as many email addresses as you want.
   e. Click **Save**.

> **Note**
> Only the report summary and the chart will be included in the PDF file sent by email. Report details will be available in the CSV file.

The reports are sent by email as .zip archives.

7.7. Printing Reports

Control Center does not currently support print button functionality. To print a report, you must first save it to your computer.

7.8. Report Builder

In Control Center, you can create and manage queries to obtain detailed reports that allow you to understand any event or change that occurred in your network, at any time.

Queries provide you the possibility to investigate a security issue using various criteria, while keeping the information concise and well-ordered. With filters, you can group the endpoints by certain criteria and select relevant data for your purpose.

From a query-based report you can find out details such as when an incident occurred, how many endpoints are affected, which users were logged in at the time

of the incident, what policies were applied, security agent status, actions taken, on a single endpoint or on a group of endpoints.

All query-based reports are available in Control Center, but you can save them to your computer or send them by email. Available formats include Portable Document Format (PDF) and comma-separated values (CSV).

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

- High-volume data addressed to create compelling reports.
- Flexible reporting due to fact that the events are not aggregated.
- High level of customization. While standard GravityZone reports offer you the possibility to opt between a couple of predefined options, with queries there is no bound in choosing your data filters.
- Event correlation, with any information being accompanied by agent and device status data.
- Minimum development effort, as you can create, save and re-use any report type.
- Comprehensive reports which, unlike standard reports, have summary and details integrated together in the same PDF document.
- Queries can retrieve information for the past two years.

To use queries, you must install the Report Builder role along with your GravityZone virtual appliance. For details regarding Report Builder installation, refer to GravityZone Installation Guide.

7.8.1. Query Types

GravityZone comes with the following query types:

- Endpoint Status
- Endpoint Events
- Exchange Events

Endpoint Status

This query provides you with information about the security status of the selected target endpoints, for a specific date. This way, you know if the security agent and the signatures are updated, outdated or disabled. Also, you can view whether the

endpoints are infected or clean, what infrastructure is used, and what modules are on/off or not installed.

This query includes details related to the target endpoints, such as:

- Machine type (physical, virtual or Security Server)
- Network infrastructure to which the endpoint belongs (Active Directory, VMWare or Citrix Xen)
- Security agent data (type, status, scanning engines configuration, security status)
- Protection modules status
- Endpoint roles (Relay, Exchange Protection)

Endpoint Events

This query allows you to view details about security events occurred on the target endpoints, for a specific date or time period. It includes information related to:

- Target machine on which the event took place (name, type, IP, OS, network infrastructure)
- Type, status and configuration of the installed security agent
- Status of the protection modules and roles installed on the security agent
- Policy name and assignment
- Logged user during the event
- Events, which can refer to blocked websites, blocked applications, malware detections or device activity

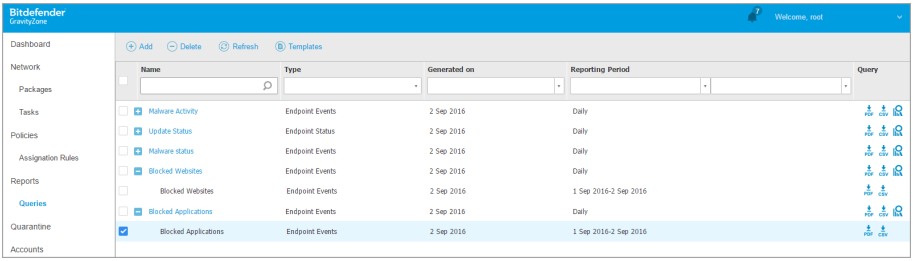
Exchange Events

Helps you to find out the incidents produced on the selected Microsoft Exchange servers, at a specific date or for a certain time period. It takes into account data about:

- Email traffic direction
- Security events (such as malware or attachment detection)
- Actions taken on each situation (disinfect, delete, replace or quarantine file, delete or reject email)

7.8.2. Managing Queries

You can create and manage queries and query-based reports in the **Report > Queries** page.

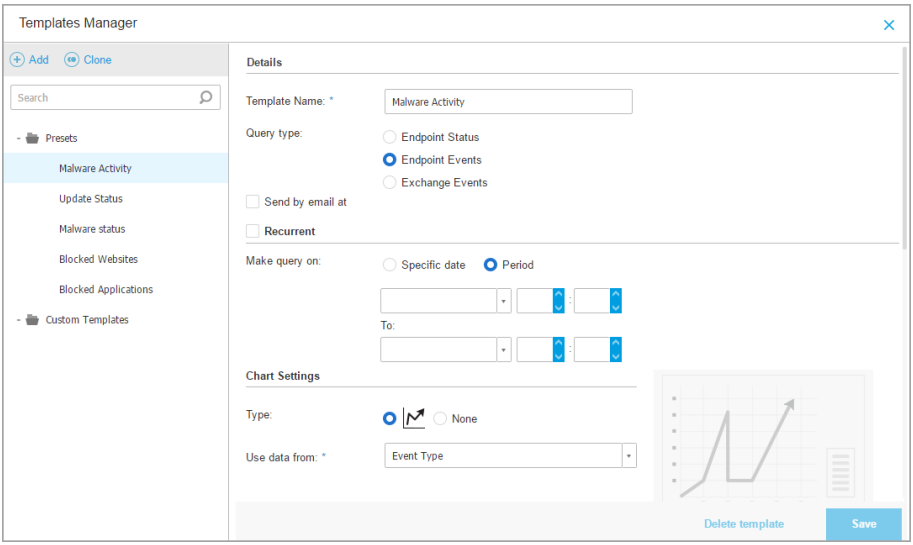


The Queries page

Queries are complex database interrogations, using a high number of filters, which can take several minutes to configure and create. Having to fill the query form every time you want a new report, similar to existing reports, can become frustrating. GravityZone helps you to easily create queries with the use of templates, which automatically fill in the query form, leaving you less customization to do.

Using Templates

You can add, clone and fast search for specific templates in the **Templates Manager** window.



To view the available query templates:

1. Go to the **Reports > Queries** page.
2. Click the **Templates** button at the upper-side of the table. The **Templates Manager** window will be displayed. All templates are displayed in the left pane, while in the right pane you can view the settings of the selected template.

To quickly find a template, enter the name in the **Search** field, at the upper side of the left pane. You can view the search results as you type. To clear the **Search** field, click the × **Delete** icon at the right-end of it.

There are two available template categories:

- Presets. These are predefined templates that come by default in GravityZone.
- Custom templates. These are the templates you create according to your needs.

Presets

GravityZone includes five presets:

- **Malware Activity**, providing you with information about the malware threats detected over a specific time period on selected endpoints.

