Bitdefender

GravityZone

ADMINISTRATOR'S GUIDE

Bitdefender GravityZone
Administrator's Guide

Publication date 2021.03.17

Digitally signed by Celonenco Vitalie
Date: 2021.04.09 10:52:01 EEST
Reason: MoldSign Signature
Location: Moldova

Legal Notice

Table of Contents

Preface

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. ix)	This is an internal link, towards some location inside the document.
option	All the product options are printed using **bold** characters.
keyword	Interface options, keywords or shortcuts are highlighted using **bold** characters.

Admonitions

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

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

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

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

1. ABOUT GRAVITYZONE

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

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

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

2. GRAVITYZONE PROTECTION LAYERS

GravityZone provides the following protection layers:

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

2.1. Antimalware

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

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

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

a virtual environment to test their impact on the system and ensure they pose no threat. If a threat is detected, the program is prevented from running.

Scanning Engines

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

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

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

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

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

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

2.2. Advanced Threat Control

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

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

2.3. HyperDetect

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

2.4. Advanced Anti-Exploit

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

2.5. Firewall

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

2.6. Content Control

The Content Control module helps enforce company policies for allowed traffic, web access, data protection and applications control. Administrators can define traffic scan options and exclusions, schedule web access while blocking or allowing

certain web categories or URLs, configure data protection rules and define permissions for the use of specific applications.

2.7. Network Attack Defense

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

2.8. Patch Management

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

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

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

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

2.9. Device Control

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

2.10. Full Disk Encryption

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

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

2.11. Security for Exchange

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

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

2.12. Application Control

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

2.13. Sandbox Analyzer

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

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

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

Note
This module's functionality can be provided by Sandbox Analyzer Cloud and Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises is available with a separate license key.

2.14. Incidents

The Incidents feature is an event correlation component, capable of identifying advanced threats or in-progress attacks. As part of our comprehensive and integrated Endpoint Protection Platform, the Incidents feature brings together device intelligence across your enterprise network. This solution comes in aid of your incident response teams' effort to investigate and respond to advanced threats.

Through Bitdefender Endpoint Security Tools, you can activate a protection module called Incidents Sensor on your managed endpoints, to gather hardware and operating system data. Following a client-server framework, the metadata is collected and processed on both sides.

This component brings detailed information of the detected incidents, an interactive incident map, remediation actions, and integration with Sandbox Analyzer and HyperDetect.

2.15. 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.

Note
The HVI module may be available for your GravityZone solution with a separate license key.

2.16. Network Traffic Security Analytics (NTSA)

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

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

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

2.17. Security for Storage

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

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

When a user requests to open, read, write, or close a file from a laptop, workstation, mobile, or other device, the ICAP client (a NAS or file-sharing system) sends a scan

request to Security Server and receives a verdict regarding the file. Depending on the result, Security Server allows access, denies access or deletes the file.

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

2.18. Security for Mobile

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

2.19. GravityZone Protection Layers Availability

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

3. GRAVITYZONE ARCHITECTURE

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

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

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

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

The GravityZone solution includes the following components:

- GravityZone Virtual Appliance
- Security Server
- HVI Supplemental Pack
- Security Agents

3.1. GravityZone VA

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

3.1.1. GravityZone Database

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

3.1.2. GravityZone Update Server

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

3.1.3. GravityZone Communication Server

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

3.1.4. GravityZone Incidents Server

The Incidents Server is the link between security agents and the database, collecting endpoint data and generating incidents based on threats detected by prevention technologies and machine learning algorithms.

3.1.5. Web Console (GravityZone Control Center)

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

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

3.2. Security Server

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

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

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

3.3. HVI Supplemental Pack

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

Note
The HVI module may be available for your GravityZone solution with a separate license key.

3.4. Security Agents

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

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

3.4.1. Bitdefender Endpoint Security Tools

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

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

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

Protection Layers

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

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

Endpoint Roles

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

Power User

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

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

Relay

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

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

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

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

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

Patch Caching Server

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

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

Exchange Protection

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

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

3.4.2. Endpoint Security for Mac

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

Protection Layers

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

- Antimalware
- Advanced Threat Control
- Content Control
- Device Control
- Full Disk Encryption

3.4.3. GravityZone Mobile Client

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

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

3.4.4. Bitdefender Tools (vShield)

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

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

3.5. Sandbox Analyzer Architecture

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

Sandbox Analyzer is available in two variants:

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

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud contains the following components:

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

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

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

Sandbox Analyzer On-Premises

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

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

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

detonation virtual machines can run Windows 7 and Windows 10 64-bit operating systems.

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

Sandbox Analyzer On-Premises operates the following feeding sensors:

- **Endpoint sensor**. Bitdefender Endpoint Security Tools for Windows acts as feeding sensor installed on endpoints. The Bitdefender agent uses advanced machine learning and neural network algorithms to determine suspicious content and to submit it to Sandbox Analyzer, including objects from centralized quarantine.
- **Network sensor**. Network Security Virtual Appliance (NSVA) is a virtual appliance deployable in the same virtualized ESXi environment as the Sandbox Analyzer instance. Network sensor extracts content from network streams and submits it to Sandbox Analyzer.
- **ICAP sensor**. Deployed on network attached storage (NAS) devices using ICAP protocol, Bitdefender Security Server supports content submission to Sandbox Analyzer.

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

4. 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.

4.1. 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+, Microsoft Edge 20+, Opera 16+
- Recommended screen resolution: 1280 x 800 or higher

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

To connect to Control Center:

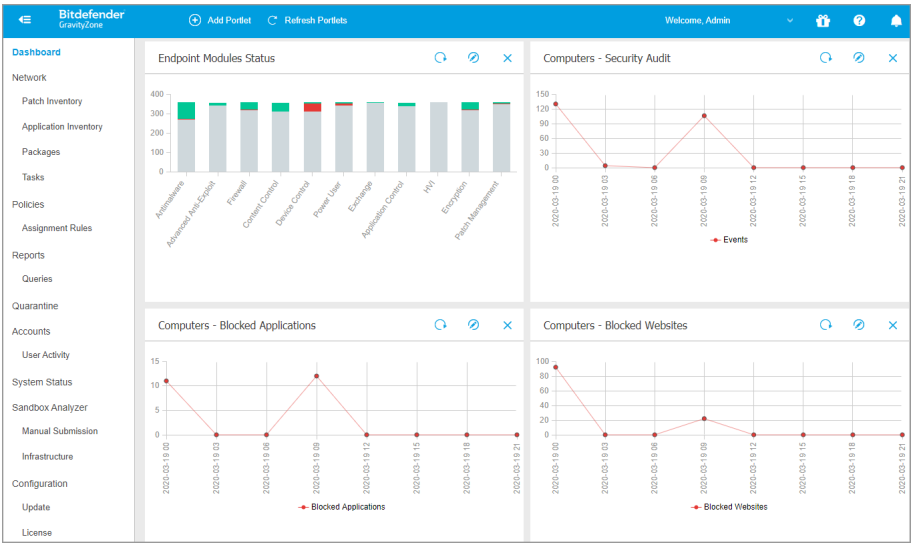
1. In the address bar of your web browser, enter the IP address or the DNS hostname of the Control Center appliance (using the `https://` prefix).
2. Enter your user name and password.
3. Enter the six-digit code from Google Authenticator, Microsoft Authenticator, or any two-factor TOTP (Time-Based One-Time Password Algorithm) authenticator - compatible with the standard RFC6238. For more details, refer to "Managing Your Account" (p. 24).
4. Click **Login**.

At the first login, you have to agree to Bitdefender Terms of Service. Click **Continue** to start using GravityZone.

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.

4.2. 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

4.2.1. 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.

Use the **View Menu** button at the upper-left corner to collapse to icon view, hide, or expand the menu options. Click the button to run though the options sequentially, or double-click to skip.

According to your role, you can access the following menu options:

Dashboard

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

Incidents
View and manage security incidents across the company 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, security certificates and Network Inventory settings, including scheduled rules for automatic cleanup of unused virtual machines.

> **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.

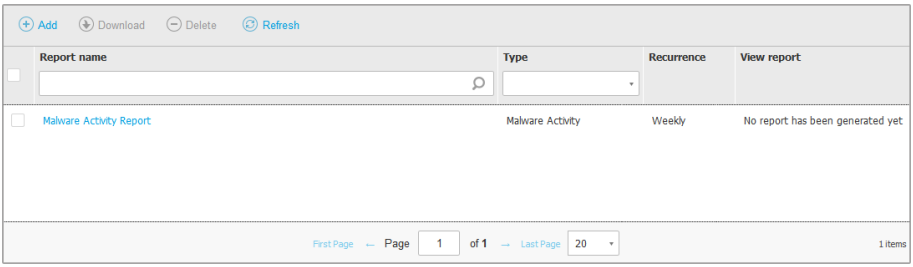
- **Feedback**. Click this option to display a form allowing you to edit and send your feedback messages regarding your experience with GravityZone.
- **Logout**. Click this option to log out of your account.

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.

4.2.2. 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

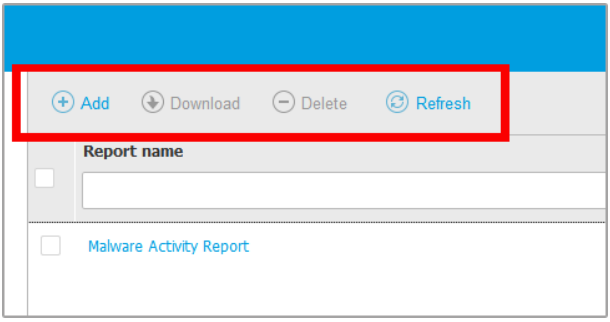
To make sure the console displays the latest information, click the **Refresh** button at the upper side of the table.

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

4.2.3. 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:

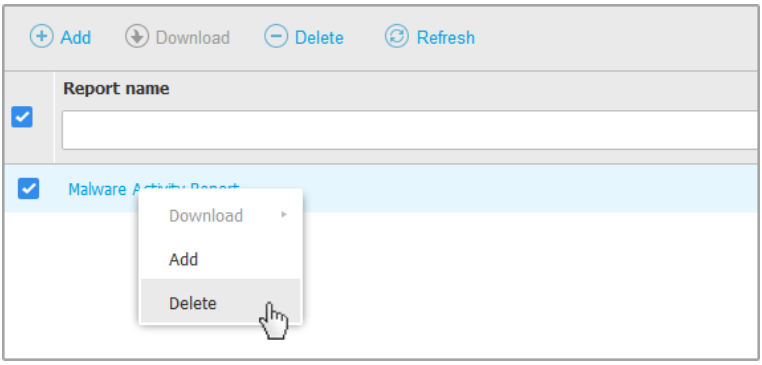
- Create a new report.
- Download a scheduled report.
- Delete a scheduled report.



The Reports page - Action Toolbar

4.2.4. 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.



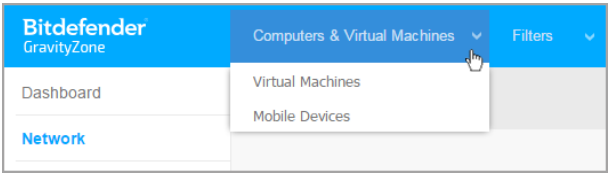
The Reports page - Contextual menu

4.2.5. 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.



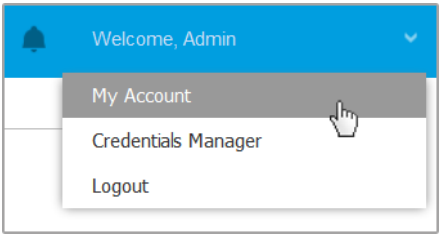
The Views Selector

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.

4.3. 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. Under **Login Security**, configure two-factor authentication and check the status of the policies available to secure your GravityZone account. Company-wide set policies are read-only.

   To enable the two-factor authentication:

a. **Two-factor authentication.** The two-factor authentication adds an extra layer of security to your GravityZone account, by requiring an authentication code in addition to your Control Center credentials.

   When first logging in to your GravityZone account you will be prompted to download and install the Google Authenticator, Microsoft Authenticator, or any two-factor TOTP (Time-Based One-Time Password Algorithm) authenticator - compatible with the standard RFC6238 on a mobile device, link it to your GravityZone account, then use it with each Control Center login. The authenticator app generates a six-digit code each 30 seconds. To complete the Control Center login, after entering the password, you will need to provide the six-digit code generated by the app.

   Note
   You may skip this process three times, after which you will not be able to log in without two-factor authentication.

   To enable the two-factor authentication:

   i. Click the **Enable** button under the **Two-factor authentication** message.

   ii. In the dialog box, click the appropriate link to download and install the selected authenticator app on your mobile device.

   iii. On your mobile device, open the app.

   iv. In the **Add an account** screen, scan the QR code to link the app to your GravityZone account.

   You can also enter the secret key manually.

   This action is required only once, to enable the feature in GravityZone.

   Important
   Make sure to copy and save the secret key in a safe location. Click **Print a backup** to create a PDF file with the QR code and secret key. If the mobile device used for activating two-factor authentication is lost or replaced, you will need to install the autheticator app of choice on a new device and provide the secret key to link it to your GravityZone account.

   v. Enter the six-digit code in the **Authenticator code** field.

   vi. Click **Enable** to complete the feature activation.

Note
Be aware that, if the currently configured 2FA is disabled for your account, this secret key will no longer be valid.

b. **Password expiration policy.** Regular changes to your password provide an added layer of protection against the unauthorized use of passwords, or limits the duration of unauthorized use. When enabled, GravityZone requires you to change your password no later than 90 days.

c. **Account lockout policy.** This policy prevents access to your account after five consecutive failed login attempts. This measure is to protect against brute-force attacks.

   To unlock your account, you need to reset your password from the login page, or contact another GravityZone administrator.

5. Click **Save** to apply the changes.

Note
You cannot delete your own account.

4.4. 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:

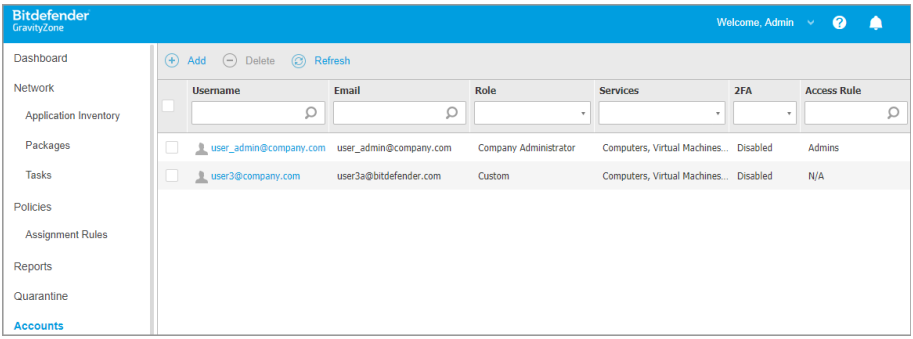
1. Click your username in the upper-right corner of the console and choose **My Account**.
2. Under **Account Details**, click **Change password**.
3. Enter your current password and the new password in the corresponding fields.
4. Click **Save** to apply the changes.

5. 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 user accounts individually or enable dynamic access for multiple accounts through Active Directory integrations or access rules. 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.
- You can only manage accounts with equal or fewer privileges than your account.



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 / security analyst / custom).

- GravityZone security services the user is allowed to manage (Computers, Virtual Machines, Mobile Devices).
- 2FA (two-factor authentication) status, which allows to quickly check if the user has enabled the two factor authentication.
- Access Rule status, indicates a user account created through an access permission rule. Manually created user accounts will display **N/A**.

5.1. 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 security analyst 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. **Security Analyst** - Security Analyst accounts are read-only accounts. They only allow access to security-related data, reports and logs. Such accounts can be allocated to personnel with security 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. 29).

Account Role	Allowed Child Accounts	User Rights
Company Administrator	Company Administrators, Network Administrators, Security Analysts	Manage Solution Manage Company Manage Users Manage Networks View and analyze data
Network Administrator	Network Administrators, Security Analysts	Manage Users Manage Networks View and analyze data
Security Analysts	-	View and analyze data

5.2. 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.
- **View and analyze data**. View security-related events and logs, manage reports and the dashboard.

5.3. Managing User Accounts

To create, edit, delete and configure user accounts, use the following methods:

- Managing User Accounts Individually. Use this method to add local user accounts or Active Directory accounts. To set up an Active Directory integration, refer to the GravityZone Installation Guide.

  Before creating a user account, make sure you have the required email address at hand. The user receives the GravityZone login details at the provisioned email address.

- Managing Multiple User Accounts. Use this method to enable dynamic access through access permission rules. This method requires an Active Directory domain integration. For more information on Active Directory integration, refer to GravityZone Installation Guide.

5.3.1. Managing User Accounts Individually

In Control Center you can create, edit and delete user accounts individually.

Dependencies

- Locally created accounts can delete accounts created through Active Directory integration regardless of their role.
- Locally created accounts cannot delete similar account regardless of their role.

Creating User Accounts Individually

To add a user account in Control Center:

1. Go to the **Accounts** page.
2. Click the ⊕ **Add** button at the upper side of the table. A configuration window appears.
3. Under the **Details** section, configure as follows:
   - For Active Directory user accounts configure the following details:

     Username for Active Directory (AD) user accounts. Choose a user account from the drop-down list and skip to step 4.

     You can add AD user accounts only if the integration is configured. When adding an AD user account, user details are imported from its associated domain. The user logs in to Control Center using the AD username and password.

Note

- 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** tab. For more details, refer to **Installing Protection > GravityZone Installation** and **Setup > Configure Control Center Center Settings** chapters from the GravityZone Installation Guide.

- For local accounts configure the following details:
  - **Username** for local account. Disable **Import from Active Directory** and enter a user name.
  - **Email**. Enter the user's email address.

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

    GravityZone uses this email address to send notifications.
  - **Full Name**. Enter the user's full name.
  - **Password**. Enter a password that the user can use to log in.

    The password must contain at least one upper case character, at least one lower case character and at least one digit or special character.
  - **Confirm password**. Confirm the password to validate.

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. 28).
   - **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. 29).

- **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 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.

Editing User Accounts Individually

To add a user account in Control Center

1. Log in to Control Center.
2. Go to the **Accounts** page.
3. Click the user's name.
4. Change user 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 or fewer privileges as your own account.

Deleting User Accounts Individually

To delete a user account in Control Center

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

   Click **Yes** to confirm.

5.3.2. Managing Multiple User Accounts

Create access rules to grant GravityZone Control Center access to Active Directory users, based on security groups.

Prerequisites

To manage multiple user account, you need an Active Directory domain integration with GravityZone. To integrate and synchronize an Active Directory domain, refer to the **Active Directory** chapter from the GravityZone Installation Guide.

Dependencies

Access permission rules are tied to Active Directory (AD) security groups and associated user accounts. Any changes done to the Active Directory domains may impact the associated access permission rules. This is what you need to know about the relation between rules, users and Active Directory domains:

- An access permission rule adds a user account only if the email is not already associated with an existing account.
- For duplicate email addresses within a security group, the access permission rule creates a GravityZone user account only for the first Active Directory user account that logs in Control Center.

  For example, a security group contains a duplicate email address for different users and they all try to log in to Control Center using their Active Directory credentials. If an access permission rule is associated to this specific Active Directory domain, it will create a user account only for the first user that logged in to Control Center using the duplicate email address.

- User accounts created through access permission rules become inactive if they are removed from their associated AD security group. The same users can become active if they are associated to a new access rule.
- Access rules become read-only once an associated Active Directory domain is no longer integrated with GravityZone. Users associated with these rules become inactive.
- User accounts created through access rules cannot delete locally created users.
- User accounts created through access rules cannot delete similar accounts that have the Company Administrator role.

Creating Multiple User Accounts

To add multiple user accounts, you create access permission rules. The access permission rules are associated to Active Directory security groups.

To add an access permission rule:

1. Go to **Configuration > Active Directory > Access Permissions**.
2. If you have multiple integrations, select a domain at the upper-left side of the table.
3. Click ⊕ **Add** at the left side of the table.
4. Configure the following access permission settings:
   - **Priority**. Rules are processed in priority order. The lower the number, the higher the priority.
   - **Name**. The name of the access rule.
   - **Domain**. The domain from which to add security groups.
   - **Security Groups**.The security groups that contain your future GravityZone users. You can use the autocomplete box. Security groups added in this list are not subject to change, addition or deletion, after you save the access rule.
   - **Timezone**. The timezone of the user.
   - **Language**. The console display language.
   - **Role**. Predefined user roles. For more details, refer to the **User Accounts** chapter from the GravityZone Administrator's Guide.

> **Note**
> You can grant and revoke privileges to other users with equal or fewer privileges than your account.

- **Rights**. Each predefined user role has a certain configuration of rights. For more details, refer to the **User Rights** chapter from the GravityZone Administrator's Guide.
- **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.

5. Click **Save**.

   The access rule is saved if there is no user impact. Otherwise you are prompted to specify user exclusions. For example, when you add a rule with a higher priority, impacted users associated to other rules are tied to the former rule.
6. If needed, select the users you want to exclude. For more information, refer to User Account Exclusions.
7. Click **Confirm**. The rule is displayed in the **Access Permissions** page.

Users within the security groups specified by the access rules can now access GravityZone Control Center with their domain credentials. Control Center automatically create new user accounts when they log in for the first time, using their Active Directory email address and password.

User accounts created through an access rule have the name of the access rule displayed in the **Accounts** page, under the **Access Rule** column.

Editing Multiple User Accounts

To edit an access permission rule:

1. Go to **Configuration > Active Directory > Access Permissions**.
2. Select the name of your access rule to open the configuration window.
3. Edit access permission settings. For more information, refer to Adding Access Permissions.

4. Click **Save**. The rule is saved if there is no user impact. Otherwise you are prompted to specify user account exclusions. For example, if you update a rule priority, impacted users can switch to different rule.
5. If needed, select the users you want to exclude. For more information, refer to User Account Exclusions.
6. Click **Confirm**.

> **Note**
> You can unlink user accounts created through an access rule by modifying their rights in Control Center. The user account cannot be linked back to the access rule.

Deleting Multiple User Accounts

To delete an access rule:

1. Go to **Configuration > Active Directory > Access Permissions**.
2. Select the access rule that you want to delete and click ⊖ **Delete**. A window prompts you to confirm your action. If there is user impact you are prompted to specify user account exclusions. For example, you may want to specify exclusions for users impacted by rule deletion.
3. If needed, select the users you want to exclude. For more information, refer to User Exclusions.
4. Click **Confirm**.

Deleting a rule will revoke access to the associated user accounts. All users created through it will be removed, unless other rules grant them access.

User Account Exclusions

When you add, edit or delete access permission rules that results in user impact, you may want to specify user account exclusions. You can also view the reasoning and effects of the impacted users.

Specify user exclusions as follows:

1. Select the users you want to exclude. Or, select the check box at the top of the table to add all users to the list.
2. Click **X** within a username box to remove it from the list.

5.4. 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.

5.5. Managing Two-factor Authentication

By clicking a user account, you will be able to view its 2FA status (enabled or disabled) under **Two-factor Authentication** section. You can take the following actions:

- **Reset or disable the user's two-factor authentication**. If a user with 2FA enabled has changed or wiped the mobile device and lost the secret key:
  1. Enter your GravityZone password in the available field.
  2. Click **Reset** (when 2FA is enforced) or **Disable** (when 2FA is not enforced).
  3. A confirmation message will inform you that two-factor authentication has been reset / disabled for the current user.

     After resetting 2FA when this feature is enforced, at login, a configuration window will prompt the user to configure again the two-factor authentication with a new secret key.
- If the user has 2FA disabled and you want to activate it, you will need to ask the user to enable this feature from his account settings.

> **Note**
> If you have a Company Administrator account, you may turn two-factor authentication mandatory for all GravityZone accounts. Find more information in the Installation Guide, under **Installing Protection > GravityZone Installation and Setup > Configure Control Center Settings** chapter.

Important
The authentication app of choice (Google Authenticator, Microsoft Authenticator, or any two-factor TOTP (Time-Based One-Time Password Algorithm) authenticator - compatible with the standard RFC6238) combines the secret key with the mobile device's current time-stamp to generate the six-digit code. Be aware that the time-stamps on both mobile device and the GravityZone appliance have to match for the six-digit code to be valid. To avoid any time-stamps synchronization issue, we recommend enabling the automatic date and time setting on the mobile device.

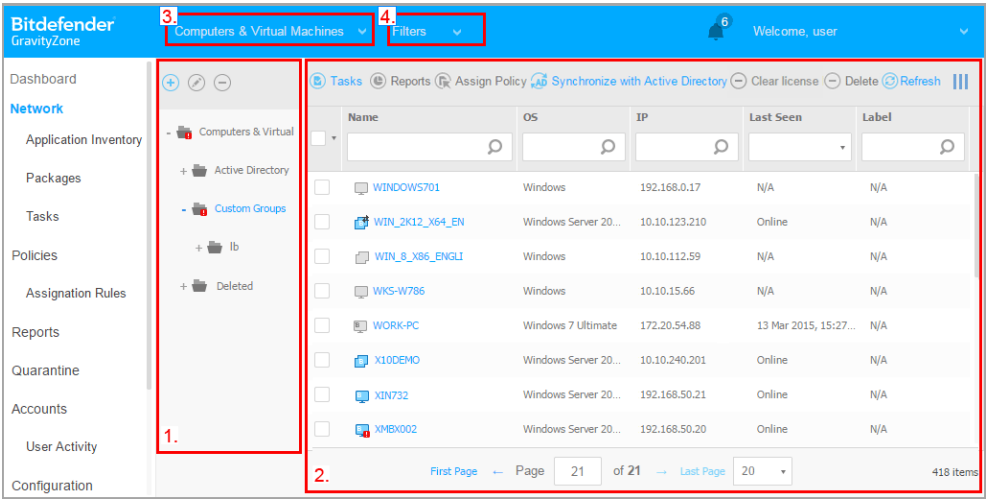
Another method of checking the 2FA changes related to user accounts is to access the **Accounts > User Activity** page and filter the activity logs using the following filters:

- Area > Accounts / Company
- Action > Edited

For more information about enabling 2FA, refer to "Managing Your Account" (p. 24)

6. 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. 195).

   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. 534).
   - 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.

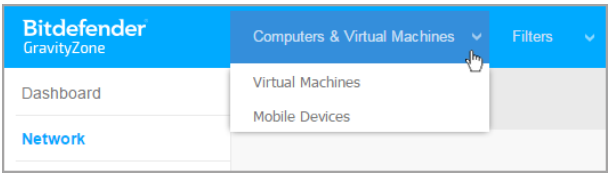
For detailed information about network objects, refer to:

- "Working with Network Views" (p. 41)
- "Computers" (p. 44)
- "Virtual Machines" (p. 98)
- "Mobile Devices" (p. 153)
- "Patch Inventory" (p. 184)
- "Viewing and Managing Tasks" (p. 191)

6.1. 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

6.1.1. 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.

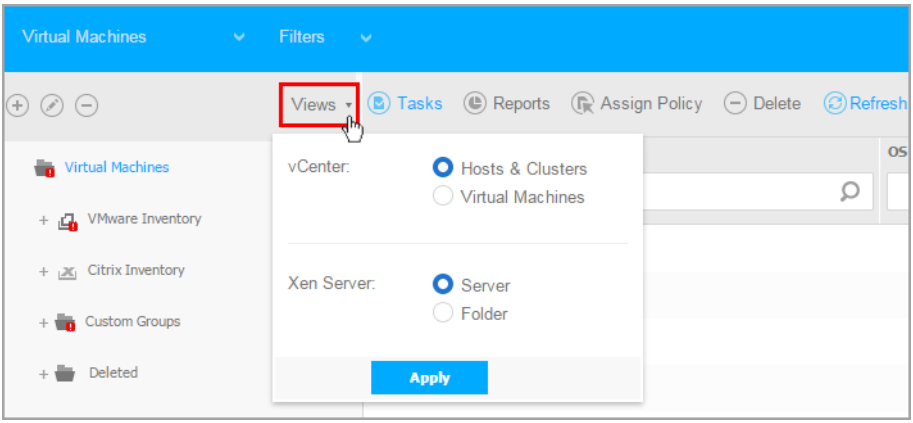
Important
Assigning policies to virtual machines from **Computers and Virtual Machines** view may be restricted by the GravityZone solution manager while configuring the vCenter Server or a Xen Server in the **Configuration > Virtualization Providers** page. To find out more, refer to **Installing Protection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

6.1.2. 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 Nutanix, 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.

6.1.3. 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.

6.2. 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
- Manage patches
- 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.

6.2.1. 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. 534) 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. 195).

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.
- Security content is 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.

6.2.2. Viewing Computer Details

You can obtain detailed information about each computer within the **Network** page, as follows:

- Checking the **Network** page
- Checking the **Information** window

Checking the Network page

To find out details about a computer, check the information available in the right-side pane table from the **Network** page.

You can add or remove columns with endpoint information by clicking the **Columns** button at the upper-right side of the pane.

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. 44).
5. Check the information displayed on columns for each computer.

   Use the header row to search as you type for specific endpoints, according to the available criteria:

   - **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. You can add a label in the endpoint's **Information** window and then use it in searches.
   - **Policy**: the policy applied to the endpoint, with a link for viewing or changing the policy settings.

Checking the Information window

In the right-side pane of the **Network** page, click the name of the endpoint you are interested in to display the **Information** window. This window displays only the data available for the selected endpoint, grouped under several tabs.

Find hereafter the exhaustive list of information you may find in the **Information** window, according to the endpoint type and its specific security information.

General tab

- General computer information, such as name, FQDN information, IP address, operating system, infrastructure, parent group and current connection status.

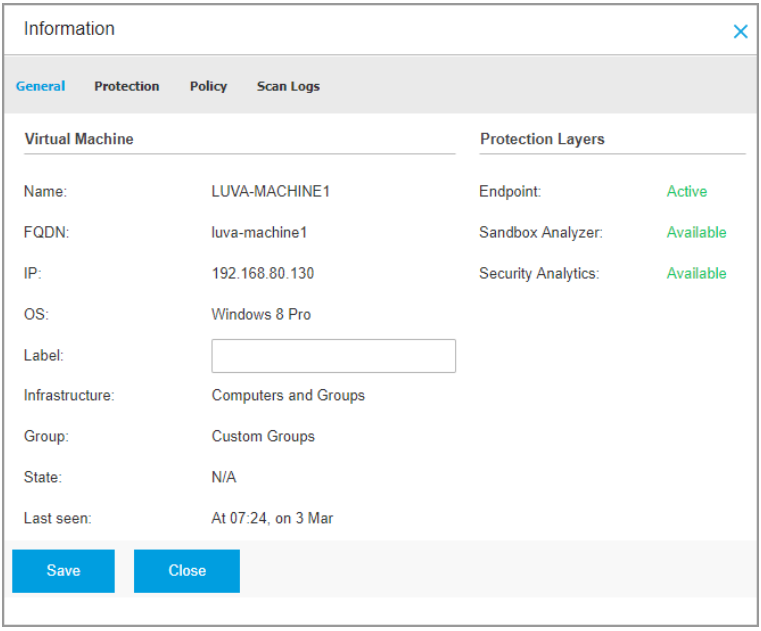
  In this section you can assign the endpoint with a label. You will be able to quickly find endpoints with the same label and take actions on them, no matter

where they are located in the network. For more information about filtering endpoints, refer to "Sorting, Filtering and Searching for Computers" (p. 62).

- Protection layers information, including the list of security technologies acquired with your GravityZone solution and their license status, which can be:
  - **Available / Active** – the license key for this protection layer is active on the endpoint.
  - **Expired** – the license key for this protection layer is expired.
  - **Pending** – the license key is not confirmed yet.

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

- **Relay Connection**: the name, IP and label of the relay to which the endpoint is connected, if the case.



Information window - General tab

Protection tab

This tab contains details about the protection applied on the endpoint, and they refer to:

- Security agent information like product name, version, update status and update locations as well as scanning engines configuration and security content versions. For Exchange Protection, antispam engine version is also available.
- Security status for each protection layer. This status appears at the right side of the protection layer's name:
  - **Secure**, when there are no security issues reported on the endpoints applied with the protection layer.
  - **Vulnerable**, when there are security issues reported on the endpoints applied with the protection layer. For more details, refer to "Security Status" (p. 46).
- Associated Security Server. Each assigned Security Server is 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.

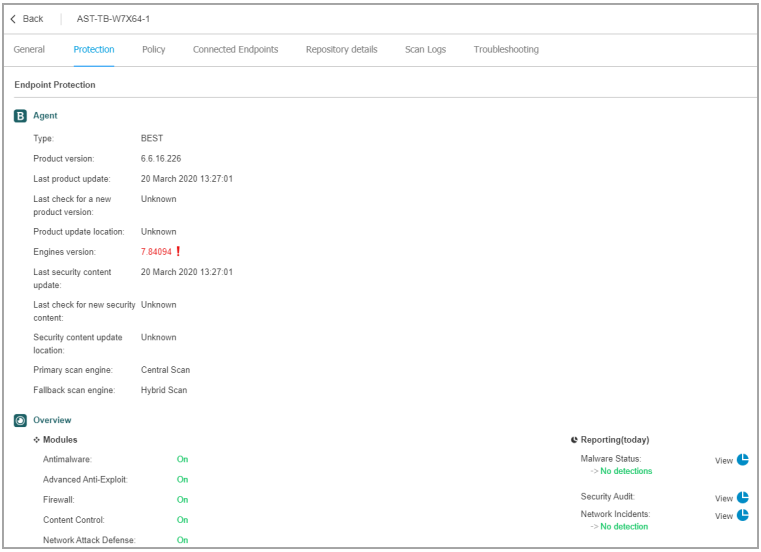
  Click the **View** link to access the report options and then generate the report. For more information, refer to "Creating Reports" (p. 465)
- Information regarding the Sandbox Analyzer protection layer:
  - Sandbox Analyzer usage status on the endpoint, displayed at the right side of the window:
    - **Active**: Sandbox Analyzer is licensed (available) and enabled via policy on the endpoint.
    - **Inactive**: Sandbox Analyzer is licensed (available) but not enabled via policy on the endpoint.
  - Name of the agent that acts as feeding sensor.
  - Module status on the endpoint:

- **On** - Sandbox Analyzer is enabled on the endpoint via policy.
- **Off** - Sandbox Analyzer is not enabled on the endpoint via policy.

– Threat detections in the last week by clicking the **View** link to access the report.

- Additional information regarding the Encryption module, such as:
  – Detected volumes (mentioning the boot drive).
  – Encryption status for each volume (which can be **Encrypted**, **Encryption in progress**, **Decryption in progress**, **Unencrypted**, **Locked** or **Paused**).

    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. 97).
- Security telemetry status, which informs you if the connection between the endpoint and the SIEM server is established and working, is disabled, or has issues.



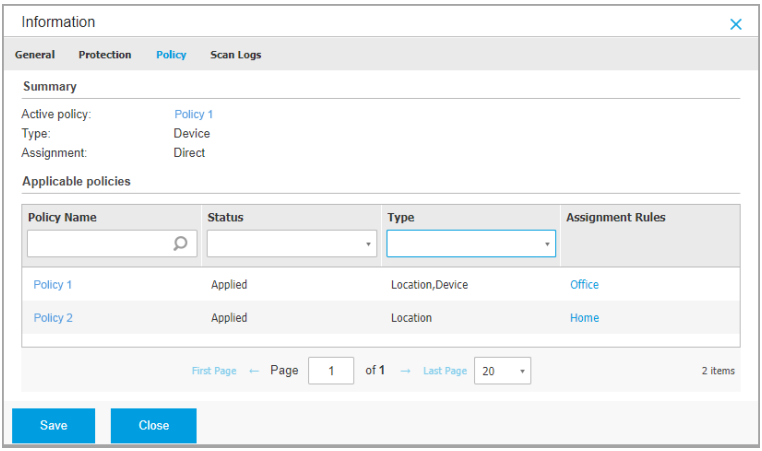
Information window - Protection tab

Policy tab

An endpoint can be applied with one or more policies, but only one policy can be active at a time. The **Policy** tab displays information about all policies that apply to the endpoint.

- The active policy name. Click the policy name to open the policy template and view its settings.
- The active policy type, which can be:
  - **Device**: when the policy is manually assigned to the endpoint by the network administrator.
  - **Location**: a rule-based policy automatically assigned to the endpoint if the endpoint's network settings match the given conditions of an existing assignment rule.

    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.
  - **User**: a rule-based policy automatically assigned to the endpoint if it matches the Active Directory target specified in an existing assignment rule.
  - **External (NSX)**: when the policy is defined in the VMware NSX environment.
- The active policy assignment type, which can be:
  - **Direct**: when the policy is directly applied to the endpoint.
  - **Inherited**: when the endpoint inherits the policy from a parent group.
- **Applicable policies**: displays the list of policies linked to existing assignment rules. These policies may apply to the endpoint when it matches the given conditions of the linked assignment rules.

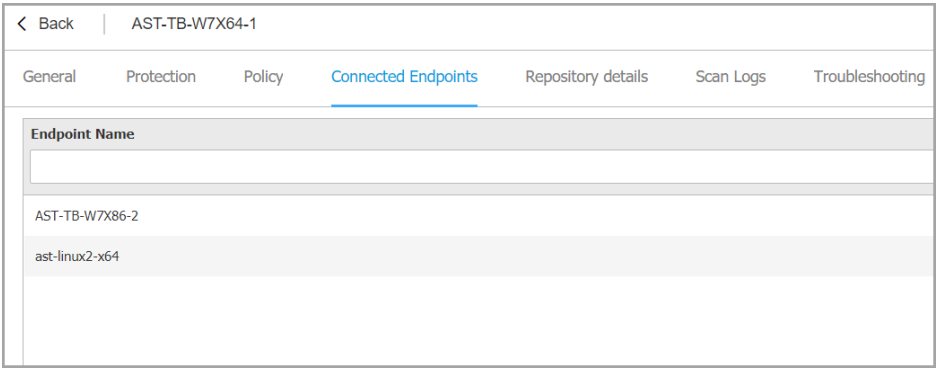


Information window - Policy tab

For more information regarding policies, refer to "Changing Policy Settings" (p. 217)

Connected Endpoints tab

The **Connected Endpoints** 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.

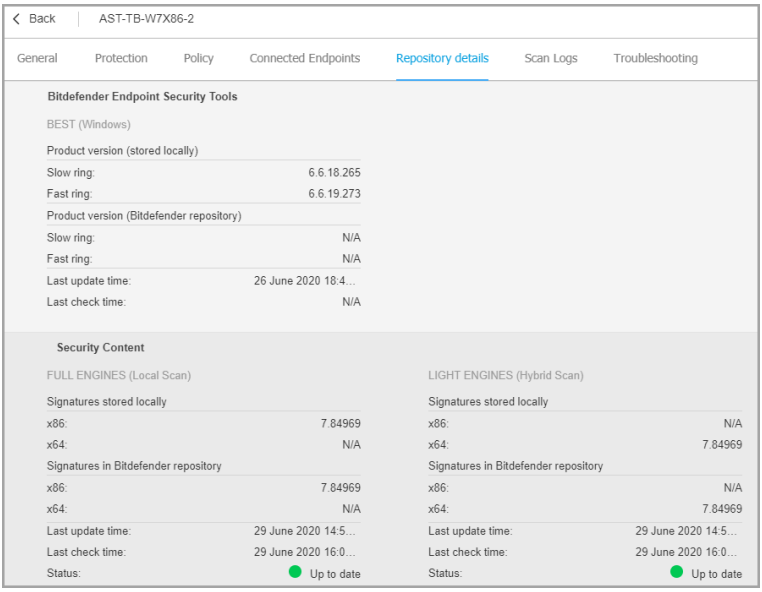


Information window - Connected Endpoints tab

Repository details tab

The **Repository details** tab is available only for endpoints with relay role and displays information about the security agent updates and security content.

The tab includes details about the product and signatures versions stored on the relay and the ones available in the official repository, update rings, the date and time of the update and last check for new versions.



Information window - Repository details tab

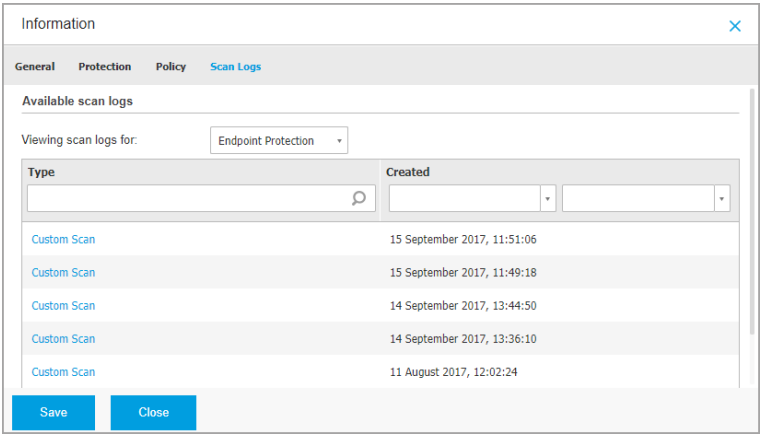
Scan Logs tab

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.

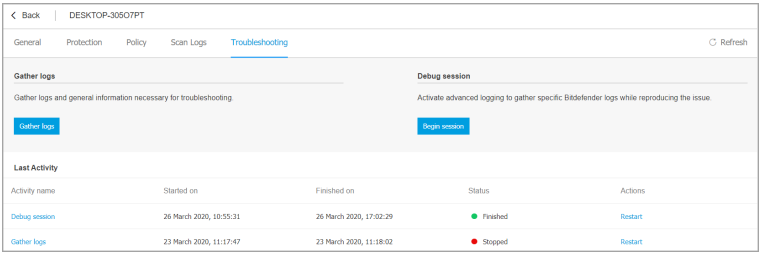


Information window - Scan logs tab

Troubleshooting tab

This section is dedicated to agent troubleshooting activity. You can gather general or specific logs from the endpoint check or take action on current troubleshooting events and view previous activity.

Important
Troubleshooting is available for Windows, Linux, macOS and all Security Server types.



Information window - Troubleshooting tab

- **Gather logs**

  This option helps you gather a set of logs and general information necessary for troubleshooting such as settings, active modules or applied policy specific to the target machine. All the generated data is saved in an archive.

  It is recommended to use the option when the cause of the issue is unclear.

  To start the troubleshooting process:

  1. Click the **Gather logs** button. A configuration window is displayed.
  2. In the **Logs Storage** section, choose a storage location:
     - **Target machine**: the logs archive is saved to the provided local path. The path is not configurable for Security Servers.
     - **Network share**: the logs archive is saved to the provided path from the shared location.

     You can use the option **Save logs also on target machine** to save a copy of the logs archive on the affected machine as a backup.
  3. Fill in with the necessary information (local path, credentials for the network share, path to the shared location) depending on the selected location.
  4. Click the **Gather logs** button.

- **Debug session**

  With Debug session, you can activate advanced logging on the target machine to gather specific logs while reproducing the issue.

  You should use this option when you have discovered which module is causing issues or at the recommendation of Bitdefender Enterprise Support. All the generated data is saved in an archive.

  To start the troubleshooting process:

  1. Click the **Begin session** button. A configuration window is displayed.
  2. In the **Issue type** section, select the issue you consider is affecting the machine.

     Issue types for Windows and macOS machines:

Issue type	Use case
Antimalware (on-access and on-demand scanning)	– Endpoint general slowdown – A program or system resource takes too long to respond – A scanning process takes longer than usual – No connection to host security service error
Update errors	– Error messages received during product or security content updates
Content Control (traffic scan and user control)	– Website does not load – Elements of the web page are not displayed properly
Cloud Services connectivity	– The endpoint does not have connectivity with Bitdefender Cloud Services
Product general issues (high verbosity logging)	– Reproduce a generic reported issue with verbose logging

Issue types for Linux machines:

Issue type	Use case
Antimalware and Update	– A scanning process takes longer than usual and consumes more resources – Error messages received during product or security content updates – The endpoint fails to connect to GravityZone console.
Product general issues (high verbosity logging)	– Reproduce a generic reported issue with verbose logging

Issue types for Security Servers:

Issue type	Use case
Antimalware (on-access and on-demand scanning)	Any unexpected behavior of the Security Server including: – Virtual machines are not properly protected – Antimalware scanning tasks fail to run or take longer than expected – Product updates are not properly installed – Generic Security Server malfunctioning (bd daemons not running)
Communication with GravityZone Control Center	Any unexpected behavior observed from GravityZone console: – Virtual machines are not properly reported in GravityZone console – Policy issues (policy is not applied) – The Security Server cannot establish a connection with GravityZone console **Note** Use this method at the recommendation of Bitdefender Enterprise Support.

3. For **Debug session duration**, choose the time interval after which the debug session automatically ends.

   Note
   It is recommended to manually stop the session using the **Finish session** option, right after you reproduce the issue.

4. In the **Logs Storage** section, choose a storage location:
   - **Target machine**: the logs archive is saved to the provided local path. The path is not configurable for Security Servers.
   - **Network share**: the logs archive is saved to the provided path from the shared location.

You can use the option **Save logs also on target machine** to save a copy of the logs archive on the affected machine as a backup.

5. Fill in the necessary information (local path, credentials for the network share, path to the shared location) depending on the selected location.
6. Click the **Begin session** button.

> **Important**
> You can run only one troubleshooting process at a time (**Gather logs** / **Debug session**) on the affected machine.

- **Troubleshooting history**

  The **Last activity** section presents the troubleshooting activity on the affected computer. The grid displays only the latest 10 troubleshooting events in chronological reversed order and automatically deletes activity older than 30 days.

  The grid displays the details for every troubleshooting process.

  The process has main and intermediary statuses. Depending on the customized settings, you can have the following status, where you are required to take action:

  – **In progress (Ready to reproduce the issue)** – access the affected machine manually or remotely and reproduce the issue.

  You have several options to stop a troubleshooting process, as follows:

  – **Finish session**: ends the debug session and the gathering process on the target machine while saving all the collected data to specified storage location.

    It is recommended to use this option right after you reproduced the issue.

  – **Cancel**: this option cancels the process and no logs are collected.

    Use this option when you do not want to collect any logs from the target machine.

  – **Force Stop**: forcefully stops the troubleshooting process.

    Use this option when canceling the session takes too long or the target machine is unresponsive and you will be able to start a new session in a few minutes.

To restart a troubleshooting process:

– **Restart**: this button, associated with each event and located under **Actions** restarts the selected troubleshooting activity while maintaining its previous settings.

Important

– To make sure the console displays the latest information use the **Refresh** button at the upper right side of the **Troubleshooting** page.

– For more details about a specific event, click the event name from the grid.

6.2.3. 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. 204).

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**.

6.2.4. 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

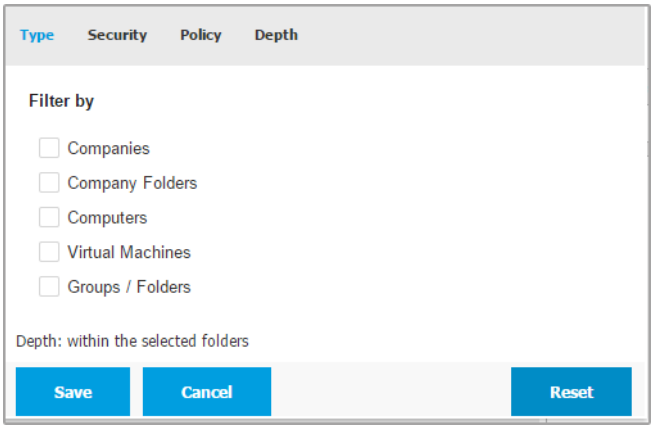
To sort data by a specific column, click the column headers. For example, if you want to order computers by name, click the **Name** heading. If you click the heading again, the computers will be displayed in reverse order.