The report contains target machine name, IP, infection status (infected or clean), malware name, action taken against the threat (ignored, present, deleted, blocked, quarantined, cleaned or restored), file type, file path and the user logged in at the moment.

- **Update Status**, showing the update status of security agent installed on selected targets. The report contains target machine name, IP, product update status (updated, outdated, disabled), signature update status (updated, outdated, disabled), security agent type, product version and signature version.
- **Malware Status**, which helps you to find out how many and which of the selected endpoints have been affected by malware over a specific time period and how the threats have been dealt with.

  The report contains target machine name, IP, infection status (infected or clean), malware name, threat action (ignored, present, deleted, blocked, quarantined, cleaned or restored).
- **Blocked Websites**, informing you about the activity of the Web Control module of the security agent.

  The report contains target machine name, IP, threat type (phishing, fraud or untrusted), rule name, website category and the blocked URL.
- **Blocked Applications**, which helps you to find out what applications have been blocked over a specific time period.

  The report offers information on target machine name, IP, the blocked application name, its file path and how the threat was contained: with ATC, IDS or Application Control.

Custom Templates

If you need another template than the presets GravityZone provides, you can create custom query templates. You can save as many templates as you want.

To create a custom template:

1. Go to the **Reports > Queries** page.
2. Click the **Templates** button at the upper-side of the table. The **Templates Manager** configuration window will be displayed.
3. Click the **Add** button in the upper-left corner of the window. A query form will be displayed in the right-side pane.

4. Complete the query form with the required information. For details about completing a query form, refer to "Creating Queries" (p. 327).
5. Click **Save**. The newly created template will be displayed in the left pane, under **Custom Templates**.

Alternately, you can create a custom template using a preset.

1. Go to the **Reports > Queries** page.
2. Click the **Templates** button at the upper-side of the table. The **Templates Manager** configuration window will be displayed.
3. Select a preset in the left-side pane. The corresponding settings will be displayed in the right-side pane.
4. Click **Clone** in the upper left-corner to create a copy of the preset.
5. Edit all settings you want in the query form. For details about completing a query form, refer to "Creating Queries" (p. 327).
6. Click **Save**. The newly created template will be displayed in the in the left pane, under **Custom Templates**.

Also, when creating a new query, you can save it as a template. For more information, refer to "Creating Queries" (p. 327).

To delete any custom template:

1. Go to the **Reports > Queries** page.
2. Click the **Templates** button at the upper-side of the table. The **Templates Manager** configuration window will be displayed.
3. Under the **Custom Templates** section, click the template you want to delete. The template settings will be displayed in the right-side pane.
4. Click **Delete template** at the lower-side of the window and then confirm your action by clicking **Yes**.

Creating Queries

To create a new query:

1. Go to the **Reports > Queries** page.
2. Click the **Add** button at the upper-side of the table. A configuration window is displayed.

3. Select **Use template** check box if you want to use a default or a previously created template.
4. Under **Details** section, enter a suggestive name for the query. When choosing a name, consider query type, targets and other settings.
5. Select the query type. For more information, refer to "Query Types" (p. 322)
6. Select **Send by email at** check box to send the query results to certain recipients. In the corresponding field, add as many email addresses as you want.
7. Under the **Recurrence** section, select:
   a. **Specific date** for a certain day.
   b. **Period**, for an extended time interval.
   c. Click the **Recurrent** check box if you want the query to be generated at specific intervals that you can set in the **Reporting Period** area.
8. Configure the chart settings.
   a. From the **Type** menu, select the chart you want to illustrate the query, or choose **None** to omit it. Depending on query type and reporting period, you can use a pie chart, a bar chart, or a line chart.
   b. In the **Take values from** field select the data categories you want to use for your query. Each query type provide specific information related to endpoints, security agents and security events. For details regarding type data, refer to "Query Types" (p. 322).
9. Under **Table Settings** section, select the columns you want the report to contain. The data you can select depend on the query type, and they may refer to endpoint type and OS, security agent status and events, modules, policy, and security events. All selected columns are displayed in the **Columns** table. Use drag-and-drop to change their order.

   Note
   Keep in mind the space available when creating the table layout. Use maximum 10 columns for a good table visualization in PDF.

10. In the **Filters** section, select the dataset you want the report to contain using the available filtering criteria:
    a. From the **Filter Type** menu, choose a filter and then click ⊕ **Add filter**.

b. In the table below, click **Value** to specify one or more filter options.

   For example, the **Host OS** filter requires specifying OS name, such as Windows or Linux, while the **Device Control Module** filter allows you to select from a drop-down list the endpoints where the module is disabled.

c. Click the ⊖ **Delete** button to eliminate a filter.

11. **Select Targets**. Scroll down to configure the report targets. Select one or several groups of endpoints you want to include in the report. Using the Views Selector, make sure you have checked the correct targets in all network views.
12. Select **Save as a template** check box to use these settings in further queries. In this case, enter a suggestive name for the template.
13. Click **Generate** to create the query. Once the query is saved, you will receive a message in the **Notifications** area.

Deleting Queries

To delete a query:

1. Go to the **Reports > Queries** page.
2. Select the report you want to delete.
3. Click the ⊖ **Delete** button at the upper-side of the table.

Note
Deleting a query will also delete all generated reports.

7.8.3. Viewing and Managing Reports

All query-based reports are displayed in the **Reports > Queries** page.

Note
Reports are available only for the user who has created them.

Viewing Reports

To view a query-based report:

1. Go to the **Reports > Queries** page.
2. Sort reports by name, type, date of generation or reporting period to easily find what you are looking for. By default, reports are ordered by the date of the last generated instance.

3. Click any name to view query information in a new window. The details cannot be edited.
4. Click the plus button in front of a query name to expand the list of a report instances and the minus button to collapse it.
5. Click the **View report** icon to display most recent instance of a report. Older instances are only available in PDF and CSV formats.

All reports consist of a summary section in the upper side of the report page, and a details section in the lower half of the report page.

The summary section provides you with statistical data (pie charts, bar charts, or line charts) for all target endpoints, general information about the query, such as recurrence, reporting period, query type, and filters used.

To configure the information displayed by the chart, click the legend entries to show or to hide the selected data. Also, click the area you are interested in the graphic to view related data in the table.

The details section provides you with information on each target endpoint. To quickly find the data you want, click the search fields or the filtering options below the column headers.

Click the **Columns** button to customize which columns to view in the table.

Saving Reports

By default, all reports are automatically saved in Control Center. You can also export them to your computer, both in PDF and CSV format.

You can save reports to your computer:

- From the report page.
- From the **Queries** table.