Sorting Computers

Filtering Computers

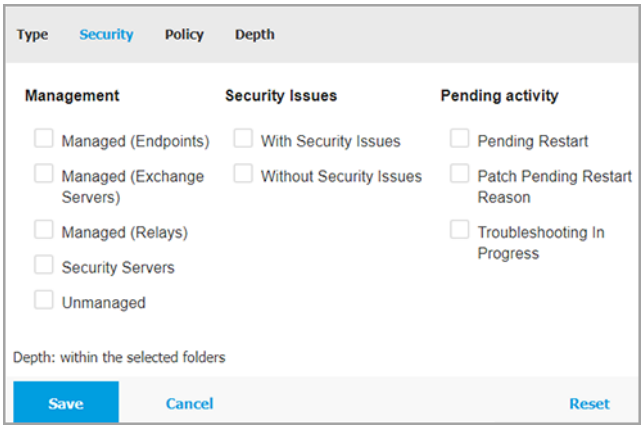
To filter your network entities, use the **Filters** menu from the upper-side of the network panes area.

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).



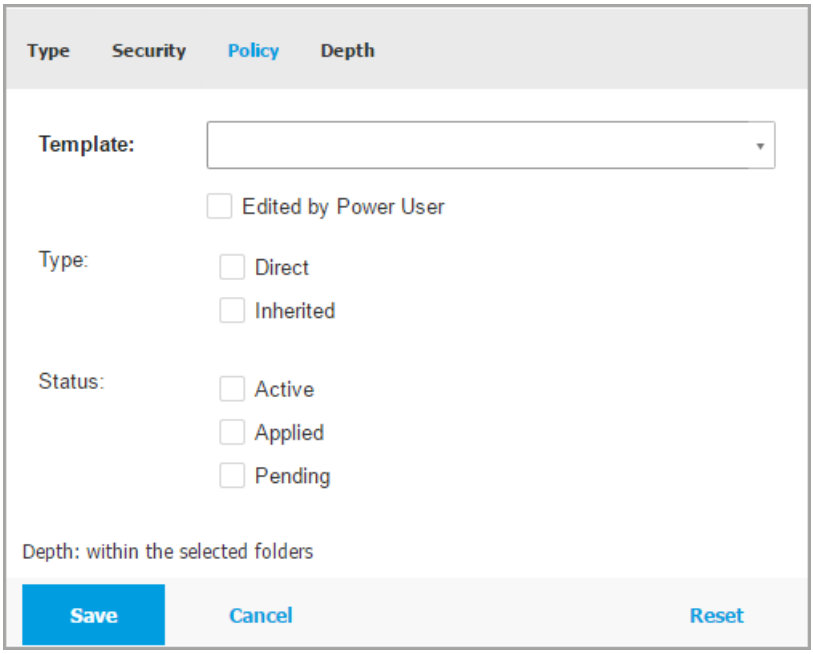
Computers - Filter by Type

- **Security**. Choose to display computers by protection management, security status or pending activity.



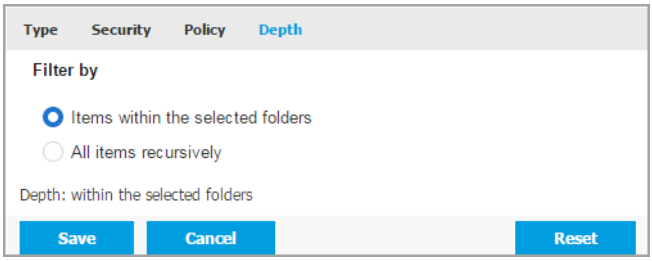
Computers - Filter by Security

- **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

6.2.5. 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. 66)
- “Patch Tasks” (p. 76)
- “Exchange Scan” (p. 78)
- “Install” (p. 82)
- “Uninstall Client” (p. 87)

- "Update Client" (p. 88)
- "Reconfigure Client" (p. 89)
- "Repair Client" (p. 91)
- "Restart Machine" (p. 91)
- "Network Discovery" (p. 92)
- "Applications Discovery" (p. 92)
- "Update Security Server" (p. 93)
- "Inject Custom Tool" (p. 94)

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. 191).

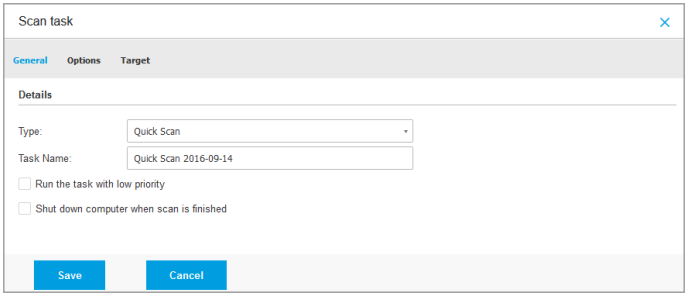
Scan

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.

> **Note**
> This option applies only to Bitdefender Endpoint Security Tools and Endpoint Security (legacy agent).

– **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.

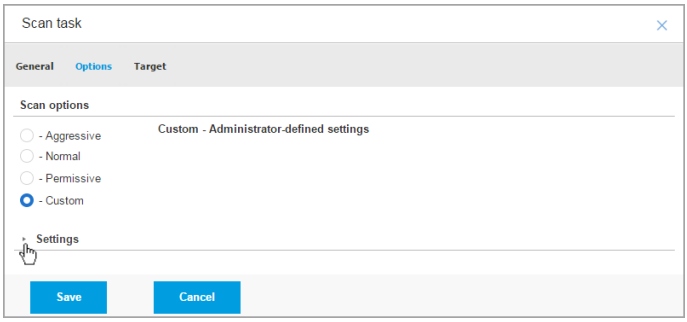
> **Note**
> This option applies to Bitdefender Endpoint Security Tools, Endpoint Security (legacy agent) and Endpoint Security for Mac.

> **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. 536).

  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.

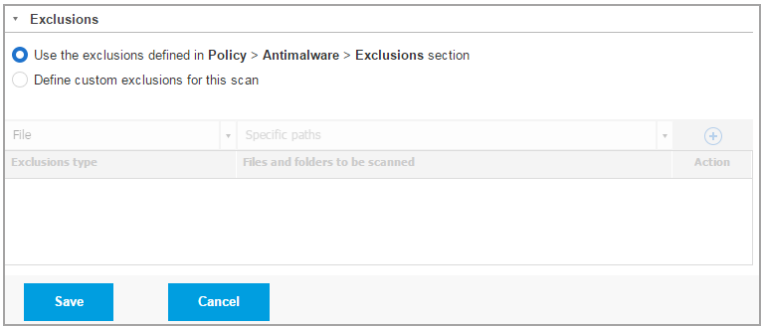
- If you have chosen **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers. For more information regarding system variables, refer to "System Variables" (p. 537).

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** section 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. 268).

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. 191).

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. 249).

Risk Scan

You can anytime choose to run on demand risk scan tasks on selected endpoints, as follows:

1. Go to the **Network** page.
2. Browse the containers from the left-side pane and select the endpoints you want to scan.
3. Click the **Tasks** button and choose **Risk Scan**.

   A message will pop up, requiring you to confirm running the risk scan task.

   Note
   The risk scan task will run with all the indicators of risk activated by default.

4. After the task has finished successfully, you can go to the Misconfigurations tab of the **Security Risks** page, analyze them and choose which indicators to ignore, if needed.

   The overall company risk score will be recalculated based on the ignored indicators of risk.

   Note
   To view the full list of indicators and their description, refer to this KB article.

Important
The **Risk Scan** tasks will not run / will fail on endpoints in the following situations:

- The endpoint does not have a Windows operating system.
- The endpoint's Bitdefender agent license is invalid.
- The policy applied to endpoint has the Risk Management module disabled.

Patch Tasks

It is recommended to regularly check for software updates and apply them as soon as possible. GravityZone automates this process through security policies, but if you need to update the software on certain endpoints right away, run the following tasks in this order:

1. Patch Scan
2. Patch Install

Prerequisites

- The security agent with Patch Management module is installed on target endpoints.
- For the scanning and installation tasks to be successful, Windows endpoints must meet these conditions:
  - **Trusted Root Certification Authorities** stores the **DigiCert Assured ID Root CA** certificate.
  - **Intermediate Certification Authorities** includes the **DigiCert SHA2 Assured ID Code Signing CA**.
  - Endpoints have installed the patches for Windows 7 and Windows Server 2008 R2 mentioned in this Microsoft article: Microsoft Security Advisory 3033929

Patch Scan

Endpoints with outdated software are vulnerable to attacks. It is recommended to regularly check the software installed on your endpoints and update it as soon as possible. To scan your endpoints for missing patches:

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 endpoints from the selected container are displayed in the right-side pane table.
4. Select the target endpoints.
5. Click the **Tasks** button at the upper side of the table and choose **Patch Scan**. A confirmation window will appear.

6. Click **Yes** to confirm the scan task.

   When the task finishes, GravityZone adds in Patch Inventory all patches your software needs. For more details, refer to "Patch Inventory" (p. 184).

You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 191).

Note
To schedule patch scanning, edit the policies assigned to the target endpoints, and configure the settings in the **Patch Management** section. For more information, refer to "Patch Management" (p. 313).

Patch Install

To install one or more patches on the target endpoints:

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 endpoints from the selected container are displayed in the right-side pane table.
4. Click the **Tasks** button at the upper side of the table and choose **Patch Install**.

   A configuration window will appear. Here, you can view all patches missing from the target endpoints.
5. If needed, use the sorting and filtering options at the upper side of the table to find specific patches.
6. Click the **Columns** button at the upper-right side of the pane to view only relevant information.
7. Select the patches you want to install.

   Certain patches depend on others. In such case, they are automatically selected once with the patch.

   Clicking the numbers of **CVEs** or **Products** will display a pane in the left side. The pane contains additional information, such as the CVEs which the patch resolves, or the products to which the patch applies. When done reading, click **Close** to hide the pane.

8. Select **Reboot endpoints after installing the patch, if required** to restart the endpoints immediately after the patch installation, if a system restart is required. Take into account that this action may disrupt the user activity.
9. Click **Install**.

   The installation task is created, together with sub-tasks for each target endpoint.

You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 191).

Note

- To schedule patch deployment, edit the policies assigned to the target endpoints, and configure the settings in the **Patch Management** section. For more information, refer to "Patch Management" (p. 313).
- You can also install a patch from the **Patch Inventory** page, starting from a certain patch that you are interested in. In this case, select the patch from the list, click the **Install** button at the upper side of the table and configure the patch installation details. For more details, refer to "Installing Patches" (p. 188).
- After installing a patch, we recommend sending a Patch Scan task to target endpoints. This action will update the patch information stored in GravityZone for your managed networks.

You can uninstall patches:

- Remotely, by sending a patch uninstall task from GravityZone.
- Locally on the endpoint. In this case, you need to log in as an administrator to the endpoint and run the uninstaller manually.

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. 336).

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

Repository type	Object format
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. 536).

    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. 191).

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.

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

When deploying the agent through a Linux Relay, the following conditions must be met:

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

  Note

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

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

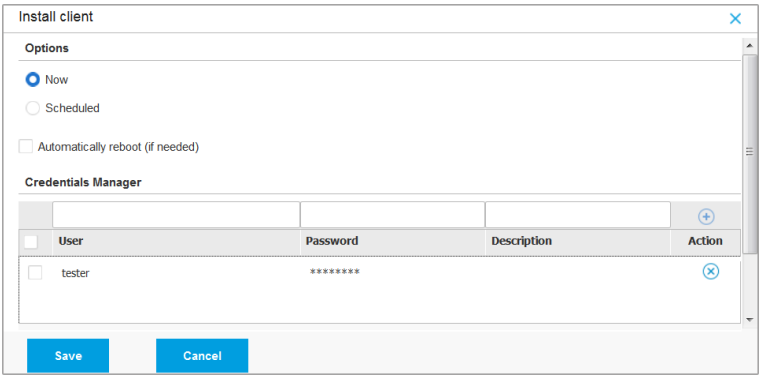
To run a remote installation task:

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.

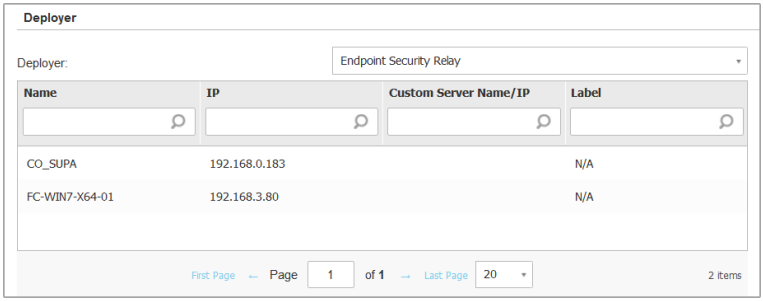
  In this case, you can also define:

  – 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.

Upgrade Client

This task is available only when Endpoint Security agent is installed and detected in the network. Bitdefender recommends upgrading from Endpoint Security to the new Bitdefender Endpoint Security Tools, for a last-generation endpoint protection.

To easily find the clients that are not upgraded, you can generate an upgrade status report. For details about how to create reports, refer to "Creating Reports" (p. 465).

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. 191).

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. 46).

Outdated clients or outdated security content 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 security content 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 security content 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. 191).

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.

Note
The **Reconfigure Client** task will remove all the unsupported modules from existing installations on legacy Windows.

You can change the installation settings from the **Network** area or from the **Endpoint Modules Status** report.

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. Select one of the following actions:

- **Add**. Add new modules besides the existing ones.
- **Remove**. Remove specific modules from the existing ones.
- **Match list**. Match the modules installed with your selection.

7. Select the modules and roles which you intend to install or remove on the target endpoints.

   Warning
   Only supported modules will install. For example, Firewall installs only on the supported Windows workstations.
   For more information, refer to GravityZone protection layers availability.

8. Select **Remove competitors, if needed** to make sure that the selected modules will not be in conflict with other security solutions installed on the target endpoints.
9. Choose one of the available scanning modes:
   - **Automatic**. The security agent detects which scanning engines are suitable for the endpoint's resources.
   - **Custom**. You explicitly choose which scanning engines to use.

     For details about the available options, refer to Creating Installation Packages section of the Installation Guide.

   Note
   This section is available only with **Match list**.

10. Under the **Scheduler** section, choose 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 (hourly, daily or weekly) and configure it according to your needs.
11. 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. 191).

Repair Client

Use the Repair Client task as an initial troubleshooting task for any number of endpoint issues. The task downloads the latest install package on the target endpoint and then performs a reinstall of the agent.

Note

- The modules currently configured on the agent will not be changed.
- The repair task will reset the security agent to the version published in the **Configuration > Update > Components** page.

To send a Repair Client task to the client:

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 repair.
5. Click the **Tasks** button at the upper side of the table and choose **Repair Client**. A confirmation window will appear.
6. Check the **I understand and agree** box and click the **Save** button to run the task.

   Note
   To finish the repair task, a client restart might be required.

   You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 191).

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. 191).

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. 191).

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. 178).

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. 191).

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. 191).

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.

Inject Custom Tool

Note
This task is related to the HVI module, which may be available for your GravityZone solution with a separate license key.

To inject tools inside the target guest operating systems:

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 from the selected container are displayed in the right-side pane table.
4. Select the check boxes of the target endpoints.
5. Click the **Tasks** button at the upper side of the table and choose **Inject Custom Tool**. A configuration window is displayed.
6. From the drop-down menu, select all tools you want to inject. For each selected tool, a collapsible section with its settings is displayed.

   These tools were previously uploaded in GravityZone. If you cannot find the right tool in the list, go to the **Tools Management Center** and add it from there. For more information, refer to "Custom Tools Injection with HVI" (p. 502).
7. For each tool displayed in the window:
   a. Click the name of the tool to view or hide its section.
   b. Enter the tool's command line, together with all needed input parameters, just like you do in Command Prompt or Terminal. For example:

```
bash script.sh <param1> <param2>
```

For BD Remediation Tools you can only select the remediation action and backup remediation action from the two drop-down menus.

c. Point the location from where the Security Server should gather the logs:

- **stdout**. Select this check box to capture the logs from the standard output communication channel.
- **Output file**. Select this check box to collect log file saved on the endpoint. In this case, you need to enter the path to where the Security Server can find the file. You can use absolute paths or system variables.

  Here you have an additional option: **Delete log files from Guest after they have been transferred**. Select it if you no longer need the files on the endpoint.

8. If you want to transfer the logs file from the Security Server to another location, you need to provide the path to the destination location and the authentication credentials.
9. Sometimes the tool may require a longer time than expected to finish its job or it may become unresponsive. To avoid crashes in such situations, in the **Safety configuration** section, choose after how many hours the Security Server should automatically terminate the tool's process.
10. Click **Save**.

    You will be able to view the task's status in the **Tasks** page. For more details, you can also check the **HVI Third Party Injection Status** report.

6.2.6. 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. 447).
6. Configure the report options. For more information, refer to "Creating Reports" (p. 465).
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.

6.2.7. 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. 218).

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. 207).

6.2.8. Using Recovery Manager for Encrypted Volumes

When endpoint users forget their encryption passwords and they cannot access encrypted volumes on their machines any longer, you can help them by retrieving recovery keys from the **Network** page.

To retrieve a recovery key:

1. Go to the **Network** page.
2. Click the **Recovery manager** button in the action toolbar of the left-side pane. A new window appears.
3. In the **Identifier** section of the window, enter the following data:
   a. The recovery key ID of the encrypted volume. The recovery key ID is a string of numbers and letters available on the endpoint, in the BitLocker recovery screen.

      On Windows, the recovery key ID is a string of numbers and letters available on the endpoint, in the BitLocker recovery screen.

      Alternately, you can use the **Recovery** option in the **Protection** tab of the computer details to automatically fill in the recovery key ID, for both Windows and macOS endpoints.

   b. The password of your GravityZone account.
4. Click **Reveal**. The window expands.

In the **Volume Information**, you are presented with the following data:

a. Volume name

b. Type of volume (boot or non-boot).

c. Endpoint name (as listed in the Network Inventory)

d. Recovery key. On Windows, the recovery key is a password generated automatically when the volume has been encrypted. On Mac, the recovery key is actually the user account password.

5. Send the recovery key to the endpoint user.

For details about encrypting and decrypting volumes with GravityZone, refer to "Encryption" (p. 357).

6.2.9. 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**.

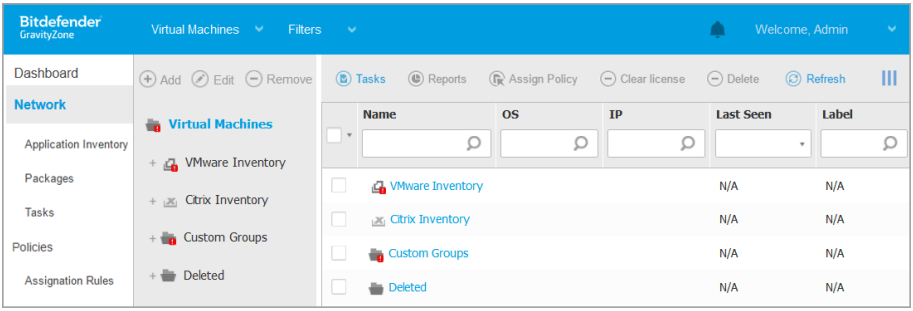
Note

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

6.3. 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. 41).



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:

- **Nutanix Inventory.** Contains the list of Nutanix Prism Element systems you have access to.
- **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.

To access 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. 200).

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

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

In the **Configuration > Network Settings** section, you can configure scheduled rules for automatic cleanup of unused virtual machines from the Network Inventory.

6.3.1. 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. 534) 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. 195).

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.
- Security content is 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.
The endpoints that do not receive any updates in the past 24 hours are automatically marked **With issues**, regardless of the security content version present on the relay or on the GravityZone Update Server.

6.3.2. Viewing Virtual Machine Details

You can obtain detailed information about each virtual machine from the **Network** page, as follows:

- Checking the **Network** page
- Checking the **Information** window

Checking the Network page

To find out details about a virtual machine, check the information available in the right-side pane table from the **Network** page.

You can add or remove columns with virtual machine information by clicking the **Columns** button at the upper-right side of the pane.

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 available in 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. 100).
5. Check the information displayed on table columns for each virtual machine.

   Use the header row to search as you type for specific virtual machines, according to the available criteria:

   - **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 endpoint. You can add a label in the virtual machine's **Information** window and then use it in searches.
   - **Policy**: the policy applied to the virtual machine, with a link for viewing or changing the policy settings.

Checking the Information window

In the right-side pane of the **Network** page, click the name of the virtual machine you are interested in to display the **Information** window. This window displays only the data available for the selected virtual machine, grouped under several tabs.

Find hereafter the exhaustive list of information you may find in the **Information** window, according to the machine type (virtual machine, Security Server instance) and its specific security information.

General tab

- General virtual machine information, such as name, FQDN information, IP address, operating system, infrastructure, parent group and current connection status.

  In this section you can assign the virtual machine with a label. You will be able to quickly find virtual machines with the same label and take actions on them, no matter where they are located in the network. For more information about filtering virtual machine, refer to "Sorting, Filtering and Searching for Virtual Machines" (p. 113).

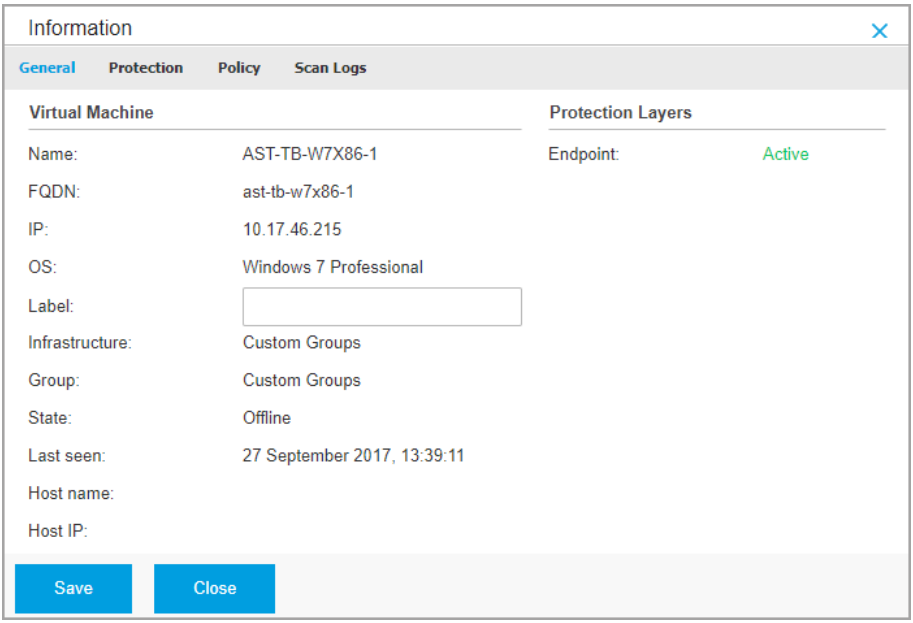
- **HVI Prerequisites**, containing information about whether you can use the Security Server to deploy HVI protection or not. Thus, if the host of the Security Server is running on a supported XenServer version and the supplemental pack is installed, you can enable HVI on virtual machines from that host.

  Note
  The HVI module may be available for your GravityZone solution with a separate license key.

- Protection layers information, including the list of security technologies acquired with your GravityZone solution and their license status, which can be:
  - **Available / Active** – the license key for this protection layer is active on the virtual machine.
  - **Expired** – the license key for this protection layer is expired.
  - **Pending** – the license key is not confirmed yet.

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

- **Relay Connection**: the name, IP and label of the relay to which the virtual machine is connected, if the case.



Information window - General tab

Protection tab

This tab contains details about each protection layer licensed on the endpoint. Details refer to:

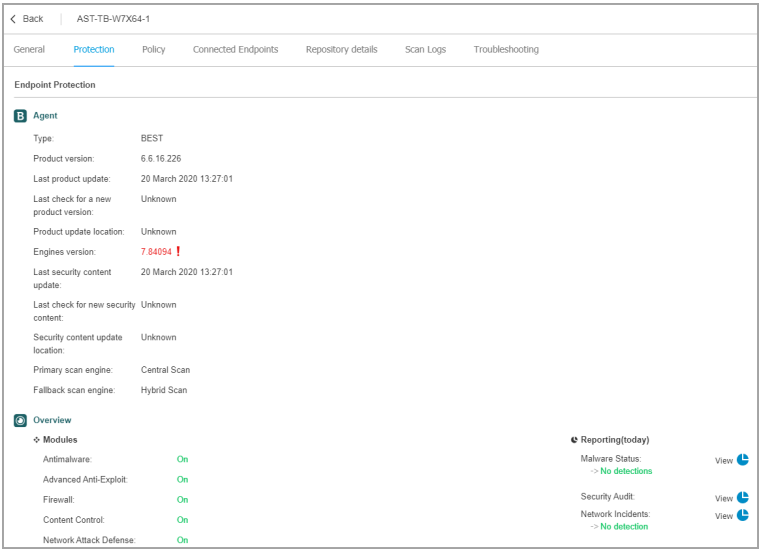
- Security agent information like product name and version, scanning engines configuration and update status. For Exchange Protection, antispam engine and signatures versions are also available.
- Security status for each protection layer. This status appears at the right side of the protection layer's name:
  - **Secure**, when there are no security issues reported on the endpoints applied with the protection layer.
  - **Vulnerable**, when there are security issues reported on the endpoints applied with the protection layer. For more details, refer to "Security Status" (p. 102).
- Associated Security Server. Each assigned Security Server is 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. 465)
- Information regarding the Sandbox Analyzer protection layer:
  - Sandbox Analyzer usage status on the virtual machine, displayed at the right side of the window:
    - **Active**: Sandbox Analyzer is licensed (available) and enabled via policy on the virtual machine.
    - **Inactive**: Sandbox Analyzer is licensed (available) but not enabled via policy on the virtual machine.
  - Name of the agent that acts as feeding sensor.
  - Module status on the virtual machine:
    - **On** - Sandbox Analyzer is enabled on the virtual machine via policy.
    - **Off** - Sandbox Analyzer is not enabled on the virtual machine via policy.
  - Threat detections in the last week by clicking the **View** link to access the report.
- Additional information regarding the Encryption module, such as:
  - Detected volumes (mentioning the boot drive).
  - Encryption status for each volume (which can be **Encrypted**, **Encryption in progress**, **Decryption in progress**, **Unencrypted**, **Locked** or **Paused**).

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. 152).



Information window - Protection tab

For Security Servers, this tab contains information about the Storage Protection module. Details refer to:

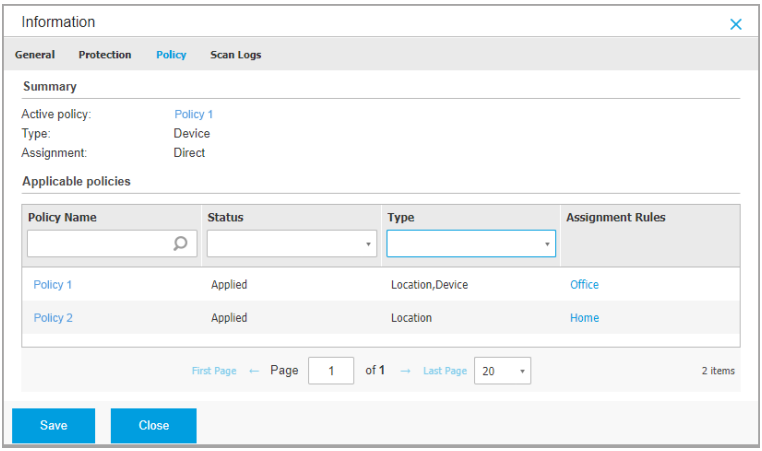
- Service status:
  - **N/A** – Storage Protection is licensed, but the service is not configured yet.
  - **Enabled** – the service is enabled in the policy and functioning.
  - **Disabled** – the service is not functioning either because it has been disabled from the policy or the license key has expired.
- List of connected ICAP-compliant storage devices with the following details:
  - Storage device name
  - Storage device IP
  - Storage device type
  - The date and time of the last communication between the storage device and Security Server.

Policy tab

A virtual machine can be applied with one or more policies, but only one policy can be active at a time. The **Policy** tab displays information about all policies that apply to the virtual machine.

- The active policy name. Click the policy name to open the policy template and view its settings.
- The active policy type, which can be:
  - **Device**: when the policy is manually assigned to the virtual machine by the network administrator.
  - **Location**: a rule-based policy automatically assigned to the virtual machine if the virtual machine's network settings match the given conditions of an existing assignment rule.
  - **User**: a rule-based policy automatically assigned to the endpoint if it matches the Active Directory target specified in an existing assignment rule.

    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.
  - **External (NSX)**: when the policy is defined in the VMware NSX environment.
- The active policy assignment type, which can be:
  - **Direct**: when the policy is directly applied to the virtual machine.
  - **Inherited**: when the virtual machine inherits the policy from a parent group.
- **Applicable policies**: displays the list of policies linked to existing assignment rules. These policies may apply to the virtual machine when it matches the given conditions of the linked assignment rules.

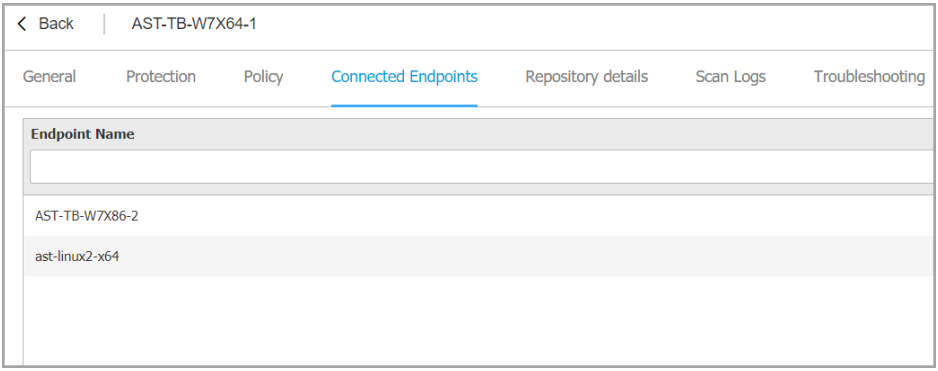


Information window - Policy tab

For more information regarding policies, refer to "Managing Policies" (p. 205)

Relay tab

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.



Information window - Relay tab

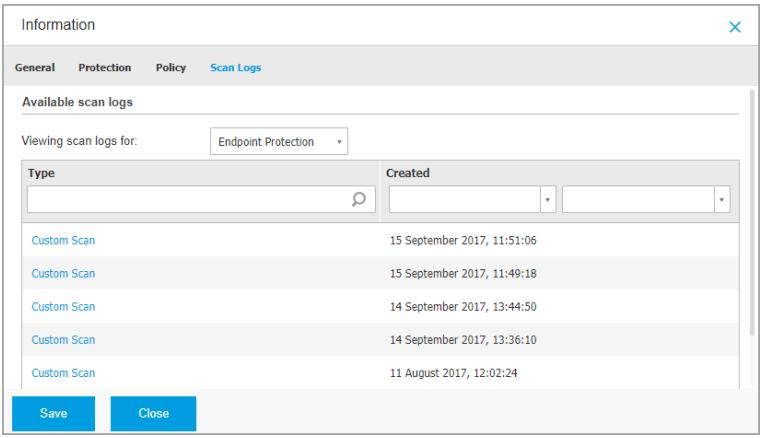
Scan Logs tab

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

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.

6.3.3. 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 Nutanix Prism Element are grouped under the **Nutanix Inventory** 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 Nutanix Inventory, 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 Nutanix Prism, 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. 204).

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**.

6.3.4. 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.

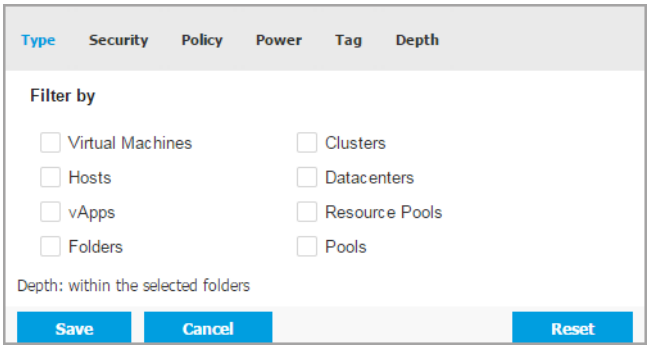
Sorting Virtual Machines

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

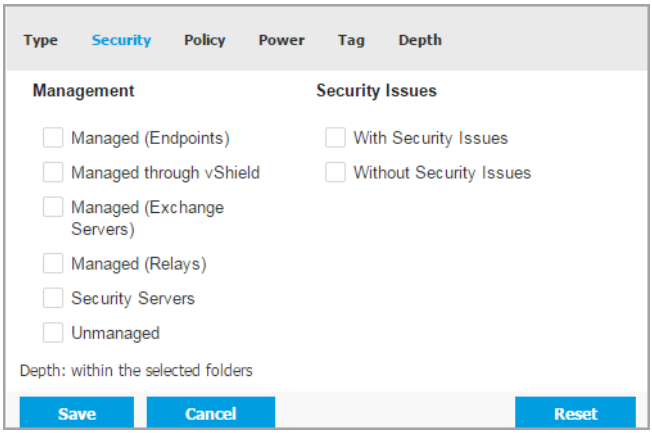
Filtering Virtual Machines

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.



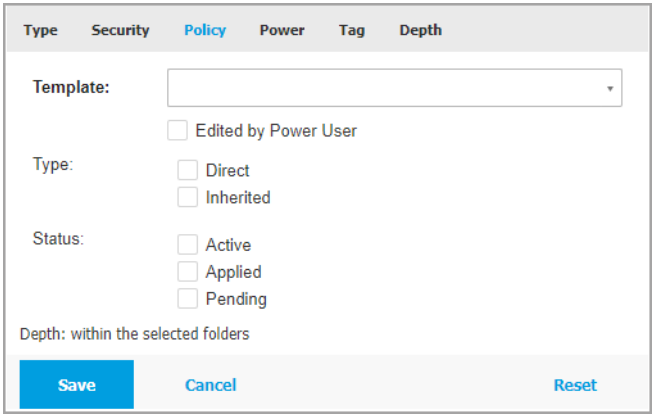
Virtual Machines - Filter by Type

   - **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.



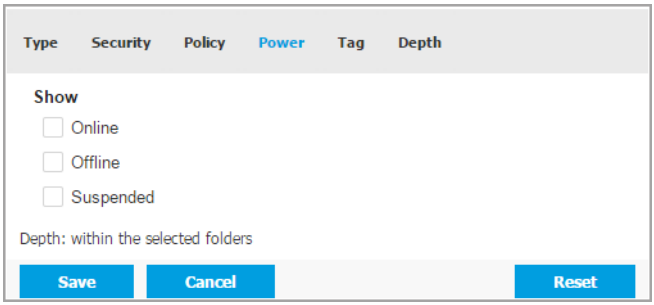
Virtual Machines - Filter by Security

- **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).



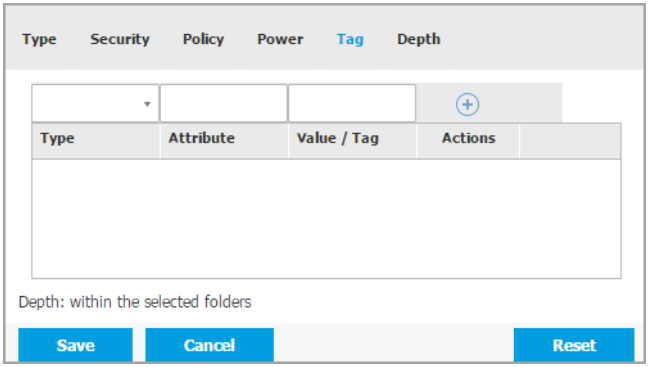
Virtual Machines - Filter by Policy

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



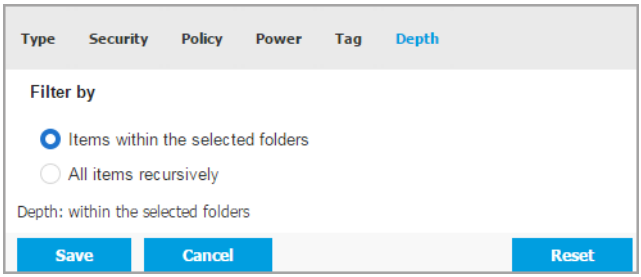
Virtual Machines - Filter by Power

- **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.

6.3.5. 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. 118)
- “Patch Tasks” (p. 127)
- “Exchange Scan” (p. 130)
- “Install” (p. 134)
- “Uninstall Client” (p. 138)
- “Update” (p. 139)
- “Reconfigure Client” (p. 140)

- "Network Discovery" (p. 141)
- "Applications Discovery" (p. 142)
- "Restart Machine" (p. 142)
- "Install Security Server" (p. 143)
- "Uninstall Security Server" (p. 146)
- "Update Security Server" (p. 146)
- "Install HVI Supplemental Pack" (p. 147)
- "Uninstall HVI Supplemental Pack" (p. 148)
- "Update HVI Supplemental Pack" (p. 148)

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.

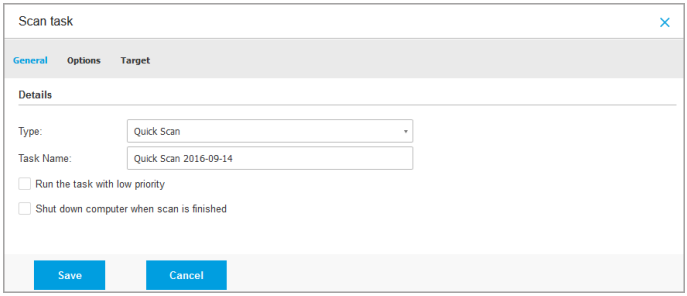
You can view and manage the task in the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 191).

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.

> **Note**
> This option applies only to Bitdefender Endpoint Security Tools and Endpoint Security (legacy agent).

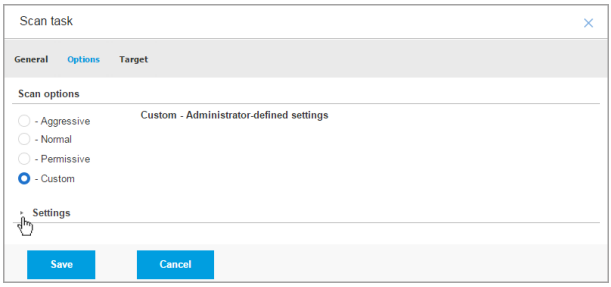
– **Shut down computer when scan is finished**. Select this check box to turn off your machine if you do not intend to use it for a while.

> **Note**
> This option applies to Bitdefender Endpoint Security Tools, Endpoint Security (legacy agent) and Endpoint Security for Mac.

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. 536).

  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.

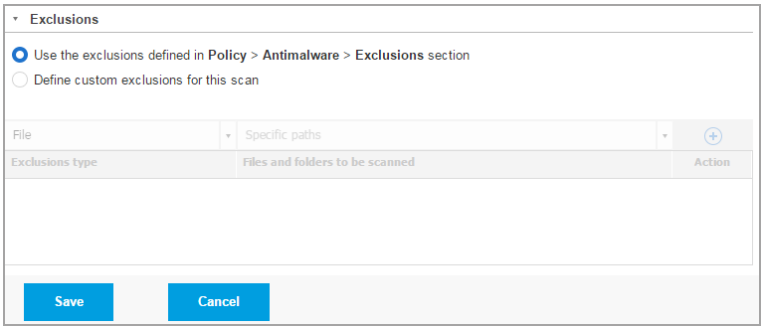
- If you have chosen a predefined location, complete the path as needed. For example, to scan the entire `Program Files` folder, it suffices to select the corresponding predefined location from the drop-down menu. To scan a specific folder from `Program Files`, you must complete the path by adding a 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. 537).

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** section 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. 268).

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. 191).

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. 249).

Patch Tasks

It is recommended to regularly check for software updates and apply them as soon as possible. GravityZone automates this process through security policies, but if you need to update the software on certain virtual machines right away, run the following tasks in this order:

1. Patch Scan
2. Patch Install

Prerequisites

- The security agent with Patch Management module is installed on target machines.

- For the scanning and installation tasks to be successful, Windows machines must meet these conditions:
  - **Trusted Root Certification Authorities** stores the **DigiCert Assured ID Root CA** certificate.
  - **Intermediate Certification Authorities** includes the **DigiCert SHA2 Assured ID Code Signing CA**.
  - Endpoints have installed the patches for Windows 7 and Windows Server 2008 R2 mentioned in this Microsoft article: Microsoft Security Advisory 3033929

Patch Scan

Virtual machines with outdated software are vulnerable to attacks. It is recommended to regularly check the software installed on your machines and update it as soon as possible. To scan your virtual machines for missing patches:

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 endpoints from the selected container are displayed in the right-side pane table.
4. Select the target endpoints.
5. Click the **Tasks** button at the upper side of the table and choose **Patch Scan**. A confirmation window will appear.
6. Click **Yes** to confirm the scan task.

   When the task finishes, GravityZone adds in Patch Inventory all patches your software needs. For more details, refer to “Patch Inventory” (p. 184).

You can view and manage the task on the **Network > Tasks** page. For more information, refer to “Viewing and Managing Tasks” (p. 191).

Note
To schedule patch scanning, edit the policies assigned to the target machines, and configure the settings in the **Patch Management** section. For more information, refer to “Patch Management” (p. 313).

Patch Install

To install one or more patches on the target 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 endpoints from the selected container are displayed in the right-side pane table.
4. Click the **Tasks** button at the upper side of the table and choose **Patch Install**.

   A configuration window will appear. Here, you can view all patches missing from the target virtual machines.
5. If needed, use the sorting and filtering options at the upper side of the table to find specific patches.
6. Click the **Columns** button at the upper-right side of the pane to view only relevant information.
7. Select the patches you want to install.

   Certain patches depend on others. In such case, they are automatically selected once with the patch.

   Clicking the numbers of **CVEs** or **Products** will display a pane in the left side. The pane contains additional information, such as the CVEs which the patch resolves, or the products to which the patch applies. When done reading, click **Close** to hide the pane.
8. Select **Reboot endpoints after installing the patch, if required** to restart the endpoints immediately after the patch installation, if a system restart is required. Take into account that this action may disrupt the user activity.
9. Click **Install**.

   The installation task is created, together with sub-tasks for each target virtual machines.

You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 191).

Note

- To schedule patch deployment, edit the policies assigned to the target machines, and configure the settings in the **Patch Management** section. For more information, refer to "Patch Management" (p. 313).
- You can also install a patch from the **Patch Inventory** page, starting from a certain patch that you are interested in. In this case, select the patch from the list, click

the **Install** button at the upper side of the table and configure the patch installation details. For more details, refer to "Installing Patches" (p. 188).

- After installing a patch, we recommend sending a Patch Scan task to target endpoints. This action will update the patch information stored in GravityZone for your managed networks.

You can uninstall patches:

- Remotely, by sending a patch uninstall task from GravityZone.
- Locally on the machine. In this case, you need to log in as an administrator to the endpoint and run the uninstaller manually.

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. 336).

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. 536).

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. 191).

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.

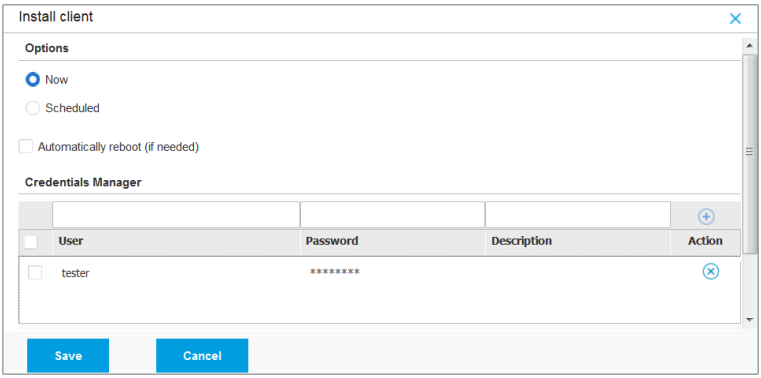
To remotely install the Security for Virtualized Environments protection on one or several virtual machines:

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

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

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

- Target Linux and Mac endpoints must have SSH enabled 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. 191).

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. 102).

Outdated clients or outdated security content 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 security content 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 security content 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. 191).

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. 191).

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. 191).

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. 178).

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. 191).

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.

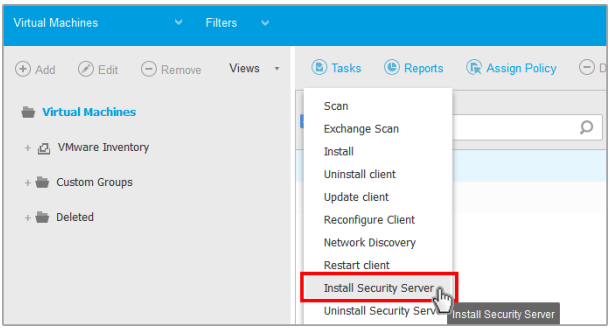
Install Security Server

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 Nutanix, VMware or Citrix inventory and select the check boxes corresponding to the desired hosts or containers (Nutanix Prism, vCenter Server, XenServer or datacenter). For a fast selection, you can directly select the root container (Nutanix Inventory, VMware Inventory or Citrix Inventory). You will be able to select hosts individually from the installation wizard.

   Note
   You cannot select hosts from different folders.

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



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

19. You can view and manage the task on the **Network > Tasks** page. For more information, refer to "Viewing and Managing Tasks" (p. 191).

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. 191).

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. 191).

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

Note
The HVI module may be available for your GravityZone solution with a separate license key.

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. Install the latest HVI Supplemental Pack available.

   For more information, refer to “Install HVI Supplemental Pack” (p. 147).

2. Go to the **Network** page.
3. 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 **Update HVI Supplemental Pack**. The configuration window opens.
7. 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.
8. Select **Automatically reboot (if needed)** if you want to restart the host unattended. Otherwise, you must restart the host manually to apply the update.
9. Click **Save**. A confirmation message will appear.

You can check the task status in the **Network > Tasks** page.

Inject Custom Tool

Note
This task is related to the HVI module, which may be available for your GravityZone solution with a separate license key.

To inject tools inside the target guest operating systems:

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 endpoints from the selected container are displayed in the right-side pane table.
4. Select the check boxes of the target endpoints.
5. Click the **Tasks** button at the upper side of the table and choose **Inject Custom Tool**. A configuration window is displayed.

6. From the drop-down menu, select all tools you want to inject. For each selected tool, a collapsible section with its settings is displayed.

   These tools were previously uploaded in GravityZone. If you cannot find the right tool in the list, go to the **Tools Management Center** and add it from there. For more information, refer to "Custom Tools Injection with HVI" (p. 502).

7. For each tool displayed in the window:

   a. Click the name of the tool to view or hide its section.

   b. Enter the tool's command line, together with all needed input parameters, just like you do in Command Prompt or Terminal. For example:

   ```
   bash script.sh <param1> <param2>
   ```

   For BD Remediation Tools you can only select the remediation action and backup remediation action from the two drop-down menus.

   c. Point the location from where the Security Server should gather the logs:

   - **stdout**. Select this check box to capture the logs from the standard output communication channel.
   - **Output file**. Select this check box to collect log file saved on the endpoint. In this case, you need to enter the path to where the Security Server can find the file. You can use absolute paths or system variables.

     Here you have an additional option: **Delete log files from Guest after they have been transferred**. Select it if you no longer need the files on the endpoint.

8. If you want to transfer the logs file from the Security Server to another location, you need to provide the path to the destination location and the authentication credentials.

9. Sometimes the tool may require a longer time than expected to finish its job or it may become unresponsive. To avoid crashes in such situations, in the **Safety configuration** section, choose after how many hours the Security Server should automatically terminate the tool's process.

10. Click **Save**.

    You will be able to view the task's status in the **Tasks** page. For more details, you can also check the **HVI Third Party Injection Status** report.

6.3.6. 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. 447).
7. Configure the report options. For more information, refer to "Creating Reports" (p. 465)
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.

6.3.7. 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. 204)

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. 207).

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.

6.3.8. Using Recovery Manager for Encrypted Volumes

When endpoint users forget their encryption passwords and they cannot access encrypted volumes on their machines any longer, you can help them by retrieving recovery keys from the **Network** page.