To save a report while you are on its page:

1. Click the **Export** button on the lower-left corner.
2. Select the desired format of the report:
   a. Portable Document Format (PDF) or
   b. Comma-Separated Values (CSV)
3. Depending on your browser settings, the file may be downloaded automatically to a default download location, or a download window will appear, where you must specify the destination folder.

To export a report while you are in the **Report > Queries** page:

1. Go to the **Reports > Queries** page.
2. Click the **PDF** or **CSV** buttons corresponding to each report.
3. Depending on your browser settings, the file may be downloaded automatically to a default download location, or a download window will appear, where you must specify the destination folder.

All reports exported in PDF have the summary and the details in the same document, on separated A4 portrait or landscape-oriented pages. The details are limited to 100 rows per PDF document.

Emailing Reports

You have two options to send reports by email:

1. In the page of the report you are viewing, click the **Email** button in the lower-left corner of the page. The report will be sent to the email address associated to your account.
2. When creating a new query, select **Send by email at** check box and enter the email addresses you want in the corresponding field.

Printing Reports

Control Center does not currently support print button functionality. To print a query-based report, you must first save it to your computer.

8. QUARANTINE

The quarantine is an encrypted folder that contains potentially malicious files, such as malware-suspected, malware-infected or other unwanted files. When a virus or other form of malware is in quarantine, it cannot do any harm because it cannot be executed or read.

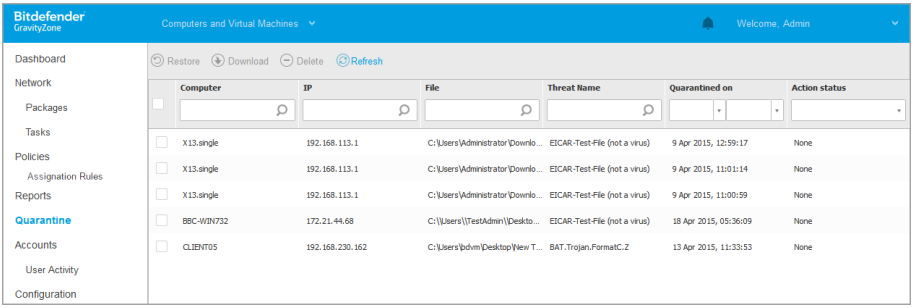
GravityZone moves files to quarantine according to the policies assigned to endpoints. By default, files that cannot be disinfected are quarantined.

The quarantine is saved locally on each endpoint, except for the VMware vCenter Server integrated with vShield Endpoint and with NSX, where it is saved on the Security Server.

Important
Quarantine is unavailable for mobile devices.

8.1. Exploring the Quarantine

The **Quarantine** page provides detailed information regarding the quarantined files from all endpoints you manage.



The Quarantine page

The Quarantine page consists of two views:

- Computers and Virtual Machines, for files detected directly in the endpoints file system.
- Exchange Servers, for emails and files attached to emails, detected on the Exchange mail servers.

The views selector at the upper side of the page allows switching between these views.

Information about quarantined files is displayed in a table. Depending on the number of managed endpoints and the infection degree, the Quarantine table can include a large number of entries. The table can span several pages (by default, only 20 entries are displayed per page).

To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

For a better visibility of the data you are interested in, you can use the search boxes from the column headers to filter displayed data. For example, you can search for a specific threat detected in the network or for a specific network object. You can also click the column headers to sort data by a specific column.

To make sure the latest information is being displayed, click the **Refresh** button at the upper side of the table. This may be needed when you spend more time on the page.

8.2. Computers and Virtual Machines Quarantine

By default, quarantined files are automatically sent to Bitdefender Labs to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware. In addition, quarantined files are scanned after each malware signature update. Cleaned files are automatically moved back to their original location. These features are relative to each security policy in the **Policies** page and you can choose whether to keep or deactivate them. For more information, refer to "Quarantine" (p. 207).

8.2.1. Viewing the Quarantine Details

The Quarantine table provides you with the following information:

- The name of endpoint the threat was detected on.
- IP of the endpoint the threat was detected on.
- Path to the infected or suspicious file on the endpoint it was detected on.
- Name given to the malware threat by the Bitdefender security researchers.
- The date and time when the file was quarantined.
- The status of the action requested to be taken on the quarantined file.

8.2.2. Managing the Quarantined Files

The behavior of the quarantine is different for each environment:

- **Security for Endpoints** stores the quarantined files on each managed computer. Using Control Center you have the option to either delete or restore specific quarantined files.
- **Security for Virtualized Environments (Multi-Platform)** stores the quarantined files on each managed virtual machine. Using Control Center you have the option to either delete or restore specific quarantined files.
- **Security for Virtualized Environments (integrated with VMware vShield Endpoint or NSX)** stores the quarantined files on the Security Server appliance. Using Control Center you have the option to delete quarantined files or download them to a location of your choice.

Restoring Quarantined Files

On particular occasions, you may need to restore quarantined files, either to their original location or to an alternate location. One such situation is when you want to recover important files stored in an infected archive that has been quarantined.

Note
Restoring quarantined files is only possible in environments protected by Security for Endpoints and Security for Virtualized Environments (Multi-Platform).

To restore one or more quarantined files:

1. Go to the **Quarantine** page.
2. Choose **Computers and Virtual Machines** from the views selector available at the upper side of the page.
3. Select the check boxes corresponding to the quarantined files you want to restore.
4. Click the **Restore** button at the upper side of the table.
5. Choose the location where you want the selected files to be restored (either the original or a custom location on the target computer).

   If you choose to restore to a custom location, you must enter the absolute path in the corresponding field.
6. Select **Automatically add exclusion in policy** to exclude the files to be restored from future scans. The exclusion applies to all policies affecting the selected files, except for the default policy, which cannot be modified.

7. Click **Save** to request the file restore action. You can notice the pending status in the **Action** column.
8. The requested action is sent to the target endpoints immediately or as soon as they get back online.

   You can view details regarding the action status in the **Tasks** page. Once a file is restored, the corresponding entry will disappear from the Quarantine table.

Downloading Quarantined Files

In VMware virtualized environments integrated with vShield Endpoint or NSX, the quarantine is saved on the Security Server. If you want to examine or recover data from quarantined files, you must download them from the Security Server using Control Center. Quarantined files are downloaded as an encrypted, password-protected ZIP archive to prevent accidental malware infection.

To open the archive and extract its content, you must use the Quarantine Tool, a Bitdefender standalone application that does not require installation.

Quarantine Tool is available for the following operating systems:

- Windows XP or newer
- Most Linux 32-bit distributions with a graphical user interface (GUI).

Note
Please note that Quarantine Tool does not have a command line interface.

Warning
Use caution when extracting the quarantined files because they can infect your system. It is recommended to extract and analyze the quarantined files on a test or isolated system, preferably running on Linux. Malware infections are easier to contain on Linux.

To download quarantined files to your computer:

1. Go to the **Quarantine** page.
2. Choose **Computers and Virtual Machines** from the views selector available at the upper side of the page.
3. Filter the table data by entering the Security Server hostname or IP address in the corresponding field from the table header.

   If the quarantine is large, to view the files you are interested in, you may need to apply additional filters or increase the number of files listed per page.
4. Select the check boxes corresponding to the files you want to download.

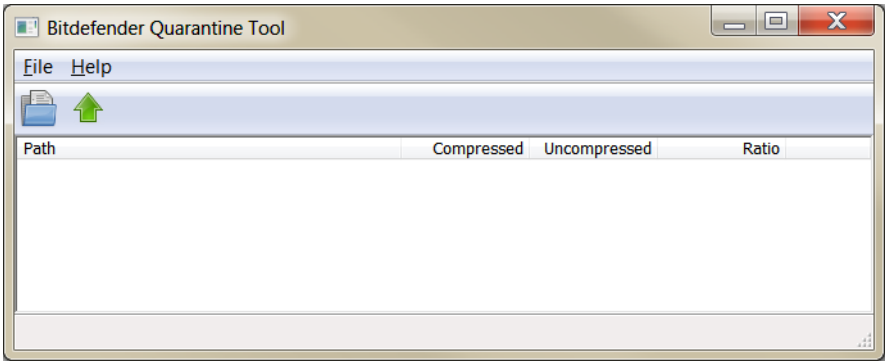
5. Click the **Download** button at the upper side of the table. Depending on your browser settings, you will be asked to save the files to a folder of your choice, or the files will be downloaded automatically to the default download location.

To access the restored files:

1. Download the appropriate Quarantine Tool for your operating system from the **Help & Support** page or from the following addresses:
   - Quarantine Tool for Windows
   - Quarantine Tool for Linux

   Note
   Quarantine Tool for Linux is archived in a `tar` file.

2. Run the Quarantine Tool executable file.



Quarantine Tool

3. On the **File** menu, click **Open** (CTRL+O) or click the **Open** button to load the archive into the tool.

   Files are organized in the archive by virtual machine they were detected on and preserving their original path.
4. Before extracting the archived files, if on-access antimalware scan is enabled on the system, make sure to either disable it or configure a scan exclusion for the location where you will extract the files. Otherwise, your antimalware program will detect and take action on extracted files.
5. Select the files you want to extract.
6. On the **File** menu, click **Extract** `(CTRL+E)` or click the **Extract** button.

7. Select the destination folder. The files are extracted at the selected location, preserving the original folder structure.

Automatic Deletion of Quarantined Files

By default, quarantined files older than 30 days are automatically deleted. This setting can be changed by editing the policy assigned to the managed endpoints.

To change the automatic deletion interval for quarantined files:

1. Go to the **Policies** page.
2. Find the policy assigned to the endpoints on which you want to change the setting and click its name.
3. Go to the **Antimalware > Settings** page.
4. In the **Quarantine** section, select the number of days after which files are being deleted.
5. Click **Save** to apply changes.

Manual Deletion of Quarantined Files

If you want to manually delete quarantined files, you should first make sure the files you choose to delete are not needed.

A file may actually be the malware itself. If your research leads you to such a situation, you can search the quarantine for the specific threat and delete it from the quarantine.

To delete one or more quarantined files:

1. Go to the **Quarantine** page.
2. Select **Computers and Virtual Machines** from the views selector available at the upper side of the page.
3. Select the check boxes corresponding to the quarantined files you want to delete.
4. Click the ⊖ **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

   You can notice the pending status in the **Action** column.

   The requested action is sent to the target network objects immediately or as soon as they get back online. Once a file is deleted, the corresponding entry will disappear from the Quarantine table.

8.3. Exchange Servers Quarantine

The Exchange quarantine contains emails and attachments. The Antimalware module quarantines email attachments, whereas Antispam, Content and Attachment Filtering quarantine the whole email.

Note
Please note that 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.

8.3.1. Viewing the Quarantine Details

The **Quarantine** page offers you detailed information about the quarantined objects from all Exchange Servers within your organization. The information is available in the Quarantine table and in the details window of each object.

The Quarantine table provides you with the following information:

- **Subject.** The subject of the quarantined email.
- **Sender.** The sender's email address as it appears in the email header field **From**.
- **Recipients.** The list of recipients as they appear in the email header fields **To** and **Cc**.
- **Real recipients.** The list of individual users' email addresses to which the email was intended to be delivered before being quarantined.
- **Status.** The object's status after it was scanned. The status shows if an email is marked as spam or contains unwanted content, or if an attachment is malware infected, suspect of being infected, unwanted or unscannable.
- **Malware name.** Name given to the malware threat by the Bitdefender security researchers.
- **Server name.** The hostname of the server on which the threat was detected.
- **Quarantined on.** Date and time when the object was quarantined.
- **Action status.** The status of the action taken on the quarantined object. This way you can quickly view if an action is still pending or it has failed.

Note

- The columns **Real recipients**, **Malware name** and **Server name** are hidden in the default view.
- When several attachments from the same email get quarantined, the Quarantine table shows a separate entry for each attachment.

To customize the quarantine details displayed in the table:

1. Click the **Columns** button at the right-side of the table header.
2. Select the columns you want to view.

   To return to the default columns view, click the **Reset** button.

You can obtain more information by clicking the **Subject** link corresponding to each object. The **Object Details** window is displayed, providing you with the following information:

- **Quarantined object.** The type of quarantined object, which can be either email or attachment.
- **Quarantined on.** Date and time when the object was quarantined.
- **Status.** The object's status after it was scanned. The status shows if an email is marked as spam or contains unwanted content, or if an attachment is malware infected, suspect of being infected, unwanted or unscannable.
- **Attachment name.** The filename of the attachment detected by the Antimalware or Attachment Filtering modules.
- **Malware name.** Name given to the malware threat by the Bitdefender security researchers. This information is available only if the object was infected.
- **Detection point.** An object is detected either at the transport level, or in a mailbox or public folder from the Exchange Store.
- **Rule matched.** The policy rule that the threat matched with.
- **Server.** The hostname of server the threat was detected on.
- **Sender IP.** Sender's IP address.
- **Sender (From).** The sender's email address as it appears in the email header field **From**.
- **Recipients.** The list of recipients as they appear in the email header fields **To** and **Cc**.