To retrieve a recovery key:

1. Go to the **Network** page.
2. Click the **Recovery manager** button in the action toolbar of the left-side pane. A new window appears.

3. In the **Identifier** section of the window, enter the following data:
   a. The recovery key ID of the encrypted volume. The recovery key ID is a string of numbers and letters available on the endpoint, in the BitLocker recovery screen.

      On Windows, the recovery key ID is a string of numbers and letters available on the endpoint, in the BitLocker recovery screen.

      Alternately, you can use the **Recovery** option in the **Protection** tab of the virtual machine details to automatically fill in the recovery key ID, for both Windows and macOS endpoints.

   b. The password of your GravityZone account.
4. Click **Reveal**. The window expands.

   In the **Volume Information**, you are presented with the following data:
   a. Volume name
   b. Type of volume (boot or non-boot).
   c. Endpoint name (as listed in the Network Inventory)
   d. Recovery key. On Windows, the recovery key is a password generated automatically when the volume has been encrypted. On Mac, the recovery key is actually the user account password.
5. Send the recovery key to the endpoint user.

For details about encrypting and decrypting volumes with GravityZone, refer to "Encryption" (p. 357).

6.4. 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

6.4.1. 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.

6.4.2. 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.

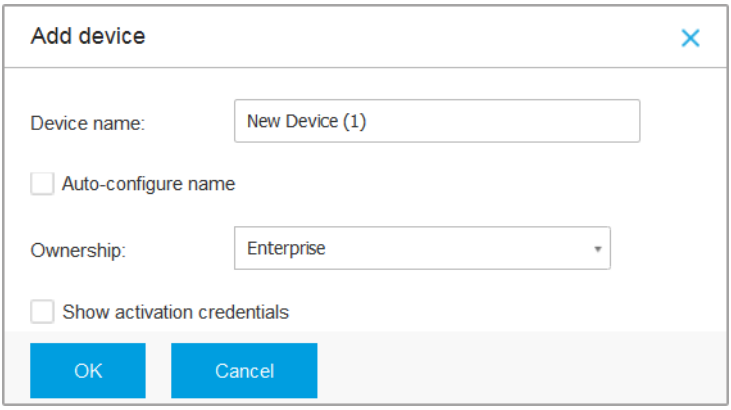
Adding a device to a single user

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

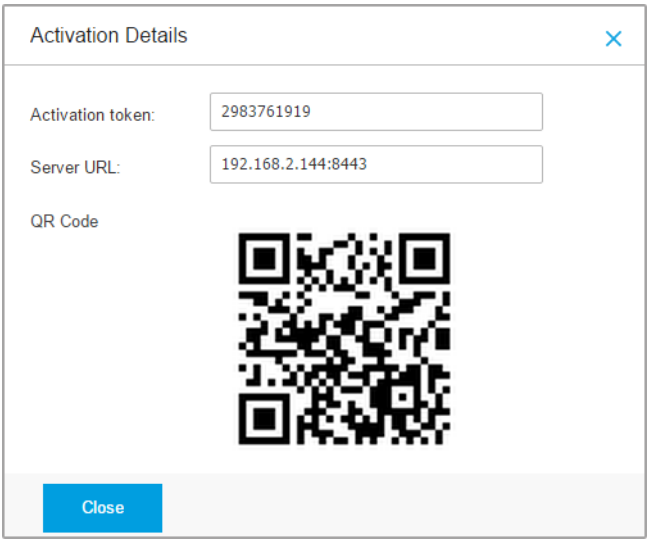
5. Configure the mobile device details:
   a. Enter a suggestive name for the device.
   b. Use the **Auto-configure name** option if you want the device name to be automatically generated. When added, the device has a generic name. Once

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. 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.

3. 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.
4. 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.

6.4.3. 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**.

6.4.4. 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. 534) 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. 175)

6.4.5. 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. 371).

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. 175)

6.4.6. 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. 175).

  - **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. 371).

  - **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.

  Important
  Starting with Android 10, GravityZone Mobile Client does not have access to the serial number, IMEI, IMSI, and MAC address of the device. This restriction leads to the following situations:
  - If the mobile device, already having GravityZone Mobile Client installed, upgrades from an older Android version to Android 10, Control Center will display the correct device details. Before upgrade, the device must run the latest version of GravityZone Mobile Client.
  - If GravityZone Mobile Client installs on an Android 10 device, Control Center will display inaccurate details about that device because of the limitation imposed by the operating system.

- **Network**. You can view here network connectivity information, available only for managed (activated) devices.

6.4.7. 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.

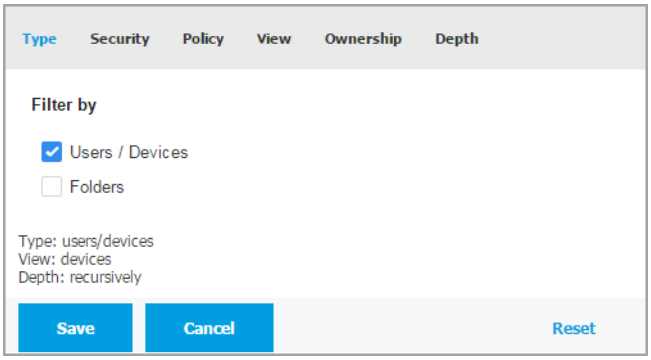
If there are too many entries, you can use the filter options to display only the entities you are interested in. For example, you can search for a specific mobile device or choose to view only the managed devices.

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.

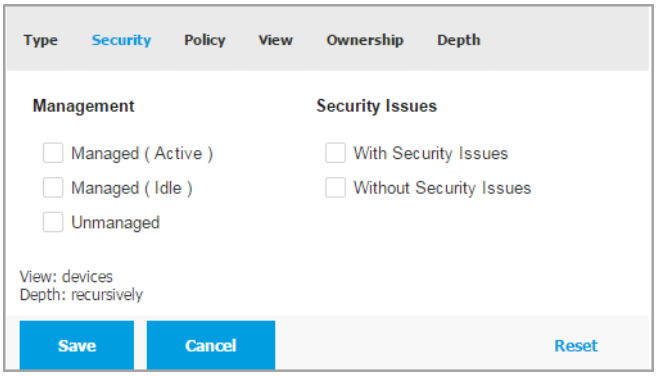
Filtering the Mobile Devices Inventory

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).



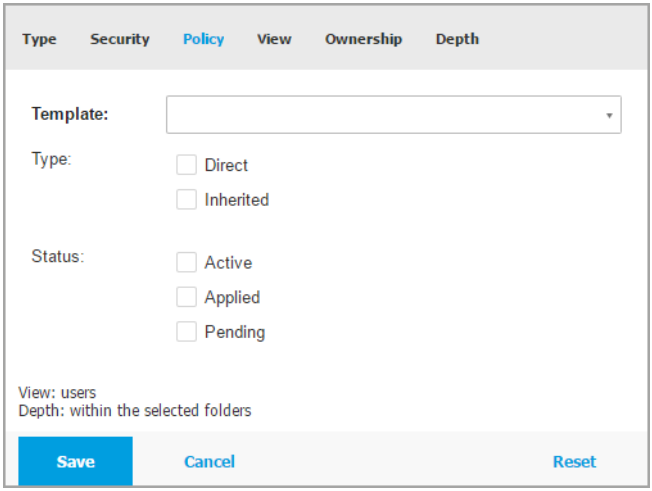
Mobile devices - Filter by Type

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



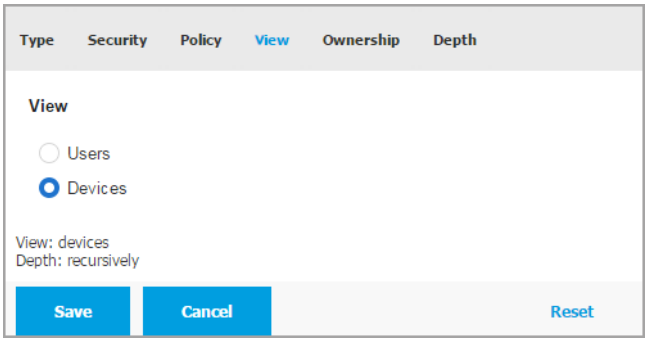
Mobile devices - Filter by Security

- **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).



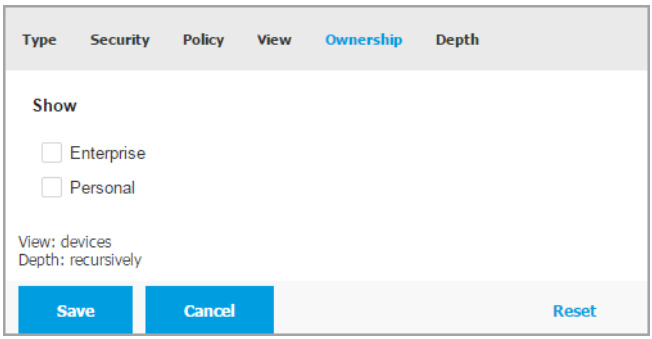
Mobile devices - Filter by Policy

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



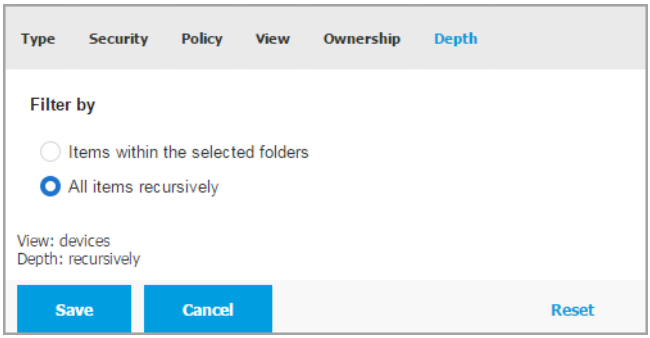
Mobile devices - Filter by View

- **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.

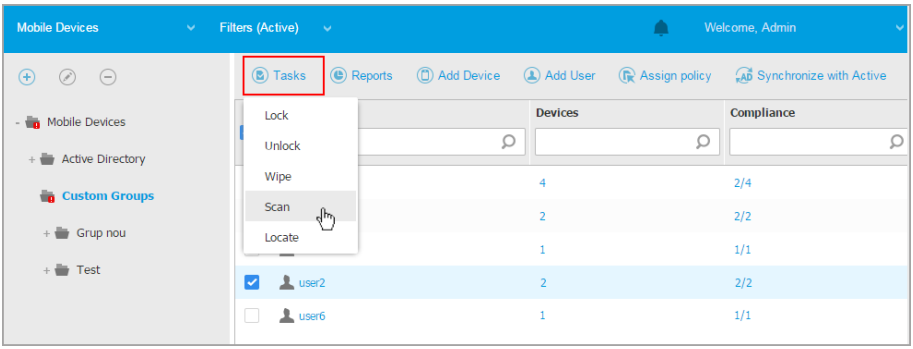
     For example, switch to the **Devices** view, click the **OS** list box and select **Android** to view only Android mobile devices.

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

6.4.8. 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. 171)
- "Wipe" (p. 172)
- "Scan" (p. 173)
- "Locate" (p. 174)



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. 191).

Lock

The Lock task immediately locks the screen of target mobile devices. The Lock task behavior is operating system dependent:

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

  Note

  - The lock screen password generated by Control Center is displayed in the Mobile Device Details window.
  - Unlock task is no longer available for Android devices (7.0 or above). Instead, users can unlock their devices manually. However, you must make sure in advance that those devices support the expected complexity requirements for the unlock password.
  - Due to technical limitations, Lock task is unavailable on Android 11.

- 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. 191).

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.

Note
Due to technical limitations, Wipe task is unavailable on Android 11.

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. 191).

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. 191).

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. 191).

6.4.9. 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. 463)
7. Configure the report options. For more information, refer to "Creating Reports" (p. 465)
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.

6.4.10. 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. 207).

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. 366)

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. 207).

6.4.11. 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.

6.4.12. 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.
> - 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**.

6.5. Application Inventory

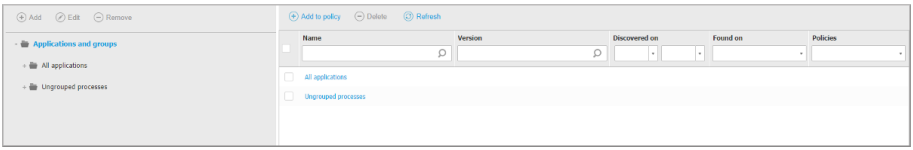
You can view all the applications discovered in your network by the **Applications Discovery** task, in the **Applications and groups** section. For more information, refer to "Applications Discovery" (p. 92).

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:

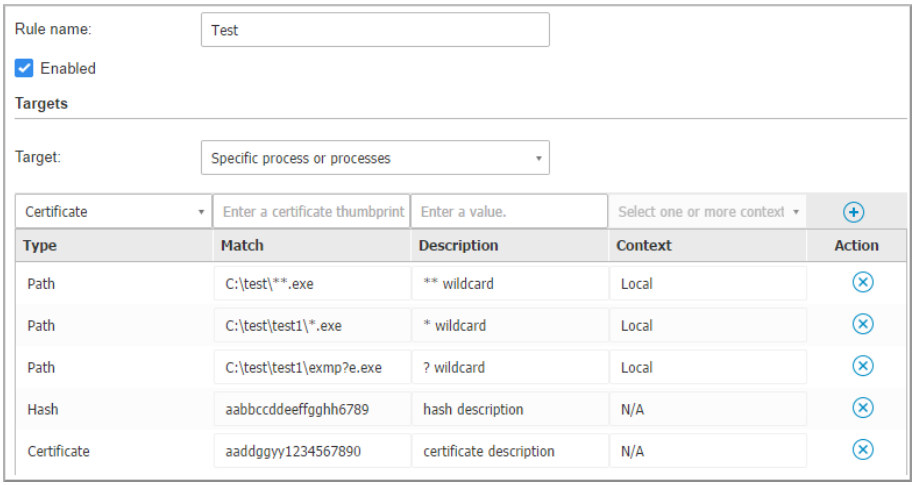
1. Select the desired folder from the **Applications and groups** tree. The folder contents is listed in the right-side pane.
2. Select the processes or applications that you want from the right-side pane.
3. Click the **Add to policy** button to open the configuration window.
4. In the **Apply rule 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. 539)

     - 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. 539)



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.

6.6. Patch Inventory

GravityZone discovers the patches your software needs through **Patch Scan** tasks and then adds it to the patch inventory.

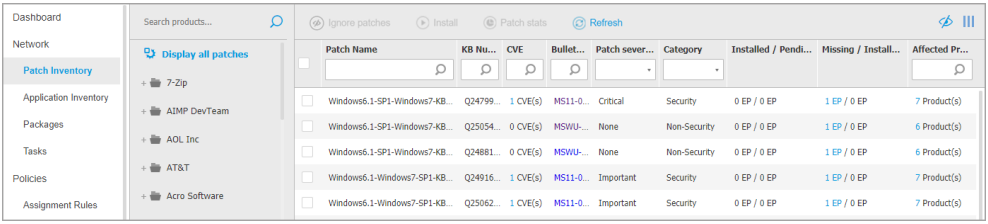
The **Patch Inventory** page displays all patches discovered for the software installed on your endpoints and provides several actions you can take on these patches.

Use Patch Inventory whenever you need to deploy immediately certain patches. This alternative allows you to easily resolve certain issues you are aware of. For example, you have read an article about a software vulnerability and you know the CVE ID. You can search the inventory for the patches addressing that CVE and then view which endpoints should be updated.

To access Patch Inventory, click the **Network > Patch Inventory** option in the main menu of Control Center.

The page is organized in two panes:

- The left-side pane displays the software products installed in your network, grouped by vendor.
- The right-side pane displays a table with available patches and details about them.



Patch Inventory

Next, you will learn how to use the inventory. This is what you can do:

- View patch details
- Search and filter patches
- Ignore patches
- Install patches
- Uninstall patches

- Create patch statistics

6.6.1. Viewing Patch Details

The patches table provides information that helps you identify patches, evaluate their importance, view their installation status and scope. The details are described herein:

- **Patch name.** This is the name of the executable file containing the patch.
- **KB number.** This number identifies the KB article that announces the patch release.
- **CVE.** This is the number of CVEs addressed by the patch. Clicking the number will display the list of CVE IDs.
- **Bulletin ID.** This is the ID of the security bulletin issued by the vendor. This ID links to the actual article, which describes the patch and provides installation details.
- **Patch severity.** This rating informs you of the patch importance relative to the damages it prevents.
- **Category.** Based on the type of issues they resolve, patches are groups in two categories: security and non-security. This field informs you in which category the patch is.
- **Installed / Pending installation.** These numbers show how many endpoints have the patch installed and how many are waiting for the patch to be installed. The numbers link to the list of these endpoints.
- **Missing / Installation failed.** These numbers show how many endpoints do not have the patch installed and on how many installation failed. The numbers link to the list of these endpoints.
- **Affected products.** This is the number of products for which the patch was released. The number links to the list of these software products.
- **Removable.** If you need to rollback a certain patch, you must first check if the patch can be uninstalled. Use this filter to find out which patches can be removed (rolled back). For more information, refer to Uninstall patches.

To customize the 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.

While you are on the page, GravityZone processes that run in the background may affect the database. Make sure you view the latest information in the table by clicking the **Refresh** button at the upper side of the table.

GravityZone reviews once a week the list of available patches and deletes those that are no longer applicable because either the related applications or the endpoints do not exist anymore.

GravityZone also reviews and deletes daily the patches unavailable in the list, although they may be present on some endpoints.

6.6.2. Searching and Filtering Patches

By default, Control Center displays all available patches for your software. GravityZone provides you with several options to quickly find the patches you need.

Filtering patches by product

1. Locate the product in the left side pane.

   You can do this either by scrolling the list to find its vendor, or by typing its name in the search box at the upper side of the pane.

2. Click the vendor's name to expand the list and view its products.
3. Select the product to view the available patches, or deselect it to hide its patches.
4. Repeat the previous steps for the other products you are interested in.

If you want to view patches for all products again, click the **Display all patches** button at the upper side of the left-side pane.

Filtering patches by utility

A patch becomes needless if, for example, itself or a newer version is already deployed on the endpoint. Because the inventory may contain at some point such patches, GravityZone allows you to ignore them. Select these patches and then click the **Ignore patches** button at the upper side of the table.

Control Center displays ignored patches in a different view. Click the **Managed/Ignored** button at the right side of the Action Toolbar to switch between views:

- - to view ignored patches.
- - to view managed patches.

Filtering patches by details

Use the power of search to filter patches after certain criteria or after known details. Enter the search terms in the search boxes at the upper side of the patches table. Matching patches are displayed in the table as you type, or upon the selection made.

Clearing the search fields will reset the search.

6.6.3. Ignoring Patches

You may need to exclude certain patches from patch inventory, if you do not plan to install them on your endpoints, by using the **Ignore patches** command.

An ignored patch will be excluded from automatic patch tasks and patch reports, and it will not be counted as a missing patch.

To ignore a patch:

1. In the **Patch Inventory** page, select one or several patches you want to ignore.
2. Click the **Ignore Patches** button at the upper side of the table.

   A configuration window will appear, where you can view details about the selected patches, together with any subordinate patches.
3. Click **Ignore**. The patch will be removed from the patch inventory list.

You can find ignored patches in a specific view and take actions on them:

- Click **Display ignored patches** button at the upper-right side of the table. You will view the list of all ignored patches.
- You can obtain more information about a certain ignored patch by generating a patch statistics report. Select the ignored patch that you want and click the **Patch stats** button at the upper side of the table. For more details, refer to "Creating Patch Statistics" (p. 191)
- To restore ignored patches, select them and click the **Restore patches** button at the upper side of the table.

  A configuration window will appear, where you can view details about the selected patches.

  Click the **Restore** button to send the patch to the inventory.

6.6.4. Installing Patches

To install patches from Patch Inventory:

1. Go to **Network > Patch Inventory**.
2. Locate the patches you want to install. If necessary, use the filtering options to quickly find them.
3. Select the patches and then click the **Install** button at the upper side of the table. A configuration window will appear, where you can edit the patch install details.

   You will view the selected patches, together with any subordinate patches.

   - Select the target groups of endpoints.
   - **Reboot endpoints after installing the patch, if required**. This option will restart the endpoints immediately after the patch installation, if a system restart is required. Take into account that this action may disrupt the user activity.

     Leaving this option disabled means that, if a system restart is needed on target endpoints, they will display the pending restart status icon in the GravityZone network inventory. In this case, you have the following options:

     – Send a **Restart machine** task to pending restart endpoints at any time you choose. For more details, refer to "Restart Machine" (p. 91).

     – Configure the active policy to notify the endpoint user that a restart is needed. To do that, access the active policy on the target endpoint, go to **General > Notifications** and enable the option **Endpoint Restart Notification**. In this case, the user will receive a pop-up each time a restart is needed due to changes made by the specified GravityZone components (in this case, Patch Management). The pop-up provides the option to postpone the reboot. If the user chooses to postpone, the restart notification will appear on-screen periodically, until the user restarts the system or until the time set by the Company Administrator has passed.

       For more details, refer to "Endpoint Restart Notification" (p. 224).
4. Click **Install**.

   The installation task is created, together with sub-tasks for each target endpoint.

Note

- You can also install a patch from the **Network** page, starting from the specific endpoints you want to manage. In this case, select the endpoints from the network inventory, click the **Tasks** button at the upper side of the table and choose **Patch Install**. For more information, refer to "Patch Install" (p. 77).
- After installing a patch, we recommend sending a Patch Scan task to target endpoints. This action will update the patch information stored in GravityZone for your managed networks.

6.6.5. Uninstalling Patches

You may need to remove patches that caused malfunctions on the target endpoints. GravityZone provides a rollback feature for patches installed in your network, which restores software to its previous state before applying the patch.

The uninstall feature is available for removable patches only. The GravityZone patch inventory includes a **Removable** column, where you can filter patches by their removability.

Note
The removability attribute depends upon how the patch was issued by the manufacturer or the changes made by the patch to the software. For patches that cannot be removed, you may need to reinstall the software.

To uninstall a patch:

1. Go to **Network > Patch Inventory**.
2. Select the patch you want to uninstall. To search for a specific patch, use the filters available on columns, such as KB number or CVE. Use the **Removable** column to display only the available patches that can be uninstalled.

   Note
   You can uninstall only one patch at a time for one or several endpoints.

3. Click the **Uninstall** button at the upper side of the table. A configuration window will appear, where you can edit the uninstall task details.
   - **Task name**. You can edit the default name of the patch uninstall task, if you want. Thus, you will identify easier the task in the **Tasks** page.

- **Add patch to the list of ignored patches**. Usually, you will not need any more a patch you want to uninstall. This option automatically adds the patch to the ignored list, once the patch is uninstalled.
- **Reboot endpoints after uninstalling the patch, if required**. This option will restart the endpoints immediately after the patch uninstallation, if a system restart is required. Take into account that this action may disrupt the user activity.

  Leaving this option disabled means that, if a system restart is needed on target endpoints, they will display the pending restart status icon in the GravityZone network inventory. In this case, you have the following options:

  – Send a **Restart machine** task to pending restart endpoints at any time you choose. For more details, refer to "Restart Machine" (p. 91).

  – Configure the active policy to notify the endpoint user that a restart is needed. To do that, access the active policy on the target endpoint, go to **General > Notifications** and enable the option **Endpoint Restart Notification**. In this case, the user will receive a pop-up each time a restart is needed due to changes made by the specified GravityZone components (in this case, Patch Management). The pop-up provides the option to postpone the reboot. If the user chooses to postpone, the restart notification will appear on-screen periodically, until the user restarts the system or until the time set by the Company Administrator field has passed.

    For more details, refer to "Endpoint Restart Notification" (p. 224).

- Under **Rollback targets** table, select the endpoints on which you want to uninstall the patch.

  You can select one or several endpoints from your network. Use the available filters to locate the endpoint that you want.

  Note
  The table displays only the endpoints where the selected patch is installed.

4. Click **Confirm**. A **Patch Uninstall** task will be created and sent to target endpoints.

   A **Patch Uninstall** report is automatically generated for each finished patch uninstall task, providing details about the patch, the target endpoints and the uninstall patch task status.

Note
After uninstalling a patch, we recommend sending a Patch Scan task to target endpoints. This action will update the patch information stored in GravityZone for your managed networks.

6.6.6. Creating Patch Statistics

If you need details about the status of a certain patch for all endpoints, use the **Patch stats** functionality, which generates an instant report for the selected patch:

1. In the **Patch Inventory** page, select the patch that you want from the right pane.
2. Click the **Patch stats** button at the upper side of the table.

   A patch statistics report shows up, providing various patch status details, including:

   - A pie chart, showing the percentage of installed, failed, missing and pending patch status for the endpoints that have reported the patch.
   - A table displaying the following information:
     - **Name**, **FQDN**, **IP** and **OS** of each endpoint that has reported the patch.
     - **Last Check**: the time when the patch was last checked on the endpoint.
     - **Patch Status**: installed, failed, missing or ignored.

Note
The patch stats functionality is available for both managed and ignored patches.

6.7. 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.

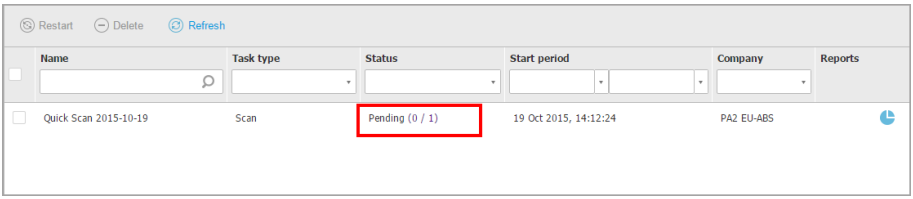
You can do the following from the **Network > Tasks** page:

- Check the task status
- View task reports
- Restart tasks
- Stop Exchange scan tasks
- Delete tasks

6.7.1. 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.

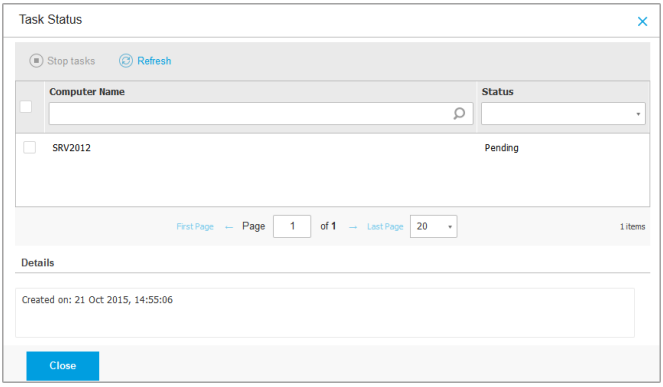
- **Checking the sub-tasks status**.

  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.

6.7.2. 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. 446).

6.7.3. 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.

6.7.4. 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.

6.7.5. 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.

6.8. Deleting Endpoints from Network Inventory

The Network inventory contains by default the **Deleted** folder, designated for storing endpoints that you do not want to manage.

However, the **Delete** action has different effects on endpoints, depending on the folder they are in:

- For endpoints in the **Custom Groups** folder:

  For endpoints in the **Computers and Groups** folder:

- When unmanaged endpoints are deleted, they are moved directly to the **Deleted** folder.
- When a managed endpoint is deleted:
  - An uninstall client task is created.
  - A license seat is released.
  - The endpoints are moved to the **Deleted** folder.

    You can view the uninstall client task in the **Network > Tasks** section. If the endpoint does not receive the task (because it is offline), the task will stay in pending for 72 hours, after which it will automatically expire.

    Note

    - If you want to exclude permanently certain endpoints from management, you must keep them in the **Deleted** folder.
    - If you delete endpoints from the **Deleted** folder, they will be completely removed from the GravityZone database. Nevertheless, excluded endpoints that are online will be detected with the next Network Discovery task and they will appear in the Network Inventory as new endpoints.

- For endpoints in an integration folder (Active Directory, vCenter Server, Xen Server etc.):

  For endpoints in an integration folder (Active Directory, Amazon EC2 etc.):

  - The endpoints become unmanaged and remain in their folders (they are not moved to the **Deleted** folder).
  - A license seat is released for each endpoint.

    If the endpoint is online, it will be licensed again.

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.

   Alternately, use the **Filters** menu and the **Depth > All items recursively** option at the upper side of the table to display all entities in the Network inventory.

4. In the right-side pane, select the check box of to the endpoint you want to delete.
5. Click the ⊖ **Delete** button at the upper side of the table. Confirm your action by clicking **Yes**.

   Depending on the endpoints, they will either be moved to the **Deleted** folder or they will only become unmanaged.

You can anytime move endpoints from the **Deleted** folder to **Custom Groups**, by using drag-and-drop.

6.9. Configuring Network Settings

In the **Configuration > Network Settings** page, you can configure settings related to Network Inventory, such as: saving filters, retaining the last browsed location, creating and managing scheduled rules for deleting unused virtual machines.

The options are organized into the following sections:

- Network Inventory settings
- Offline machines cleanup

6.9.1. Network Inventory Settings

Under the **Network Inventory settings** section, the following options are available:

- **Save Network Inventory filters**. Select this check box to save your filters in the **Network** page between Control Center sessions.
- **Remember last browsed location in Network Inventory until I log out**. Select this check box to save the last location you have accessed when leaving the **Network** page. The location is not saved between sessions.
- **Avoid duplicates of cloned endpoints**. Select this option to enable a new type of network objects in GravityZone, called golden images. This way you can differentiate the source endpoints from their clones.

  For endpoints enrolled in Active Directory, use the following options:

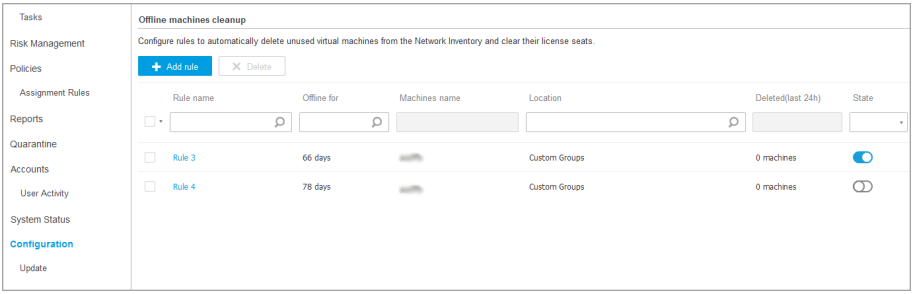
  - **Applies to cloned physical endpoints that are joined in Active Directory**. This option resolves cloned HDD drives from decommissioned machines.
  - **Applies to cloned virtual endpoints that are joined in Active Directory**. This option resolves clones created using VMware Instant Clones.

  Further on, you need to mark each endpoint you clone as follows:

1. Go to the **Network** page.
2. Select the endpoint you want to clone.
3. From its contextual menu, select **Mark as Golden Image**.

6.9.2. Offline Machines Cleanup

Under the **Offline machines cleanup** section, you can schedule rules to automatically delete unused virtual machines from the Network Inventory.



Configuration - Network Settings - Offline machines cleanup

Creating Rules

To create a cleanup rule:

1. Under the **Offline machines cleanup** section, click the **Add rule** button.
2. In the configuration page:
   a. Enter a rule name.
   b. Select an hour for everyday cleanup.
   c. Define cleanup criteria:
      - The number of days in which the machines were offline (from 1 to 90).
      - A name pattern, which can apply to a single virtual machine or to multiple virtual machines.

        For example, use `machine_1` to delete the machine with this name. Alternatively, add `machine_*` to delete all machines whose name begins with `machine_`.

This field is case sensitive and accepts only letters, digits and the special characters asterisk (*), underscore (_), and hyphen (-). The name cannot start with asterisk (*).

d. Select the target groups of endpoints in Network Inventory where to apply the rule.

3. Click **Save**.

Viewing and Managing Rules

The **Network Settings > Offline machines cleanup** section displays all the rules you have created. A dedicated table provides you with the following details:

- Rule name.
- The number of days since the machines went offline.
- Machines name pattern.
- Location in the Network Inventory.
- The number of machines deleted in the last 24 hours.
- State: enabled, disabled, or invalid.

Note
A rule is invalid when targets are no longer valid, due to certain reasons. For example, the virtual machines have been deleted or you do not have access to them anymore.

A newly created rule is enabled by default. You can enable and disable rules at any time by using the On/Off switch in the **State** column.

If needed, use the sorting and filtering options at the upper side of the table to find specific rules.

To modify a rule:

1. Click the name of the rule.
2. In the configuration page, edit the rule details.
3. Click **Save**.

To delete one or more rules:

1. Use the check boxes to select one or more rules.

2. Click the **Delete** button at the upper side of the table.

6.10. Configuring Security Server Settings

Security Servers use their caching mechanism to deduplicate antimalware scanning, optimizing this process. One step further with scanning optimization is to share this cache with other Security Servers.

Cache sharing works only between Security Servers of the same type. For example, a Security Server Multi-Platform will share its cache only with another Security Server Multi-Platform and not with a Security Server for NSX.

To enable and configure cache sharing:

1. Go to the **Configuration > Security Server Settings** page.
2. Select the **Security Server Cache Sharing** check box.
3. Choose the sharing scope:
   - All available Security Servers.

     It is recommended to use this option if all Security Servers are in the same network.
   - Security Servers available in the Assignment list.

     Use this option when Security Servers are spread in different networks and cache sharing may generate a high amount of traffic.
4. If limiting the scope, create the group of Security Servers. Select the Security Servers from the drop-down list and click **Add**.

   Only Security Servers in the table will share their cache.

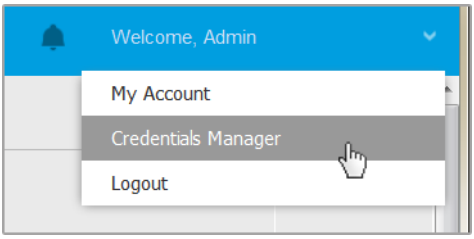
   Note
   Security Servers for NSX-T and NSX-V exchange cache information only within the same vCenter Server.

5. Click **Save**.

6.11. Credentials Manager

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

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



The Credentials Manager menu

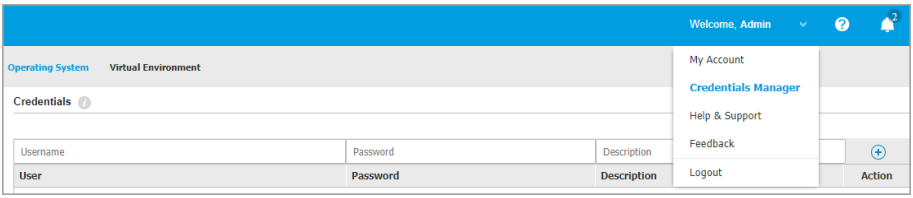
The **Credentials Manager** window contains two tabs:

- Operating System
- Virtual Environment

6.11.1. Operating System

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

To add a set of credentials:



Credentials Manager

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

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

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

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

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

6.11.2. Virtual Environment

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

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

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

1. Select the server from the corresponding menu.

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

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

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

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

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

6.11.3. Deleting Credentials from Credentials Manager

To delete obsolete credentials from the Credentials Manager:

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

7. 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.

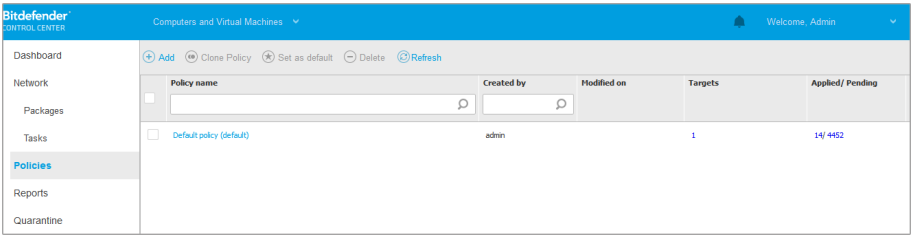
This is what you need to know about policies:

- 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. When assigning a policy, you will also define the policy inheritance options. By default, each endpoint inherits the policy of the parent group.
- 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.

7.1. 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.

7.1.1. 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. 218)
   - "Mobile Device Policies" (p. 366)
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**.

7.1.2. 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.

  Note
  The HVI module may be available for your GravityZone solution with a separate license key.

Assigning Device Policies

In GravityZone, you can assign policies in multiple ways:

- Assign the policy directly to the target.
- Assign the policy of the parent group through inheritance.
- Force policy inheritance to the target.

By default, each endpoint or group of endpoints inherits the policy of the parent group. If you change the policy of the parent group, all descendants will be affected, excepting those with an enforced policy.

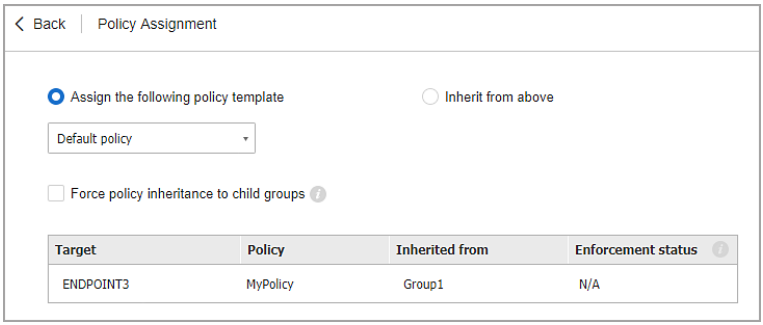
To assign a device policy:

1. Go to the **Network** page.
2. Choose the network view from the views selector.
3. Select the target endpoints. You can select one or several endpoints or groups of endpoints.

For inheritance purposes, you cannot change the policy of the root group from default. For example, **Computer and Virtual Machines** will always have the **Default policy** assigned.

4. Click the **Assign Policy** button at the upper side of the table, or select the **Assign Policy** option from the contextual menu.

   The **Policy Assignment** page is displayed:



Policy Assignment Settings

5. Check the table with target endpoints. For each endpoint, you can view:
   - The assigned policy.
   - The parent group from which the target inherits the policy, if the case.

     If the group is enforcing the policy, you can click its name to view the **Policy Assignment** page with this group as target.
   - The enforcement status.

     This status shows whether the target is forcing policy inheritance or is forced to inherit the policy.

     Notice the targets with enforced policy (**Is forced** status). Their policies cannot be replaced. In such case, a warning message is displayed.
6. In case of warning, click the **Exclude these targets** link to continue.
7. Choose one of the available options to assign the policy:
   - **Assign the following policy template** - to appoint a specific policy directly to the target endpoints.

- **Inherit from above** - to use the policy of the parent group.

8. If you chose to assign a policy template:
   a. Select the policy from the drop-down list.
   b. Select **Force policy inheritance to child groups** to achieve the following:
      - Assign the policy to all descendants of the target groups, with no exception.
      - Prevent changing it from elsewhere lower in the hierarchy.

      A new table displays recursively all affected endpoints and groups of endpoints, together with the policies that will be replaced.
9. Click **Finish** to save and apply changes. Otherwise, click **Back** or **Cancel** to return to the previous page.

When finished, policies are pushed to target endpoints immediately. Settings should be applied on endpoints in less than a minute (provided they are online). If an endpoint is not online, settings will be applied as soon as it gets back online.

To check if the policy was successfully assigned:

1. In the **Network** page, click the name of the endpoint you are interested in. Control Center will display the **Information** window.
2. Check the **Policy** section to view the status of the current policy. It must show **Applied**.

Another method to check the assignment status is from the policy details:

1. Go to the **Policies** page.
2. Find the policy you assigned.

   In the **Active/Applied/Pending** column, you can view the number of endpoints for each of the three statuses.
3. Click any number to view the list of endpoints with the respective status in the **Network** page.

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
   - Tag 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/IP address range	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.

Type	Value
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.

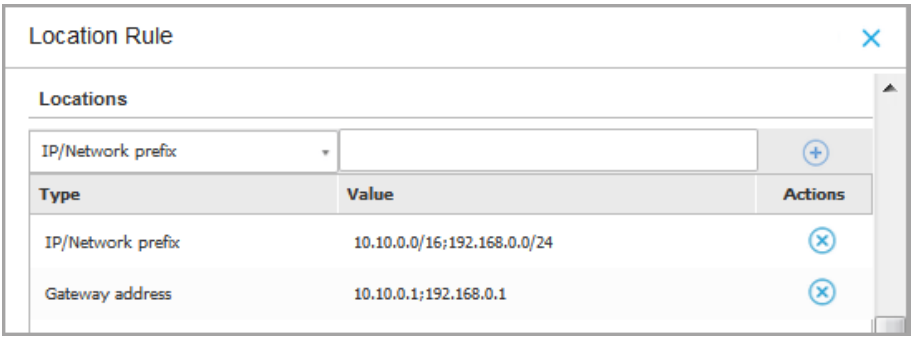
Hostname	Hostname
	For example: `cmp.bitdefender.com`
	Important
	You can also use wildcards. Asterisk (*) substitutes for zero or more characters and the question mark (?) substitutes exactly one character. Examples:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

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 "Configuring Location Rules" (p. 212).
   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.

Configuring Tag Rules

Important
You can create tag rules only if an Amazon EC2 or Microsoft Azure integration is available.

You can use the tags defined in the cloud infrastructures to assign a specific GravityZone policy to your virtual machines hosted in the cloud. All virtual machines

having the tags specified in the tag rule will be applied with the policy set by the rule.

Note
According to the cloud infrastructure, you can define the virtual machine tags as follows:

- For Amazon EC2: in the **Tags** tab of the EC2 instance.
- For Microsoft Azure: in the **Overview** section of the virtual machine.

A tag rule can contain one or several tags. To create a tag rule:

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 tag rule.
4. In the **Tag** table, add one or several tags.

   A tag consists in a case-sensitive key-value pair. Make sure to enter the tags as defined in your cloud infrastructure. Only valid key-value pairs will be taken into account.

   To add a tag:

   a. In the **Tag Key** field, enter the key name.

   b. In the **Tag Value** field, enter the value name.

   c. Click the ⊕ **Add** button at the right side of the table.

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**.

7.1.3. 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. 218)
   - "Mobile Device Policies" (p. 366)
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.

7.1.4. 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.

7.1.5. 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. 216).

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**.

7.2. 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 sections:
   - General
   - HVI
   - Antimalware
   - Sandbox Analyzer
   - Firewall
   - Network Protection
   - Patch Management
   - Application Control
   - Device Control
   - Relay
   - Exchange Protection
   - Encryption
   - NSX
   - Storage Protection
   - Incidents Sensor

   Navigate through sections 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. 205).

7.2.1. 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:

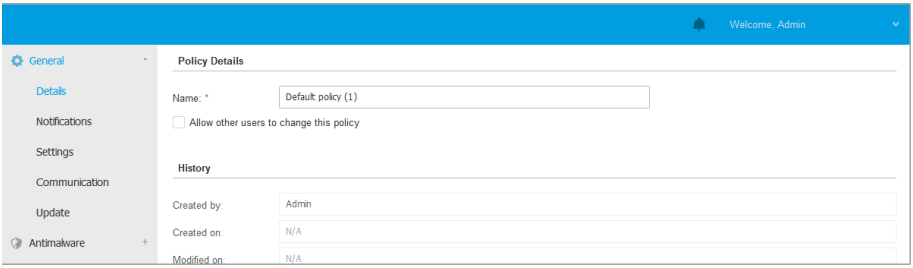
- Details
- Notifications
- Settings

- 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.

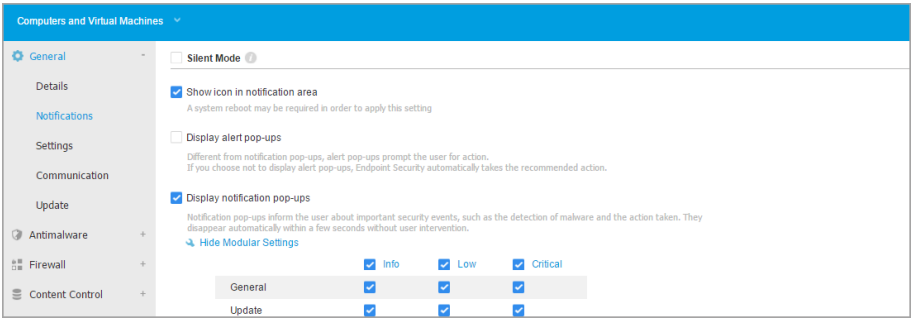
To configure an email address in the **About** window so that it opens the default email application on the endpoint, you must add it in the **Email** field with the "mailto:" prefix. Example: `mailto: name@domain.com`.

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.
- **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.

For example, after selecting the check boxes associated to Sandbox Analyzer, Bitdefender Endpoint Security Tools informs the user when a file is submitted to behavioral analysis.

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.

- **Endpoint Restart Notification.** This option displays a restart alert on the endpoint each time a system reboot is required due to changes made to the endpoint by the GravityZone modules selected under modular settings.

  Note
  Endpoints requiring a system restart have a specific status icon ( ) in the GravityZone inventory.

  You can further customize restart alerts by clicking on **Show modular settings**. The following options are available:

  - **Update** - Select this option to activate agent update restart notifications.
  - **Patch Management** - Select this option to activate patch install restart notifications.

Note
You can also set a limit to how many hours a user can postpone a restart. To do this, select **Auto-restart machine after** and insert a value from 1 to 46.

The restart alert requires the user to choose one of the following actions:

- **Reboot now**. In this case, the system will restart immediately.
- **Postpone reboot**. In this case, a restart notification will pop up periodically, until the user restarts the system or until the time set by the Company Administrator has passed.

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.
  - **Submit HVI memory violations to Bitdefender.** By default, HVI sends anonymized information regarding detected violations to Bitdefender Cloud Servers, to be used in statistics and to improve product detection rates. You can clear this check box if you do not want to submit such information from your network.

    Note
    The HVI module may be available for your GravityZone solution with a separate license key.

Note
For information on how these settings interfere with HIPAA regulations, refer to the "GravityZone and HIPAA" section in the Installation Guide.

Communication

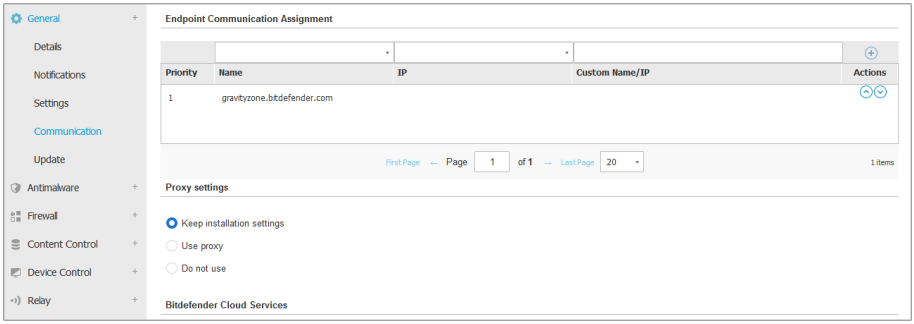
In this section, you can assign one or several relay machines to the target endpoints, then configure the proxy preferences for the communication between the target endpoints and GravityZone.

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

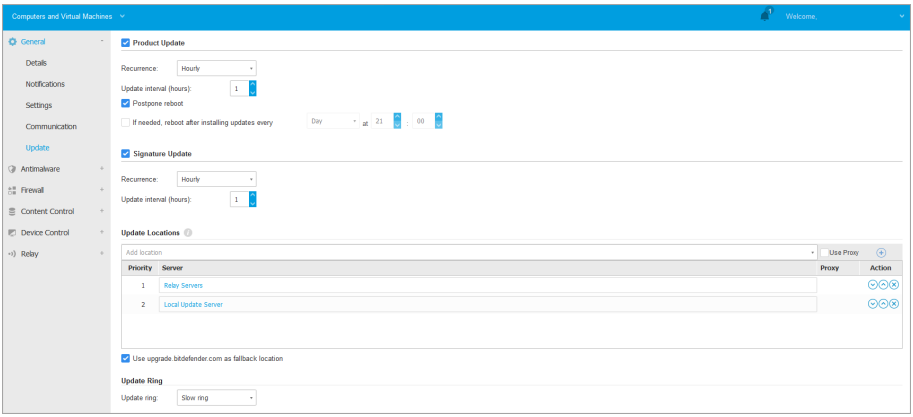
In this section, you can configure the proxy preferences for the communication between the target endpoints and Bitdefender Cloud Services (requiring internet connection):

- **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 security content 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 security content 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).