- **Real recipients.** The list of individual users' email addresses to which the email was intended to be delivered before being quarantined.
- **Subject.** The subject of the quarantined email.

Note
The ellipsis mark at the end of the text indicates that a part of the text is omitted. In this case, move the mouse over the text to view it in a tooltip.

8.3.2. Managing the Quarantined Objects

Emails and files quarantined by the Exchange Protection module are stored locally on the server as encrypted files. Using Control Center you have the option to restore quarantined emails, as well as delete or save any quarantined files or emails.

Restoring Quarantined Emails

If you decide a quarantined email does not represent a threat, you can release it from the quarantine. Using Exchange Web Services, Exchange Protection sends the quarantined email to its intended recipients as an attachment to a Bitdefender notification email.

Note
You can restore only emails. To recover a quarantined attachment, you must save it to a local folder on the Exchange server.

To restore one or several emails:

1. Go to the **Quarantine** page.
2. Choose **Exchange** from the views selector available at the upper side of the page.
3. Select the check boxes corresponding to the emails you want to restore.
4. Click the **Restore** button at the upper side of the table. The **Restore credentials** window will appear.
5. Select the credentials of an Exchange user authorized to send the emails to be restored. If the credentials you intend to use are new, you have to add them to the Credentials Manager first.

   To add the required credentials:

a. Enter the required information in the corresponding fields from the table header:
   - The username and password of the Exchange user.

     Note
     The username must include the domain name, as in `user@domain` or `domain\user`.

   - The email address of the Exchange user, necessary only when the email address is different from the username.
   - The Exchange Web Services (EWS) URL, necessary when Exchange Autodiscovery does not work. This is usually the case with Edge Transport servers in a DMZ.

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

6. Click the **Restore** button. A confirmation message will appear.

   The requested action is sent to the target servers immediately. Once an email is restored, it is also deleted from quarantine, so the corresponding entry will disappear from the Quarantine table.

   You can check the status of the restore action in any of these places:

   - **Action status** column of the Quarantine table.
   - **Network > Tasks** page.

Saving Quarantined Files

If you want to examine or recover data from quarantined files, you can save the files to a local folder on the Exchange Server. Bitdefender Endpoint Security Tools decrypts the files and saves them to the specified location.

To save one or several quarantined files:

1. Go to the **Quarantine** page.
2. Choose **Exchange** from the views selector available at the upper side of the page.
3. Filter the table data to view all files you want to save, by entering the search terms in the column header fields.

4. Select the check boxes corresponding to the quarantined files you want to restore.
5. Click the **Save** button at the upper side of the table.
6. Enter the path to the destination folder on the Exchange Server. If the folder does not exist on the server, it will be created.

   Important
   You must exclude this folder from file system level scanning, otherwise the files will be moved to the Computers and Virtual Machines Quarantine. For more information, refer to "Exclusions" (p. 207).

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

   You can notice the pending status in the **Action status** column. You can also view the action status in the **Network > Tasks** page.

Automatic Deletion of Quarantined Files

By default, quarantined files older than 30 days are automatically deleted. You can change this setting by editing the policy assigned to the managed Exchange Server.

To change the automatic deletion interval for quarantined files:

1. Go to the **Policies** page.
2. Click the name of the policy assigned to the Exchange Server you are interested in.
3. Go to the **Exchange Protection > General** page.
4. In the **Settings** section, select the number of days after which files are being deleted.
5. Click **Save** to apply changes.

Manual Deletion of Quarantined Files

To delete one or more quarantined objects:

1. Go to the **Quarantine** page.
2. Select **Exchange** from the views selector.
3. Select the check boxes corresponding to the files you want to delete.
4. Click the **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

You can notice the pending status in the **Action status** column.

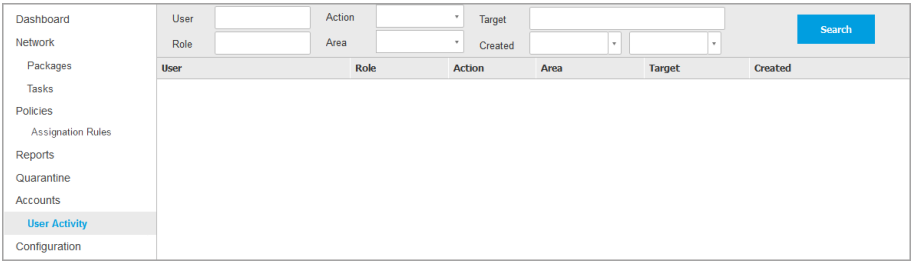
The requested action is sent to the target servers immediately. Once a file is deleted, the corresponding entry will disappear from the Quarantine table.

9. USER ACTIVITY LOG

Control Center logs all the operations and actions performed by users. The user activity list includes the following events, according to your administrative permission level:

- Logging in and logging out
- Creating, editing, renaming and deleting reports
- Adding and removing dashboard portlets
- Creating, editing, and deleting credentials
- Creating, modifying, downloading and deleting network packages
- Creating network tasks
- Creating, editing, renaming and deleting user accounts
- Deleting or moving endpoints between groups
- Creating, moving, renaming and deleting groups
- Deleting and restoring quarantined files
- Creating, editing and deleting user accounts
- Creating, editing, renaming, assigning and deleting policies
- Updating the GravityZone appliance.

To examine the user activity records, go to the **Accounts > User Activity** page and choose the network view that you want from the views selector.



The User Activity Page

To display recorded events that you are interested in, you have to define a search. Fill in the available fields with the search criteria and click the **Search** button. All the records matching your criteria will be displayed in the table.

The table columns provide you with useful information about the listed events:

- The username of who performed the action.

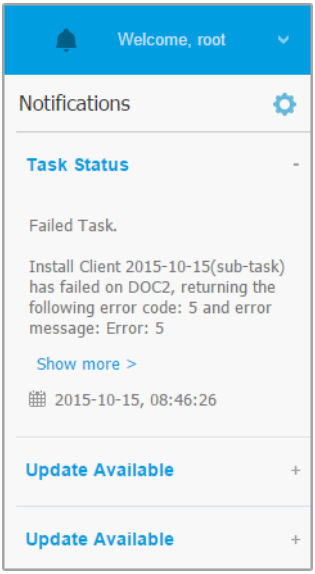
- User role.
- Action that caused the event.
- Type of console object affected by the action.
- Specific console object affected by the action.
- Time when the event occurred.

To sort events by a specific column, simply click the header of that column. Click the column header again to reverse the sorting order.

To view detailed information about an event, select it and check the section under the table.

10. NOTIFICATIONS

Depending on the events that might occur throughout your network, Control Center will show various notifications to inform you of the security status of your environment. The notifications will be displayed in the **Notification Area**, located in the right side of the Control Center.



Notification Area

When new events are detected in the network, the 11 icon in the upper right corner of Control Center will display the number of newly detected events. Clicking the icon displays the Notification Area containing the list of detected events.

10.1. Notification Types

This is the list of available notifications types:

Malware Outbreak

This notification is sent to the users that have at least 5% of all their managed network objects infected by the same malware.

You can configure the malware outbreak threshold according to your needs in the **Notifications Settings** window. For more information, refer to "Configuring Notification Settings" (p. 352).

License Expires
This notification is sent 30, seven days and also one day before the license expires.

Note
You must have **Manage Company** right to view this notification.

License Usage Limit Has Been Reached
This notification is sent when all of the available licenses have been used.

Note
You must have **Manage Company** right to view this notification.

License Limit Is About To Be Reached
This notification is sent when 90% of the available licenses have been used.

Note
You must have **Manage Company** right to view this notification.

Exchange License Usage Limit Has Been Reached
This notification is triggered each time the number of protected mailboxes from your Exchange servers reaches the limit specified on your license key.

Invalid Exchange user credentials
This notification is sent when an on-demand scan task could not start on the target Exchange server due to invalid Exchange user credentials.

Update Available
This notification informs you about the availability of a new GravityZone, new package or new product update.

Internet Connection
This notification is triggered when Internet connectivity changes are detected by the following processes:

- License validation
- Obtaining an Apple Certificate Signing Request
- Communication with Apple and Android mobile devices

- Accessing MyBitdefender account

SMTP Connection

This notification is sent each time Bitdefender GravityZone detects changes regarding the mail server connectivity.

Mobile device users without email address

This notification is sent after adding mobile devices to multiple users and one or several selected users have no email address specified for their account. This notification is intended to warn you that users with no specified email address cannot enroll the mobile devices assigned to them, since the activation details are automatically sent by email.

For details about adding mobile devices to multiple users, refer to the GravityZone Installation Guide.

Database Backup

This notification informs you about the status of a scheduled database backup, whether successful or unsuccessful. If the database backup has failed, the notification message will display also the failure reason.

For details about configuring GravityZone database backups, refer to the GravityZone Installation Guide.

Exchange Malware Detected

This notification informs you when malware is detected on an Exchange Server in your network.

Antimalware event

This notification informs you when malware is detected on an endpoint in your network. This notification is created for each malware detection, providing details about the infected endpoint (name, IP, installed agent), detected malware and detection time.

Antiphishing event

This notification informs you each time the endpoint agent blocks a known phishing web page from being accessed. This notification also provides details such as the endpoint that attempted to access the unsafe website (name and IP), installed agent or blocked URL.

Firewall event

With this notification you are informed each time the firewall module of an installed agent has blocked a port scan or an application from accessing the network, according to applied policy.

ATC/IDS event

This notification is sent each time a potentially dangerous application is detected and blocked on an endpoint in your network. You will also find details about the dangerous application type, name and path.

User Control event

This notification is triggered each time a user activity such as web browsing or software application is blocked by the endpoint client according to applied policy.

Data Protection event

This notification is sent each time data traffic is blocked on an endpoint according to data protection rules.

Product Modules event

This notification is sent each time a security module of an installed agent gets enabled or disabled.

Security Server Status event

This type of notification provides information about the status changes of a certain Security Server installed in your network. The Security Server status changes refer to the following events: powered off / powered on, product update, signatures update and reboot required.

Overloaded Security Server event

This notification is sent when the scan load on a Security Server in your network exceeds the defined threshold.

Product Registration event

This notification informs you when the registration status of an agent installed in your network has changed.

Authentication Audit

This notification informs you when another GravityZone account, except your own, was used to log in to Control Center from an unrecognized device.

Login from New Device

This notification informs you that your GravityZone account was used to log in to Control Center from a device you have not used for this purpose before. The notification is automatically configured to be visible both in Control Center and on email and you can only view it.

Certificate Expires

This notification informs you that a security certificate expires. The notification is sent 30, seven and one day prior to expiration date.

GravityZone Update

The notification is sent when a GravityZone update is completed. If failed, the update will run again in 24 hours.

Task Status

This notification informs you either each time a task status changes, or only when a task finishes, according to your preferences.

Outdated Update Server

This notification is sent when an update server in your network has outddated malware signatures.

Custom Report Has Been Generated

This notification informs you when a query-based report has been generated.

Detected Memory Violation

This notification informs you when HVI detects an attack that violates the memory of protected virtual machines in Citrix Xen environment. The notification provides you with important details, such as the name and IP of the infected machine, incident description, the source and target of the attack, action taken to remove the threat and detection time.

Notifications are created for the following incidents:

- Attempts to use a memory area differently than the hypervisor has intended, via the Extended Page Tables (EPT).
- Attempts of processes to inject code into other processes.
- Attempts to change process addresses in the translation tables.
- Attempts to change the Model Specific Registers (MSR).
- Attempts to change the contents of specific Driver Objects or of the Interrupt Descriptor Table (IDT).
- Attempts to load specific Control Registers (CR) with invalid values.
- Attempts to load specific Extended Control Registers (XCR) with invalid values.
- Attempts to change the Global or Interrupt Descriptor Tables.

New Application in Application Inventory

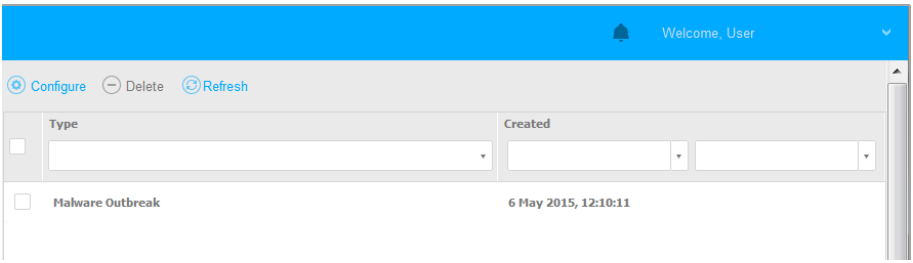
This notification informs you when Application Control detects a new application installed on monitored endpoints.

Blocked Application

This notification informs you when Application Control blocked or would have blocked a process of an unauthorized application, depending on the module configuration (Production or Test Mode).

10.2. Viewing Notifications

To view the notifications, click the **Notifications** button and then click **See All Notifications**. A table containing all the notifications is displayed.



The Notifications page

Depending on the number of notifications, the table can span several pages (only 20 entries are displayed per page by default).

To move through the pages, use the navigation buttons at the bottom of the table.

To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

If there are too many entries, you can use the search boxes under the column headers or the filter menu at the top of the table to filter displayed data.