– For more control over when changing the configuration and updating the staging process, you can configure the BEST agent on your Linux machines to execute EDR kernel module updates via **Product Update**.

When the **Product Update** check box is enabled:

- If you enable the **Update Linux EDR modules using product update** check box, GravityZone will update kernel versions via **Product Update**.
- If you leave this option disabled, the kernel versions will be updated via **Security Content Update**.

Note
If you enable the **Update Linux EDR modules using product update** check box but disable the **Product Update** option, the Linux EDR modules will not be updated.

- **Security Content Update.** Security content refers to static and dynamic means of detecting threats, such as, but not limited to, scan engines, machine learning models, heuristics, rules, signatures, and blacklists. Bitdefender security agent automatically checks for security content 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.

Warning
Relay Servers are not supported on legacy operating systems. For more information, refer to the Installation Guide.

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 Bitdefender Servers 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.
- BEST for Windows Legacy does not support staging. The legacy endpoints on staging location must be moved to the production location.

7.2.2. HVI

Note
HVI provides protection only to virtual machines on Citrix Xen hypervisors.
The HVI module may be available for your GravityZone solution with a separate license key.

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.

Following the memory separation principle of the operating systems, HVI 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.

Additionally, the HVI policy includes two features to help you manage security and maintain the protected virtual machines:

- Exclusions, for viewing and managing processes excepted from scanning.
- Custom Tools, for injecting tools that are necessary in operational and forensics activities, inside the guest operating systems.

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.

Exclusions

GravityZone allows you to exclude processes from HVI scanning, using the **Blocked Applications** and **HVI Activity** reports. The **Exclusions** section gathers all these processes from the mentioned reports and displays them under the form of a table.

For each excluded process you can view a comment with the reason of exclusion.

If you change your mind about an excluded process, click the **Delete** button at the upper side of the table and it will be included in future scans.

Custom Tools

In this section you can configure tools injection inside the target guest operating systems. These tools must be uploaded to GravityZone before using them. For more information, refer to "Custom Tools Injection with HVI" (p. 502).

To configure injections:

1. Use the **Activate injections** check box to enable or disable the feature.
2. Click the ⊕ **Add** button at the upper side of the table to add a new tool. A configuration window is displayed.
3. Select the tool you want to use from the **Choose tool** drop-down list.

   These tools were previously uploaded in GravityZone. If you cannot find the right tool in the list, go to the **Tools Management Center** and add it from there. For more information, refer to "Custom Tools Injection with HVI" (p. 502).
4. Under **Tool description**, enter the intended use of the tool or any other information you may find useful.
5. Enter the tool's command line, together with all needed input parameters, just like you do in Command Prompt or Terminal. For example:

   ```
   bash script.sh <param1> <param2>
   ```

   .

For BD Remediation Tools you can only select the remediation action and backup remediation action from the two drop-down menus.

6. Point the location from where the Security Server should gather the logs:
   - **stdout**. Select this check box to capture the logs from the standard output communication channel.
   - **Output file**. Select this check box to collect log file saved on the endpoint. In this case, you need to enter the path to where the Security Server can find the file. You can use absolute paths or system variables.

     Here you have two additional options:

     a. **Delete log files from Guest after they have been transferred**. Select this option if you no longer need the files on the endpoint.

     b. **Transfer logs to**. Select this option to move the logs file from the Security Server to another location. In this case, you need to provide the path to the destination location and the authentication credentials.
7. Select how the injection will be triggered. You have the following options:
   - **After a violation is detected in the guest virtual machine.** The tool is injected right when a threat is detected on the virtual machine.
   - **By e specific schedule.** Use the scheduling options to configure the injection schedule. You can choose to run the tool every few hours, days or weeks, starting with a specified date and time.

     Please consider that the virtual machine must be on when the schedule is due. A scheduled injection will not run when due if the machine is powered off or paused. In such situations, it is recommended to enable the check box **If scheduled injection time is missed run task as soon as possible**.
   - Sometimes the tool may require a longer time than expected to finish its job or it may become unresponsive. To avoid crashes in such situations, in the **Safety configuration** section, choose after how many hours the Security Server should automatically terminate the tool's process.
   - Click **Save**. The tool will be added in the table.

You can add as many tools you need following the previously mentioned steps.

7.2.3. Antimalware

Note
This module is available for:

- Windows for workstations
- Windows for servers
- Linux
- macOS

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 three categories:

- On-access scanning: prevents new malware threats from entering the system.
- On-execute scanning: proactively protects against threats, and automatically discovers and blocks fileless attacks at pre-execution.
- 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.

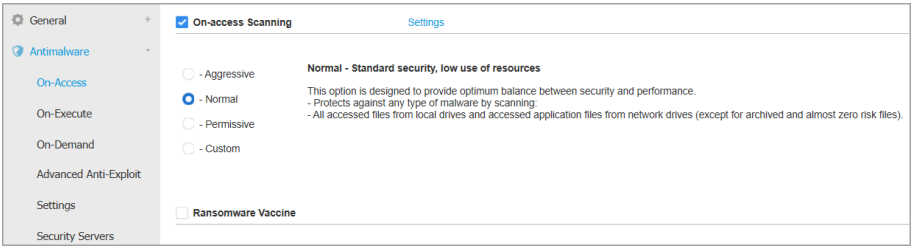
The settings are organized into the following sections:

- On-Access
- On-Execute
- On-Demand
- HyperDetect
- Advanced Anti-Exploit
- Settings
- Security Servers

On-Access

In this section you can configure the components that provide protection when a file or application is accessed:

- On-access scanning
- Ransomware vaccine



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).

Note
This feature has certain limitations on Linux-based systems. For details, refer to the requirements chapter of GravityZone Installation Guide.

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. 536).

  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.

  > **Note**
  > On Linux-based systems, file extensions are case sensitive and the files with the same name but with different extension are considered distinct objects. For example, `file.txt` is different from `file.TXT`.

  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.

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 security content update, to address the latest threats.

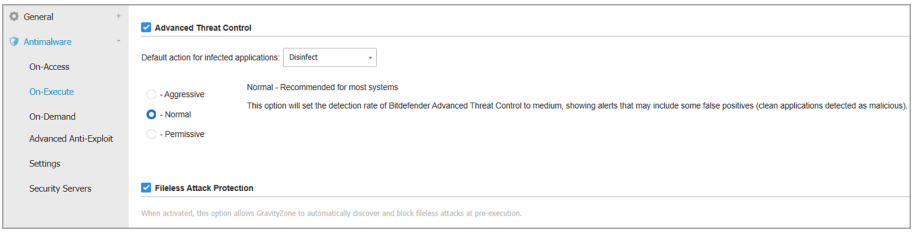
Warning
To further increase protection against ransomware infections, be cautious about unsolicited or suspicious attachments and make sure security content is updated.

Note
Ransomware vaccine is available only with Bitdefender Endpoint Security Tools for Windows.

On-Execute

In this section you can configure protection against malicious processes, when they are executed. It covers the following protection layers:

- Cloud-based threat detection
- Advanced Threat Control
- Fileless Attack Protection
- Ransomware Mitigation



Policies - On-Execute Settings

Advanced Threat Control

Note
This module is available for:

- Windows for workstations
- Windows for servers
- macOS

Bitdefender Advanced Threat Control is a 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.

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.

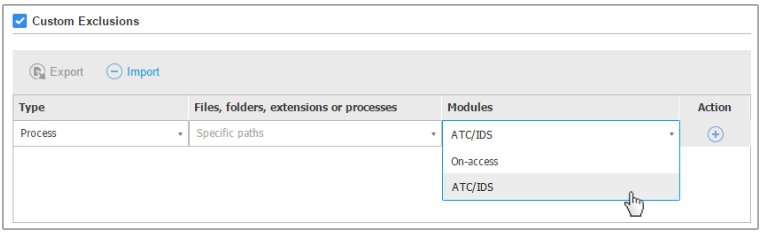
To configure Advanced Threat Control:

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 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

Fileless Attack Protection

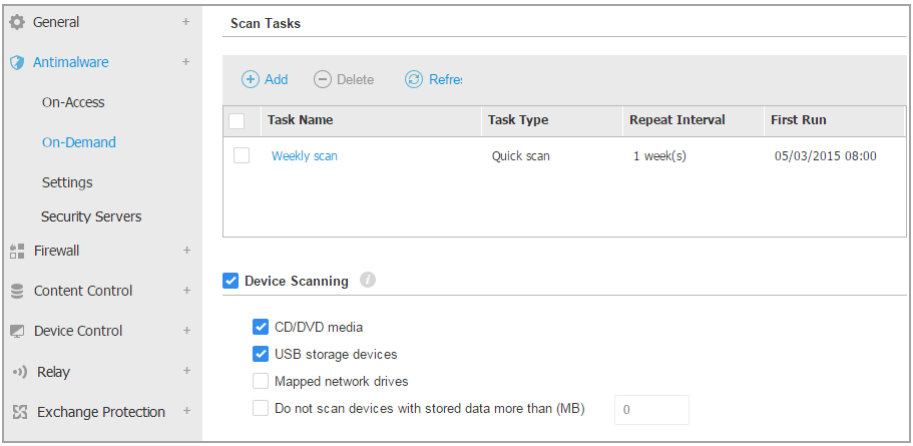
Note
This module is available for:

- Windows for workstations
- Windows for servers

Fileless Attack Protection detects and blocks fileless malware at pre-execution, including terminating PowerShell running malicious command line, blocking malicious traffic, analyzing memory buffer prior to code injection and blocking the code injection process.

On-Demand

In this section, you can add and configure antimalware scan tasks that will run regularly on the target computers, according to the defined 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.

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.

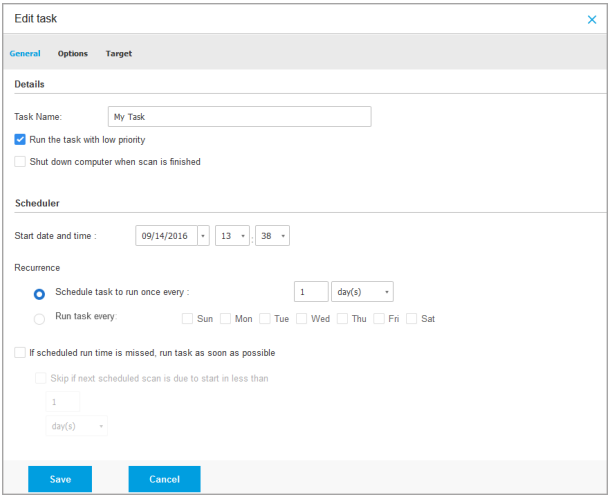
To remove a task from the list, select the task and click the ⊖ **Delete** button at the right side of the table.

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.

Note
This option applies only to Bitdefender Endpoint Security Tools and Endpoint Security (legacy agent).

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
This option applies to Bitdefender Endpoint Security Tools, Endpoint Security (legacy agent) and Endpoint Security for Mac.

- **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.

  Endpoints must be powered-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. 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).

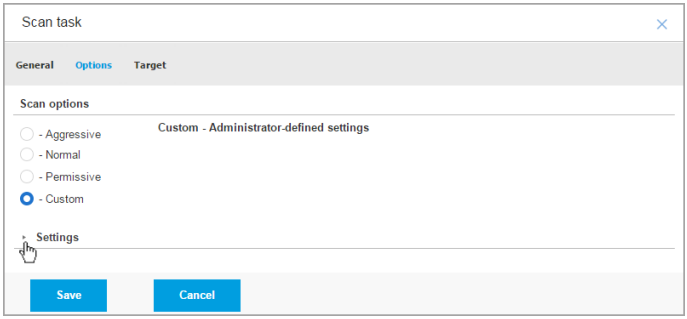
  Optionally, you can specify what happens when the scan task could not start at the scheduled time (endpoint was offline or shutdown). Use the option **If scheduled run time is missed, run task as soon as possible** according to your needs:

  – When you leave the option unchecked, the scan task will attempt to run again at the next scheduled time.

  – When you select the option, you force the scan to run as soon as possible. To fine-tune the best timing for the scan runtime and avoid disturbing the user during the work hours, select **Skip if next scheduled scan is due to start in less than**, then specify the interval that you want.

- **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. 536).

  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. 268).

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
- 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. Please note that some

devices such as CDs/DVDs are read-only. No action can be taken on infected files contained on such storage support.

Note
During a device scan, the user can access any data from the device.

If alert pop-ups are enabled in the **General > Notifications** 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 > Notifications** 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**
- **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.

HyperDetect

Note
This module is available for:

- Windows for workstations
- Windows for servers
- Linux

HyperDetect adds an extra layer of security over the existing scanning technologies (On-Access, On-Demand and Traffic Scan), to fight against the new generation of cyber-attacks, including advanced persistent threats. HyperDetect enhances the Antimalware and Content Control protection modules with its powerful heuristics based on artificial intelligence and machine learning.

With its ability to predict targeted attacks and detect most sophisticated malware in the pre-execution stage, HyperDetect exposes threats much faster than the signature-based or behavioral scanning technologies.

To configure HyperDetect:

1. Use the **HyperDetect** check box to turn the module on or off.
2. Select which type of threats you want to protect your network from. By default, protection is enabled for all types of threats: targeted attacks, suspicious files and network traffic, exploits, ransomware, or grayware.

   Note
   The heuristics for network traffic require **Content Control > Traffic Scan** to be enabled.

3. Customize the protection level against threats of the selected types.

   Use the master switch at the top of the threats list to choose a unique level of protection for all types of threats, or select individual levels to fine tune protection.

   Setting the module at a certain level will result in actions being taken up to that level. For example, if set to **Normal**, the module detects and contains threats that trigger the **Permissive** and **Normal** thresholds, but not the **Aggressive** one.

   Protection increases from **Permissive** to **Aggressive**.

   Keep in mind that an aggressive detection may conduct to false positives, while a permissive one can expose your network to some threats. It is recommended to first set protection level to the maximum and then lower it in case of many false positives, until you achieve the optimal balance.

   Note
   Whenever you enable protection for a type of threats, detection is automatically set to the default value (**Normal** level).

4. Under the **Actions** section, configure how HyperDetect should react to detections. Use the drop-down menu options to set the action to be taken on threats:
   - For files: deny access, disinfect, delete, quarantine, or just report the file.
   - For network traffic: block or just report the suspicious traffic.

5. Select the check box **Extend reporting on higher levels** next to the drop-down menu, if you want to view the threats detected at higher protection levels than the one set.

If you are uncertain of the current configuration, you can easily restore the initial settings by clicking the **Reset to default** button at the lower side of the page.

Advanced Anti-Exploit

Note
This module is available for:

- Windows for workstations and servers

Advanced Anti-Exploit is a proactive technology that detects exploits in real-time. Based on machine learning, it protects against a series of known and unknown exploits, including memory file-less attacks.

To enable protection against exploits, select the **Advanced Anti-Exploit** check box.

Advanced Anti-Exploit is set to run with the recommended settings. You can adjust protection differently, if needed. To restore the initial settings, click the **Reset to Default** link at the right side of the section heading.

GravityZone has the anti-exploit settings organized in three sections:

- **System-wide detections**

  The anti-exploit techniques in this section monitor the system processes that are targets of exploits.

  For more information about the available techniques and how to configure their settings, refer to “Configure System-Wide Mitigation” (p. 262).

- **Predefined applications**

  Advanced Anti-Exploit module is preconfigured with a list of the common applications such as Microsoft Office, Adobe Reader or Flash Player, which are the most exposed to exploitations.

  For more information about the available techniques and how to configure their settings, refer to “Configure Application-Specific Techniques” (p. 262).

- **Additional applications**

  In this section you can add and configure protection for as many other applications you want.

For more information about the available techniques and how to configure their settings, refer to "Configure Application-Specific Techniques" (p. 262).

You can expand or collapse each section by clicking its heading. This way, you will quickly reach the settings you want to configure.

Configure System-Wide Mitigation

Under this section, you have the following options:

Technique	Description
Privilege escalation	Prevents processes from gaining unauthorized privileges and access to resources. Default action: Kills process
LSASS process protection	Protects the LSASS process from leaking secrets such as password hashes and security settings. Default action: Blocks process

These anti-exploit techniques are enabled by default. To disable any of them, clear their check box.

Optionally, you can change the action taken automatically upon detection. Choose an action available in the associated menu:

- **Kill process**: ends immediately the exploited process.
- **Block process**: prevents the malicious process from accessing unauthorized resources.
- **Report only**: GravityZone reports the event without taking any mitigation action. You can view the event details in the **Advanced Anti-Exploit** notification, and in Blocked Applications and Security Audit reports.

Configure Application-Specific Techniques

Whether predefined or additional applications, they all share the same set of anti-exploit techniques. You can find them described herein:

Technique	Description
ROP Emulation	Detects attempts to make executable the memory pages for data, using the Return-Oriented Programming (ROP) technique. Default action: Kill process
ROP Stack Pivot	Detects attempts to hijack the code flow using the ROP technique, by validating stack location. Default action: Kill process
ROP Illegal Call	Detects attempts to hijack the code flow using the ROP technique, by validating callers of sensitive system functions. Default action: Kill process
ROP Stack Misaligned	Detects attempts to corrupt the stack using the ROP technique, by validating the stack address alignment. Default action: Kill process
ROP Return to Stack	Detects attempts to execute code directly on stack using the ROP technique, by validating return address range. Default action: Kill process
ROP Make Stack Executable	Detects attempts to corrupt the stack using the ROP technique, by validating the stack page protection. Default action: Kill process
Flash Generic	Detects Flash Player exploitation attempts. Default action: Kill process
Flash Payload	Detects attempts to execute malicious code into Flash Player, by scanning Flash objects in memory. Default action: Kill process
VBScript Generic	Detects VBScript exploitation attempts. Default action: Kill process
Shellcode Execution	Detects attempts to create new processes or download files, using shellcode. Default action: Kill process

Technique	Description
Shellcode LoadLibrary	Detects attempts to execute code via network paths, using shellcode. Default action: Kill process
Anti-Detour	Detects attempts to bypass security checks for creating new processes. Default action: Kill process
Shellcode EAF (Export Address Filtering)	Detects attempts of malicious code to access sensitive system functions from DLL exports. Default action: Kill process
Shellcode Thread	Detects attempts to inject malicious code, by validating newly-created threads. Default action: Kill process
Anti-Meterpreter	Detects attempts to create a reverse shell, by scanning executable memory pages. Default action: Kill process
Obsolete Process Creation	Detects attempts to create new processes using obsolete techniques. Default action: Kill process
Child Process Creation	Blocks creation of any child process. Default action: Kill process
Enforce Windows DEP	Enforces Data Execution Prevention (DEP) to block code execution from data pages. Default: Disabled
Enforce Module Relocation (ASLR)	Prevents code from being loaded in predictable locations, by relocating memory modules. Default: Enabled
Emerging Exploits	Protects against any new emerging threats or exploits. Rapid updates are used for this category before more comprensive changes can be made. Default: Enabled

To monitor other applications except the predefined ones, click the **Add Application** button available at the top and at the bottom of the page.

To configure the anti-exploit settings for an application:

1. For existing applications, click the application name. For new applications, click the **Add** button.

   A new page displays all techniques and their settings for the selected application.

   Important
   Use caution when adding new applications to be monitored. Bitdefender cannot guarantee the compatibility with any application. Thus, it is recommended to test the feature first on a few non-critical endpoints, and then deploy it in the network.

2. If adding a new application, enter its name and its processes names in the dedicated fields. Use the semicolon (;) to separate process names.
3. If you need to quickly check the description of a technique, click the arrow next to its name.
4. Select or clear the check boxes of the exploitation techniques, as needed.

   Use the **All** option if you want to mark all techniques at once.
5. If needed, change the automatic action upon detection. Choose an action available in the associated menu:
   - **Kill process**: ends immediately the exploited process.
   - **Report only**: GravityZone reports the event without taking any mitigation action. You can view the event details in the **Advanced Anti-Exploit** notification and in reports.

   By default, all techniques for predefined applications are set to mitigate the issue, while for additional applications are set to just report the event.

   To quickly change the action taken for all techniques at once, select the action from the menu associated with **All** option.

Click the **Back** button at the upper side of the page to return to the Anti-Exploit general settings.

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.

  Note
  For information on how this setting interferes with HIPAA regulations, refer to the "GravityZone and HIPAA" section in the Installation Guide.

- **Rescan quarantine after security content updates.** Keep this option selected to automatically scan quarantined files after each security content 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.
- **Allow users to take actions on local quarantine.** This option is controlling the actions that endpoint users can take on local quarantined files via the Bitdefender Endpoint Security Tools interface. By default, local users can restore or delete quarantined files from their computer using the options available in Bitdefender Endpoint Security Tools. By disabling this option, users will not

have access anymore to the quarantined files action buttons from the Bitdefender Endpoint Security Tools interface.

Centralized Quarantine

If you want to keep the quarantined files from your managed endpoints for further analysis, use the **Centralized Quarantine** option, which sends an archived copy of each local quarantined file to a network share.

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

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

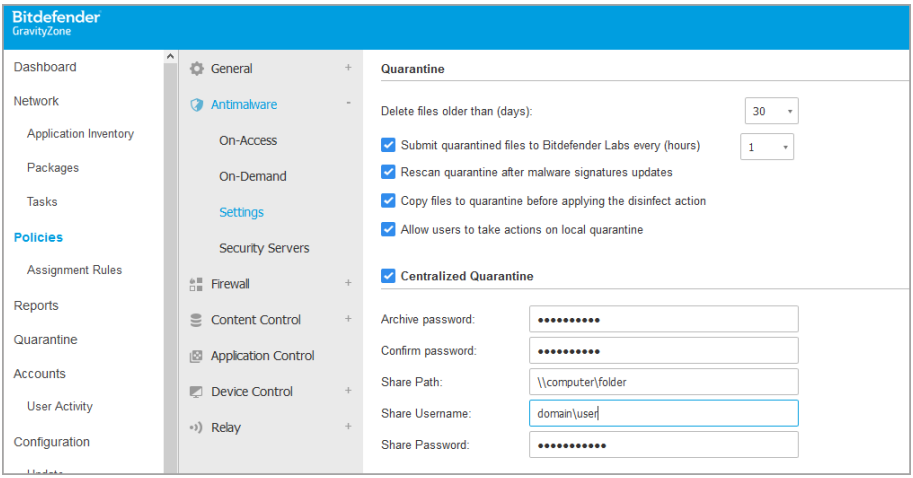
To configure the centralized quarantine settings, fill in the following fields:

- **Archive password**: enter the password required for the quarantined files archive. The password must contain at least one upper case character, at least one lower case character and at least one digit or special character. Confirm the password in the following field.
- **Share path**: enter the network path where you want to store the archives (for example, `\\computer\folder`).
- Username and password required to connect to the network share. The supported formats for username are as follows:
  - `username@domain`
  - `domain\username`
  - `username`.

For the centralized quarantine to work properly, make sure the following conditions are met:

- The shared location is accessible in the network.
- The endpoints have connectivity to the network share.
- The login credentials are valid and provide write access to the network share.
- The network share has enough disk space.

Note
Centralized quarantine does not apply to mail servers quarantine.



Centralized Quarantine

If you have a local Sandbox Analyzer instance configured in the **Sandbox Analyzer > Endpoint Sensor** section, you can select the check box **Automatically submit items from quarantine to a Sandbox Analyzer**. Please note that the submitted items must have a maximum size of 50 MB.

Exclusions

Bitdefender security agent can exclude from scanning certain object types. Antimalware 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.

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.

- You can also define **Custom Exclusions** for in-house developed applications or customized tools, according to your specific needs.

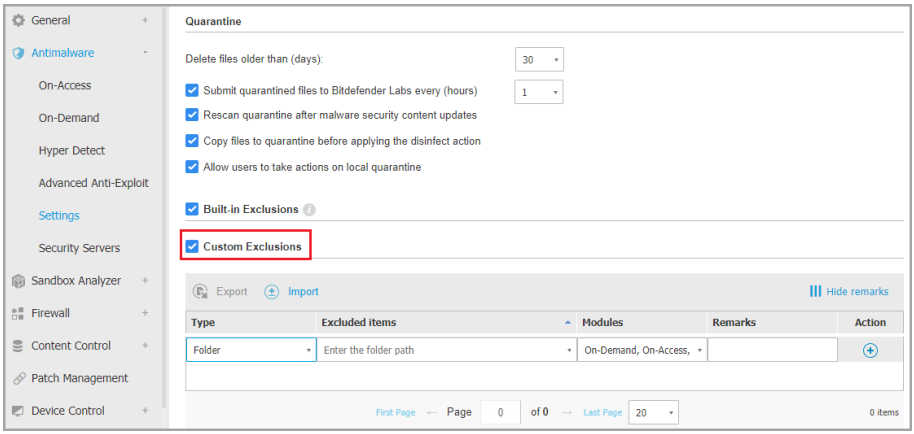
  Custom antimalware exclusions apply to one or more of the following scanning methods:

  – On-access scanning
  – On-demand scanning
  – Advanced Threat Control
  – Fileless Attack Protection

  Important

  – 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 7 and App Volumes AppStacks, refer to this VMware document.

  To exclude specific items from scanning, select the **Custom Exclusions** option and then add the rules into the table underneath.



Computers and Virtual Machines Policies - Custom Exclusions

To add a custom exclusion rule:

1. Select the exclusion type from the menu:

- **File**: only the specified file
- **Folder**: only the specified folder, without all files and processes inside that folder or from all of its subfolders
- **Extension**: all items having the specified extension
- **Process**: any object accessed by the excluded process
- **File Hash**: the file with the specified hash
- **Certificate Hash**: all the applications under the specified certificate hash (thumbprint)
- **Threat Name**: any item having the detection name (not available for Linux operating systems)
- **Command Line**: the specified command line (available only for Windows operating systems)

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.

2. Provide the details specific to the selected exclusion type:

   File, Folder or Process

   Enter the path to the item to be excluded from scanning. You have several helpful options to write the path:

   - Declare the path explicitly.

     For example: `C:\temp`

     To add exclusions for UNC paths, use any of the following syntaxes:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   - Use the system variables available in the drop-down menu.

For process exclusions, you must also add the name of the application's executable file.

For example:

`%ProgramFiles%` - excludes the Program Files folder

`%WINDIR%\system32` – excludes folder system32 within Windows folder

Note
It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

– Use wildcards.

The double asterisk (**) substitutes for zero or more characters. The single asterisk (*) substitutes for zero or more characters. The 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.

Note
The option is available in both Control Center and Power User policy settings, under **Antimalware** > **Settings** > **Custom Exclusions** section.

For example:

File exclusions:

`**\example.txt` – excludes any file named example.txt, regardless of its location on the endpoint

`C:\Test` – excludes all files and folders under a certain directory

`C:\Test\*.png` – excludes all PNG files, from the Test folder

Folder exclusion:

`C:\Test\*` - excludes all folders from Test folder

`C:\Test` – excludes all files and folders under a certain directory

Process exclusion:

`C:\Program Files\WindowsApps\Microsoft.Not??.exe` – excludes the Microsoft Notes processes.

Note
Processes exclusions do not support wildcards on Linux operating systems.

Extension

Enter 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
On Linux-based systems, file extensions are case sensitive and the files with the same name but with different extension are considered distinct objects. For example, `file.txt` is different from `file.TXT`.

File hash, Certificate hash, Threat name, or Command line

Enter the file hash, certificate thumbprint (hash), the exact name of the threat or the command line depending on the exclusion rule. You can use one item per exclusion.

3. Select the scanning methods to which the rule applies. Some exclusions may be relevant for On-access scanning, On-demand scanning, ATC/IDS, while others may be recommended for all of the three modules.
4. Optionally, click the **Show remarks** button to add a note in the **Remarks** column about the rule.
5. 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.

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**.

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

5, for file hash exclusions

6, for certificate hash exclusions

7, for threat name exclusions

8, for command line 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
The Windows paths must have the backslash (\) character doubled. For example, `%WinDir%\\System32\\LogFiles`.

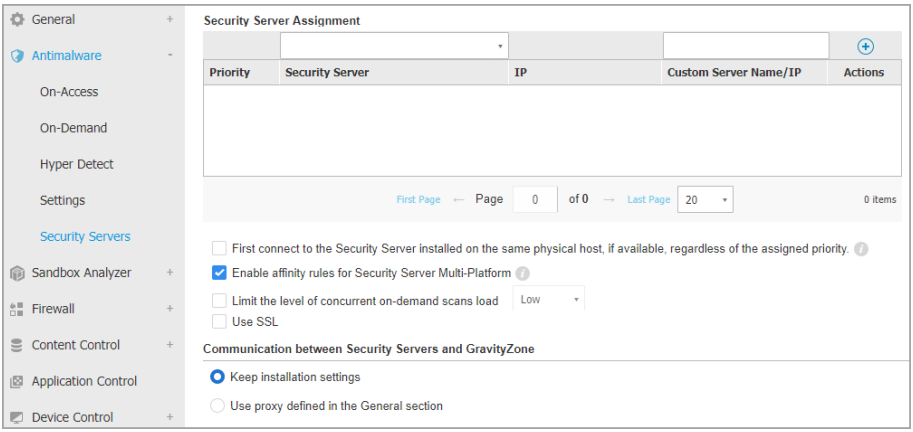
To import custom exclusions:

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:

- Security Server assignment
- Security Server specific settings



Policy - Computers and Virtual Machines - Antimalware - Security Servers

Security Server Assignment

You can assign one or several Security Servers to the target endpoints, and set the priority with which endpoints will elect a Security Server to send scanning requests.

Note
It is recommended to use Security Servers for scanning virtual machines or computers with low resources.

To assign a Security Server to the target endpoints, add the Security Servers you want to use, in the **Security Server Assignment** table, as follows:

1. Click the **Security Server** drop-down list and then select a Security Server.
2. If the Security Server is in DMZ or behind a NAT server, enter the FQDN or IP of the NAT server in the **Custom Server Name/IP** field.

   Important
   Make sure that port forwarding is correctly configured on the NAT server so that the traffic from endpoints can reach the Security Server. For details, refer to the GravityZone Communication Ports KB article.

3. Click the ⊕ **Add** button in the **Actions** column.

   The Security Server is added to the list.
4. Repeat the previous steps to add other Security Servers, if available or needed.

To set the priority of the Security Servers:

1. Use the up and down arrows available in the **Actions** column to increase or decrease each Security Server's priority.

   When assigning more Security Servers, the one on top of the list has the highest priority and will be selected first. If this Security Server is unavailable or overloaded, the next Security Server is selected. Scan traffic is redirected to the first Security Server that is available and has a convenient load.
2. Select **First connect to the Security Server installed on the same physical host, if available, regardless the assigned priority** for a uniform distribution of endpoints and for optimized latency. If this Security Server is unavailable, then a Security Server from the list will be elected, in order of priority.

Important
This option works only with Security Server Multi-Platform and only if GravityZone is integrated with the virtualized environment.

To remove a Security Server from the list, click the corresponding ⊗ **Delete** button in the **Actions** column.

Security Server Settings

When assigning the policy to Security Servers, you can configure the following settings for them:

- **Limit the number of concurrent on-demand scans**.

  Running multiple on-demand scan tasks on virtual machines sharing the same datastore can create antimalware scanning storms. To prevent this and to allow only a certain number of scan tasks to run at the same time:

  1. Select the **Limit the number of concurrent on-demand scans** option.
  2. Select the level of allowed concurrent scan tasks from the drop-down menu. You can choose a predefined level or enter a custom value.

     The formula to find the maximum limit of scan tasks for each predefined level is: `N = a x MAX(b ; vCPUs - 1)`, where:

     - `N` = maximum limit of scan tasks
     - `a` = multiplying coefficient, having the following values: `1` - for Low; `2` - for Medium; `4` - for High
     - `MAX(b;vCPU-1)` = a function that returns the maximum number of scan slots available on the Security Server.
     - `b` = the default number of on-demand scan slots, which currently is set to four.
     - `vCPUs` = number of virtual CPUs assigned to the Security Server

     For example:

     For a Security Server with 12 CPUs and a High level of concurrent scans, we have a limit of:

     `N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44` concurrent on-demand scan tasks.

- **Enable affinity rules for Security Server Multi-Platform**

  Choose which behavior the Security Server should have when its host enters in maintenance mode:

  – If enabled, the Security Server remains tied to the host and GravityZone shuts it down. When maintenance is over, GravityZone automatically restarts the Security Server.

    This is the default behavior.

  – If disabled, the Security Server is moved to another host and continues to run. In this case, the Security Server name changes in Control Center to point the former host. The name change persists until the Security Server is moved back to its native host.

    If the resources are sufficient, the Security Server can land on a host where another Security Server is installed.

    Important
    This option has no effect if the Security Server is also used by HVI.

- **Use SSL**

  Enable this option if you want to encrypt the connection between the target endpoints and the specified Security Server appliances.

  By default, GravityZone uses self-signed security certificates. You can change them with your own certificates in the **Configuration > Certificates** page of Control Center. For more information, refer to "Configure Control Center Settings" chapter of Installation Guide.

- **Communication between Security Servers and GravityZone**

  Choose one of the available options to 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 proxy**, when the target endpoints do not communicate with the specific Bitdefender components via proxy.

7.2.4. Sandbox Analyzer

Note
This module is available for:

- Windows for workstations
- Windows for servers

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

In this section, you can configure the following:

- Submission via endpoint sensor
- Submission via network sensor
- Submission via ICAP sensor
- Sandbox Manager settings

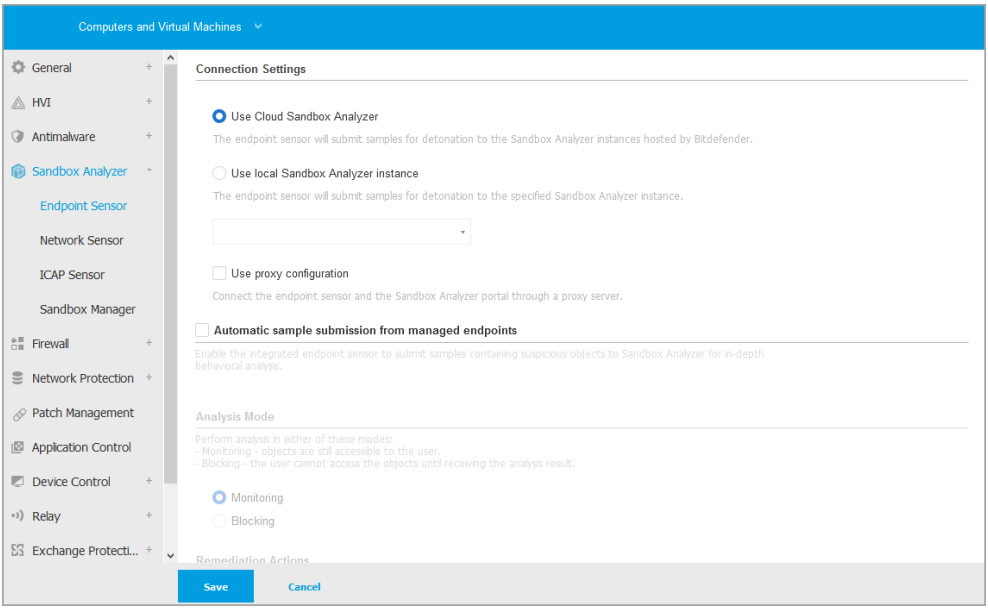
In the policy settings, you can also configure automatic submission from the centralized quarantine. For details, refer to "Centralized Quarantine" (p. 267).

For details about manual submission, refer to "Manual Submission" (p. 492). For details about submission via API, refer to the **Sandbox** and **Sandbox Portal** chapters in the GravityZone API Guide (On-Premises).

Note
For information on how Sandbox Analyzer interferes with HIPAA regulations, refer to the "GravityZone and HIPAA" section in the Installation Guide.

Endpoint Sensor

Bitdefender Endpoint Security Tools can act as a feeding sensor for Sandbox Analyzer from Windows endpoints.



Policies > Sandbox Analyzer > Endpoint Sensor

To configure automatic submission via endpoint sensor:

1. Under **Connection Settings**, select one of the options:
   - **Use Cloud Sandbox Analyzer** - the endpoint sensor will submit samples to a Sandbox Analyzer instance hosted by Bitdefender, depending on your region.
   - **Use local Sandbox Analyzer instance** - the endpoint sensor will submit samples to a Sandbox Analyzer On-Premises instance. Choose the preferred Sandbox Analyzer instance from the drop-down menu.

   If you have your network behind a proxy server or a firewall, you can configure a proxy to connect to Sandbox Analyzer by selecting the **Use proxy configuration** check box.

   You have to fill in the following fields:
   - **Server** - the IP of the proxy server.
   - **Port** - the port used to connect to the proxy server.

- **Username** - a user name recognized by the proxy.
- **Password** - the valid password for the specified user.

2. Select the **Automatic sample submission from managed endpoints** check box to enable automatic submission of suspicious files to Sandbox Analyzer.

   Important
   - Sandbox Analyzer requires on-access scanning. Make sure you have the **Antimalware > On-access Scanning** module enabled.
   - Sandbox Analyzer uses the same targets and exclusions as defined in **Antimalware > On-access Scanning**. Review carefully the On-access Scanning settings when configuring Sandbox Analyzer.
   - To prevent false positives (incorrect detection of legitimate applications), you can set up exclusions by file name, extension, file size and file path. For more information about On-access Scanning, refer to "Antimalware" (p. 241).
   - The upload limit for any file or archive is 50 MB.

3. Choose the **Analysis Mode**. Two options are available:
   - **Monitoring**. The user can access the file during the sandbox analysis, but he is recommended not to execute it until receiving the analysis result.
   - **Blocking**. The user cannot execute the file until the analysis result is returned to endpoint from Sandbox Analyzer Cluster via Sandbox Analyzer Portal.

4. Specify the **Remediation Actions**. These are taken when Sandbox Analyzer detects a threat. For each analysis mode you are provided with a dual setup, consisting of one default action and one fallback action. Sandbox Analyzer initially performs the default action, then the fallback action, if the former cannot be completed.

   When accessing this section for the first time, the following setups are available:

   Note
   As best practices, it is recommended to use remediation actions in this configuration.

   - In the **Monitoring** mode, the default action is **Report only**, with the fallback action disabled.
   - In the **Blocking** mode, the default action is **Quarantine**, while the fallback action is **Delete**.

Sandbox Analyzer provides you the following remediation actions:

- **Disinfect**. It removes the malware code from the infected files.
- **Delete**. It removes the entire detected file from the disk.
- **Quarantine**. It moves 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 quarantined files in the **Quarantine** page of Control Center.
- **Report only**. Sandbox Analyzer only reports detected threats without taking any other action on them.

Note
Depending on the default action, a fallback action may be unavailable.

5. Both default and fallback remediation actions are set to **Report only** mode.
6. Under **Content Prefiltering**, customize the protection level against potential threats. The endpoint sensor has embedded a content filtering mechanism which determines whether a suspicious file needs to be detonated in Sandbox Analyzer.

   The object types supported are: applications, documents, scripts, archives, emails. For more details on the supported object types, refer to "File Types Supported by Content Prefiltering at Automatic Submission" (p. 540).

   Use the main switch at the top of the threats list to choose a unique level of protection for all types of objects, or select individual levels to fine tune protection.

   Setting the module at a certain level will result in a certain number of submitted samples:

   - **Permissive**. The endpoint sensor automatically submits to Sandbox Analyzer only the objects with the highest probability of being malicious and ignores the rest of the objects.
   - **Normal**. The endpoint sensor finds a balance between the submitted and ignored objects and sends to Sandbox Analyzer both objects with a higher and with a lower probability of being malicious.
   - **Aggressive**. The endpoint sensor submits to Sandbox Analyzer almost all objects, regardless of their potential risk.

In a dedicated field, you can define exceptions for the object types that you do not want to submit to Sandbox Analyzer.

You can also define size limits of the submitted objects by selecting the corresponding check box and entering any desired values between 1 KB and 50 MB.

7. Under **Detonation profile**, adjust the complexity level of behavioral analysis, while affecting the Sandbox Analyzer throughput. For example, if set to **High**, Sandbox Analyzer would perform a more accurate analysis on fewer samples, in the same interval, than on **Medium** or **Low**.

Sandbox Analyzer supports local file submission through endpoints with relay role, which are able to connect to different Sandbox Analyzer Portal addresses depending on your region. For details regarding the relay configuration settings, refer to "Relay" (p. 326).

Note
A proxy configured in the Sandbox Analyzer connection settings will override any endpoints with relay role.

Network Sensor

In this section you can configure automatic submission of network traffic samples to Sandbox Analyzer via the network sensor. This module requires the Network Security Virtual Appliance to be deployed and configured with Sandbox Analyzer On-Premises.

To configure automatic submission via network sensor:

1. Select the **Automatic samples submission from network sensor** check box to enable automatic submission of suspicious files to Sandbox Analyzer.
2. Under **Content Prefiltering**, customize the protection level against potential threats. The network sensor has embedded a content filtering mechanism which determines whether a suspicious file needs to be detonated in Sandbox Analyzer.

   The object types supported are: applications, documents, scripts, archives, emails. For more details on the supported object types, refer to "File Types Supported by Content Prefiltering at Automatic Submission" (p. 540).

   Use the master switch at the top of the threats list to choose a unique level of protection for all types of objects, or select individual levels to fine tune protection.

Setting the module at a certain level will result in a certain number of submitted samples:

- **Permissive**. The network sensor automatically submits to Sandbox Analyzer only the objects with the highest probability of being malicious and ignores the rest of the objects.
- **Normal**. The network sensor finds a balance between the submitted and ignored objects and sends to Sandbox Analyzer both objects with a higher and with a lower probability of being malicious.
- **Aggressive**. The network sensor submits to Sandbox Analyzer almost all objects, regardless of their potential risk.

In a dedicated field, you can define exceptions for the object types that you do not want to submit to Sandbox Analyzer.

You can also define size limits of the submitted objects by selecting the corresponding check box and entering any desired values between 1 KB and 50 MB.

3. Under **Connection Settings**, select the preferred Sandbox Analyzer instance for submitting network content.

   If you have your network behind a proxy server or a firewall, you can configure a proxy to connect to Sandbox Analyzer by selecting the **Use proxy configuration** check box.

   You have to fill in the following fields:

   - **Server** - the IP of the proxy server.
   - **Port** - the port used to connect to the proxy server.
   - **Username** - a user name recognized by the proxy.
   - **Password** - the valid password for the specified user.

4. Under **Detonation profile**, adjust the complexity level of behavioral analysis, while affecting the Sandbox Analyzer throughput. For example, if set to **High**, Sandbox Analyzer would perform a more accurate analysis on fewer samples, in the same interval, than on **Medium** or **Low**.

ICAP Sensor

In this section you can configure automatic submission to Sandbox Analyzer via ICAP sensor.

Note
Sandbox Analyzer requires a Security Server configured to scan network-attached storage (NAS) devices that use the ICAP protocol. For details, refer to "Storage Protection" (p. 361)

1. Select the **Automatic samples submissions from ICAP sensor** check box to enable automatic submission of suspicious files to Sandbox Analyzer.
2. Under **Content Prefiltering**, customize the protection level against potential threats. The network sensor has embedded a content filtering mechanism which determines whether a suspicious file needs to be detonated in Sandbox Analyzer.

   The object types supported are: applications, documents, scripts, archives, emails. For more details on the supported object types, refer to "File Types Supported by Content Prefiltering at Automatic Submission" (p. 540).

   Use the master switch at the top of the threats list to choose a unique level of protection for all types of objects, or select individual levels to fine tune protection.

   Setting the module at a certain level will result in a certain number of submitted samples:

   - **Permissive**. The ICAP sensor automatically submits to Sandbox Analyzer only the objects with the highest probability of being malicious and ignores the rest of the objects.
   - **Normal**. The ICAP sensor finds a balance between the submitted and ignored objects and sends to Sandbox Analyzer both objects with a higher and with a lower probability of being malicious.
   - **Aggressive**. The ICAP sensor submits to Sandbox Analyzer almost all objects, regardless of their potential risk.

   In a dedicated field, you can define exceptions for the object types that you do not want to submit to Sandbox Analyzer.

   You can also define size limits of the submitted objects by selecting the corresponding check box and entering any desired values between 1 KB and 50 MB.
3. Under **Connection Settings**, select the preferred Sandbox Analyzer instance for submitting network content.

If you have your network behind a proxy server or a firewall, you can configure a proxy to connect to Sandbox Analyzer by selecting the **Use proxy configuration** check box.

You have to fill in the following fields:

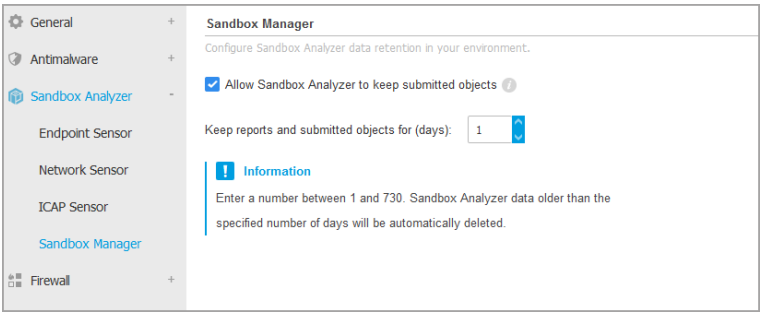
- **Server** - the IP of the proxy server.
- **Port** - the port used to connect to the proxy server.
- **Username** - a user name recognized by the proxy.
- **Password** - the valid password for the specified user.

4. Under **Detonation profile**, adjust the complexity level of behavioral analysis, while affecting the Sandbox Analyzer throughput. For example, if set to **High**, Sandbox Analyzer would perform a more accurate analysis on fewer samples, in the same interval, than on **Medium** or **Low**.

Sandbox Manager

In this section you configure data retention for your Sandbox Analyzer instances:

- Select the check box **Allow Sandbox Analyzer to keep submitted objects**. This setting allows you to use the **Resubmit to analyze** option in the submission cards area of the Sandbox Analyzer reporting interface.
- Specify the number of days you want Sandbox Analyzer to keep reports and submitted objects on the datastore. The maximum data you can enter is 730. After the defined period expires, all data will be deleted.



Policies > Sandbox Analyzer > Sandbox Manager

7.2.5. Firewall

Note
This module is available for Windows for workstations.

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. 288).

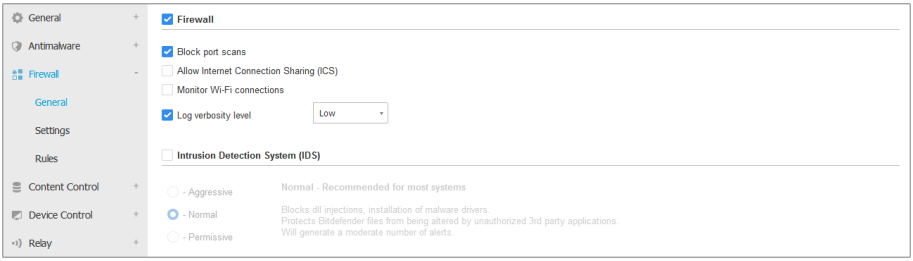
Important
The Firewall module is available only for supported Windows workstations.

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.).

  Note
  Intrusion Detection System (IDS) policy settings only apply to Endpoint Security (legacy security agent). Bitdefender Endpoint Security Tools agent integrates Host-Based Intrusion Detection System capabilities in its Advanced Threat Control (ATC) module.

  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.