- To filter notifications, select the notification type you want to see from the **Type** menu. Optionally, you can select the time interval during which the notification was generated, to reduce the number of entries in the table, especially if a high number of notifications has been generated.

- To view the notification details, click the notification name in the table. A **Details** section is displayed below the table, where you can see the event that generated the notification.

10.3. Deleting Notifications

To delete notifications:

1. Click the **Notification Area** button at the right side of the menu bar, then click **See All Notifications**. A table containing all the notifications is displayed.
2. Select the notifications you want to delete.
3. Click the **Delete** button at the upper side of the table.

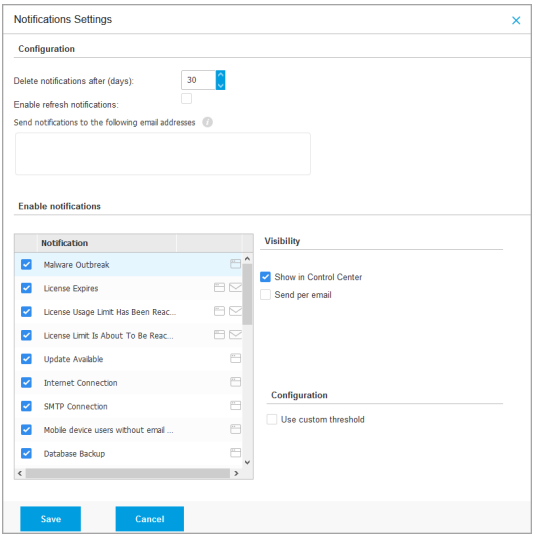
You can also configure notifications to be automatically deleted after a specified number of days. For more information, refer to "Configuring Notification Settings" (p. 352).

10.4. Configuring Notification Settings

The type of notifications to be sent and the email addresses they are sent to can be configured for each user.

To configure the notification settings:

1. Click the **Notification Area** button at the right side of the menu bar and then click **See All Notifications**. A table containing all the notifications is displayed.
2. Click the **Configure** button at the upper side of the table. The **Notification Settings** window is displayed.



Notifications Settings

Note
You may also access the **Notification Settings** window directly using the **Configure** icon from upper-right corner of the **Notification area** window.

3. Under **Configuration** section you can define the following settings:
   - Automatically delete notifications after a certain period of time. Set any number you wish between 0 and 365 in the **Delete notifications after (days)** field.
   - Select the **Enable refresh notifications** check box if you want the notifications area to automatically update every 60 seconds.
   - Additionally, you may send the notifications by email to specific recipients. Type the email addresses in the dedicated field, pressing `Enter` key after each address.
4. Under **Enable Notification** section you can choose the type of notifications you want to receive from GravityZone. You can also configure the visibility and sending options individually for each notification type.

Select the notification type that you want from the list. For more information, refer to "Notification Types" (p. 346). While a notification type is selected, you can configure its specific options (when available) in the right-side area:

Visibility

- **Show in Control Center** specifies that this type of event is displayed in Control Center, with the help of **Notifications area** icon.
- **Log to server** specifies that this type of event is also sent to the `syslog` file, in the case when a syslog is configured.

  To learn about how to configure syslog servers, refer to the GravityZone Installation Guide.
- **Send per email** specifies that this type of event is also sent to certain email addresses. In this case, you are required to enter the email addresses in the dedicated field, pressing `Enter` after each address.

Configuration

- **Use custom threshold** - allows defining a threshold for the occurred events, from which the selected notification is being sent.

  For example, the Malware Outbreak notification is sent by default to users that have at least 5% of all their managed network objects infected by the same malware. To change the malware outbreak threshold value, enable the option **Use Custom Threshold**, then enter the value that you want in the **Malware Outbreak Threshold** field.
- For **Database Backup** notification, you can choose to be notified only when a database backup has failed. Leave this option unchecked if you want to be notified of all database backup-related events.
- For **Security Server Status event**, you can select the Security Server events that will trigger this type of notification:
  - **Out of date** - notifies each time a Security Server in your network is outdated.
  - **Powered off** - notifies each time a Security Server in your network has been shut down.

- **Reboot required** - notifies each time a Security Server in your network requires a reboot.

- For **Task Status**, you can select the status type that will trigger this type of notification:
  - **Any status** - notifies each time a task sent from Control Center is done with any status.
  - **Failed only** - notifies each time a task sent from Control Center has failed.

5. Click **Save**.

11. 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.

11.1. 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.

11.2. Asking for Assistance

You can contact us for assistance through our online Support Center:

1. Go to http://www.bitdefender.com/support/contact-us.html.
2. Use the contact form to open an email support ticket or access other available contact options.

11.3. 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.

11.3.1. Using Support Tool on Windows Operating Systems

1. Download the Support Tool and distribute it to the affected computers. To download the Support Tool:
   a. Connect to Control Center using your account.
   b. Click your username in the upper-right corner of the console and choose **Help & Support**.
   c. The download links are available in the **Support** section. Two versions are available: one for 32-bit systems and the other for 64-bit systems. Make sure to use the correct version when running the Support Tool on a computer.
2. Run the Support Tool locally on each of the affected computers.
   a. Select the agreement check box and click **Next**.
   b. Complete the submission form with the necessary data:
      i. Enter your email address.
      ii. Enter your name.
      iii. Choose your country from the corresponding menu.
      iv. Enter a description of the issue you encountered.
      v. Optionally, you can try to reproduce the issue before starting to collect data. In this case, proceed as follows:
         A. Enable the option **Try to reproduce the issue before submitting**.
         B. Click **Next**.
         C. Select the type of issue you have experienced.
         D. Click **Next**.
         E. Reproduce the issue on your computer. When done, return to Support Tool and select the option **I have reproduced the issue**.

c. Click **Next**. The Support Tool gathers product information, information related to other applications installed on the machine and the software and hardware configuration.

d. Wait for the process to complete.

e. Click **Finish** to close the window. A zip archive has been created on your desktop.

Send the zip archive together with your request to the Bitdefender support representative using the email support ticket form available in the **Help & Support** page of the console.

11.3.2. 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`.
  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).

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 `/tmp/bdinstall.log` file, containing installation information
- The `network.txt` file, containing network settings / machine connectivity information
- 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

11.3.3. 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.

11.4. Contact Information

Efficient communication is the key to a successful business. During the past 15 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.

11.4.1. 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

11.4.2. 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.

11.4.3. 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/professionnel.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
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Phone (office&sales): +49 (0)2301 91 84 222
Phone (technical support): +49 (0)2301 91 84 444
Sales: vertrieb@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
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
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/world
Support Center: http://www.bitdefender.com/support/business.html

A. Appendices

A.1. Network Object Types and Statuses

A.1.1. Network Object Types

Each type of object available in the **Network** page is represented by a specific icon.

Find in the table presented hereinafter the icon and description for all available object types.

Icon	Type
	Network Group
	Computer
	Relay Computer
	Exchange Server Computer
	Relay Exchange Server Computer
	Virtual Machine
	Relay Virtual Machine
	Exchange Server Virtual Machine
	Relay Exchange Server Virtual Machine
	Virtual Machine with vShield
	Relay Virtual Machine with vShield
	VMware Inventory
	VMware vCenter
	VMware Datacenter
	VMware Resource Pool
	VMware Cluster
	Citrix Inventory
	Xen Server
	Xen Pool

Icon	Type
	Host without Security Server
	Host with Security Server
	Security Server
	Security Server with vShield
	VMware vApp
	Mobile Device User
	Mobile Device

A.1.2. Network Object Statuses

Each network object can have different statuses regarding the management state, security issues, connectivity and so on. Find in the next table all the available status icons and their description.

Note
The table below contains a few generic status examples. The same statuses may apply, single or combined, to all network object types, such as network groups, computers and so on.

Icon	Status
	Host without Security Server, Disconnected
	Virtual Machine, Offline, Unmanaged
	Virtual Machine, Online, Unmanaged
	Virtual Machine, Online, Managed
	Virtual Machine, Online, Managed, With Issues
	Virtual Machine, Pending restart
	Virtual Machine, Suspended
	Virtual Machine, Deleted

A.2. Application File Types

The antimalware scanning engines included in the Bitdefender security solutions can be configured to limit scanning to application (or program) files only. Application files are far more vulnerable to malware attacks than other types of files.

This category includes files with the following extensions:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.3. Attachment Filtering File Types

The Content Control module offered by Security for Exchange can filter email attachments based on the file type. The types available in Control Center include the following file extensions:

Executable files

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Images

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Multimedia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Archives

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Spreadsheets

fm3; ods; wk1; wk3; wks; xls; xlsx

Presentations

odp; pps; ppt; pptx

Documents

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.4. System Variables

Some of the settings available in the console require specifying the path on the target computers. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

Here is the list of the predefined system variables:

`%ALLUSERSPROFILE%`

The All Users profile folder. Typical path:

`C:\Documents and Settings\All Users`

`%APPDATA%`

The Application Data folder of the logged-in user. Typical path:

- Windows XP:

  `C:\Documents and Settings\{username}\Application Data`

- Windows Vista/7:

  `C:\Users\{username}\AppData\Roaming`

`%LOCALAPPDATA%`
The temporary files of Applications. Typical path:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`
The Program Files folder. A typical path is `C:\Program Files`.

`%PROGRAMFILES(X86)%`
The Program Files folder for 32-bit applications (on 64-bit systems). Typical path:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`
The Common Files folder. Typical path:

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`
The Common Files folder for 32-bit applications (on 64-bit systems). Typical path:

`C:\Program Files (x86)\Common Files`

`%WINDIR%`
The Windows directory or SYSROOT. A typical path is `C:\Windows`.

A.5. Application Control Tools

To set Application Control rules based on the hash of the executable or the certificate thumbprint, you must download the following tools:

- **Fingerprint**, to obtain the custom value of the hash.
- **Thumbprint**, to obtain the custom value of the certificate thumbprint.

Fingerprint

Click here to download the Fingerprint executable, or go to http://download.bitdefender.com/business/tools/ApplicationControl/

To obtain the application hash:

1. Open the **Command Prompt** window.
2. Navigate to the location of the Fingerprint tool. For example:

```
cd/users/fingerprint.exe
```

3. To display the hash value of an application, run the following command:

```
fingerprint <application_full_path>
```

4. Return to Control Center and configure the rule based on the value you obtained. For more information refer to "Application Control" (p. 236).

Thumbprint

Click here to download the Thumbprint executable, or go to http://download.bitdefender.com/business/tools/ApplicationControl/

To obtain the certificate thumbprint:

1. Run **Command Prompt** as Administrator.
2. Navigate to the location of the Thumbprint tool. For example:

```
cd/users/thumbprint.exe
```

3. To display the certificate thumbprint, run the following command:

```
thumbprint <application_full_path>
```

4. Return to Control Center and configure the rule based on the value you obtained. For more information refer to "Application Control" (p. 236).

Glossary

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Antivirus storm

An intensive use of system resources that occurs when antivirus software simultaneously scans multiple virtual machines on a single physical host.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Bootkit

A bootkit is a malicious program having the ability of infecting the master boot record (MBR), volume boot record (VBR) or boot sector. The bootkit remains active even after a system reboot.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Downloader

It is a generic name for a program having a primary functionality of downloading content for unwanted or malicious purposes.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

Exploit

An exploit generally refers to any method used to gain unauthorized access to computers or a vulnerability in a system's security that opens a system to an attack.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Grayware

A class of software applications between legitimate software and malware. Though they are not as harmful as malware which affects the system's integrity, their behavior is still disturbing, driving to unwanted situations such as data theft and unauthorized usage, unwanted advertising. Most common grayware applications are spyware and adware.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Keylogger

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they

are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Malware

Malware is the generic term for software that is designed to do harm - a contraction of 'malicious software'. It is not yet in universal usage, but its popularity as a general term for viruses, Trojan Horses, worms, and malicious mobile code is growing.

Malware signature

Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware. Signatures are also used to remove the malware code from infected files.

The Bitdefender Malware Signature Database is a collection of malware signatures updated hourly by the Bitdefender malware researchers.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Password stealer

A password stealer collects pieces of data that can be account names and associated passwords. These stolen credentials are then used for malicious purposes, like account takeovers.

Phishing

The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to

visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Ransomware

A malware that locks you out of your computer or blocks access to your files and applications. Ransomware will demand that you pay a certain fee (ransom payment) in return for a decryption key that allows you to regain access to your computer or files.

Report file

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited email.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Suspicious files and network traffic

Suspicious files are those with a doubtful reputation. This ranking is given by many factors, among which to name: existence of the digital signature, number of occurrences in computer networks, packer used, etc. Network traffic is considered suspicious when it deviates from the pattern. For example, unreliable source, connection requests to unusual ports, increased bandwidth usage, random connection times, etc.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

Targeted attacks

Cyber-attacks that mainly aim financial advantages or denigration of reputation. The target can be an individual, a company, a software or a system, well studied before the attack takes place. These attacks are rolled out over a long period of time and in stages, using one or more infiltration points. They are hardly noticed, most times when the damage has already been done.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.