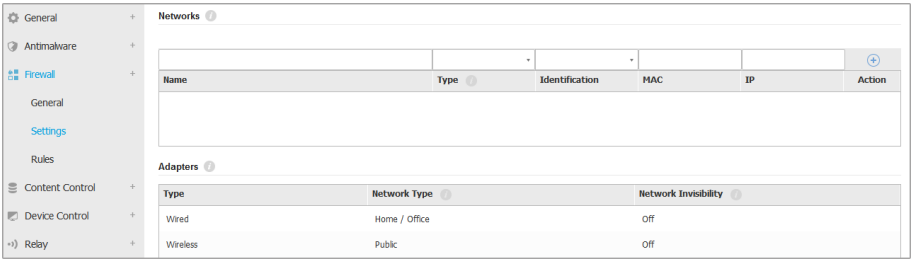
Important
Intrusion Detection System is only available for Endpoint Security clients.

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.

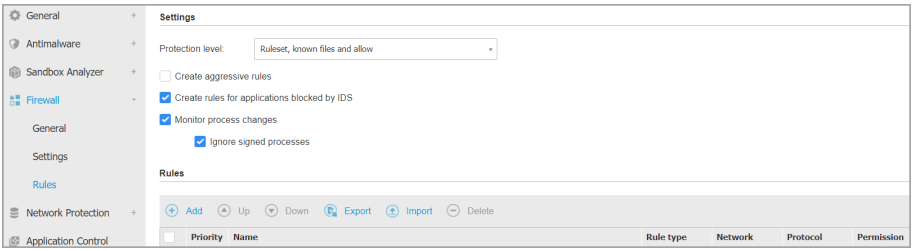
  If you select **Let Windows decide**, for any new network connection detected after the policy is applied, Bitdefender security agent applies a profile for the firewall based on the network classification in Windows, ignoring the settings from the **Adapters** table.

  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**.

  When the endpoint joined in Active Directory connects to the domain, the firewall profile is automatically set to **Home/Office** and the stealth settings are set to **Remote**. If the computer is not in a domain, this condition is not applicable.
- **Network Discovery.** Hides the computer from malicious software and hackers in the network or the Internet. Configure computer visibility in the network as needed, for each adapter type, by selecting one of the following options:
  - **Yes.** Anyone from the local network or the Internet can ping and detect the computer.
  - **No.** The computer is invisible from both the local network and the Internet.
  - **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 allowed.

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.

Network Printing
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.

Importing and Exporting Rules

You can export and import firewall rules to use them in other policies or companies. To export rules:

1. Click **Export** at the upper side of the rules 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.

Important

- Each row in the CSV file corresponds to a single rule and has multiple fields.
- The position of firewall rules in the CSV file determines their priority. You can change the priority of a rule by moving the entire row.

For the default set of rules, you can modify only the following elements:

- **Priority**: Set the priority of the rule in any order you wish by moving the CSV row.
- **Permission**: Modify the field `set.Permission` using the available permissions:
  - 1 for **Allow**
  - 2 for **Deny**

Any other adjustments are discarded at import.

For custom firewall rules, all field values are configurable as follows:

Field	Name and Value
`ruleType`	**Rule type**: 1 for **Application Rule** 2 for **Connection Rule**
`type`	The value for this field is optional.
`details.name`	**Rule name**
`details.applictionPath`	**Application path** (only for application-based rules)
`details.commandLine`	**Command line** (only for application-based rules)
`details.applicationMd5`	**Application MD5** (only for application-based rules)
`settings.protocol`	**Protocol** 1 for **Any** 2 for **TCP** 3 for **UDP** 4 for **Other**
`settings.customProtocol`	Required only if **Protocol** is set to **Other**. For specific values, consider this page. The values 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141-143 are not supported.
`settings.direction`	**Direction**: 1 for **Both** 2 for **Inbound** 3 for **Outbound**

Field	Name and Value
settings.ipVersion	**IP version**: 1 for **Any** 2 for **IPv4** 3 for **IPv6**
settings.localAddress.any	**Local Address** is set to **Any**: 1 for True 0 or empty for False
settings.localAddress.ipMask	**Local Address** is set to **IP or IP/Mask**
settings.remoteAddress.portRange	**Remote Address** is set to **Port or port range**
settings.directlyConnected.enable	**Apply rule only for directly connected computers**: 1 for enabled 0 for empty or disabled
settings.directlyConnected.remoteMac	**Apply rule only for directly connected computers** with **MAC address** filter.
permission.home	The **Network** to which the rule applies is **Home/Office**: 1 for True 0 for empty or False
permission.public	The **Network** to which the rule applies is **Public**: 1 for True 0 for empty or False
permission.setPermission	Available permissions: 1 for **Allow** 2 for **Deny**

To import rules:

1. Click **Import** at the upper side of the Rules table.
2. In the new window, click **Add** and select the CSV file.
3. Click **Save**. The table is populated with the valid rules.

7.2.6. Network Protection

Use the Network Protection section to configure your preferences regarding content filtering, data protection for user activity including web browsing, email and software applications, and detection of network attack techniques that try to gain access on specific endpoints. You can restrict or allow web access and application usage, configure traffic scan, antiphishing and data protection rules.

Please note that the configured Network Protection settings will apply to all users who log on to the target computers.

The settings are organized into the following sections:

- General
- Content Control
- Web Protection
- Network Attacks

Note

- The Content Control module is available for:
  - Windows for workstations
  - macOS
- The Network Attack Defense module is available for:
  - Windows for workstations

Important

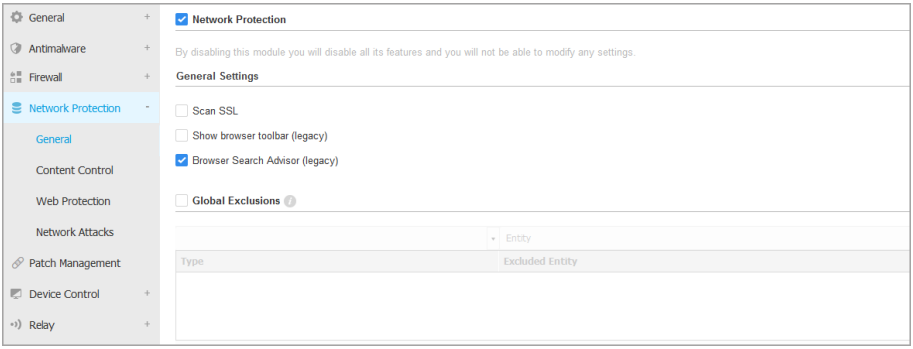
On macOS, Content Control relies on a kernel or system extension. Installing the extension requires your approval on macOS High Sierra (10.13) and later. The system notifies the user that a system extension from Bitdefender was blocked. User can allow it from **Security & Privacy** preferences. Until the user approves the Bitdefender system extension, this module will not work and the Endpoint Security for Mac user interface will show a critical issue prompting for approval.
To eliminate user intervention, you can pre-approve the Bitdefender extension by whitelisting it using a Mobile Device Management tool. For details about Bitdefender extensions, refer to this KB article.

General

In this page, you can configure options such as enabling or disabling functionalities and configure exclusions.

The settings are organized into the following sections:

- General Settings
- Global Exclusions



Computers and Virtual Machines Policies - Network Protection - General

General Settings

- **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 (legacy)**. 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.

Note

- This option is not available for macOS.
- This option is removed from Windows starting with new installations of Bitdefender Endpoint Security Tools version 6.6.5.82.

- **Browser Search Advisor (legacy).** 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.

  Note

  - This option is not available for macOS.
  - This option is removed from Windows starting with new installations of Bitdefender Endpoint Security Tools version 6.6.5.82.

Global Exclusions

You can choose to skip certain traffic of being scanned for malware while the **Network Protection** options are enabled.

Note
These exclusions apply to **Traffic Scan** and **Antiphishing**, in the **Web Protection** section, and to **Network Attack Defense**, in the **Network Attacks** section. **Data Protection** exclusions are configurable separately, in the **Content Control** section.

To define an 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/mask**. Enter the IP address or the IP mask for which you do not want to scan the incoming and outgoing traffic, which includes network attack techniques.

- **URL**. Excludes from scanning the specified web addresses. Take into account that URL-based scan exclusions apply differently for HTTP versus HTTPS connections, as explained hereinafter.

  You can define a URL-based scan exclusion as follows:

  – Enter a specific URL, such as `www.example.com/example.html`

    - In the case of HTTP connections, only the specific URL is excluded from scanning.
    - For HTTPS connections, adding a specific URL excludes the entire domain and any of its subdomains. Therefore, in this case, you can specify directly the domain to be excluded from scanning.

  – Use wildcards to define web address patterns (only for HTTP connections).

    Important
    Wildcard exceptions do not work for HTTPS connections.

    You can use the following wildcards:

    - Double asterisk (**) substitutes for zero or more characters.
    - Single asterisk (*) substitutes for zero or more charactersbetween th path delimiters.
    - 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.

    Note
    The option is available in both Control Center and Power User policy settings, under **Antimalware** > **Settings** > **Custom Exclusions** section.

  In the following table, you can find several syntax samples for specifying web addresses (URLs).

Syntax	Exception Applicability
`**\example.txt`	Any file named `example.txt` will be excluded (regardless of its location on the endpoint).

Syntax	Exception Applicability
`www.example*`	Any URL 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 URL ending in `example.com`, including subdomains thereof.
`*example.com*`	Any URL that contains the specified string.
`*.com`	Any website having the `.com` domain extension, including 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`.

Note
You can use protocol-relative URLs.

- **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".

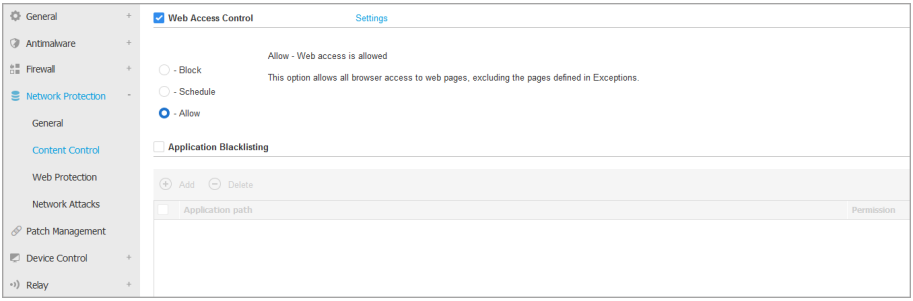
3. Click the ⊕ **Add** button at the right side of the table.

To remove an entity from the list, click the corresponding ⊗ **Delete** button.

Content Control

The Content Control settings are organized into the following sections:

- Web Access Control
- Application Blacklisting
- Data Protection



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.

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. For more information about the available website categories, refer to this KB article.

4. 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.
5. 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 detailed alerts on client** if you want to hide this information from the user.

   Note
   This option is not available for macOS.

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.

Application Blacklisting

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.

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.

Data Protection

Data Protection prevents unauthorized disclosure of sensitive data based on administrator-defined rules.

Note
This feature is not available for macOS.

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.

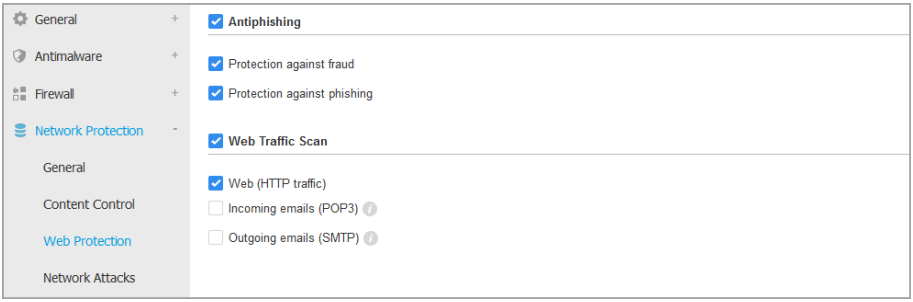
Note
If an email containing blocked data is addressed to multiple recipients, those for which exclusions have been defined will receive it.

To remove a rule or an exclusion from the list, click the corresponding ⊗ **Delete** button at the right side of the table.

Web Protection

In this page, the settings are organized under the following sections:

- Antiphishing
- Web Traffic Scan



Computers and Virtual Machines Policies - Network Protection - Web Protection

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. Go to **General** settings and click **Global 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**.

Web 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.

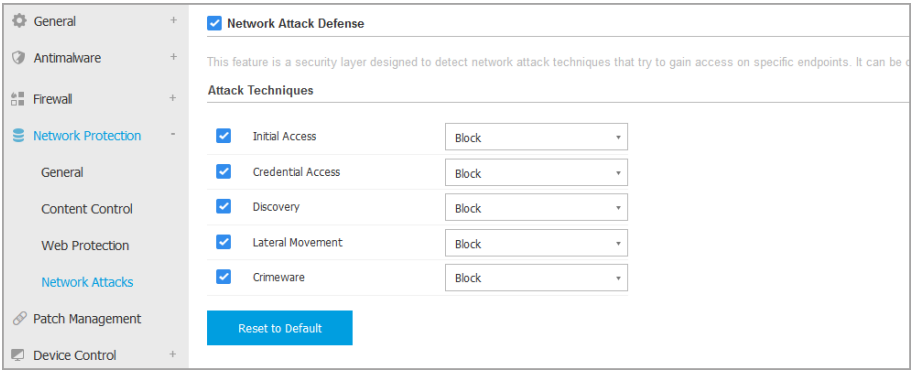
When an email is found infected, it is replaced automatically with a standard email informing the receiver of the original infected email. If a web page contains or distributes malware, it is automatically blocked. A special warning page is displayed instead to inform the user that the requested web 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.

Note
The **Incoming emails** and **Outgoing emails** options are not available for macOS.

Network Attacks

Network Attack Defense provides a security layer based on a Bitdefender technology that detects and takes actions against network attacks designed to gain access on endpoints through specific techniques such as: brute-force attacks, network exploits and password stealers.



Computers and Virtual Machines Policies - Network Protection - Network Attacks

To configure Network Attack Defense:

1. Select the **Network Attack Defense** check box to enable the module.
2. Select the corresponding check boxes to enable protection against each network attack category. The network attack techniques are grouped according to MITRE's ATT&CK knowledge base as follows:
   - **Initial Access** - the attacker gains entry within a network by various means, including vulnerabilities of public-facing web servers. For example: information disclosure exploits, SQL injection exploits, drive-by download injection vectors.
   - **Credential Access** - the attacker steals credentials like usernames and passwords to gain access into the systems. For example: brute-force attacks, unauthorized authentication exploits, password stealers.

- **Discovery** - the attacker, once infiltrated, tries to obtain information about the systems and the internal network, before deciding what to do next. For example: directory traversal exploits, HTTP directory traversal exploits.
- **Lateral Movement** - the attacker explores the network, often by moving through multiple systems, to find the main target. The attacker may use specific tools to accomplish the objective. For example: command injection exploits, Shellshock exploits, double extention exploits.
- **Crimeware** - this category comprises techniques designed to automate cybercrime. For example, Crimeware techniques are: nuclear exploits, various malware software such as Trojans and bots.

3. Select the actions you want to take against each category of network attack techniques from the following options:
   a. **Block** - Network Attack Defense stops the attack attempt once detected.
   b. **Report Only** - Network Attack Defense informs you about the detected attack attempt, but it will not try to stop it.

You can easily restore the initial settings by clicking the **Reset to Default** button at the lower side of the page.

Details about network attack attempts are available in the Network Incidents report and in the Network Incidents event notification.

7.2.7. Patch Management

Note
This module is available for:

- Windows for workstations
- Windows for servers

The Patch Management module releases you from the burden of keeping the endpoints updated with the latest software patches, by automatically distributing and installing patches for a vast variety of products.

Note
You can check the list of supported vendors and products in this KB article.

This policy section contains the settings for automatic patch deployment. First you will configure how patches are downloaded to the endpoints, and then which patches to install and when.

Configuring Patch Download Settings

The patch dissemination process is using Patch Caching Servers to optimize the network traffic. Endpoints connect to these servers and download patches through the local network. For high availability of patches, it is recommended to use more than one server.

To assign Patch Caching Servers to target endpoints:

1. Under the **Patch Download Settings** section, click the field at the upper side of the table. The list of detected Patch Caching Servers is displayed.

   If the list is empty, then you need to install the Patch Cashing Server role on Relays in your network. For more information, refer to the Installation Guide.

2. Select the server you want from the list.
3. Click the ⊕ **Add** button.
4. Repeat the previous steps to add more servers, if needed.
5. Use the up and down arrows at the right side of the table to establish server priority. Priority decreseases from top to bottom of the list.

   An endpoint requests a patch from the assigned servers in order of priority. The endpoint downloads the patch from the server where it finds it first. A server that lacks a requested patch will automatically download it from the vendor, to make it available for future requests.

To delete servers you no longer need, click the corresponding ⊖ Delete button at the right side of the table.

Select the option **Use vendors websites as fallback location for downloading the patches** to make sure your endpoints receive software patches in case Patch Caching Servers are unavailable.

Configuring Patch Scanning and Installation

GravityZone performs patch deployment in two independent phases:

1. Assessment. When requested via the management console, endpoints scan for missing patches and report them back.

2. Installation. The console sends the agents a list of patches you want to install. The endpoint downloads the patches from the Patch Caching Server and then installs them.

The policy provides the settings to automate these processes, partly or entirely, so that they run periodically based on the preferred schedule.

To set up automatic patch scanning:

1. Select the **Automatic patch scan** check box.
2. Use the scheduling options to configure the scan recurrence. You can set the scan to run daily or in certain days of the week, at a certain time.
3. Select **Smart scan when a new app/program is installed** to detect whenever a new application has been installed on the endpoint and what patches are available for it.

To configure automatic patch installation:

1. Select the **Install patches automatically after scan** check box.
2. Select which types of patches to install: security, others or both.
3. Use the scheduling options to configure when to run the installation tasks. You can set the scan to run immediately after the patch scan finishes, daily or in certain days of the week, at a certain time. We recommend to install security patches immediately they are discovered.
4. By default, all products are eligible for patching. If you want to automatically update only a set of products, which you consider essential to your business, follow these steps:
   a. Select the **Specific vendor and product** check box.
   b. Click the **Vendor** field at the upper side of the table. A list with all supported vendors is displayed.
   c. Scroll the list and select a vendor for the products you want to patch.
   d. Click the **Products** field at the upper side of the table. A list with all products of the selected vendor is displayed.
   e. Select all products you want to patch.
   f. Click the ⊕ **Add** button.
   g. Repeat the previous steps for the remaining vendors and products.

If you forgot to add a product or you want to remove one, find the vendor in the table, double-click the **Products** field and select or deselect the product in the list.

To remove a vendor with all of its products, find it in the table and click the corresponding ⊖ **Delete** button at the right side of the table.

5. From various reasons, an endpoint may be offline when patch installation is scheduled to run. Select the option **If missed, run as soon as possible** to install the patches immediately after the endpoint comes back online.
6. Some patches may require system reboot to finish installation. If you want to do this manually, select the option **Postpone reboot**.

Important
For the assessment and installation to be successful on Windows endpoints, you must ensure the following requirements are met:

- **Trusted Root Certification Authorities** stores the **DigiCert Assured ID Root CA** certificate.
- **Intermediate Certification Authorities** includes the **DigiCert SHA2 Assured ID Code Signing CA**.
- Endpoints have installed the patches for Windows 7 and Windows Server 2008 R2 mentioned in this Microsoft article: Microsoft Security Advisory 3033929

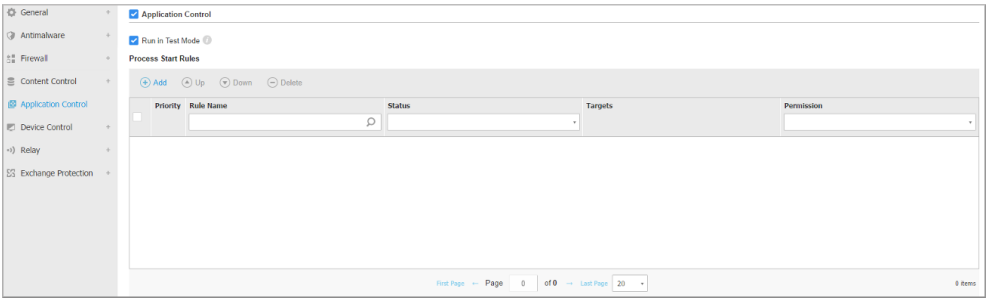
7.2.8. Application Control

Note
This module is available for:

- Windows for workstations
- Windows for servers

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. 92). 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. 178).

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. 504).
- **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. 539)

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.

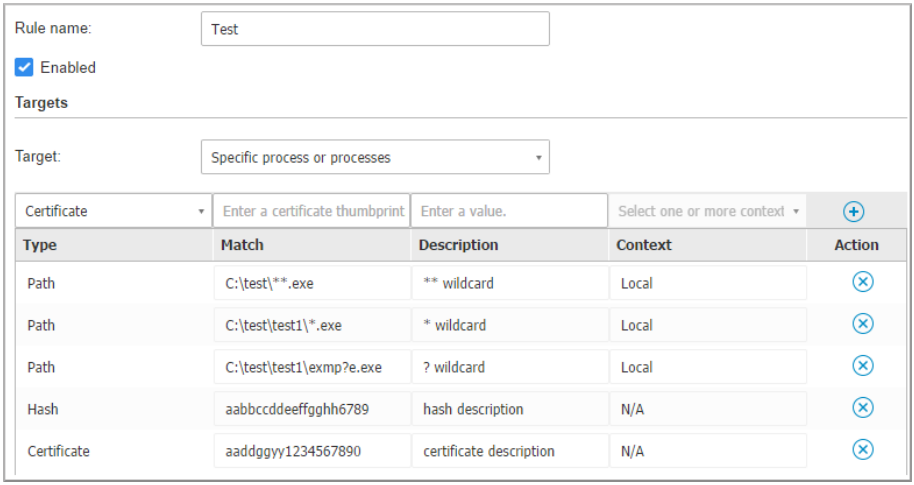
To create a process start rule:

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. 539)

     - 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. 539)



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. 178).

  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.

7.2.9. Device Control

Note
This module is available for:

- Windows for workstations
- Windows for servers
- macOS

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
On macOS, Device Control relies on a kernel or system extension. Installing the extension requires user's approval on macOS High Sierra (10.13) and later. The system

notifies the user that a system extension from Bitdefender was blocked. User can allow it from **Security & Privacy** preferences. Until the user approves the Bitdefender system extension, this module will not work and the Endpoint Security for Mac user interface will show a critical issue prompting for approval.
To eliminate user intervention, you can pre-approve the Bitdefender extension by whitelisting it using a Mobile Device Management tool. For details about Bitdefender extensions, refer to this KB article.

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.

In the following table, you can find the types of devices supported by Device Control on Windows and macOS systems:

Device Type	Windows	macOS
Bluetooth Devices	x	x
CD-ROM Devices	x	x
Floppy Disc Drives	x	N/A
IEEE 1284.4	x	
IEEE 1394	x	
Imaging devices	x	x
Modems	x	Managed under Network Adapters
Tape Drives	x	N/A
Windows Portable	x	x
COM/LPT Ports	x	LPT to serial ports supported
SCSI Raid	x	
Printers	x	Supports only locally connected printers
Network Adapter	x	x (including Wi-Fi dongles)
Wireless Network Adapters	x	x
Internal Storage	x	

Device Type	Windows	macOS
External Storage	x	x

Note

- On macOS, if the **Custom** permission is selected for a specific device class, only the permission configured for the **Other** subcategory will apply.
- On Windows and macOS, Device Control allows or denies access to the entire Bluetooth adapter at the system level, according to the policy. There is no possibility of setting granular exclusions per paired device.

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:

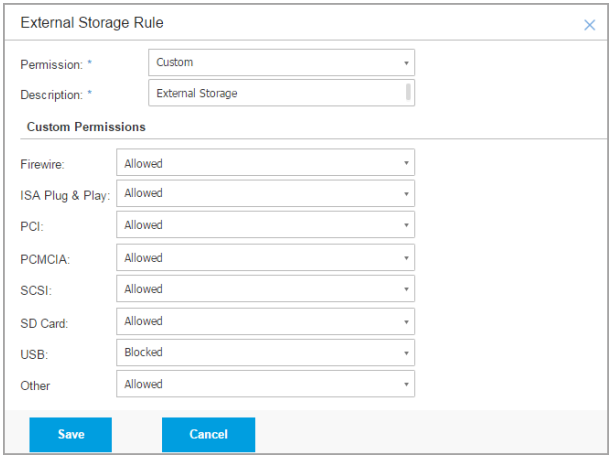
1. Go to **Device Control > Rules**.
2. Click the device name in the available table.
3. Select one permission type from the available options. Please note that the available set of permissions may vary according to the device type:
   - **Allowed**: the device can be used on the target endpoint.
   - **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.

     Important
     Connected devices previously blocked are not automatically unblocked by changing the permission to **Allowed**. The user must restart the system or reconnect the device to be able to use it.

   - **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**.

     Note
     You can manually configure wildcard exclusions based on Device ID, by using the syntax `wildcards:deviceID`. Use the question mark (?) to replace one character, and the asterisk (*) to replace any number of characters in the `deviceID`. For example, for `wildcards:PCI\VEN_8086*`, all devices containing the string `PCI\VEN_8086` in their ID will be excluded from the policy rule.

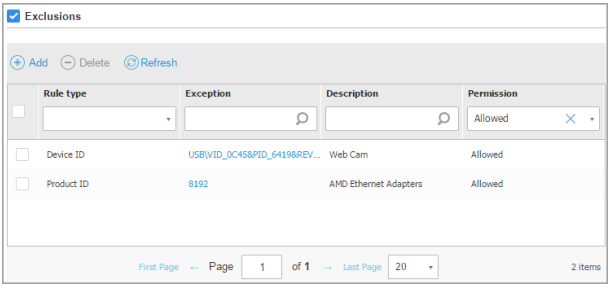
   - **From Discovered Devices**. In this case, you can select the Devices IDs or Product IDs to exclude from a list of all discovered devices in your network (concerning the managed endpoints only):
     a. Select the exclusion type (by Product ID or by Device ID).
     b. In the **Exclusions** table, 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.
     - Connected devices previously blocked are not automatically unblocked by setting an exception with the permission **Allowed**. The user must restart the system or reconnect the device to be able to use it.

All device exclusions will appear in the **Exclusions** table.

To remove an exclusion:

1. Select it in the table.
2. Click the ⊕ **Delete** button at the upper side of the table.



Computers and Virtual Machines Policies - Device Control - Exclusions

7.2.10. Relay

Note
This module is available for:

- Windows for workstations
- Windows for servers
- Linux

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.

7.2.11. Exchange Protection

Note
This module is available for Windows for servers.

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. 536).

    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. 536).

    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. 343).
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. 341).

  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. 345)

  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. If no DNS server address is configured, or if the DNS server is unavailable, the RBL filter uses the system's DNS servers.
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. 347).

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. 347).

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. 537).

   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**.

7.2.12. Encryption

Note
This module is available for:

- Windows for workstations
- Windows for servers
- macOS

The Encryption module manages full disk encryption on endpoints by leveraging BitLocker on Windows and FileVault and the diskutil command-line utility on macOS, respectively.

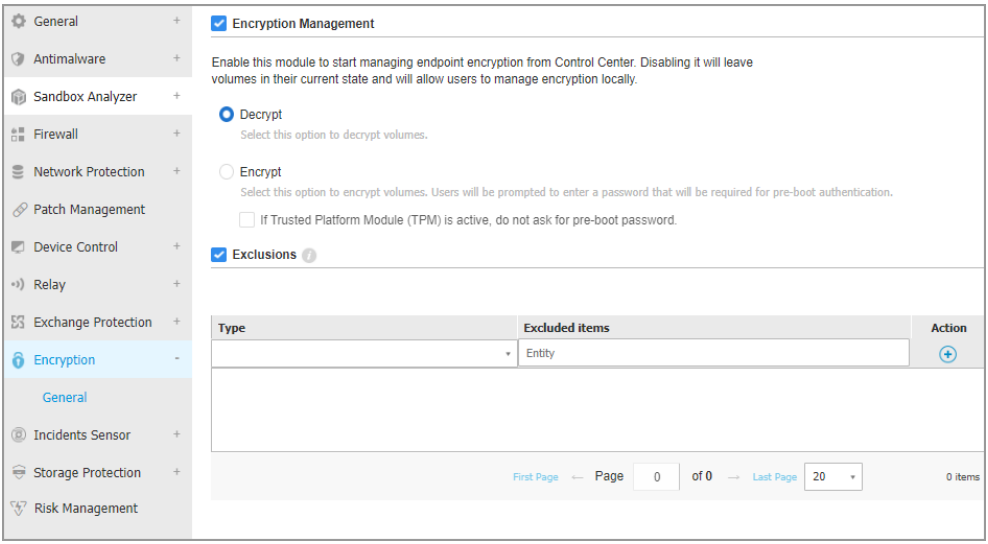
With this approach, GravityZone is able to provide some consistent benefits:

- Data secured in case of lost or stolen devices.
- Extensive protection for the most popular computer platforms in the world, by using recommended encryption standards with full support from Microsoft and Apple.
- Minimal impact on the endpoints' performance due to the native encryption tools.

The Encryption module operates the following solutions:

- BitLocker version 1.2 and later, on Windows endpoints with a Trusted Platform Module (TPM), for boot and non-boot volumes.
- BitLocker version 1.2 and later, on Windows endpoints without a TPM, for boot and non-boot volumes.
- FileVault on macOS endpoints, for boot volumes.
- diskutil on macOS endpoints, for non-boot volumes.

For the list of operating systems supported by the Encryption module, refer to GravityZone Installation Guide.



The Encryption page

To start managing endpoint encryption from Control Center, select the **Encryption Management** check box. As long as this setting is enabled, the endpoint users cannot manage encryption locally and all their actions will be canceled or reverted. Disabling this setting will leave the endpoint volumes in their current state (encrypted or unencrypted) and the users will be able to manage encryption on their machines.

To manage the encryption and decryption processes, three options are available:

- **Decrypt** – decrypts volumes and keeps them unencrypted when the policy is active on the endpoints.
- **Encrypt** – encrypts volumes and keeps them encrypted when the policy is active on the endpoints.

  Under the Encrypt option, you can select the check box **If Trusted Platform Module (TPM) is active, do not ask for password to encrypt**. This setting provides encryption on Windows endpoints with TPM, without requiring an encryption password from users. For details, refer to “Encrypting Volumes” (p. 359).
- **Exclusions** - excludes specific drives, including drive letters or partition labels and names.

GravityZone supports the Advanced Encryption Standard (AES) method with 128 and 256-bit keys on Windows and macOS. The actual encryption algorithm used depends on each operating system configuration.

Note
GravityZone detects and manages volumes manually encrypted with BitLocker, FileVault and diskutil. To start managing these volumes, the security agent will prompt the endpoint users to change their recovery keys. In case of using other encryption solutions, the volumes must be decrypted before applying a GravityZone policy.

Encrypting Volumes

To encrypt volumes:

1. Select the **Encryption Management** check box.
2. Choose the **Encrypt** option.

The encryption process begins after the policy becomes active on the endpoints, with some particularities on Windows and Mac.

On Windows

By default, the security agent will prompt the users to configure a password to start encryption. If the machine has a functional TPM, the security agent will prompt the users to configure a personal identification number (PIN) to start encryption. The users have to enter the password or PIN configured at this stage every time the endpoint starts, in a pre-boot authentication screen.

Note
The security agent allows you to configure the PIN complexity requirements and the users' privileges to change their PIN through BitLocker Group Policy (GPO) settings.

To start encryption without requiring a password from the endpoint users, enable the check box **If Trusted Platform Module (TPM) is active, do not ask for pre-boot password**. This setting is compatible with Windows endpoints having TPM and UEFI.

When the check box **If Trusted Platform Module (TPM) is active, do not ask for pre-boot password** is enabled:

- On unencrypted endpoint:
  - The encryption proceeds without requiring a password.

  - The pre-boot authentication screen does not appear when starting the machine.
- On endpoint encrypted with password:
  - The password is removed.
  - The volumes remain encrypted.
- On encrypted or unencrypted endpoint without TPM or with TPM not detected or not functioning:
  - The user is prompted to enter a password for encryption.
  - The pre-boot authentication screen appears when starting the machine.

When the check box **If Trusted Platform Module (TPM) is active, do not ask for pre-boot password** is disabled:

- The user must enter a password for encryption.
- The volumes remain encrypted.

On Mac

To start encryption on boot volumes, the security agent will prompt the users to enter their system credentials. Only users having local accounts with administrative privileges can enable encryption.

To start encryption on non-boot volumes, the security agent will prompt the users to configure an encryption password. This password will be required to unlock the non-boot volume every time the computer starts. If the computer has more than one non-boot volume, the users must configure an encryption password for each one of them.

Decrypting Volumes

To decrypt volumes on the endpoints:

1. Select the **Encryption Management** check box.
2. Choose the **Decrypt** option.

The decryption process begins after the policy becomes active on the endpoints, with some particularities on Windows and Mac.

On Windows

The volumes are decrypted with no interaction from users.

On Mac

For boot volumes, the users must enter their system credentials. For non-boot volumes, the users must enter the password configured during the encryption process.

In case the endpoint users forget their encryption passwords, they need recovery keys to unlock their machines. For details about retrieving the recovery keys, refer to "Using Recovery Manager for Encrypted Volumes" (p. 97).

Excluding Partitions

You can create a list of exclusions from encryption by adding specific drive letters, partition labels and names, and partition GUID. To create a rule to exclude partitions from encryption:

1. Select the **Exclusions** check box.
2. Click **Type** and choose a drive type from the dropdown menu.
3. Enter a drive value in the **Excluded items** field and consider the following conditions:
   - For a **Drive Letter** enter `D:`, or your drive letter followed by a colon.
   - For a **Label/Name** you can enter any label, such as `Work`.
   - For a **GUID** partition enter a value as follows: `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.
4. Click **Add** ⊕ to add the exclusion to the list.

To delete an exclusion, choose and item and click **Delete** ⊗.

7.2.13. 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 GravityZone Control Center. In vSphere it will appear preceded by the `Bitdefender_` prefix. Choose this name wisely as it will become read-only after the policy is saved.

7.2.14. Storage Protection

Note
Storage Protection is available for Network-Attached Storage (NAS) devices and file-sharing solutions compliant with Internet Content Adaptation Protocol (ICAP).

In this section you can configure Security Servers as scanning service for NAS devices and file-sharing solutions compliant with ICAP, such as Nutanix Files and Citrix ShareFile.

Security Servers scan any files, including archives, when requested by the storage devices. Depending on the settings, Security Servers take appropriate actions on infected files, such as disinfecting or denying access.

The settings are organized into the following sections:

- ICAP
- Exclusions

ICAP

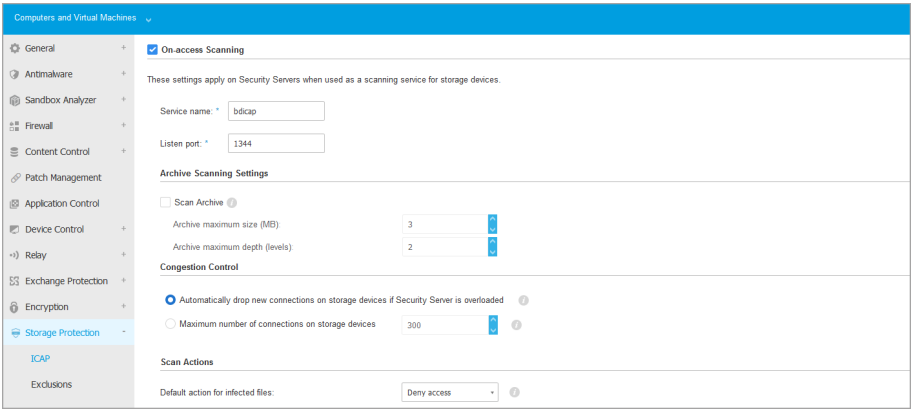
You can configure the following options for Security Servers:

- Select the **On-access Scanning** check box to enable the Storage Protection module. The required settings for communication between Security Servers and the storage devices are predefined as follows:
  - Service name: `bdicap`.
  - Listen port: `1344`.
- Under **Archive Scanning Settings**, select the **Scan Archive** check box to enable archive scanning. Configure the maximum size and the maximum depth of the archives to be scanned.

  Note
  If you set the archive maximum size to 0 (zero), Security Server scans archives regardless of their size.

- Under **Congestion Control**, choose the preferred method of managing the connections on storage devices in case of Security Server overloading:
  - **Automatically drop new connections on storage devices if Security Server is overloaded**. When one Security Server has reached a maximum number of connections, the storage device will redirect the surplus to a second Security Server.
  - **Maximum number of connections on storage devices**. The default value is set to 300 connections.

- Under **Scan Actions**, the following options are available:
  - **Deny access** – Security Server denies access to infected files.
  - **Disinfect** – Security Server removes the malware code from infected files.



Policies - Storage Protection - ICAP

Exclusions

If you want specific objects to be excluded from scanning, select the **Exclusions** check box.

You can define exclusions:

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

Configuring Exclusions

To add an exclusion:

1. Select the exclusion type from the menu.
2. Depending on the exclusion type, specify the object to be excluded as follows:
   - **Hash** – enter SHA-256 hashes separated by comma.
   - **Wildcard** – specify an absolute or a relative pathname by using wildcard characters. The asterisk symbol (*) matches any file within a directory. A question mark (?) matches exactly one character.

3. Add a description for the exclusion.
4. Click the ⊕ **Add** button. The new exclusion 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 exclusions in more policies, you can choose to export and import them.

To export 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 exclusion, having the fields in the following order:

```
<exclusion type>, <object to be excluded>, <description>
```

These are the available values for the CSV fields:

Exclusion type:
`1`, for for SHA-256 hash

`2`, for for wildcard

Object to be excluded:
A hash value or a pathname

Description
A text to help identify the exclusion.

Example of exclusions in the CSV file:

```
2,*/file.txt,text
2,*/image.jpg,image
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

To import exclusions:

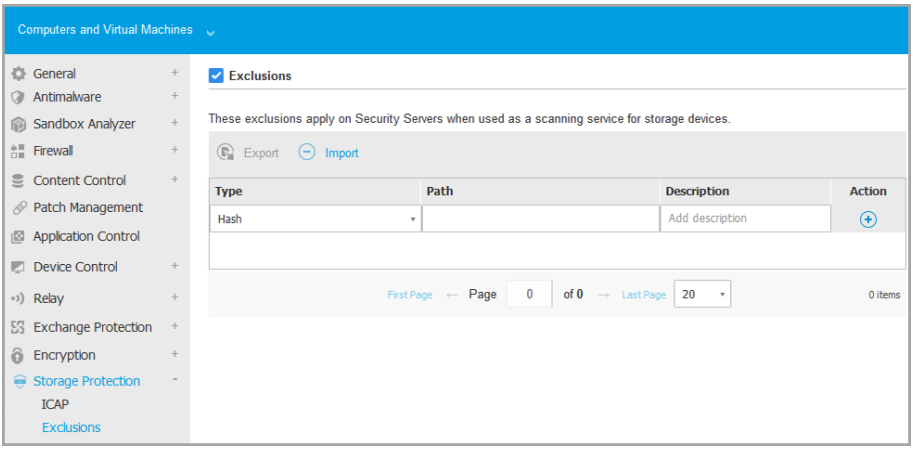
1. Click **Import**. The **Import Policy Exclusions** window opens.

2. Click **Add** and then select the CSV file.
3. Click **Save**. The table is populated with the valid exclusions. If the CSV file contains invalid exclusions, a warning informs you of the corresponding row numbers.

Editing Exclusions

To edit an exclusion:

1. Click the exclusion name in the **Path** column or the description.
2. Edit the exclusion.
3. Press `Enter` when finished.

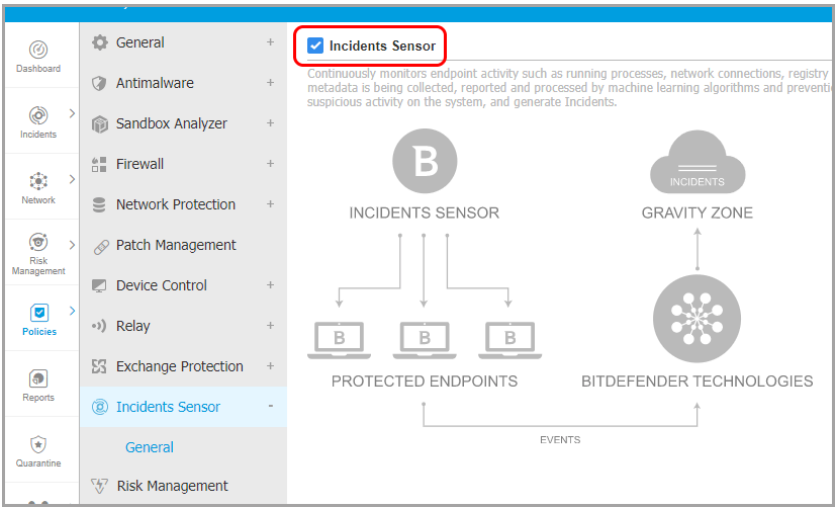


Policies - Storage Protection - ICAP

7.2.15. Incidents Sensor

The Incidents Sensor continuously monitors endpoint activity such as running processes, network connections, registry changes, and user behavior.This metadata is being collected, reported and processed by machine learning algorithms and prevention technologies that detect suspicious activity on the system, and generate Incidents.

Check the Incidents Sensor box to enable this module.



Incidents Sensor

7.3. 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**.

7.3.1. 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.

7.3.2. 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.

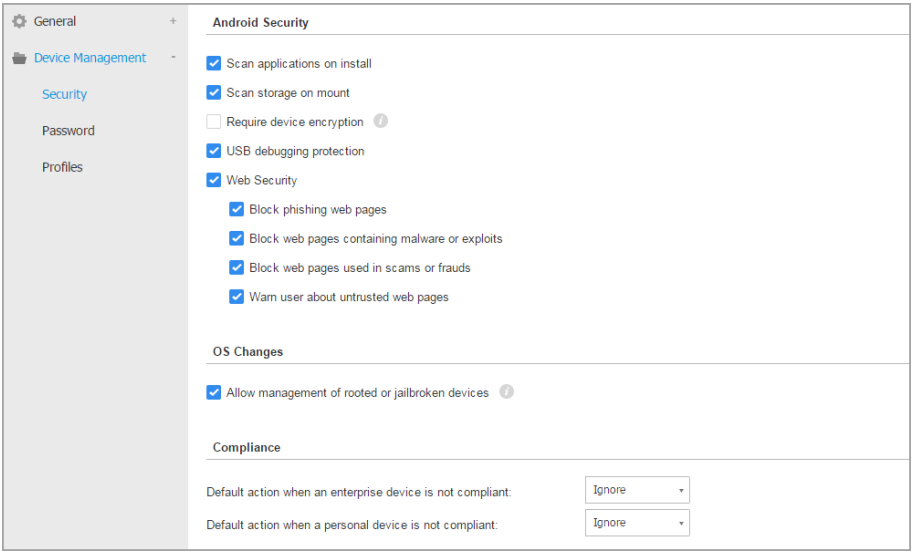
The settings are organized into the following sections:

- 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 up to Android 5, and 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 only if there is no lock protection configured on the device. This will not override an already configured lock screen option such as Pattern, PIN, Password, Fingerprint or Smart Lock.
  - 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.

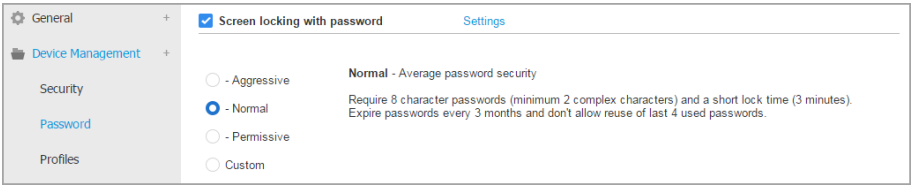
  Note
  Wipe does not currently erase data from mounted devices (SD cards).

- **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

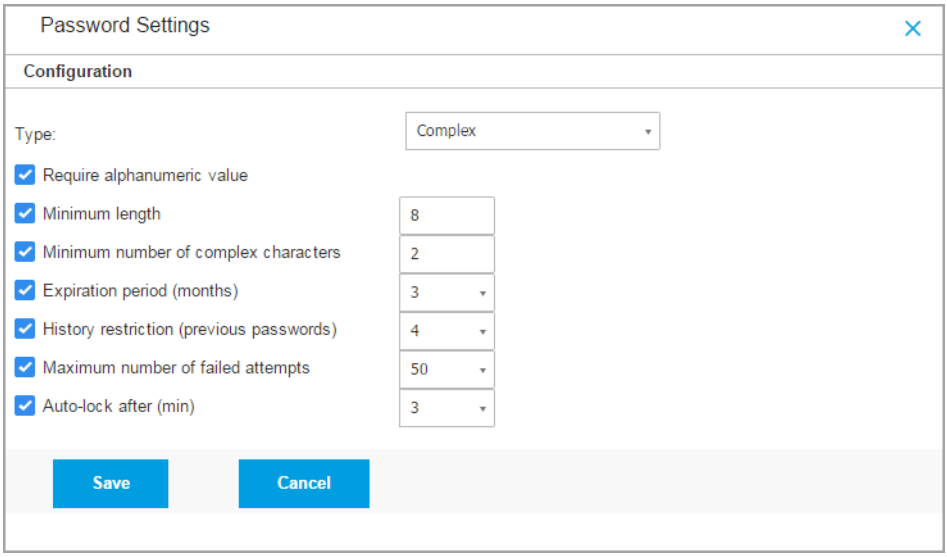
If the user does not set a password when prompted, the device can be used without a lock screen password up to 24 hours after the first notification. During this time, a message asking the user to enter a lock screen password is prompted every 15 minutes on the screen.

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.

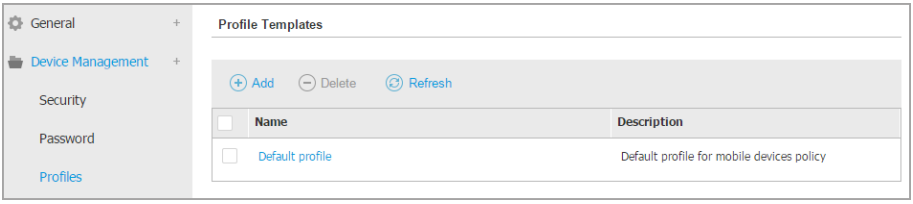
> **Note**
> The iOS devices have a predefined list for auto-lock time and do not allow custom values. When assigning a policy with an incompatible auto-lock value, the device enforces the next more restrictive time period available in the list. For example, if the policy has auto-lock set at three minutes, 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. 378)
   - "Networks" (p. 378)
   - "Web Access" (p. 382)
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**.

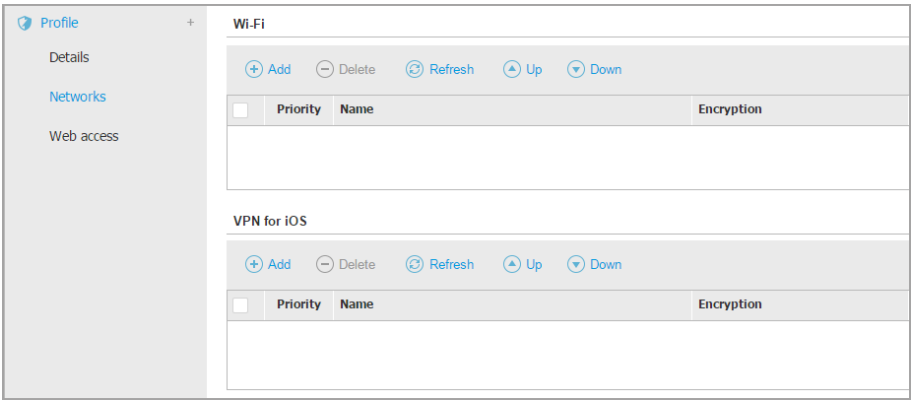
Details

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.

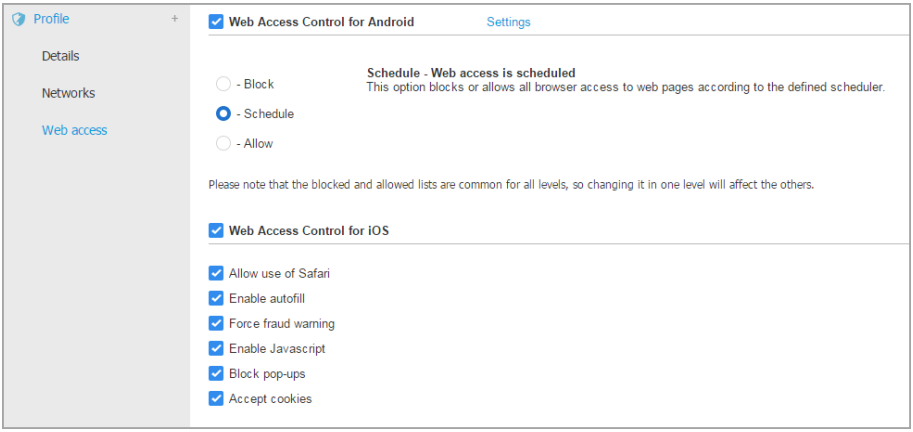
3. Click **Save**. The new VPN connection will be added to the list.

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 Chrome and 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.

  Important
  Web Access Control for Android works only up to Android 5, and only with Chrome and the built-in Android browser.

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.

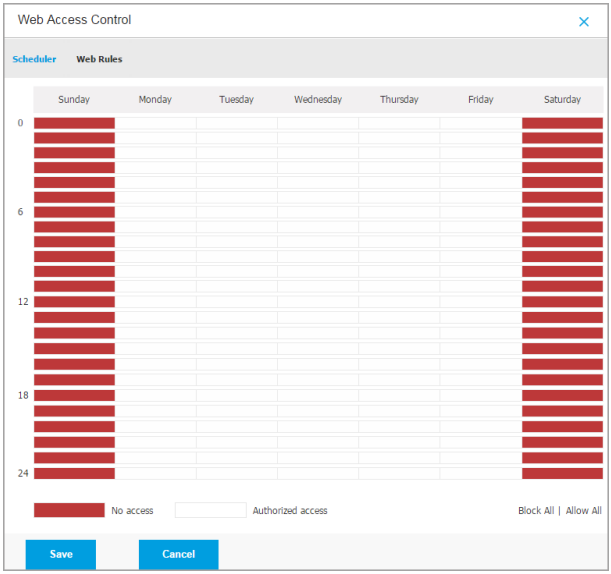
Either if you choose to allow or block the web access, you can define exceptions to these actions for entire web categories or only for specific web addresses. Click **Settings** to configure your web access schedule and exceptions as follows:

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.

Important
Web Access Control for iOS is not supported starting with iOS 13.

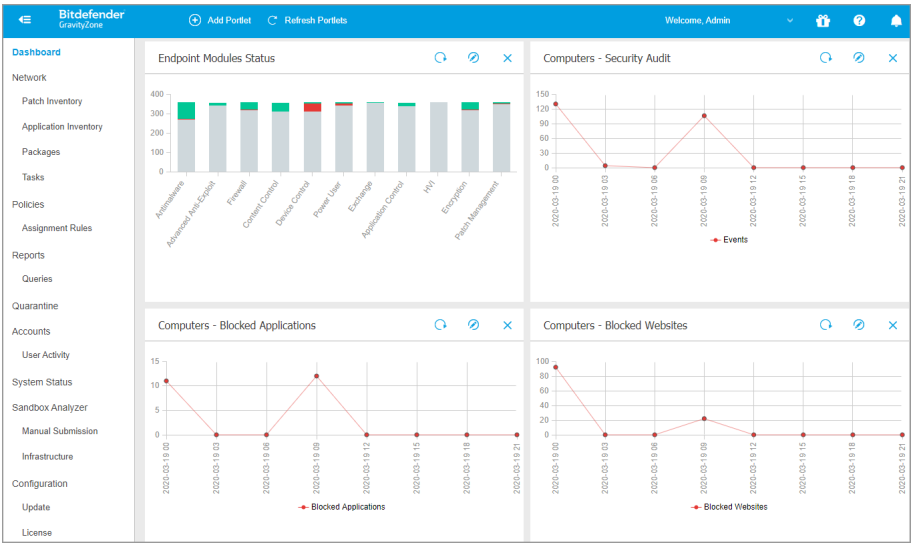
8. MONITORING DASHBOARD

Proper analysis of your network security requires data accessibility and correlation. Having centralized security information allows you to monitor and ensure compliance with the organization security policies, quickly identify issues, analyze threats and vulnerabilities.

8.1. Dashboard

The Control Center Dashboard is a customizable visual display providing a quick security overview of all protected endpoints and network status.

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 vertical scroll bar or the up and down arrow keys 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.

8.1.1. Refreshing Portlet Data

To make sure the portlet displays the latest information, click the **Refresh** button on its title bar.

To update the information for all the portlets at once, click the **Refresh Portlets** button at the top of the dashboard.

8.1.2. 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.

8.1.3. 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. 446).
4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

8.1.4. 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.

8.1.5. Rearranging Portlets

You can rearrange dashboard portlets to better suit your needs. To rearrange portlets:

1. Go to the **Dashboard** page.
2. Drag and drop each portlet to the desired position. All other portlets between the new and old positions are moved to preserve their order.

Note
You can move portlets only within the positions already taken.

9. INVESTIGATING INCIDENTS

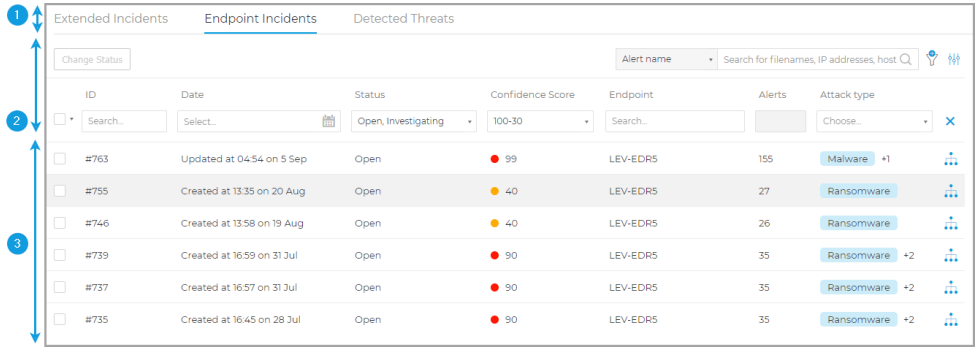
The **Incidents** section helps you filter, investigate and take actions on all security events detected by Incidents Sensor over a specific time interval.

The **Incidents** section contains the following pages:

- **Incidents**: allows viewing and investigating security events.
- **Blocklist**: manages blocked files involved in security events.

9.1. The Incidents Page

Use the **Incidents** page to filter and manage security events.



Incidents page overview

Note
Availability of these tabs may differ depending on the license included in your current plan.

This page contains the following areas:

1. A window bar with tabs that include different incident types:
   - **Detected Threats**: displays all security events identified as threats by GravityZone prevention modules. These incidents are detected at endpoint level and are acted upon with actions predefined in the security policies applied to your environment.
2. Filtering options to customize your grid:

- Click the **Show/Hide Columns** button to add or remove filter columns.

  The page will update automatically, loading the security event cards with information matching the added columns.

- Click the **Show/Hide Filters** button to show or hide the filters bar.

- Click the **Clear Filters** button to reset all filters.

3. The Incidents grid, which displays a list of security events according to the applied filters.

Note
This feature no longer provides support for Internet Explorer.

The Overview bar

The **Overview** bar lists open incidents, top alerts, affected devices, among other relevant data, to give you a quick view of the overall situation on the threats your environment is facing.

The Overview bar

Note
Availability and content of the **Overview** bar may differ depending on the license included in your current plan.

Filtering incidents from the Overview bar

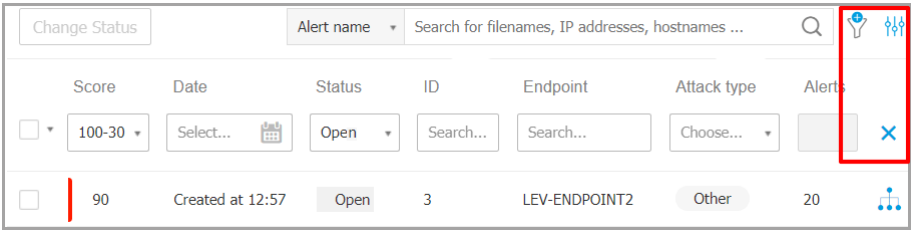
You can filter the incidents list by selecting values in the Overview bar:

- If you click a value in the **OPEN INCIDENTS** section it will display only the incidents with the selected level of severity.
- If you click a value in the **TOP ALERTS** section it will populate the search field with the alert name and display only the incidents where the alert was detected.

- If you click a value in the **TOP TECHNIQUES** section it will populate the search field with the technique name and display only the incidents where the technique was detected.
- If you click a value in the **TOP AFFECTED DEVICES** section, it will display only the incidents affecting the selected device.

9.1.1. The Filters Grid

The **Incidents** page allows you to choose what incidents to display by customizing the filters grid.



The Filters Grid

- Click the **Show/Hide Columns** button to add or remove filter columns.

  The page will update automatically, loading the security event cards with information matching the added columns.
- Click the **Show/Hide Filters** button to show or hide the filters bar.
- Click the **Clear Filters** button to reset all filters.

Find details of the available filtering options in the following table:

Filtering Option	Details
Score	The confidence score is a number between 100 and 10, indicating how potentially dangerous a security event is. The higher the score, the more certain the event is dangerous. To filter by confidence score, drag the slider bar to the chosen values. Or, you can use the number fields below the slider bar. Click **OK** to confirm the score selection.

Filtering Option	Details
Date	To filter by date: 1. Click the calendar icon or the **Date** field to open the date configuration page. 2. Select the time frame when the incident occurred: • Click the **From** and **To** tabs to select the dates defining the time interval. **Note** You can specify the exact time for the start and end dates, using the hours and minutes fields below the calendar. • You can also select a predetermined time frame, relative to the current time. 3. Click **OK** to apply the filter.
Status	Filter the incidents by their current status by checking one or more of the status options available in the **Status** drop-down menu: • **Open**: for uninvestigated security events • **Investigating**: for security events under investigation • **False Positive**: for security events labeled as false alarm • **Closed**: for security events with closed investigation
ID	Narrow the incident list by searching a specific security event ID number.
Endpoint	Narrow the incident list by searching a specific endpoint name from your managed network.
Attack Type	The attack type is a dynamic list of the most common types of attack, which changes based on the attack indicators found in the listed security events.
Alerts	The **Alerts** column displays the number of alerts triggered per incident.
Endpoint OS	This option filters the security events by operating system of involved endpoints.

Note
Filtering options may vary depending on the type of license key included in your current plan.

To search for more elements that are not visible in the filter grid, select one of the search options from the **Search** drop-down menu:

- **Alert name** - 3 to 1000 max. characters.
- **Endpoint IP** - 45 maximum characters.
- **MD5** - 32 maximum characters.
- **SHA256** - 64 maximum characters.
- **Node name** - 360 maximum characters.
- **Username** - 1000 maximum characters.

The page will update automatically, loading only the security event cards matching the searched element.

9.1.2. Viewing the List of Security Events

The **Incidents** page displays a list of security events matching the selected filters.

By default, there are 20 events per page, bundled by date. The page auto-refreshes at regular intervals, as the **Incidents Sensor** detects new events.

Important
All security events older than 90 days are automatically deleted from the **Detected Threats** section, and also from the security events repository.

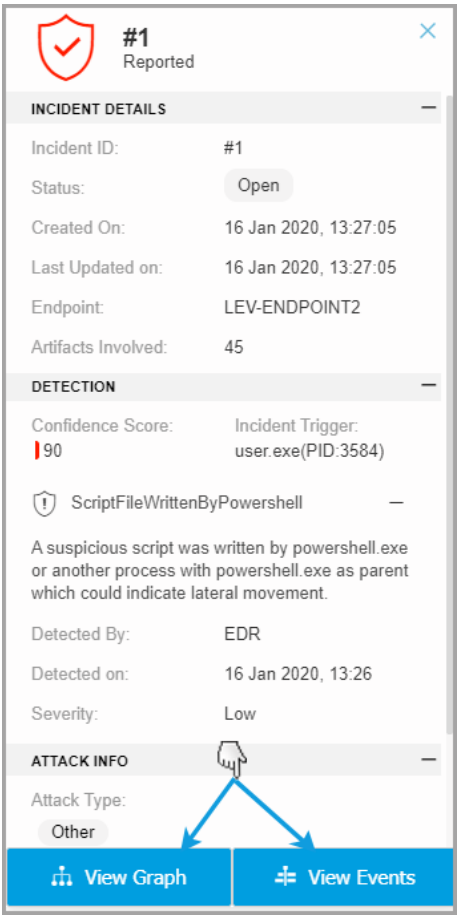
To navigate through the page, use the arrow keys, scroll wheel, or click the scroll bar. Change the number of displayed events at the bottom of the page. You can go up to 100 events per page.

Each security event entry is listed in a rich card format, providing an overview of each incident, with information based on the selected filters.

Note
Check the left-border color for quickly assessing the confidence level (low, medium or high).

Security Event Card

- If you click the corresponding **View Graph** button of a security event card, it will open it in a new page, where you can analyze the incident in detail and take appropriate actions.
- If you click on a security event card, it will open a side quick view panel with information about the selected incident.



Quick View of Incident Details

- Click the **View Graph** button to access the graphic visualization of the incident.
- Click the **View Events** button to access the incident's timeline.

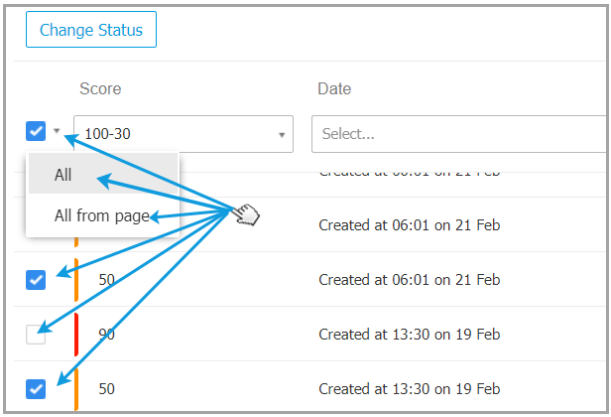
- If you select the check box of any security event card, it will activate the **Change Status** button, allowing you to change the current status of the incident.

Changing the Status of Security Events

The investigation status helps you keep track of incidents that have already been investigated, and marked as closed or false positive, incidents that are currently under investigation, and open, or new incidents that have yet to be analyzed.

You can choose to change the status of one or multiple security events at a time:

1. Check the boxes of the security event cards that will undergo a status change.

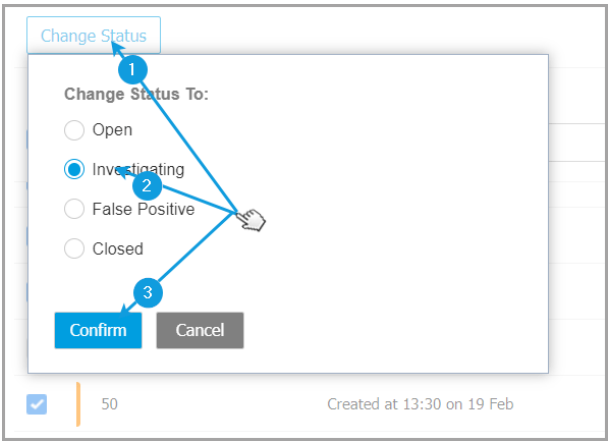


Selecting Security Event Cards

You can select them individually or by using the bulk selection options in the drop-down menu.

Note
You can also browse through several security event pages while keeping your selection.

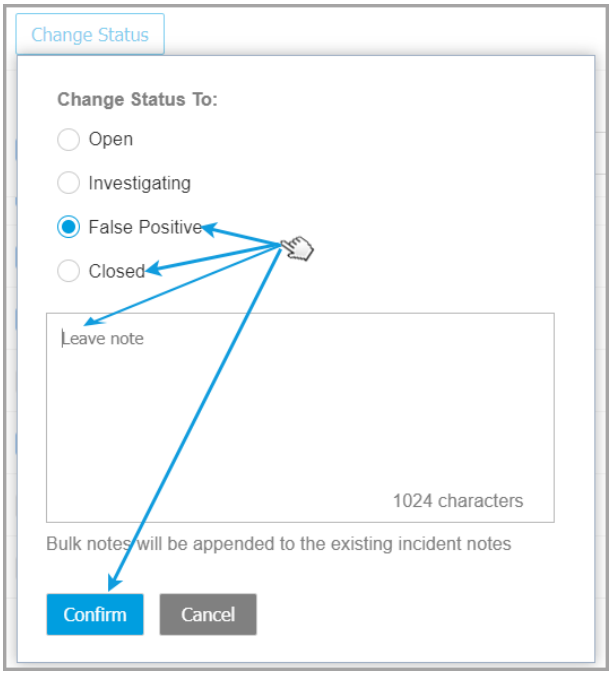
2. Click the **Change Status** button and select the desired options:



Changing the Status of Security Event

- **Open** - when the security event is not yet under investigation.
- **Investigating** - when you have started to investigate the event.
- **False Positive** - when you analyzed the event and identified it as a false positive.
- **Closed** - when you have done investigating.

Note
A box will open when changing the status of events to **False Positive** or **Closed**, where you can leave a note on the reasons for changing the event status, for later consultation.



Leaving Note for False Positive and Closed events

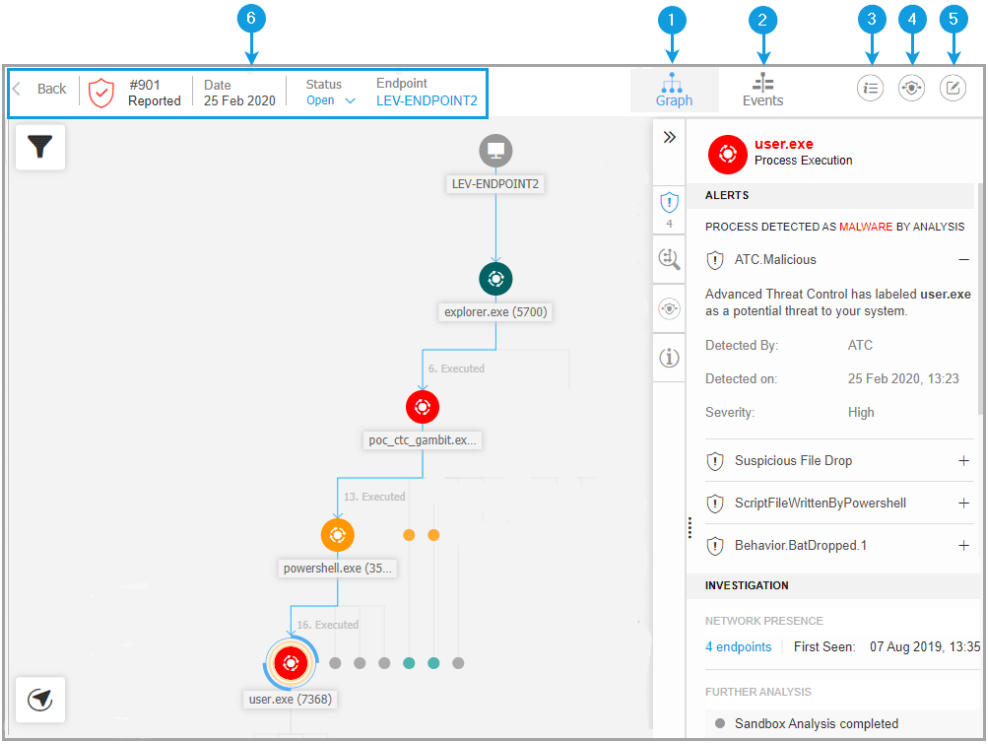
Note
The note will be appended to the ones already existing inside the filtered incidents.

3. Click **Confirm** to apply the selected status option.

9.1.3. Reviewing a Detected Threat

In the **Incidents** page, identify the security event you want to analyze and click the **View Graph** button to display it in a new page.

Each security incident has a dedicated page containing detailed information about the sequence of events (displayed in the graph as linked security event nodes) that led to triggering the incident, and provides options to take remediation actions.


6
1
2
3
4
5
Back
#901
Reported
Date
25 Feb 2020
Status
Open
Endpoint
LEV-ENDPOINT2
Graph
Events
LEV-ENDPOINT2
explorer.exe (5700)
6. Executed
poc_ctc_gambit.ex...
13. Executed
powershell.exe (35...
16. Executed
user.exe (7368)
user.exe
Process Execution
ALERTS
PROCESS DETECTED AS MALWARE BY ANALYSIS
ATC.Malicious
Advanced Threat Control has labeled user.exe as a potential threat to your system.
Detected By: ATC
Detected on: 25 Feb 2020, 13:23
Severity: High
Suspicious File Drop
ScriptFileWrittenByPowershell
Behavior.BatDropped.1
INVESTIGATION
NETWORK PRESENCE
4 endpoints
First Seen: 07 Aug 2019, 13:35
FURTHER ANALYSIS
Sandbox Analysis completed

1. Graph tab

   The Graph displays the security incident and its consisting elements, highlighting the Critical Path of the incident and displaying the details of the node that triggered the incident in the **Node Details** panel.

2. Events tab

   The Events tab displays filterable detected system events and alerts, and their corresponding event descriptions.

3. Incident Info panel

   This panel contains collapsible sections with details like incident ID, current status, timestamp when it was created and last updated, number of involved artifacts, trigger name and attack info.

4. Remediation panel

   This panel includes collapsible sections with actions taken automatically by GravityZone and recommended steps you can follow to mitigate the incident.

5. Notes clipboard

   Clicking the **Notes** button opens a clipboard where you can add notes on the current incident which you may read when you revisit the incident at a later time.

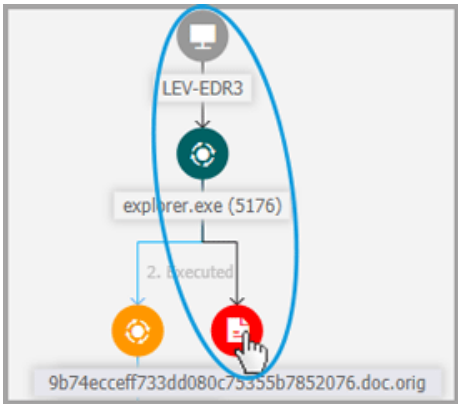
6. Incident status bar

   The status bar offers details on the ID of the incident, the time and date it was generated, status, incident trigger and the endpoint it affects. Clicking the **Back** button will take you back to the main **Incidents** page.

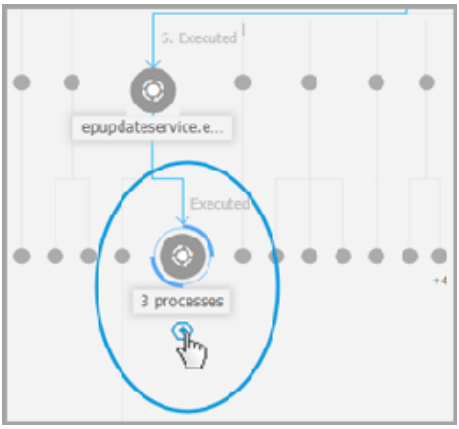
Security Event Nodes

This is what you need to know about security event nodes:

- Each node represents a specific element involved in the investigated incident.
- All nodes that make the critical path are shown by default in detail when you open the incident, while the other elements are faded out, to avoid cluttering the view.
  - Hovering over a node that is not part of the critical path will highlight it and show the path to the point of origin, without breaking the Critical Path.



- Three or more same action type event nodes spawning from a parent node are grouped into an expandable cluster-node.



  - Only nodes without child elements will be hidden from the incident graph when the cluster-node is collapsed.
  - Nodes where suspicious activity has been detected will not be added to the cluster-node.
- Clicking a node will display the following details:

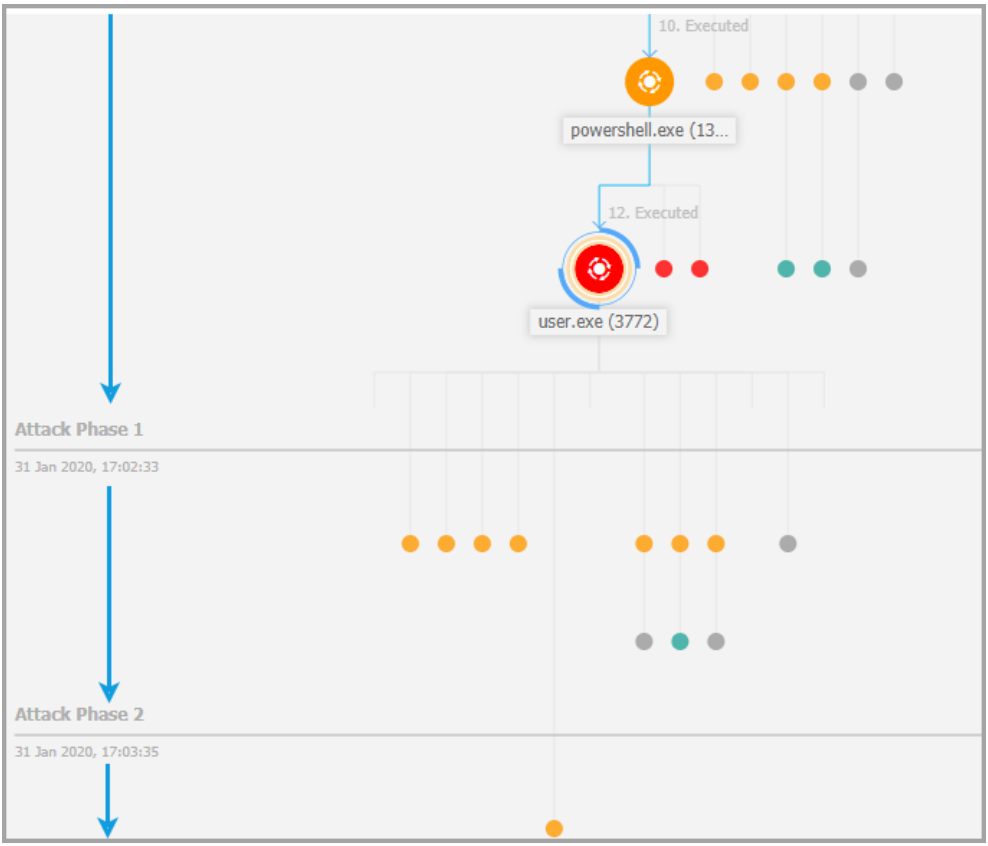
  - It will highlight in blue the path to the endpoint node along with all the other involved elements.
  - A side panel with expandable sections that provide detailed information of the selected node, alerts in case detections are triggered, available actions and recommendations. Refer to "Node Details" (p. 414) for more information.
- Nodes are linked by arrow-lines indicating the course of actions that occurred on the endpoint during the incident. Each line is labeled with the action name and its chronological number.

The following elements of an incident can be represented as nodes:

Node Type	Description
Endpoint	Displays endpoint details and patch management status.
Domain	Shows information about the domain host and its endpoints.
Process	Shows details about the process role in the current incident, file information, process executions details, network presence and further investigation options.
File	Shows details about the file role in the current incident, file information, network presence and further investigation options.
Registry	Displays Registry information and the parent process details.

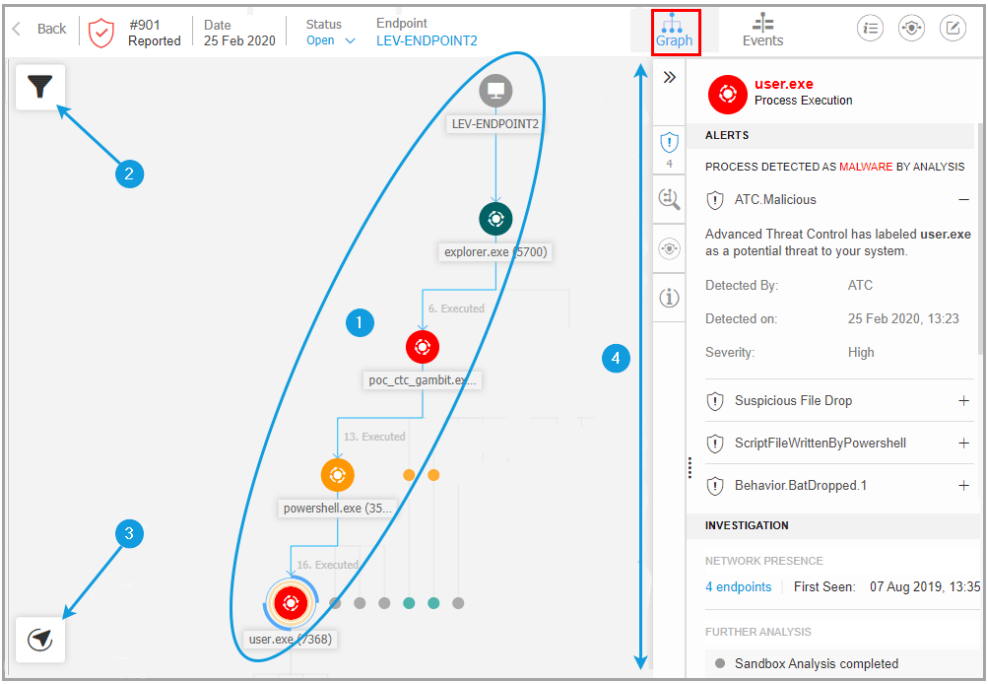
Graph

The **Graph** provides an interactive graphical representation of the investigated incident and its context, highlighting the sequence of elements directly involved in triggering it, known as the **Critical Path** of the incident, as well as all the other elements involved, which are faded out by default. In case of incidents that evolve over time, the graphic displays every single stage of the attack.



Staged Attack

The Graph includes filtering options that allow the customization of the incident graphic to improve visualization, features to navigate the incident map, and details panels with more information about each element.



The Graph Tab

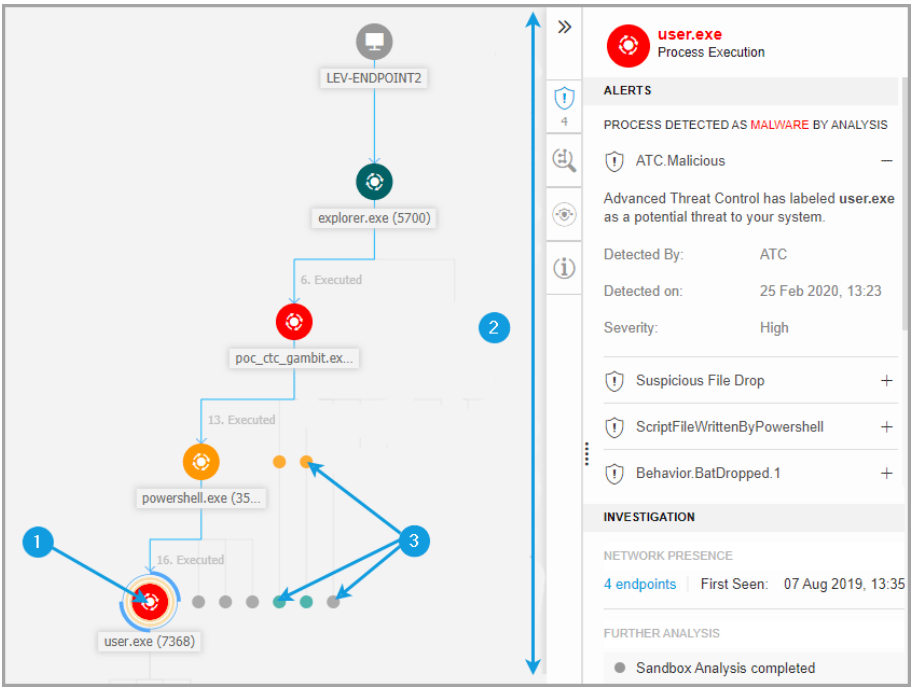
1. Critical Path
2. Filters Menu
3. Navigator Menu
4. Node Details Panel

Critical Path

The **Critical Path** is the sequence of linked security events that have led up to setting off an alert, starting from the point of entry in the network down to the event node that triggered the incident. The critical path of the incident is highlighted by default in the graph, along with all consisting event nodes on it, while the other elements are minimized.

The trigger node easily stands out from the rest of the elements in the graph, being surrounded by additional highlight features (two orange circles), and a related info

panel is displayed by default alongside the incident graph, providing detailed trigger node information.



Critical Path

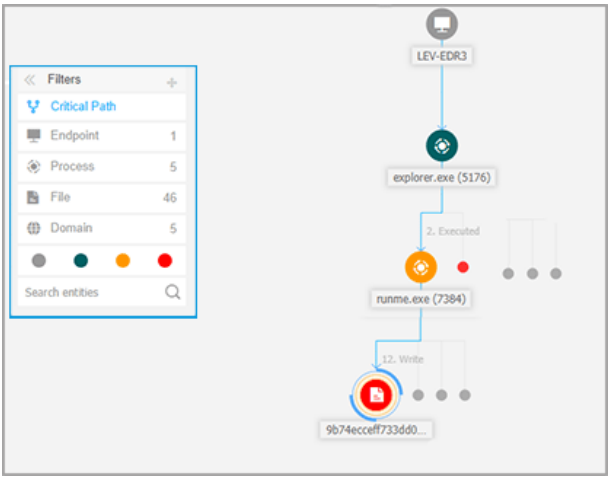
1. Trigger Node
2. Node Details panel with information grouped in categories and collapsible sections
3. Faded out nodes indirectly involved in the incident

Note
Clicking any other element than the trigger node will break the critical path and highlight the path to origin, from the selected node upstream to endpoint node.

Filters

The **Filters** menu provides you with enhanced filtering capabilities, allowing full manipulation of the incident graphic, by highlighting the elements based either on their type or relevance, or by hiding them to make the incident more compact and easier to analyze.

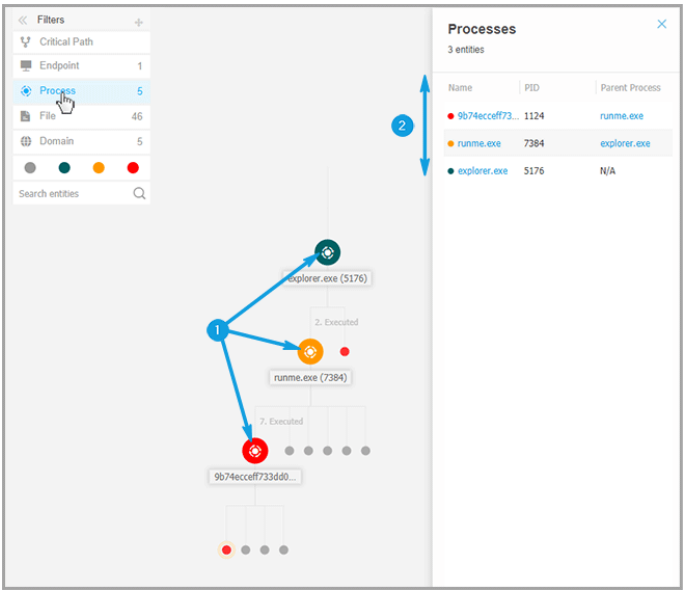
Click and hold the **Drag** icon to position the floating Filters panel anywhere inside the incident graph.



Incident Graph Filters

When selecting an element-type filter:

1. The incident graphic zooms out and highlights all the elements of the selected type, while the elements of different type are faded out.
2. It instantly opens a panel with the list of all the highlighted elements.



Note
Selecting an element from the displayed list will highlight it in the incident graphic, and open a details panel with information related to that element.
Only one filter can be applied at a time.

Filtering options include:

- **Critical Path**: It highlights the critical path of the incident of compromise.
- **Endpoint**: It highlights the endpoints affected by the incident.
- **Process**: It highlights all process-type nodes involved in the incident.
- **File**: It highlights file-type nodes involved in the incident.
- **Domain**: It highlights all domain-type nodes involved in the incident.
- **Registry**: It highlights all registry-type nodes involved in the incident.

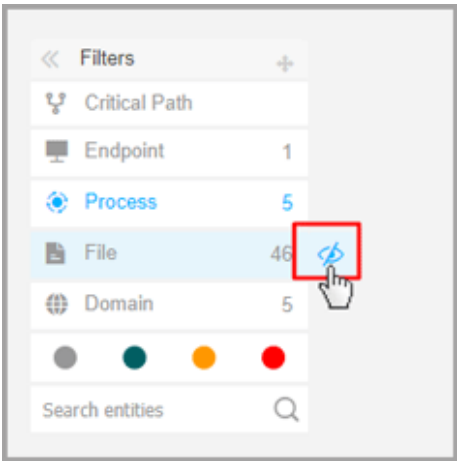
- **Element Relevance**: You can also filter elements by their importance inside the incident.
  - **Neutral node**: Elements with no direct impact in the security incident.
  - **Important node**: Elements with relevant role in the security incident.
  - **Origin node**: Entry point of the attack inside the network.
  - **Suspicious node**: Elements with suspicious behavior, directly involved in the security incident.
  - **Malicious node**: Elements that caused damage to your network.

    Note
    Hovering over any of the color filters displays how many elements with same relevance are involved in the incident.

- **Search entities**: You can search names or file extensions of incident components in the search field and the results will be displayed in the side panel.

If no filters are selected, the incident graph is reset to its default state, with endpoint, origin and trigger elements highlighted, while the other elements are faded out.

You can also hide certain elements from the incident graph by clicking the **Show/Hide** button displayed when positioning the mouse over filters of the type: File, Domain, and Registry.



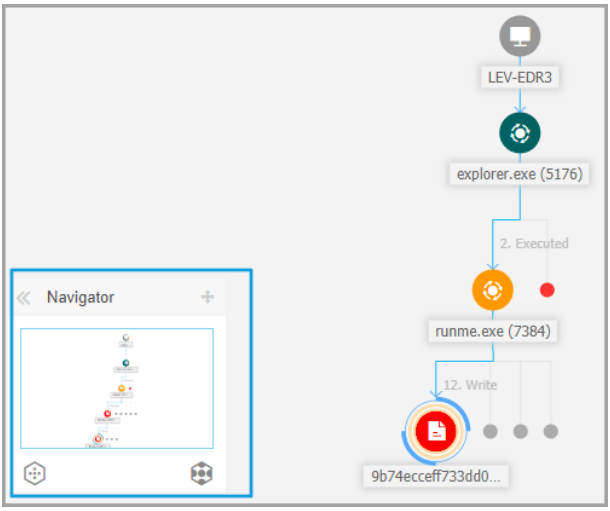
Hiding an element type redraws the incident graph by removing all corresponding elements, even if they are zoomed out, excepting the trigger node and nodes with child elements.

Navigator

The **Navigator** enables you to quickly move through the incident graph and explore all displayed elements by using the mini-map and the different levels of visualization.

Click and hold the **Drag** icon to position the floating Navigator panel anywhere inside the incident graph.

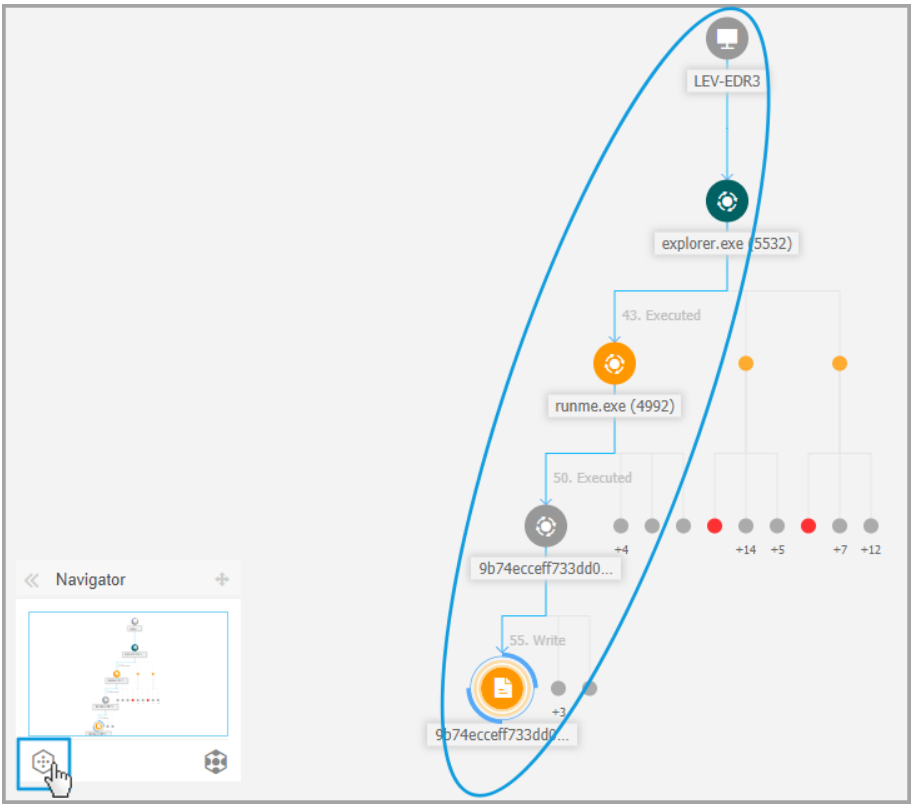
The **Navigator** is collapsed by default. When expanding it, the menu will display the miniaturized version of the entire incident map, and action buttons to adjust the level of visualization.



Navigator

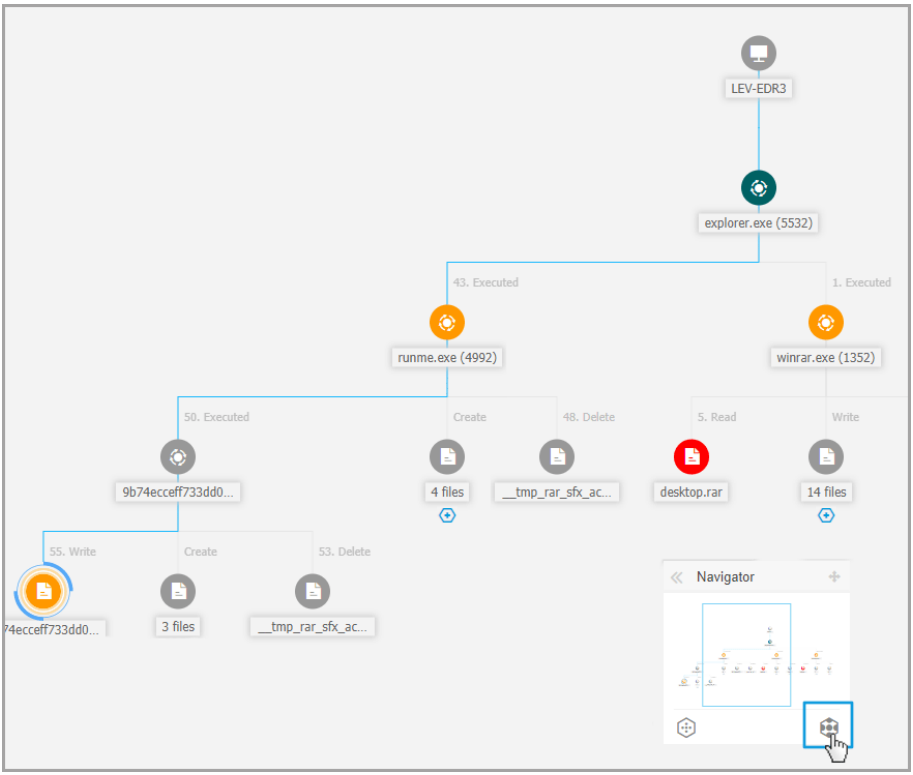
The **Navigator** menu provides two action buttons to adjust how you visualize the incident graph, the **Fewer Details** button, and **More Details** button.

When you click the **Fewer Details** button, the graph is set to its default state, highlighting only the critical path of the incident.



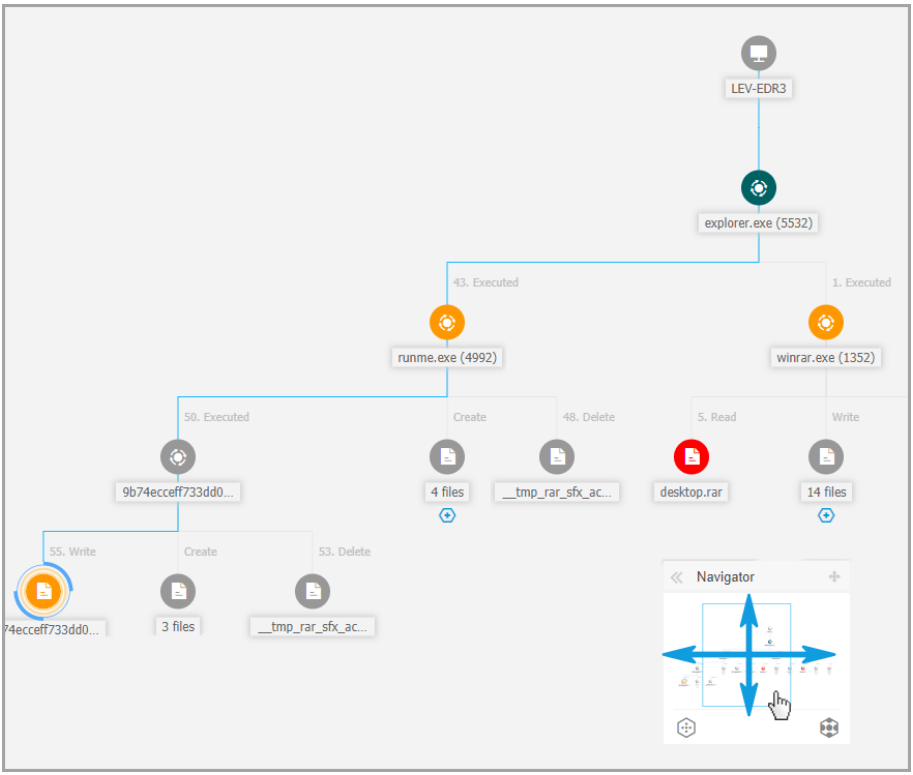
Overview Visualization

When you click the **More Details** button, all the incident graph elements are expanded, highlighting every node and node clusters.



Zoomed-in Visualization

When the incident is zoomed-in and all elements are highlighted the graph may often expand beyond screen limits. In this case hold and drag the map selector within the navigator mini-map to easily slide to the desired incident map area, or simply drag the graph area to the desired direction.

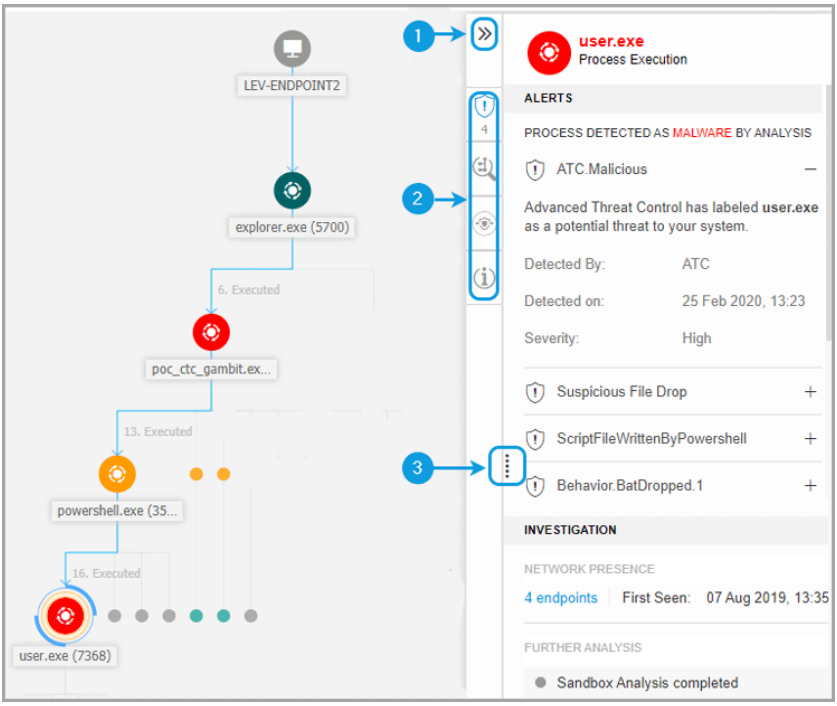


Mini-map Selector

Node Details

The **Node Details** panel includes sections with detailed information of the selected node, including preventive or remediation actions you can take to mitigate the incident, details on the type of detection and alerts detected on the node, network presence, process execution details, additional recommendations to manage the security event, or actions to further investigate the element.

To view this information and take actions within the panel, select a node within the security event map.



Node Details Panel

1. You can collapse or expand the **Node Details** panel by clicking the **Collapse** button.
2. You can easily navigate the information displayed in the **Node Details** panel by clicking the icons of each of the four major categories:
   - **ALERTS**

     This section displays one or multiple detections triggered on the selected node, including details about the Bitdefender technology that included the element in the incident, the reason that triggered the detection, detection name, and the date when it has been detected.
   - **INVESTIGATION**

     This section displays date stamps for the initial detection and all the endpoints where this element was spotted.

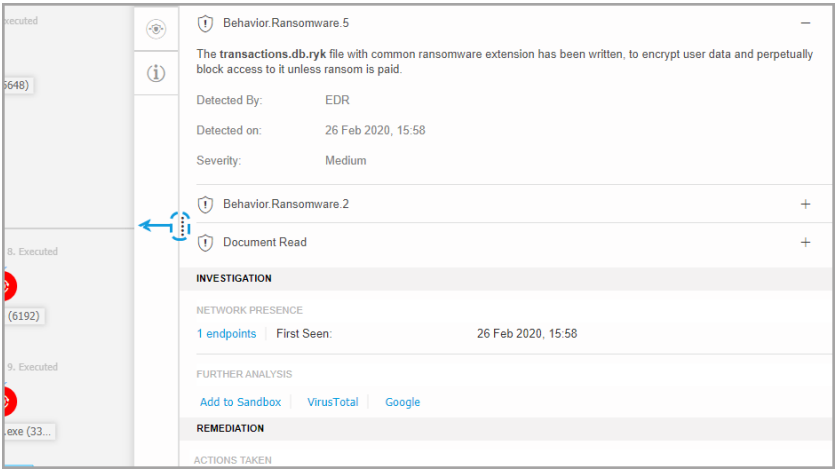
- **REMEDIATION**

  This section displays actions taken automatically by GravityZone, actions you can take immediately to mitigate the threat, as well as detailed recommendations for each alert detected on the selected node to assist you in mitigating the incident and increase the security level of your environment.

- **INFO**

  This section displays general information about each file, and specific information depending on the type of node selected.

3. You can drag the **Node Details** panel towards the center of the screen to easily go through its contents.



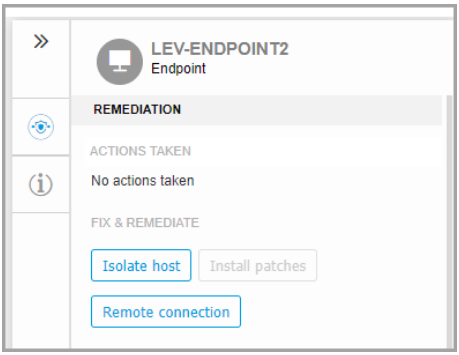
Expanded Panel

Details Panel for Endpoint Nodes

The **Node Details** panel for endpoints includes two categories:

- **REMEDIATION**

  Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:

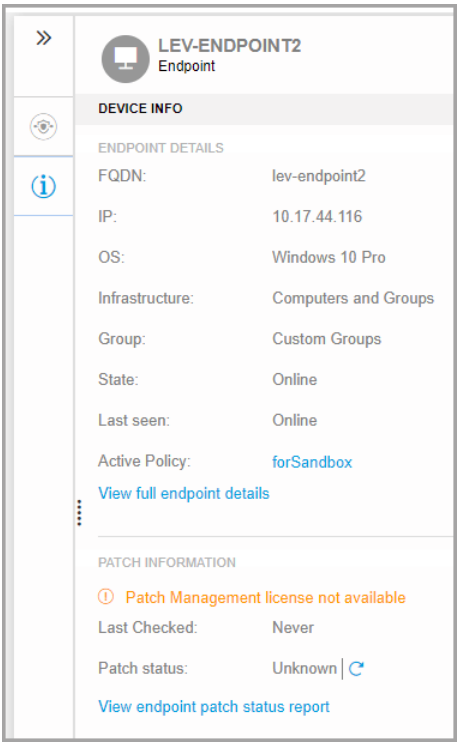


- **Isolate host** - Use this remediation solution to isolate the endpoint from the network.
- **Install patches** - Use this action to install a missing security patch on the target endpoint. This option is visible only with the Patch Management module, an add-on available with a separate license key. Refer to Patch Install for more information.
- **Remote Connection** - Use this action to to establish a remote connection to the endpoint involved in the current incident and run a number of custom shell commands directly on its operating system, for mitigating the threat instantly or collecting data for further investigation.

  Clicking this button will display the Remote Connection window.

- **DEVICE INFO**

  Displays general information about the affected endpoint, such as endpoint name, IP address, operating system, pertaining group, state, active policies, and a link that opens a new window where full endpoint details are displayed.



It also provides with information such as the number of installed patches, failed patches, or any missing security and non-security patches. In addition, you can generate an endpoint patch status report. This section is provided on demand for the target endpoint.

You can take the following actions within the panel:

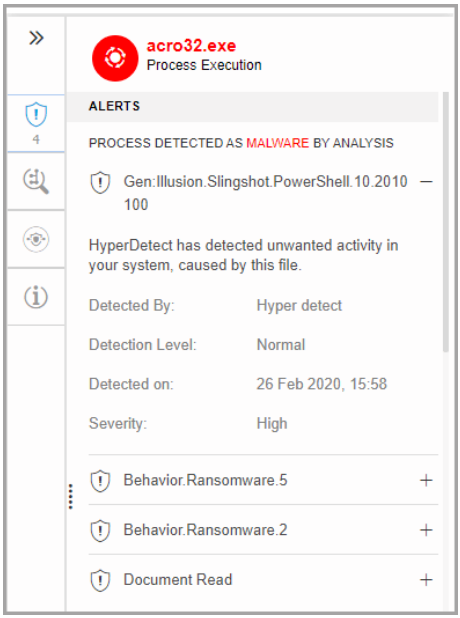
- View patch information for target endpoint. To view patch details, click **Refresh** inside this section.
- View patch status report for target endpoint. To generate the report, click **View endpoint patch status report**.

Details Panel for Process Nodes

The **Node Details** panel for process nodes includes four categories:

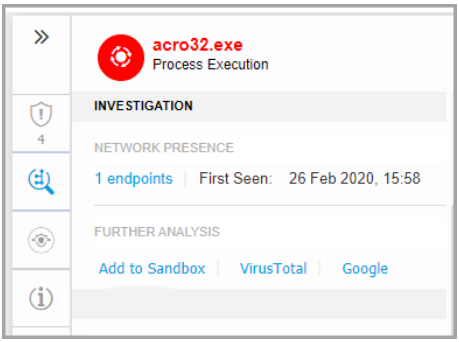
- **ALERTS**

  Displays one or multiple detections triggered on the selected node, including details about the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, detection name, and the date when it has been detected. The description for each alert follows the latest MITRE standards.

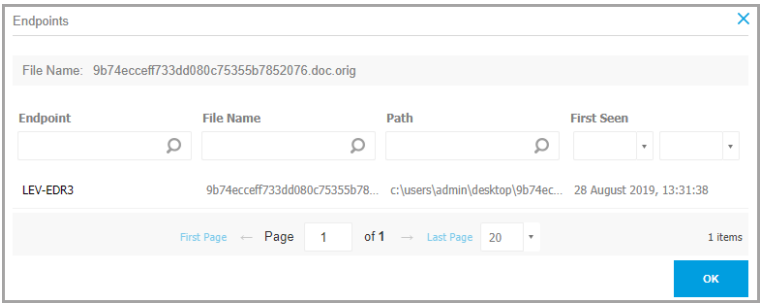


- **INVESTIGATION**

  Displays date stamps for the initial detection and all the endpoints where this element was spotted.



To view this list, click the number shown in the **endpoints** field and a new window will pop up.

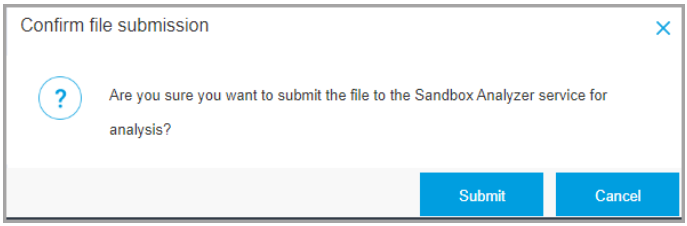


This section also provides external analysis through internal components and third-party solutions.

The following actions are available:

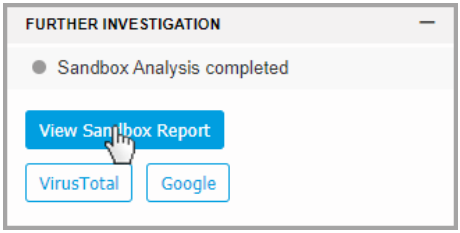
– **Add to Sandbox** - Use this action to generate a Sandbox Analyzer report.

  Choosing **Add to Sandbox** prompts you with a screen to confirm file submission.



After confirmation, you are automatically redirected to the submission screen.

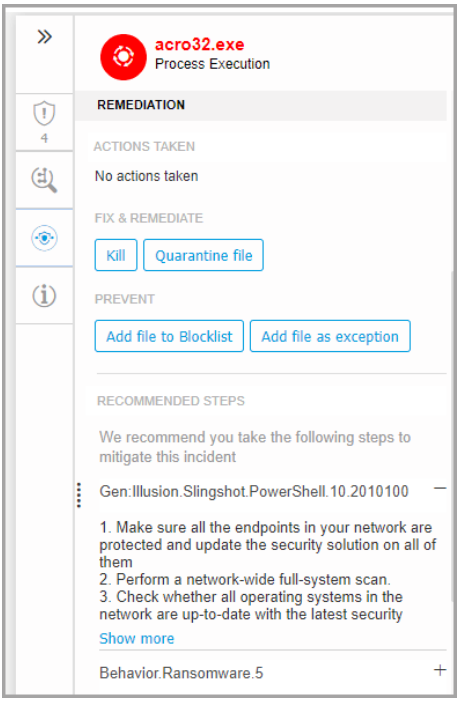
When the analysis is completed, click the **View Sandbox Report** button to open the full report.



- **VirusTotal** - Use this action to submit a file externally for analysis.
- **Google** - Use this action to search the hash value of a file.

- **REMEDIATION**

  Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:

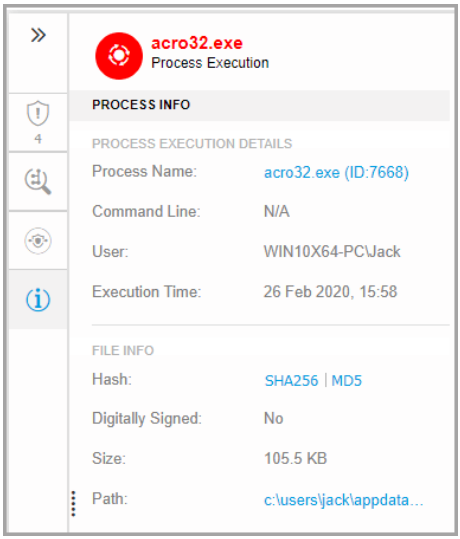


- **Kill** - Use this action to stop a process execution. This action creates a kill process task visible in the process execution bar. `System32` and Bitdefender processes are excluded from this action.
- **Quarantine file** - Use this action to store the item in question and prevent it from executing its payload. This action requires the Firewall module to be installed on the target endpoint.
- **Add file to Blocklist** - Manage blocked items in the Blocklist section.
- **Add file as Exception** - Use this option to exclude legitimate activity on a specific policy. When you choose this action, a configuration window prompts you to select the policy where you want to add an exception. Manage exclusion under **Policies > Antimalware > Settings**.

This section also provides detailed recommendations for each alert detected on the selected node to assist you in mitigating the incident and increase the security level of your environment.

- **PROCESS INFO**

  Displays details about the selected process node, including process name, executed command line, user, time of execution, file origin and path, hash value, or digital signature.



You can copy the hash value to clipboard by clicking the available hashing algorithms within the **Hash** field and then **Copy to Clipboard**, and use it to add a file hash value to **Blocklist**. For more information, refer to **Blocklisting Files**.

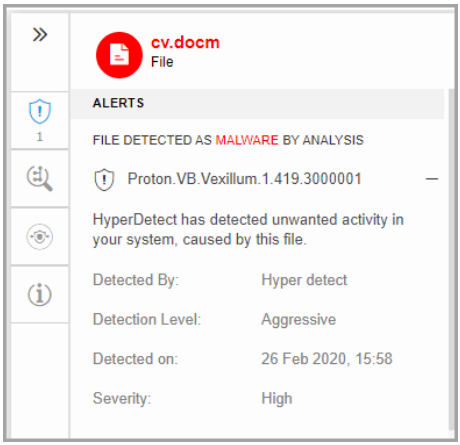
Details Panel for File Nodes

The **Node Details** panel for file nodes includes four categories:

- **ALERTS**

  Displays one or multiple detections triggered on the selected node, including details about the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, detection name, and the date when it

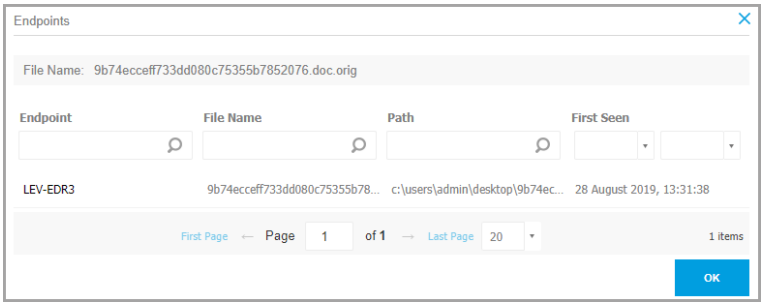
has been detected. The description for each alert follows the latest MITRE standards.



- **INVESTIGATION**

  Displays date stamps for the initial detection and all the endpoints where this element was spotted.

  To view this list, click the number shown in the **endpoints** field and a new window will pop up.

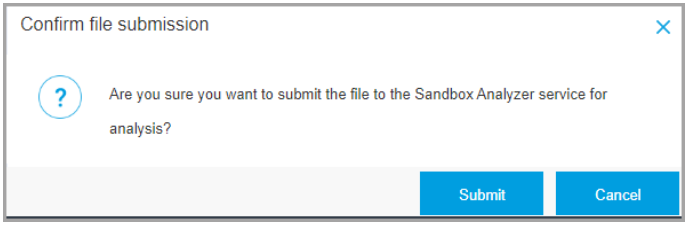


This section also provides external analysis through internal components and third-party solutions.

The following actions are available:

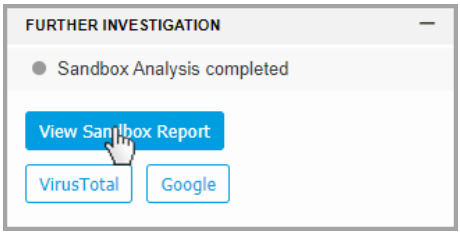
– **Add to Sandbox** - Use this action to generate a Sandbox Analyzer report.

  Choosing **Add to Sandbox** prompts you with a screen to confirm file submission.



  After confirmation, you are automatically redirected to the submission screen.

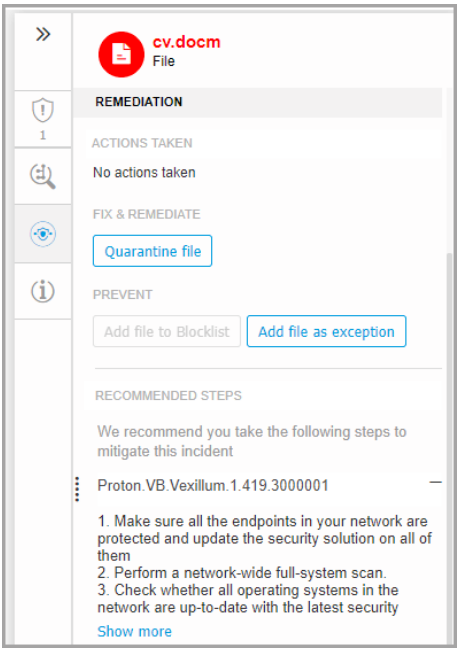
  When the analysis is completed, click the **View Sandbox Report** button to open the full report.



  - **VirusTotal** - Use this action to submit a file externally for analysis.
  - **Google** - Use this action to search the hash value of a file.

- **REMEDIATION**

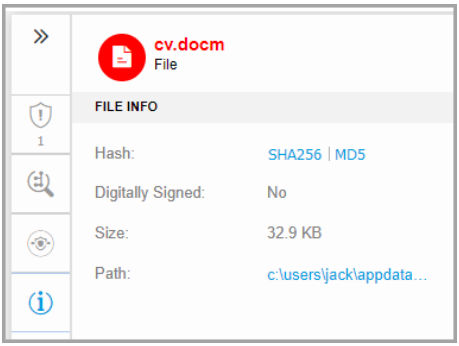
  Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:



- **Add file to Blocklist** - Manage blocked items in the Blocklist section.
- **Add file as Exception** - Use this option to exclude legitimate activity on a specific policy. When you choose this action, a configuration window prompts you to select the policy where you want to add an exception. Manage exclusion under **Policies > Antimalware > Settings**.

This section also provides detailed recommendations for each alert detected on the selected node to assist you in mitigating the incident and increase the security level of your environment.

- **FILE INFO**



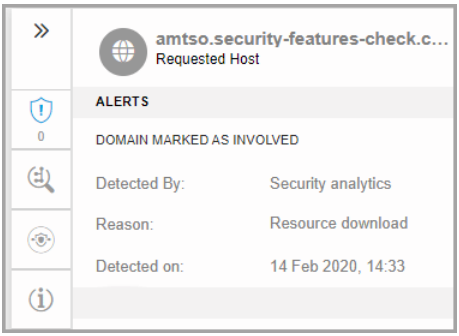
You can copy the hash value to clipboard by clicking the available hashing algorithms within the **Hash** field and then **Copy to Clipboard**, and use it to add a file hash value to **Blocklist**. For more information, refer to **Blocklisting Files**.

Details Panel for Domain Nodes

The **Node Details** panel for domain nodes includes four categories:

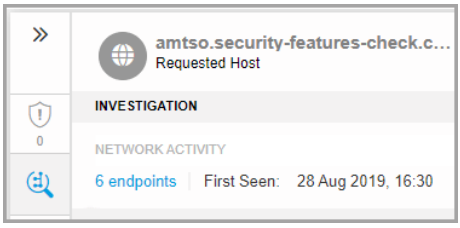
- **ALERTS**

  Displays the severity of the domain as marked by the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, and the date when it has been detected.

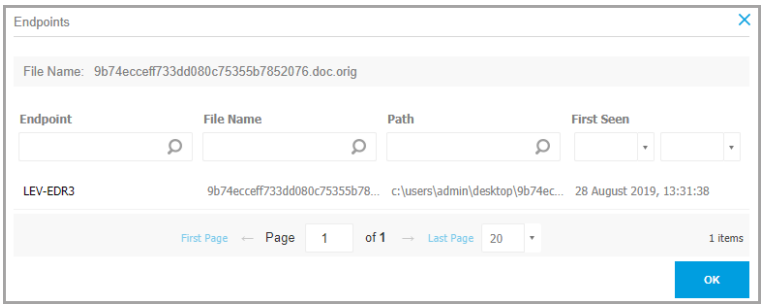


- **INVESTIGATION**

Displays date stamps for the initial detection and all the endpoints where this element was spotted.

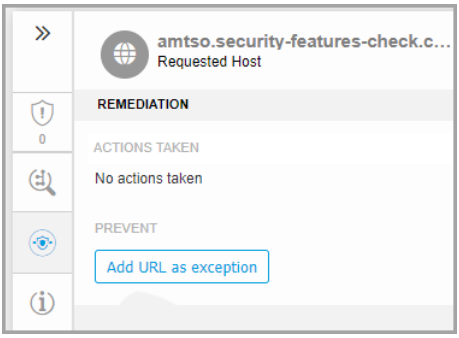


To view this list, click the number shown in the **endpoints** field and a new window will pop up.



- **REMEDIATION**

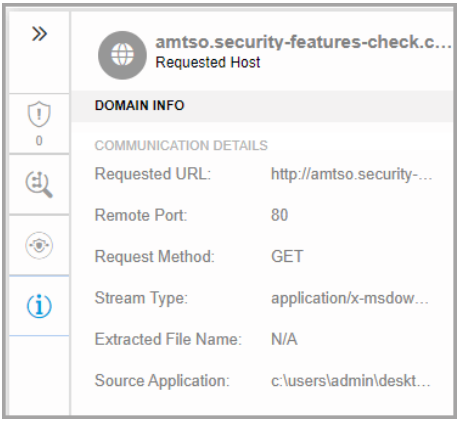
  Displays info about the actions taken automatically by GravityZone to mitigate threats and actions you can take:



– **Add URL as Exception** - Use this option to exclude legitimate activity on a specific policy. When you choose this action, a configuration window prompts you to select the policy where you want to add an exception. Manage exclusion under **Policies > Antimalware > Settings**.

- **DOMAIN INFO**

  Displays details about the selected domain node, including requested URL, port used, request method, stream type, extracted file name, source application.

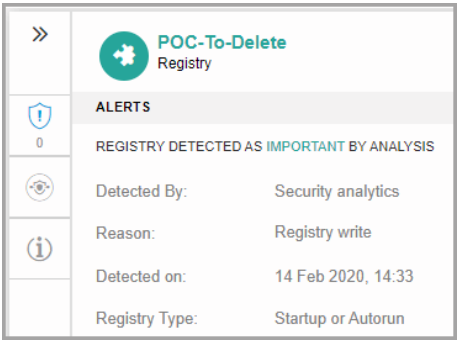


Details Panel for Registry Nodes

The **Node Details** panel for registry nodes includes three categories:

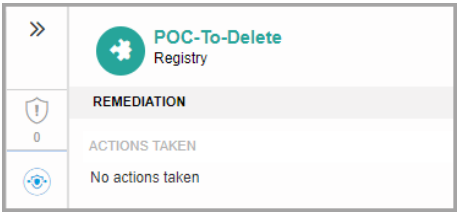
- **ALERTS**

  Displays the severity of the registry manipulation as marked by the Bitdefender technology that included this entity in the incident, the reason that triggered the detection, the date when it has been detected, and registry type.



- **REMEDIATION**

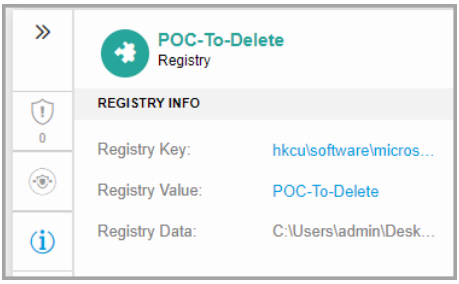
  Displays info about the actions taken automatically by GravityZone.



  The **REMEDIATION** section for registry nodes does not provide any user action option.

- **REGISTRY INFO**

  Displays details about the selected registry node, including registry key, value and data.

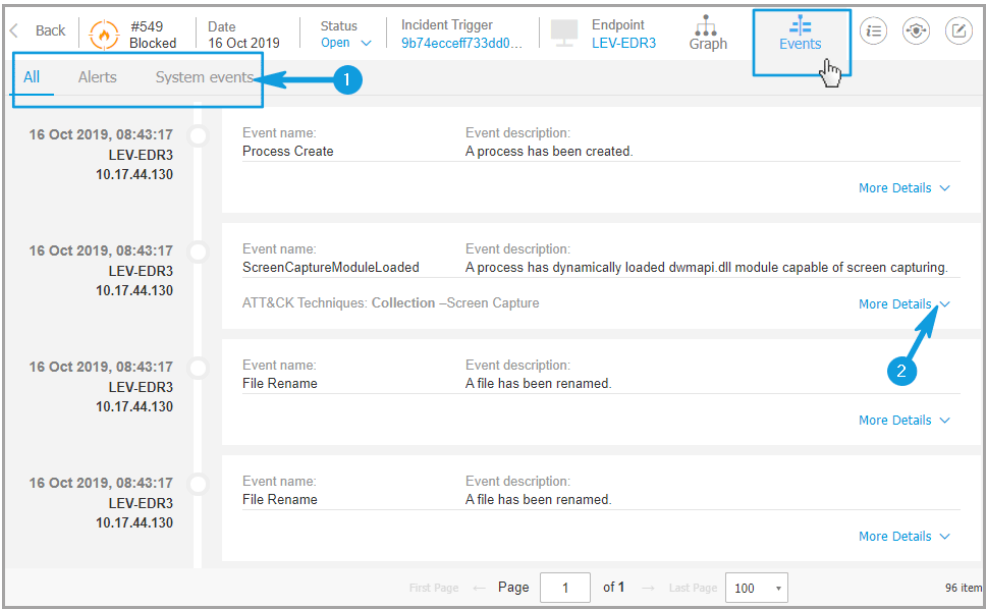


You can click the registry key and value to copy it to clipboard for further analysis purposes.

Events

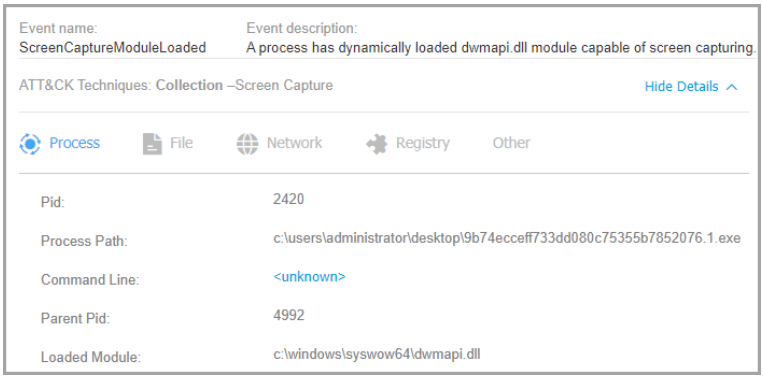
Use the **Events** tab to view how the sequence of events unfolded into triggering the currently investigated incident. This window displays the correlated system events and alerts detected by GravityZone technologies such as Network Attack Defense, Anomaly Detection, Advanced Anti-Exploit, Windows Antimalware Scan Interface (AMSI).

Every complex event has a detailed description explaining what was detected and what might happen if the artifact is used for malicious purposes, in accordance with the latest MITRE techniques and tactics.



Events Tab

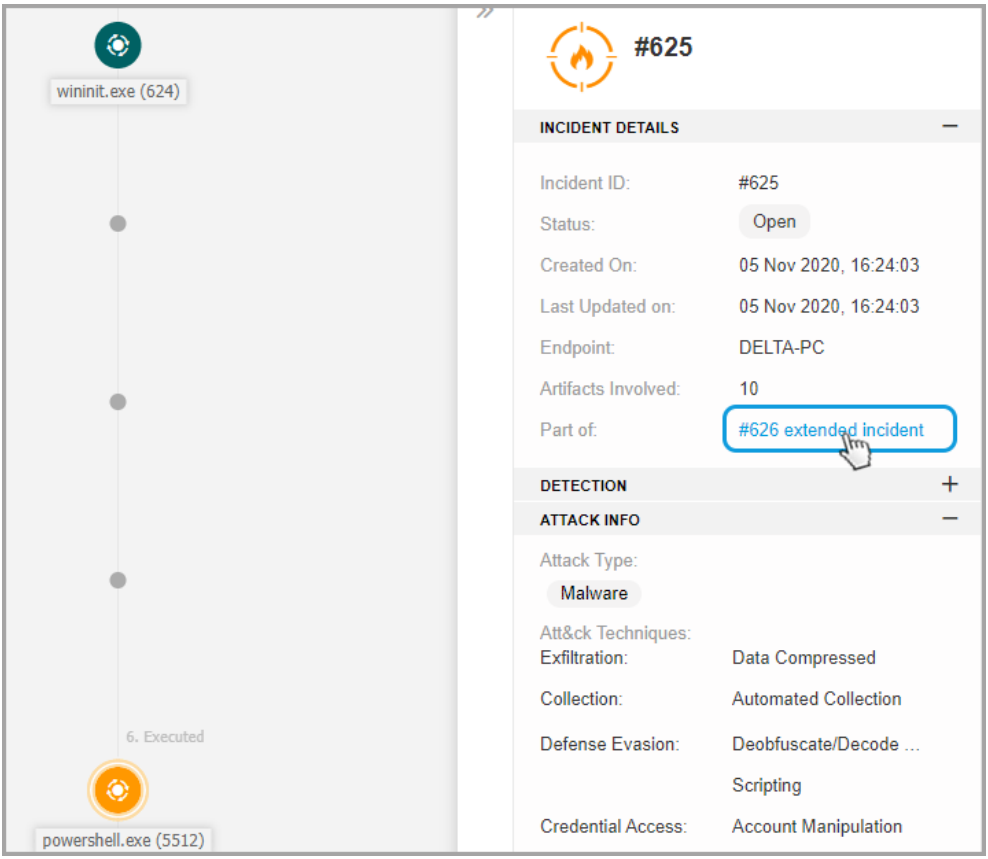
1. Use the filtering options to display all events, or either only system events or complex events (alerts).
2. Click the **More details** button to expand each event and have access to additional information.



Incident Info

This panel contains collapsible sections with details like incident ID, current state, time and date when it was created and last updated, number of involved artifacts, trigger name and description, and attack info.

From this section you can access the extended incident which includes this endpoint incident, if the case.

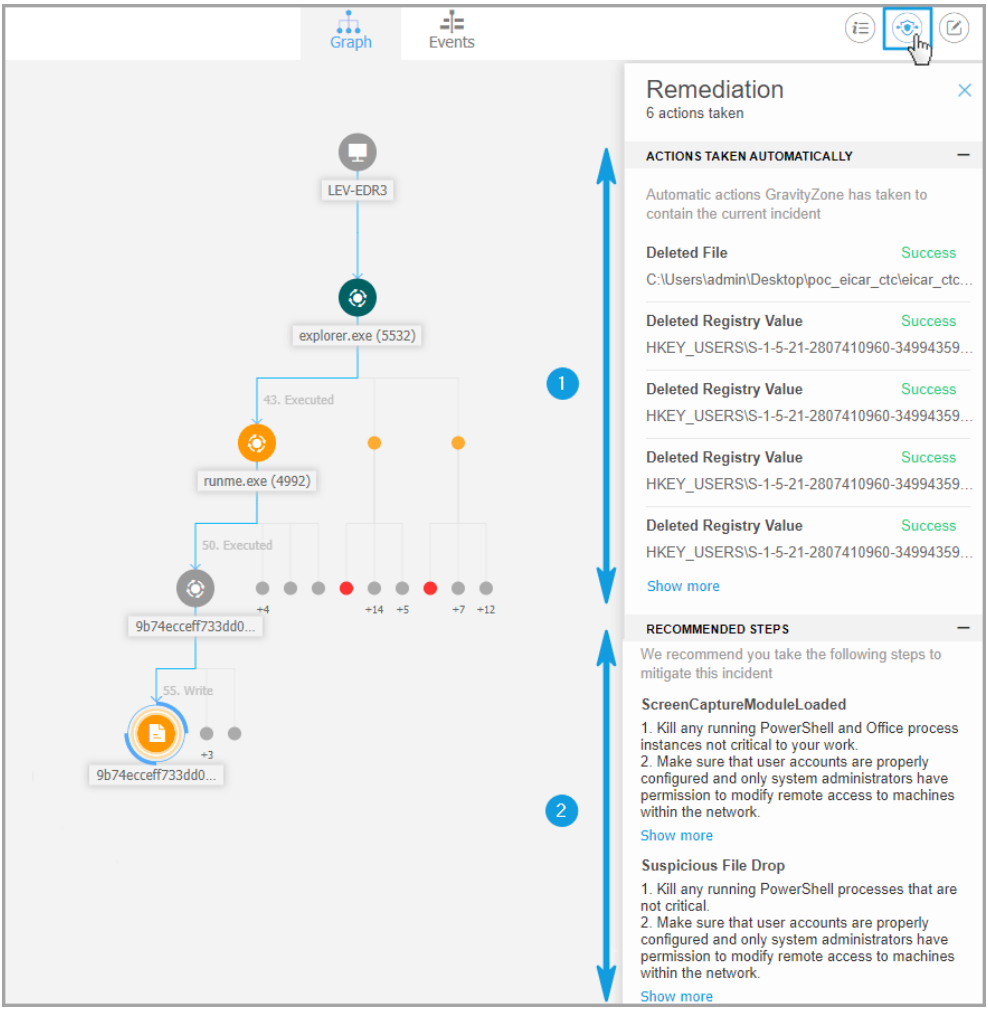


Incidents Info Panel

The panel also includes the alerts detected on the element that triggered the incident.

Remediation

The **Remediation** panel provides you insightful information about what corrective actions were taken automatically by GravityZone in case of attacks blocked by technologies such as Advanced Threat Control (ATC), HyperDetect, Antimalware, as well as recommended steps you may follow in order to mitigate the incident and to increase the security level of your system.



Remediation Panel

1. Actions taken automatically by GravityZone.
2. Recommendations to further mitigate the incident and boost security.

Note
The recommended steps correspond to the alerts detected on the node that triggered the investigated incident.

Notes

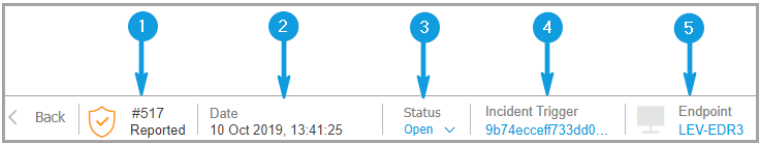
The **Notes** section allows you to add a note for tracking recent changes and ease incident ownership change.

Notes Clipboard

1. To leave a note for the current event, click the **Notes** button to display a new window.
2. Enter your message in this window (maximum 2048 characters).

Incident Status Bar

The incident status bar provides security event tags that can help you detect key information about the involved network endpoints.



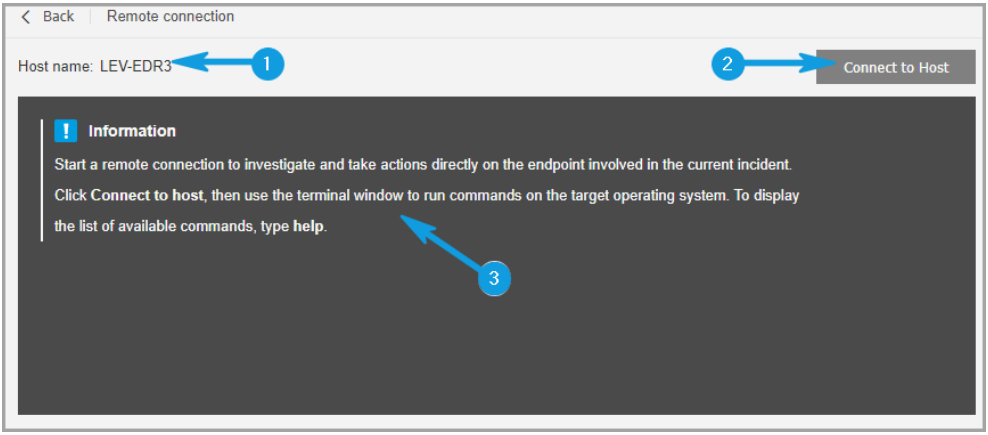
Incident Status Bar

1. Incident ID - the id number of the incident under investigation and if the incident is either blocked or reported only.
2. Detection timestamp - the date and time the incident was triggered.
3. Incident status - the current incident status.
4. Incident Trigger - the name of the element that generated the incident.
5. Endpoint - the name of the target endpoint.

Clicking the **Back** button takes you back to the main **Incidents** page.

Remote Connection

Use this tab to establish a remote connection to the endpoint involved in the current incident and run a number of custom shell commands directly on its operating system, for canceling the threat instantly or collecting data for further investigation.



Remote Connection tab

The **Remote Connection** tab contains the following items:

1. The name of the endpoint involved in the current security event
2. The button controlling the remote connection (connect / disconnect)
3. The terminal window

Terminal Session Prerequisites

- The version of Bitdefender agent installed on the endpoint supports the Remote Connection feature.
- The endpoint must be powered-on and online.
- The endpoint must have Windows OS.
- GravityZone is able to communicate with the endpoint.
- Your GravityZone account must have manage permissions for the target endpoint.

Creating a Remote Connection

This is how the remote connection works:

1. Start the live session by clicking the **Connect to Host** button.

   The connection status will be displayed next to the endpoint name.

   If the connection fails, an error message will be displayed in the terminal window.

   Note
   You can open maximum five terminal session with the same endpoint simultaneously.

2. Once connected, the terminal displays the list of available commands and their description. Type the command that you want in the terminal window followed by `Enter`.

   To learn more about a command, type `help` followed by the command name (for example, `help ps`).

3. The terminal displays the command output, when the command is successful.

   If the endpoint fails to complete the command execution, the command will be discarded.

   The command history is logged in the terminal window. However, you can view the previously typed commands by pressing the arrow keys.

4. To end the connection, click the **End Session** button.

   The terminal session expires automatically after five minutes of inactivity.

By navigating outside the **Remote Connection** tab while connected to an endpoint will also end the terminal session.

Terminal Session Commands

EDR terminal session commands are custom-built shell commands, platform independent, using a generic syntax. Find hereinafter the list of available commands you can use on endpoints through the terminal session:

- `ps`
  - **Description**: Displays information about the current running processes on the target endpoint, such as process ID (PID), name, path or memory usage.
  - **Syntax**: `ps`
  - **Aliases**: `tasklist`
  - **Parameters**: -
- `kill`
  - **Description**: Terminates a running process or application on the target endpoint by its PID. Use the `ps/tasklist` command to obtain the PID.
  - **Syntax**: `kill [PID]`
  - **Aliases**: -
  - **Parameters**: `[PID]` - the ID of a process from the target endpoint.
- `ls (dir)`
  - **Description**: Displays information about all files and folders from the specified directory, such as name, type, size and modify date. Allows wildcards to specify the path. For example:

    `C:\Users\admin\Desktop\s*` all contents of Desktop folder starting with "s"

    `C:\Users\publ??` lists all contents of specified path, with any last two letters.
  - **Syntax**: `ls [path]`
  - **Aliases**: `dir`

  - **Parameters**: `[Path]` - the path to a file or folder on the target endpoint.

- `rm (del, delete)`
  - **Description**: Deletes files and folders from the specified path on the target endpoint.
  - **Syntax**: `rm [path]`
  - **Aliases**: `del/delete`
  - **Parameters**: `[Path]` - the path to a file or folder on the target endpoint.

- `reg query`
  - **Description**: Returns all information (name, type and value) for the specified registry key path.
  - **Syntax**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Aliases**: -
  - **Parameters**:
    - `keypath`- returns all registry keys information from the specified path.
    - `/k [keyname]` - filters the registry keys results by a specific key name. You can also use wildcards (*, ?) to filter for a wider range of names.
    - `/v [valuename]` - filters the registry values by a specific value name. You can also use wildcards (*, ?) in the value name to filter a wider range of names.

- `reg add`
  - **Description**: Adds a new registry key or value. Overwrites a registry value, if it already exists. When overwriting registry information, you must specify all defined parameters.
  - **Syntax**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Aliases**: -
  - **Parameters**:
    - `[keyname]` - the registry key name.

- `/v [valuename]` - the registry value name. It also require adding at least /d [data] parameter.
- `/t [datatype]` - the registry value data type. You can add one of the following data types:

  `REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY, REG_DWORD_LITTLE_ENDIAN, REG_LINK, REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ`

  When unspecified, the `REG_SZ` type is assigned by default.

  When the type is set to `REG_BINARY`, registry data are interpreted as hex values.

- `reg delete`
  - **Description**: Deletes a registry key or its values.
  - **Syntax**:

    ```
    reg delete [keyname] [/v] [valuename]
    ```

    ```
    reg delete [keyname] [/va]
    ```

  - **Aliases**: -
  - **Parameters**:

    `[keyname]` - deletes the registry key and all its values.

    `/v [valuename]` - deletes the specified registry value.

    `/va` - deletes all values of the specified registry key.

- `cd`
  - **Description**: Changes the working directory to the specified path. This command requires, as parameter, the path to a drive or folder from the target endpoint.
  - **Syntax**: `cd [path]`
  - **Aliases**: -
  - **Parameters**: `[Path]` - the path to a file or folder on the target endpoint.

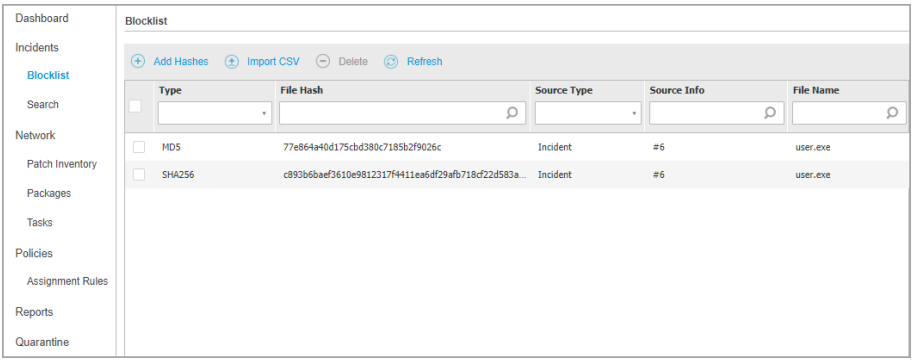
- `help`

- **Description**: Without specifying a parameter, help lists all available commands along with a short description. When entering help followed by a parameter, it displays the complete syntax of that command, short description and usage example.
- **Syntax**: `help [command]`
- **Aliases**: -
- **Parameters**: command name (for example: `cd, kill, ls, ps`)

- `clear (cls)`
  - **Description**: Clears up the terminal window and displays prompt with the current working folder.
  - **Syntax**: `clear`
  - **Aliases**: `cls`
  - **Parameters**: -

9.2. Blocklisting Files

In the **Blocklist** page you can view and manage items by their hash values. View activity records in User Activity Log.



Blocklist page

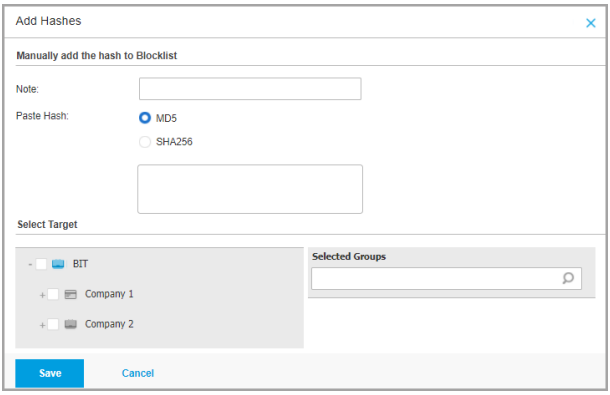
In a data table, you can view the following details for each item:

- File type:

  - MD5
  - SHA256
- File Hash Value
- Source Type:
  - Incident
  - Import
  - Manual
- Source Info
- File Name
- Company

Add hash values to the existing Blocklist:

1. Copy the hash value from **File Info**.
2. Choose from **MD5** or **SHA256** and paste the value in the box below. Add a note if required.
3. Click **Save**.

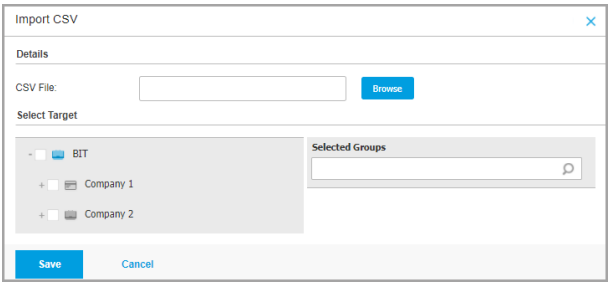


Add hash value window

Important
Incidents Sensor will block any binary whose hash value has been added to **Blocklist** from starting a process.

Import hash records to the existing Blocklist. To import a CSV file:

1. Click **Import CSV**.
2. Browse for your CSV file and click **Save**.



Import CSV window

You may also import local CSV files from your device into the **Blocklist** page, but first you must make sure your CSV is valid.

To create a valid CSV file for import you must populate the first three columns with the following data:

1. The first column of the CSV must contain the Hash type: either `md5` or `sha256`.
2. The second column must contain corresponding hexadecimal hash values.
3. The third column may contain optional string information related to the **Source Info** column in the **Blocklist** page.

Note
Information corresponding to the other columns in the **Blocklist** page will be filled in automatically, upon importing the CSV file.

10. USING REPORTS

GravityZone 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.
- 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).

10.1. Report Types

Different report types are available for each endpoint type:

- Computer and Virtual Machine Reports
- Exchange Reports
- Mobile Device Reports

10.1.1. 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, Advanced Anti-Exploit, 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 Encryption Status

Provides you with data regarding the encryption status on the endpoints. A pie chart displays the number of the machines compliant, respectively non-compliant with the encryption policy settings.

A table below the pie chart delivers details such as:

- Endpoint name.
- Full Qualified Domain Name (FQDN).
- Machine IP.
- Operating system.
- Device policy compliance:
  - **Compliant** – when the volumes are all encrypted or unencrypted according to the policy.

- **Non-compliant** – when the volumes status is not consistent with the assigned policy (for example, only one of two volumes is encrypted or an encryption process is in progress on that volume).

- Device policy (**Encrypt** or **Decrypt**).
- Click the numbers in the Volumes Summary column to view information about each endpoint's volumes: ID, name, encryption status (**Encrypted** or **Unencrypted**), issues, type (**Boot** or **Non-boot**), size, Recovery Key ID.

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.

By clicking the **Reconfigure Client** button, you can start a task to change the initial settings of one or several selected endpoints. For details, refer to Reconfigure Client.

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.

HyperDetect Activity

Informs you about the activity of the HyperDetect module of Bitdefender Endpoint Security Tools.

The chart in the upper side of the report page shows you the dynamics of the attack attempts over the specified period of time and their distribution by type of attack. Moving the mouse over the legend entries will highlight the associated attack type in the chart. Clicking the entry will show or hide the respective line in the chart. Clicking any point on a line will filter your table data according to the selected type. For example, if you click any point on the orange line, the table will display only exploits.

The details in the lower part of the report help you identify the breaches in your network and if they were addressed. They refer to:

- The path to the malicious file, or the detected URL, in the case of infected files. For file-less attacks it is provided the name of the executable used in the attack, with a link to a details window which displays the detection reason and the malicious command line string.
- The endpoint on which the detection was made
- The protection module which detected the threat. As HyperDetect is an additional layer of the Antimalware and Content Control modules, the report will provide information about one of these two modules, depending on the type of detection.
- The type of the intended attack (targeted attack, grayware, exploits, ransomware, suspicious files and network traffic)
- The threat status
- The module protection level at which the threat was detected (Permissive, Normal, Aggressive)
- Number of times the threat was detected
- Most recent detection
- Identification as file-less attack (yes or no), to quickly filter the file-less attacks detections

Note
A file may be used in more types of attacks. Therefore, GravityZone reports it for each type of attack it was involved in.

From this report, you can quickly resolve false positives, by adding exceptions in the assigned security policies. To do so:

1. Select as many entries in the table as you need.

   Note
   File-less attack detections cannot be added to the exceptions list, due to the fact that the detected executable is not a malware itself, but can be a threat when using a malicious encoded command line.

2. Click the **Add exception** button at the upper side of the table.
3. In the configuration window, select the policies to which the exception should be added and then click **Add**.

   By default, related information for each added exception is sent to Bitdefender Labs, to help improving the detection capabilities of Bitdefender products. You can control this action using the **Submit this feedback to Bitdefender for a better analysis** checkbox.

If the threat was detected by the Antimalware module, the exception will apply to both On-access and On-demand scanning modes.

Note
You can find these exceptions in the following sections of the selected policies: **Antimalware > Settings** for files, and **Content Control > Traffic** for URLs.

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 with unresolved 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 unresolved targets, by clicking the **Scan infected targets** button from the Action Toolbar above the data table.

Network Incidents

Informs you about the activity of the Network Attack Defense module. A graph displays the number of the attack attempts detected over a specified interval. The report details include:

- Endpoint name, IP and FQDN
- Username
- Detection name
- Attack technique
- Number of attempts
- Attacker's IP
- Targeted IP and port
- When the attack was blocked most recently

Clicking the **Add exceptions** button for a selected detection automatically creates an entry in **Global Exclusions** from the **Network Protection** section.

Network Patch Status

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

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

Network Protection Status

Provides detailed information on the overall security status of the target endpoints. For example, you can view information about:

- Name, IP, and FQDN
- Status:
  - **Has issues** - the endpoint has protection vulnerabilities (security agent not up to date, security threats detected, etc.)
  - **No issues** - the endpoint is protected and there are no reasons for concern.
  - **Unknown** - the endpoint was offline when the report was generated.

  - **Unmanaged** - the security agent is not installed on the endpoint yet.
- Available protection layers
- Managed and unmanaged endpoints (the security agent is installed or not)
- License type and status (additional license related columns are hidden by default)
- Infection status (the endpoint is "clean" or not)
- Update status of the product and security content
- Software security patch status (missing security or non-security patches)

For unmanaged endpoints, you will view the **Unmanaged** status under other columns.

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.

Sandbox Analyzer Failed Submissions

Displays all failed submissions of objects sent from the endpoints to Sandbox Analyzer over a specified time period. A submission is considered failed after several retry attempts.

The graphic shows the variation of the failed submissions during the selected period, while in the report details table you can view which files could not be sent to Sandbox Analyzer, the machine where the object was sent from, date and time for each retry, the error code returned, description of each failed retry and the company name.

Sandbox Analyzer Results (Deprecated)

Provides you with detailed information related to the files on target endpoints, which were analyzed in the sandbox over a specified time period. A line chart displays the number of the clean or dangerous analyzed files, while the table presents you with details on each case.

You are able generate a Sandbox Analyzer Results report for all analyzed files or only for those detected as malicious.

You can view:

- Analysis verdict, saying whether the file is clean, dangerous or unknown (**Threat detected** / **No threat detected** / **Unsupported**). This column shows up only when you select the report to display all analyzed objects.

  To view the complete list with file types and extensions supported by Sandbox Analyzer, refer to "Supported File Types and Extensions for Manual Submission" (p. 540).
- Threat type, such as adware, rootkit, downloader, exploit, host-modifier, malicious tools, password stealer, ramsomware, spam or Trojan.
- Date and time of the detection, which you can filter depending on the reporting period.
- Hostname or IP of the endpoint where the file was detected.
- Name of the files, if they were submitted individually, or number of analyzed files in case of a bundle. Click the file name or bundle link to view details and actions taken.
- Remediation action status for the submitted files (**Partial**, **Failed**, **Reported Only**, **Successful**).
- Company name.
- More information about the properties of the analyzed file is available by clicking the **Read more** button in the **Analysis Result** column. Here you can view security insights and detailed reporting on the sample behavior.

Sandbox Analyzer captures the following behavioral events:

- Writing / deleting / moving / duplicating / replacing files on the system and on removable drives.
- Execution of newly-created files.
- Changes to the file system.
- Changes to the applications running inside the virtual machine.
- Changes to the Windows taskbar and Start menu.
- Creating / terminating / injecting processes.
- Writing / deleting registry keys.
- Creating mutex objects.
- Creating / starting / stopping / modifying / querying / deleting services.
- Changing browser security settings.
- Changing Windows Explorer display settings.
- Adding files to firewall exception list.

- Changing network settings.
- Enabling execution at system startup.
- Connecting to a remote host.
- Accessing certain domains.
- Transferring data to and from certain domains.
- Accessing URLs, IPs and ports through various communication protocols.
- Checking the indicators of virtual environment.
- Checking the indicators of monitoring tools.
- Creating snapshots.
- SSDT, IDT, IRP hooks.
- Memory dumps for suspicious processes.
- Windows API functions calls.
- Becoming inactive for a certain time period to delay execution.
- Creating files with actions to be executed at certain time intervals.

In the **Analysis Result** window, click the **Download** button to save to your computer the Behavior Summary content in the following formats: XML, HTML, JSON, PDF.

This report will continue to be supported for a limited amount of time. It is recommended for you to use instead submission cards to gather the necessary information on analyzed samples. The submission cards are available in the **Sandbox Analyzer** section, in the main menu of Control Center.

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
- Advanced Anti-Exploit events
- Network Attack Defense 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 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 Security Servers without load issues.
  - **Near overload**, when the scan load is between 85 and 90% of the full scan capacity.
  - **Near underload**, when the scan load is between 5 and 10% of its full scan load.
- **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.
- **Connected Storage Devices**: informs how many ICAP-compliant storage devices are connected to Security Server. Clicking the number will display the list of storage devices, with details for each one: name, IP, type, date and time of the last connection.

- **Storage Scanning Status**: indicates if the Security for Storage service is enabled or disabled.

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 and security content versions.

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.

Note
The HVI module may be available for your GravityZone solution with a separate license key.

HVI Third Party Tools Injection Status

Offers you a detailed status for each injection run on the target endpoints. The information includes:

- The name of the endpoint.
- The name of the injected tool.
- The IP address of the endpoint.

- The guest operating system.
- The trigger. This may be a memory violation, an on-demand task or a scheduled run.
- The number of successful runs. Clicking the number will pop up a window with the logs path and timestamp for each tool run. Clicking the icon in front of the path will copy it to Clipboard.
- The number of unsuccessful runs. Clicking the number will pop up a window where you can view the reason for failing and the timestamp.
- Last successful injection.

Injections are grouped by target endpoints. You can filter the report to view data only related to a specific tool by using the filtering options in the table's header.

Note
The HVI module may be available for your GravityZone solution with a separate license key.

Ransomware Activity

Informs you with regards to the ransomware attacks that GravityZone detected on the endpoints you manage, and provides you with the necessary tools to recover the files affected during the attacks.

The report is available as a page in Control Center, distinct from the other reports, accessible right from the GravityZone main menu.

The **Ransomware Activity** page consists of a grid that, for each ransomware attack, lists the following:

- The name, IP address and FQDN of the endpoint on which the attack took place
- The company to which the endpoint belongs
- The name of the user who was logged in during the attack
- The type of attack, respectively a local or a remote one
- The process under which the ransomware ran for local attacks, or the IP address from which the attack was initiated for remote ones
- Date and time of the detection

- Number of files encrypted until the attack was blocked
- The restore action status for all files on the target endpoint

Some details are hidden by default. Click the **Show/Hide Columns** button in the upper right side of the page to configure the details you want to view in the grid. If you have many entries in the grid, you can choose to hide filters using the **Show/Hide filters** button in the upper right side of the page.

Additional information is available by clicking the number for files. You can view a list with the full path to the original and restored files, and the restore status for all files involved in the selected ransomware attack.

Important
The backup copies are available for maximum 30 days. Please mind the date and time until files may still be recovered.

To recover files from ransomware:

1. Select the attacks you want in the grid.
2. Click the **Restore files** button. A confirmation window shows up.

   A recovery task is being created. You can check its status in the **Tasks** page, just like for any other task in GravityZone.

If detections are the result of legitimate processes, follow these steps:

1. Select the records in the grid.
2. Click the **Add exclusion** button.
3. In the new window, select the policies to which the exclusion must apply.
4. Click **Add**.

   GravityZone will apply all possible exclusions: on folder, on proccess, and on IP address.

   You can check or modify them in the **Antimalware > Settings > Custom Exclusions** policy section.

Note
Ransomware Activity keeps record of events for two years.

10.1.2. 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.

10.1.3. 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)

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. 372).

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. 160).

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. 377).

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. 368).

10.2. Creating Reports

You can create two categories of reports:

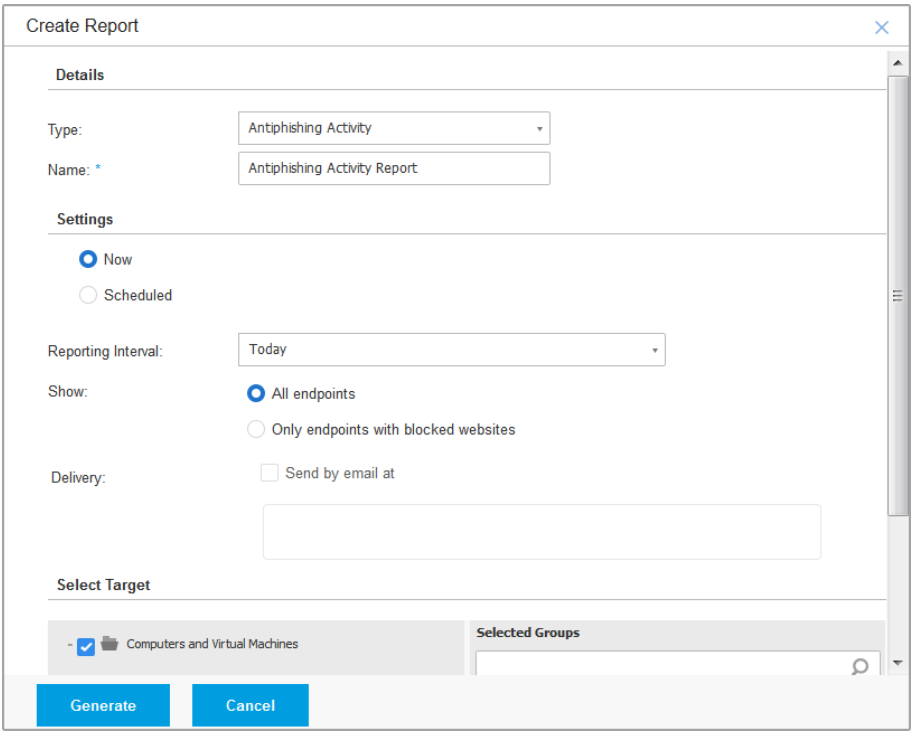
- **Instant reports.** Instant reports are automatically displayed after you generate them.

- **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. 446)
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).

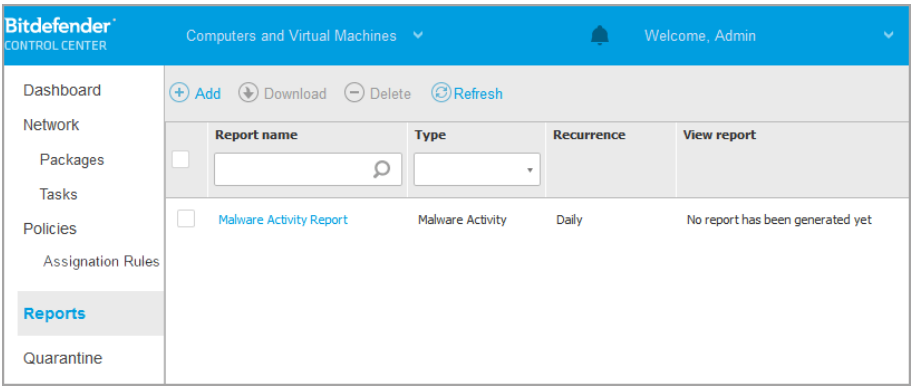
- Weekly, in the specified days of the week and at the selected start time (hour and minutes).
- Monthly, at each specified day on the month and at the selected start time (hour and minutes).

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.

10.3. 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 recurrence
- 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.

10.3.1. 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. 473)

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.

10.3.2. 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.

10.3.3. 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.

10.4. 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.

  Note
  The HVI module may be available for your GravityZone solution with a separate license key.

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.

10.5. 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

10.5.1. Exporting Reports

To export the report to your computer:

1. Choose a format and click either **Export CSV** or **Export PDF**.
2. 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.

10.5.2. 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.

10.6. Emailing Reports

You can send reports by email using the following options:

1. To email the report you are viewing, click the **Email** button. 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.

10.7. Printing Reports

Control Center does not currently support print button functionality. To print a report, you must first save it to your computer.

11. 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.

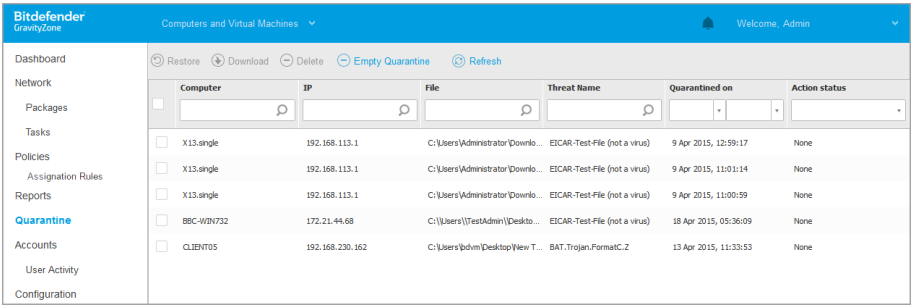
GravityZone moves files to quarantine according to the policies assigned to endpoints. By default, files that cannot be disinfected are quarantined.

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.

11.1. 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.

11.2. 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. 266).

11.2.1. 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.

11.2.2. 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 7 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.

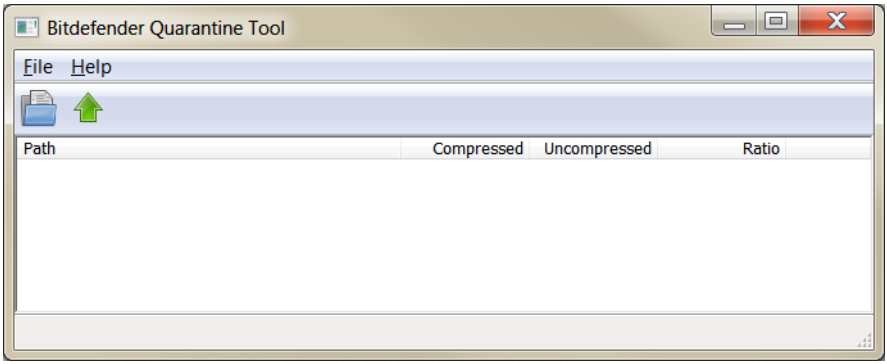
5. Click the **Download** button at the upper side of the table. Depending on your browser settings, you will be asked to save the files to a folder of your choice, or the files will be downloaded automatically to the default download location.

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.

Emptying the Quarantine

To delete all the quarantined objects:

1. Go to the **Quarantine** page.
2. Select **Computers and Virtual Machines** from the views selector.
3. Click the **Empty Quarantine** button.

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

All the entries from the Quarantine table are cleared. The requested action is sent to the target network objects immediately or as soon as they get back online.

11.3. 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.

11.3.1. 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.

11.3.2. 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. 268).

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.

Emptying the Quarantine

To delete all the quarantined objects:

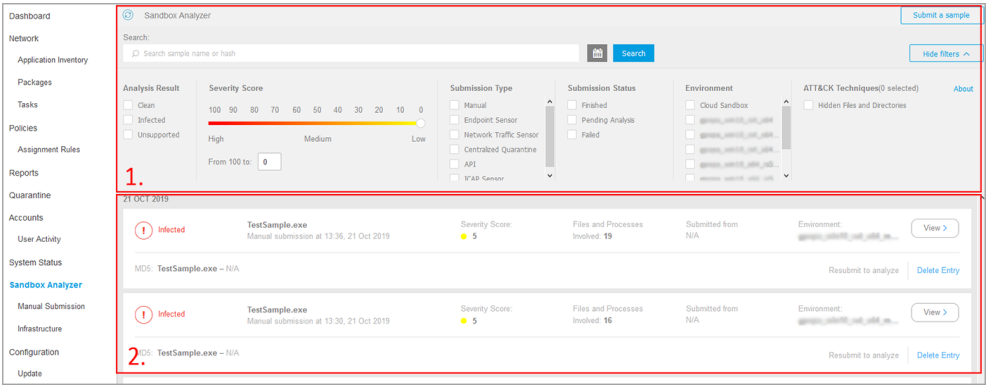
1. Go to the **Quarantine** page.
2. Select **Exchange** from the view selector.
3. Click the **Empty Quarantine** button.

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

All the entries from the Quarantine table are cleared. The requested action is sent to the target network objects immediately.

12. USING SANDBOX ANALYZER

The **Sandbox Analyzer** page provides a unified interface for viewing, filtering and searching automatic and manual submissions to the sandbox environment. The **Sandbox Analyzer** page consists of two areas:



The Sandbox Analyzer page

1. The **filtering area** allows you to search and filter submissions by various criteria: name, hash, date, analysis result, status, detonation environment and MITRE's ATT&CK techniques.
2. The **submission cards area** displays all submissions in a compact format with detailed information about each one.

In the Sandbox Analyzer page, you can do the following:

- Filter submission cards
- View the list of submissions and the analysis details
- Resend samples to analysis from the submission card
- Delete submission cards
- Make manual submissions

12.1. Filtering Submission Cards

This is what you can do in the filters area:

- Filter submissions by various criteria. The page will automatically load only the security event cards matching the selected criteria.
- Reset filters by clicking the **Clear Filters** button.
- Hide the filters area by clicking the **Hide Filters** button. You can display again the hidden options by clicking **Show Filters**.

You can filter the Sandbox Analyzer submissions by the following criteria:

- **Sample name and hash (MD5)**. Enter in the search field a part or the entire name or hash of the sample you are looking for, then click the **Search** button at the right side.
- **Date**. To filter by date:
  1. Click the calendar icon to configure the searching timeframe.
  2. Define the interval. Click the **From** and **To** buttons at the upper side of the calendar to select the dates defining the time interval. You can also select a predetermined period from the right side list of options, relatively to the current time (for example, the last 30 days).

     You can also specify the hour and minutes for each date of the time interval, using the options beneath the calendar.
  3. Click **OK** to apply the filter.
- **Analysis result**. Select one or more of the following options:
  - **Clean** – the sample is secure.
  - **Infected** – the sample is dangerous.
  - **Unsupported** – the sample has a format that Sandbox Analyzer could not detonate. To view the complete list with file types and extensions supported by Sandbox Analyzer, refer to "Supported File Types and Extensions for Manual Submission" (p. 540).
- **Severity score**. The value indicates how dangerous is a sample on a scale from 100 to 0 (zero). The higher the score, the more dangerous the sample is. The severity score applies to all submitted samples, including those with **Clean** or **Unsupported** status.
- **Submission type**. Select one or more of the following options:
  - **Manual**. Sandbox Analyzer has received the sample via **Manual Submission** option.

  - **Endpoint sensor**. Bitdefender Endpoint Security Tools has sent the sample to Sandbox Analyzer based on policy settings.
  - **Network traffic sensor**. Network sensor has sent the sample to a local Sandbox Analyzer instance based on policy settings.
  - **Centralized quarantine**. GravityZone has sent the sample to a local Sandbox Analyzer instance based on policy settings.
  - **API**. The sample has been submitted to a local Sandbox Analyzer instance by using API methods.
  - **ICAP sensor**. Security Server has submitted the sample to a local Sandbox Analyzer instance after scanning an ICAP server.
- **Submission status**. Select one or more of the following check boxes:
  - **Finished** – Sandbox Analyzer has delivered the analysis result.
  - **Pending analysis** – Sandbox Analyzer is detonating the sample.
  - **Failed** – Sandbox Analyzer could not detonate the sample.
- **Environment**. Here are listed the virtual machines available for detonation, including the Sandbox Analyzer instance hosted by Bitdefender. Select one or more check boxes to view what samples have been detonated in certain environments.
- **ATT&CK techniques**. This filtering option integrates MITRE's ATT&CK knowledge base, if applicable. The ATT&CK techniques values change dynamically, based on the security events.

  Click the **About** link to open ATT&CK Matrix in a new tab.

12.2. Viewing Analysis Details

The **Sandbox Analyzer** page displays submission cards by day, in reverse chronological order. The submission cards include the following data:

- Analysis result
- Sample name
- Submission type
- Severity score
- Files and processes involved
- Detonation environment
- Hash value (MD5)

- ATT&CK techniques
- Submission status when a result is unavailable

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

The HTML report provides rich information organized on multiple levels, with descriptive text, graphics and screen captures that illustrate the sample's behavior in the detonation environment. This is what you can learn from a Sandbox Analyzer HTML report:

- General data about the analyzed sample, such as: malware name and classification, submission details (file name, type and size, hash, submission time and analysis duration).
- Behavioral analysis results, which include all the security events captured during detonation, organized into sections. The security events refer to:
  - Writing / deleting / moving / duplicating / replacing files on the system and on removable drives.
  - Execution of newly-created files.
  - Changes to the file system.
  - Changes to the applications running inside the virtual machine.
  - Changes to the Windows taskbar and Start menu.
  - Creating / terminating / injecting processes.
  - Writing / deleting registry keys.
  - Creating mutex objects.
  - Creating / starting / stopping / modifying / querying / deleting services.
  - Changing browser security settings.
  - Changing Windows Explorer display settings.
  - Adding files to firewall exception list.
  - Changing network settings.
  - Enabling execution at system startup.
  - Connecting to a remote host.
  - Accessing certain domains.
  - Transferring data to and from certain domains.
  - Accessing URLs, IPs and ports through various communication protocols.
  - Checking the indicators of virtual environment.
  - Checking the indicators of monitoring tools.
  - Creating snapshots.
  - SSDT, IDT, IRP hooks.
  - Memory dumps for suspicious processes.

- Windows API functions calls.
- Becoming inactive for a certain time period to delay execution.
- Creating files with actions to be executed at certain time intervals.

Important
The HTML reports are available only in English, regardless of the language you use with GravityZone Control Center.

12.3. Sample Resubmission

From the submission cards area, you can resend already detonated samples to a local Sandbox Analyzer instance without having to upload them again. You may do this for samples previously submitted to the local Sandbox Analyzer instance by any sensor or method, automatically, manually or via API.

To resubmit a sample:

1. Click **Resubmit to analyze** in the submission card.
2. In the configuration window, keep the settings from the previous submission or change them as follows:
   a. Under **Image management**, select the virtual machine image you want to use for detonation.
   b. Under **Detonation configurations**, configure the following settings:
      i. **Time limit for sample detonation (minutes)**. Allocate a fixed amount of time to complete the sample analysis. The default value is 4 minutes, but sometimes the analysis may take more time. At the end of the configured interval, Sandbox Analyzer interrupts the analysis and generates a report based on the data collected up to that moment. If interrupted when incomplete, the analysis may contain inaccurate results.
      ii. **Number of reruns allowed**. In case of unexpected errors, Sandbox Analyzer tries to detonate the sample as configured until completes the analysis. The default value is 2. That means Sandbox Analyzer will try two more times to detonate the sample in case of error.
      iii. **Prefiltering**. Select this option to exclude from detonation samples already analyzed.

iv. **Internet access during detonation**. During analysis, some samples require internet connection to complete the analysis. For best result, it is recommended to keep this option enabled.

c. Under **Detonation profile**, adjust the complexity level of behavioral analysis, while affecting the Sandbox Analyzer throughput. For example, if set to **High**, Sandbox Analyzer would perform a more accurate analysis on fewer samples, in the same interval, than on **Medium** or **Low**.

3. Click **Resubmit**.

After resubmission, the **Sandbox Analyzer** page displays a new card and the data retention for that sample is extended accordingly.

Note
The **Resubmit to analyze** option is available for samples still present on the Sandbox Analyzer datastore. Make sure that data retention is configured in the **Sandbox Analyzer > Sandbox Manager** page of the policy settings.

12.4. Deleting Submission Cards

To delete a submission card that you no longer need:

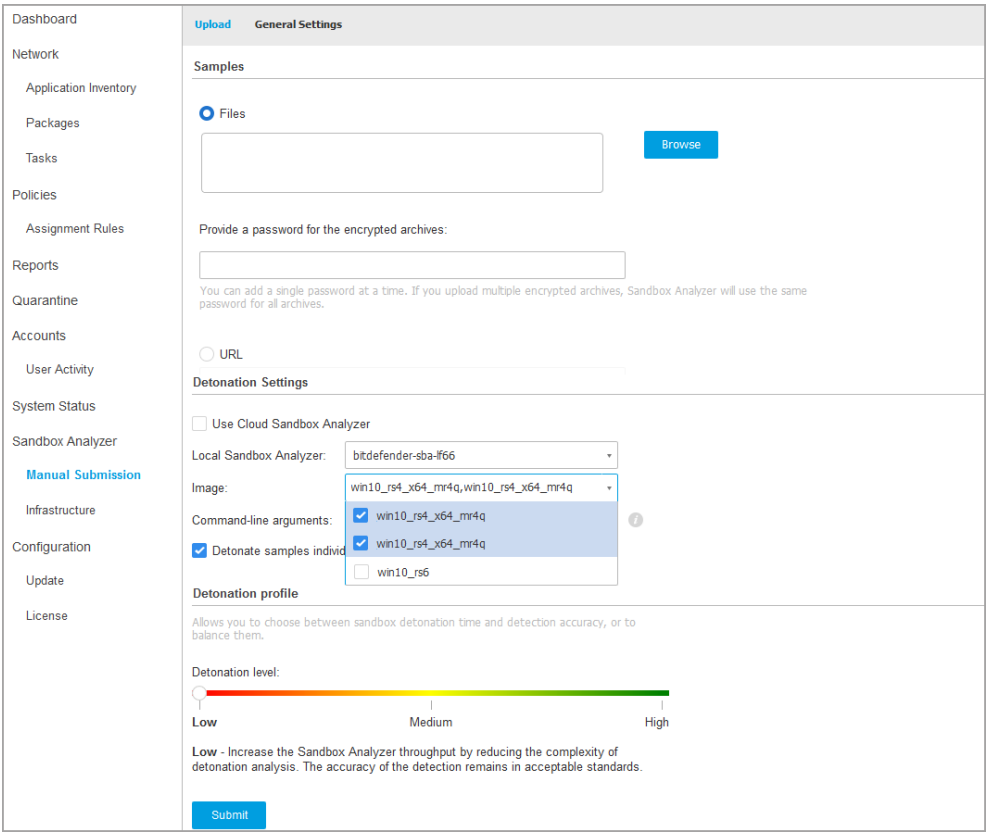
1. Go to the submission card you want to delete.
2. Click the **Delete Entry** option at the left side of the card.
3. Click **Yes** to confirm the action.

Note
By following these steps, you only delete the submission card. The information regarding the submission continues to be available in the **Sandbox Analyzer Results (Deprecated)** report. However, this report will continue to be supported only for a limited amount of time.

12.5. Manual Submission

From the **Sandbox Analyzer > Manual Submission**, you can send samples of suspicious objects to Sandbox Analyzer, to determine whether they are threats or harmless files. You can also access the **Manual Submission** page by clicking the **Submit a sample** button at the upper-right side of the filtering area in the Sandbox Analyzer page.

Note
Sandbox Analyzer Manual Submission is compatible with all web browsers required by Control Center, except Internet Explorer 9. To send objects to Sandbox Analyzer, log in to Control Center using any other supported web browser specified in "Connecting to Control Center" (p. 18).
For information on how Sandbox Analyzer interferes with HIPAA regulations, refer to the "GravityZone and HIPAA" section in the Installation Guide.



Sandbox Analyzer > Manual Submission

To submit samples to Sandbox Analyzer:

1. In the **Upload** page, under **Samples**, select the object type:

a. **Files**. Click the **Browse** button to select the objects you want to submit for behavioral analysis. In case of password-protected archives, you can define one password per upload session in a dedicated field. During the analysis process, Sandbox Analyzer applies the specified password to all submitted archives.

b. **URL**. Fill in the corresponding field with any URL you want to analyze. You can only submit one URL per session.

> **Note**
> The length limit for detonated URLs is 1,000 characters.

2. Under **Detonation settings**, configure the analysis parameters for the current session:
   - The Sandbox Analyzer instance you want to use. You can select either the Cloud instance or a Sandbox Analyzer instance installed locally.

     If choosing to use a local Sandbox Analyzer instance, you can select multiple virtual machines where you can send the sample at once.
   - **Command-line arguments**. Add as many command-line arguments as you want, separated by spaces, to alter the operation of certain programs, such as executables. The command-line arguments apply to all submitted samples during analysis.
   - **Detonate samples individually**. Select the check box to have the files from bundle analyzed one by one.
3. Under **Detonation profile**, adjust the complexity level of behavioral analysis, while affecting the Sandbox Analyzer throughput. For example, if set to **High**, Sandbox Analyzer would perform a more accurate analysis on fewer samples, in the same interval, than on **Medium** or **Low**.
4. In the **General settings** page, you can make configurations that apply to all manual submissions, regardless of session:
   a. **Time limit for sample detonation (minutes)**. Allocate a fixed amount of time to complete the sample analysis. The default value is 4 minutes, but sometimes the analysis may take more time. At the end of the configured interval, Sandbox Analyzer interrupts the analysis and generates a report based on the data collected up to that moment. If interrupted when incomplete, the analysis may contain inaccurate results.

b. **Number of reruns allowed**. In case of unexpected errors, Sandbox Analyzer tries to detonate the sample as configured until completes the analysis. The default value is 2. That means Sandbox Analyzer will try two more times to detonate the sample in case of error.

c. **Prefiltering**. Select this option to exclude from detonation samples already analyzed.

d. **Internet access during detonation**. During analysis, some samples require internet connection to complete the analysis. For best result, it is recommended to keep this option enabled.

e. Click **Save** to retain the changes.

5. Go back to the **Upload** page.
6. Click **Submit**. A progress bar indicates the submission status.

   After submission, the **Sandbox Analyzer** page displays a new card. When the analysis is complete, the card provides the verdict and the corresponding details.

Note
To manually submit samples to Sandbox Analyzer you must have **Manage Networks** rights.

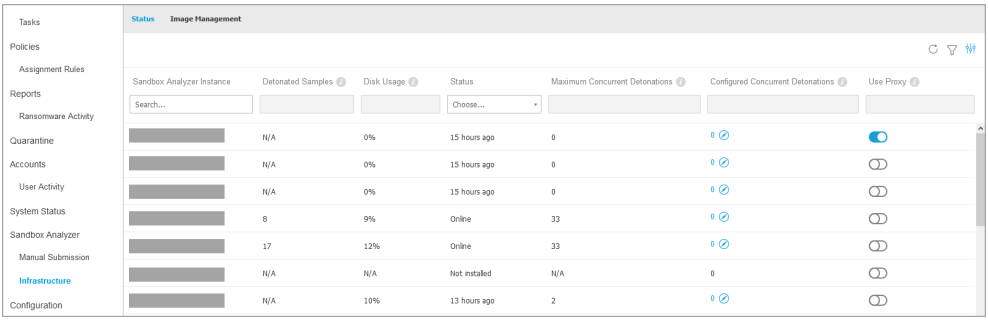
12.6. Managing Sandbox Analyzer Infrastructure

In the **Sandbox Analyzer > Infrastructure** section, you can do the following actions related to the Sandbox Analyzer instance installed locally:

- Check the Sandbox Analyzer instance status
- Configure concurrent detonations
- Check the virtual machine images status
- Configure and manage virtual machine images

12.6.1. Checking the Sandbox Analyzer Status

After deploying and configuring the Sandbox Analyzer Virtual Appliance on the ESXi hypervisor, you can obtain information about the local Sandbox Analyzer instance from the **Status** page.



Sandbox Analyzer > Infrastructure > Status

The table provides you with the following details:

- **Sandbox Analyzer instance name**. Each name corresponds to a Sandbox Analyzer instance installed on one ESXi hypervisor. You can install Sandbox Analyzer on multiple ESXi hypervisors.
- **Detonated samples**. The value indicates the number of samples analyzed since the Sandbox Analyzer instance has been licensed for first time.
- **Disk usage**. The percentage indicates the amount of the disk space consumed by Sandbox Analyzer on datastore.
- **Status**. In this column, you see whether the Sandbox Analyzer instance is online, offline, not installed, the installation is ongoing or the installation has failed.
- **Maximum concurrent detonations**. The value represents the maximum number of virtual machines that Sandbox Analyzer can create to detonate samples. At a given time, one virtual machine can perform one detonation. The number of virtual machines is determined by the amount of hardware resources available on ESXi.
- **Configured concurrent detonations**. This is the actual number of virtual machines created based on the available license.
- **Use proxy**. Click the On/Off switch to enable or disable communication between GravityZone Control Center and Sandbox Analyzer instances through a proxy server. To set up a proxy, go to **Configuration > Proxy** in the main menu of Control Center. If no proxy is set, Control Center disregards this option.

For details about proxy configuration, refer to **Installing Protection > GravityZone Installation and Setup > Configure Control Center Settings > Proxy** in the GravityZone Installation Guide.

Note
The proxy servers configured in GravityZone have different roles:

- Control Center uses the proxy server specified in **Configuration > Proxy** to communicate with the local instances of Sandbox Analyzer and with the Sandbox Analyzer Cloud portal.
- The security agents installed on endpoints use for submission the proxy specified in the **Sandbox Analyzer** page in the policy settings.
- The proxy specified in the **General > Settings** page in the policy settings ensures communication between security agents and other GravityZone components.

Important
Manual submissions to the Sandbox Analyzer Cloud portal require an HTTPS proxy server.

You can search and filter columns by Sandbox Analyzer instance name and status. Use the buttons at the upper-right corner of the table to refresh the page, and to show and hide filters and columns.

12.6.2. Configuring Concurrent Detonations

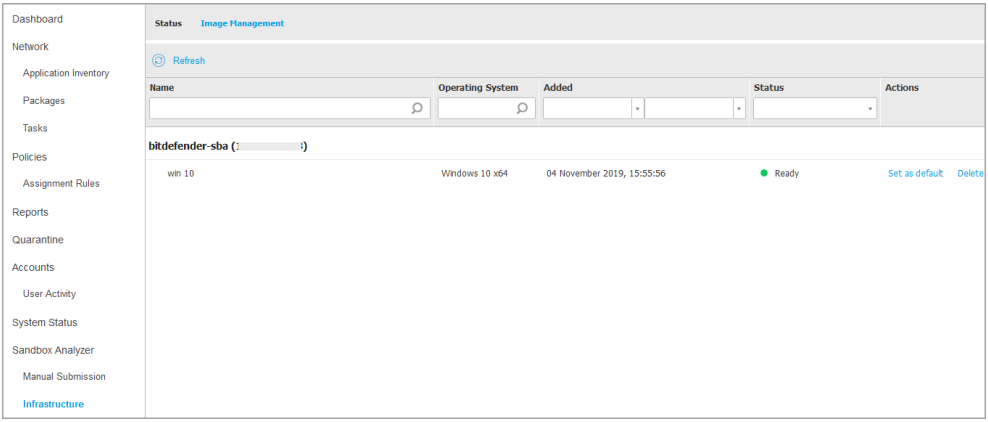
In the **Status** page, you can configure concurrent detonations, representing the number of virtual machines that can simultaneously run and detonate samples on a Sandbox Analyzer instance. The number of concurrent detonations depend on hardware resources and the license slots distribution across multiple Sandbox Analyzer instances.

To configure concurrent detonations:

1. Click the number or the **Edit** icon in the **Configured Concurrent Detonations** column.
2. In the new window, specify in the corresponding field the number of concurrent detonations you want to allocate to the Sandbox Analyzer instance.
3. Click **Save**.

12.6.3. Checking the VM Images Status

Sandbox Analyzer uses virtual machine images as detonation environments to perform behavioral analysis on submitted samples. You can check the status of the virtual machines in the **Image Management page**.



Sandbox Analyzer > Infrastructure > Image Management

The table provides you the following details:

- **Name** of the available virtual machine images, as specified in the Sandbox Analyzer appliance console. Multiple virtual machine images are grouped under the same Sandbox Analyzer instance.
- **Operating system**, as specified in the Sandbox Analyzer appliance console.
- The time when the virtual machine image was added.
- **Status**. In this column, you find out whether a virtual machine image is new and can be prepared for detonation, is ready for detonation or the preparation process has failed.
- **Actions**. In this column, you find out what you can do with the virtual machine images, depending on their status: building images for detonation, setting them as default detonation environment, or deleting them.

12.6.4. Configuring and Managing VM Images

Building Detonation Virtual Machines

To detonate samples using the local Sandbox Analyzer instance, you need to build dedicated virtual machines. The **Image Management** page allows you to create detonation virtual machines, provided you have added VM images in the Sandbox Analyzer appliance console.

Note
To learn how to add VM images in the Sandbox Analyzer appliance console, refer to the **Installing Sandbox Analyzer Virtual Appliance** chapter in the GravityZone Installation Guide.

To build detonation virtual machines, in the **Actions** column, click the **Build image** option for VM images having the status: **New – Requires build**. Building a virtual machine typically requires between 15 and 30 minutes, depending on its size. When the build is complete, the virtual machines status changes to **Ready**.

Configuring a Default Virtual Machine

A Sandbox Analyzer instance can have multiple images installed and configured as detonation virtual machines. In case of automatic submissions, Sandbox Analyzer will use the first built VM image to detonate samples.

You can change this behavior by configuring a default VM image. To do so, click the **Set as default** option for the preferred VM image.

Deleting Virtual Machines

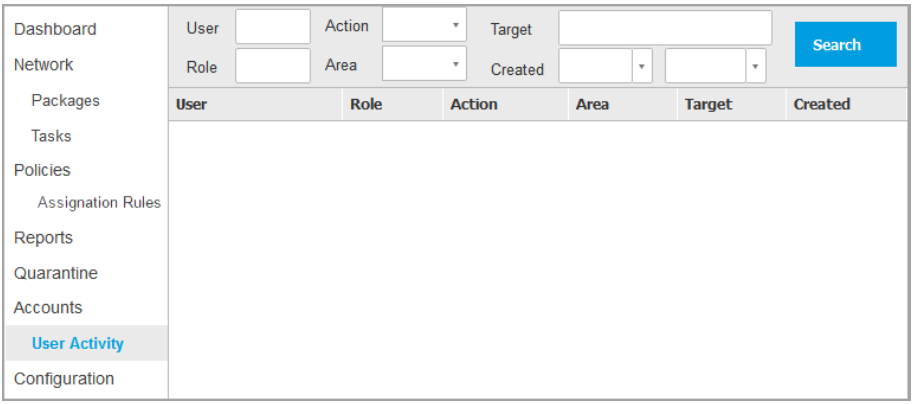
To delete a virtual machine image from the **Image Management** page, click **Delete** in the **Actions** column. In the confirmation window, click **Delete image**.

13. 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
- Starting, ending, canceling, and stopping troubleshooting processes on affected machines
- 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 and deleting access permission rules.
- Creating, editing, renaming, assigning and deleting policies
- Editing authentication settings for the GravityZone accounts.
- Creating, editing, synchronizing and deleting Amazon EC2 integrations
- Creating, editing, synchronizing and deleting Microsoft Azure integrations
- 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.

14. USING TOOLS

14.1. Custom Tools Injection with HVI

Bitdefender HVI releases you from the burden of troubleshooting issues, collecting forensics data, or running regular maintenance tasks on virtual machines in your Citrix environment, by allowing you to inject third party tools on-the-fly inside the guest operating systems. These operations are performed via Direct inspect APIs (no TCP/IP connection needed) and without disturbing the end users. For this purpose, the tools must be able to run silently.

GravityZone gives you 3 GB space to keep your tools safe and from where to inject inside the guest operating systems.

To upload tool kits to GravityZone:

1. Download the tool's latest kit version to your computer.
2. Archive the kit in a ZIP file.
3. Go to GravityZone Control Center and click the **Tools** menu in the lower-left corner of the page. The **Tools Management Center** page is displayed.
4. Click the appropriate upload button at the upper side of the table, based on the destination operating system: **Upload Windows tool** or **Upload Linux tool**.
5. If the tools is for Windows, you must also choose the applicable computer architecture from the drop-down menu.
6. Locate the ZIP file, select it and then click **Open**.

   For big files, you may have to wait a couple of minutes until upload is complete. When finished, the tool is added in the table and the progress bar above the table refreshes the information on the available space for future uploads.

Along with the tool's name, the table displays more useful details, such as:

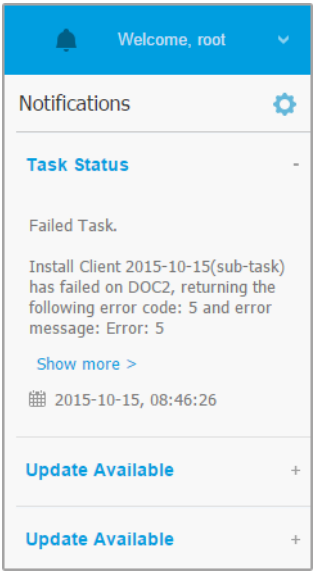
- The operating system and platform on which the tool runs.
- A brief description of the tool. You can edit this field at any time, if you want.
- The name of the user who uploaded the tool.
- Upload status. Check this field to make sure the tool uploaded successfully.
- Date and time of the upload.

Next, you can schedule via policies when to inject the tools, or you can inject them at any time by running tasks from the **Network** page.

When you no longer use the tools, select them and then click the **Delete** button at the upper side of the table to remove them. You will need to confirm by clicking **Yes**.

15. 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 

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.

15.1. 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. 515).

Threats detected by HyperDetect are out of the scope of this notification.

Syslog format availability: JSON, CEF

License Expires

This notification is sent 30, seven days and also one day before the license expires.

You must have **Manage Company** right to view this notification.

Syslog format availability: JSON, CEF

License Usage Limit Has Been Reached

This notification is sent when all of the available licenses have been used.

Syslog format availability: JSON, CEF

License Limit Is About To Be Reached

This notification is sent when 90% of the available licenses have been used.

You must have **Manage Company** right to view this notification.

Syslog format availability: JSON, CEF

Servers License Usage Limit Has Been Reached

This notification is sent when the number of protected servers reaches the limit specified on your license key.

You must have **Manage Company** right to view this notification.

Syslog format availability: JSON, CEF

Servers License Limit is About to Be Reached

This notification is sent when 90% of the available license seats for servers have been used.

You must have **Manage Company** right to view this notification.

Syslog format availability: JSON, CEF

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.

You must have **Manage Company** right to view this notification.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

Upgrade Status

This notification is triggered weekly, if old product versions are found in your network.

Syslog format availability: JSON, CEF

Update Available

This notification informs you about the availability of a new GravityZone, new package or new product update.

Syslog format availability: JSON, CEF

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

Syslog format availability: JSON, CEF

SMTP Connection

This notification is sent each time Bitdefender GravityZone detects changes regarding the mail server connectivity.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

Exchange Malware Detected

This notification informs you when malware is detected on an Exchange Server in your network.

Syslog format availability: JSON, CEF

Advanced Anti-Exploit

This notification informs you when Advanced Anti-Exploit has detected exploit attempts in your network.

Syslog format availability: JSON, CEF

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) the type of scan, detected malware, signature version, detection time and the scan engine type.

Syslog format availability: JSON, CEF

Out of Sync Integration

This notification is sent when an existing virtual platform integration could not synchronize with GravityZone. In the notification settings, you can select the integrations for which you want to be notified when a synchronization error occurs. You can check more information about the synchronization status in the notification details.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

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 find details about the application type, name and path as well as the parent process ID and path and the command line that started the process, if the case.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

Data Protection event

This notification is sent each time data traffic is blocked on an endpoint according to data protection rules.

Syslog format availability: JSON, CEF

Product Modules event

This notification is sent each time a security module of an installed agent gets enabled or disabled.

Syslog format availability: JSON, CEF

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, security content update and reboot required.

Syslog format availability: JSON, CEF

Overloaded Security Server event

This notification is sent when the scan load on a Security Server in your network exceeds the defined threshold.

Syslog format availability: JSON, CEF

Product Registration event

This notification informs you when the registration status of an agent installed in your network has changed.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

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.

Syslog format availability: JSON, CEF

Certificate Expires

This notification informs you that a security certificate expires. The notification is sent 30, seven and one day prior to expiration date.

Syslog format availability: JSON, CEF

GravityZone Update

The notification is sent when a GravityZone update is completed. If failed, the update will run again in 24 hours.

Syslog format availability: JSON, CEF

Task Status

This notification informs you either each time a task status changes, or only when a task finishes, according to your preferences.

Syslog format availability: JSON, CEF

Outdated Update Server

This notification is sent when an update server in your network has outdated security content.

Syslog format availability: JSON,CEF

Network Incidents event

This notification is sent each time the Network Attack Defense module detects an attack attempt on your network. This notification also informs you if the attack attempt was conducted either from outside the network or from a compromised endpoint inside the network. Other details include data about the endpoint, attack technique, attacker's IP, and the action taken by Network Attack Defense.

Syslog format availability: JSON, CEF

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.

Note
The HVI feature may be available for your GravityZone solution with a separate license key.

Syslog format availability: JSON, CEF

New Application in Application Inventory

This notification informs you when Application Control detects a new application installed on monitored endpoints.

Syslog format availability: JSON, CEF

Sandbox Analyzer Detection

This notification alerts you every time Sandbox Analyzer detects a new threat among the submitted samples. You are presented with details such as hostname or IP of the endpoint, time and date of the detection, threat type, path, name, size of the files and the remediation action taken on each one.

> **Note**
> You will not receive notifications for clean analyzed samples. Information on all submitted samples is available in the **Sandbox Analyzer Results (Deprecated)** report and in the **Sandbox Analyzer** section, in the main menu of Control Center.

Syslog format availability: JSON, CEF

HyperDetect Activity

This notification informs you when HyperDetect finds any antimalware or unblocked events in the network. This notification is sent for each HyperDetect event and provides the following details:

- Affected endpoint information (name, IP, installed agent)
- Malware type and name
- Infected file path. For file-less attacks it is provided the name of the executable used in the attack.
- Infection status
- The SHA256 hash of the malware executable
- The type of the intended attack (targeted attack, grayware, exploits, ransomware, suspicious files and network traffic)
- Detection level (Permissive, Normal, Aggressive)
- Detection time and date

Syslog format availability: JSON, CEF

You can view details about the infection and further on investigate the issues by generating a **HyperDetect Activity** report right from the **Notifications** page. To do so:

1. In Control Center, click the **Notification** button to display the Notification Area.
2. Click the **Show more** link at the end of the notification to open the **Notifications** page.
3. Click the **View report** button in the notification details. This opens the report configuration window.
4. Configure the report if needed. For more information, refer to "Creating Reports" (p. 465).
5. Click **Generate**.

Note
To avoid spamming, you will receive maximum one notification per hour.

Out of Sync Integration
This notification informs you when an integration has issues and can no longer synchronize. This may happen due to various resons such as integration details that have changed, or temporary unavailability of the server.

Syslog format availability: JSON, CEF

Missing Patch Issue
This notification occurs when endpoints in your network are missing one or more available patches.

GravityZone automatically sends a notification containing all findings within the last 24 hours to the notification date.

You can view which endpoints are in this situation by clicking the **View report** button in notification details.

By default, the notification refers to security patches, but you may configure it to inform you of non-security patches as well.

Syslog format availability: JSON, CEF

New Incident
This notification informs you when a new incident occurs. Once enabled, the notification is generated every time a new incident is displayed under the **Incidents** section of Control Center. The corresponding syslog event contains a list of relevant items extracted from the incident details which you can use to enrich Security information and event management (SIEM) driven correlations. For more details click the **Incident Name**.

Syslog format availability: JSON, CEF

Storage Antimalware
This notification is sent when malware is detected on an ICAP-compliant storage device. This notification is created for each malware detection, providing details about the infected storage device (name, IP, type), detected malware and detection time.

Syslog format availability: JSON, CEF

Blocked Devices
This notification is triggered when a blocked device or a device with read-only permission connects to the endpoint. If the exact same device connects multiple times in one hour, only one notification is sent during this interval. If the device connects again after one hour a new notification is triggered.

Syslog format availability: JSON, CEF

Password Expiration Enabled
This notification informs you when the password expiration is enabled on your account.

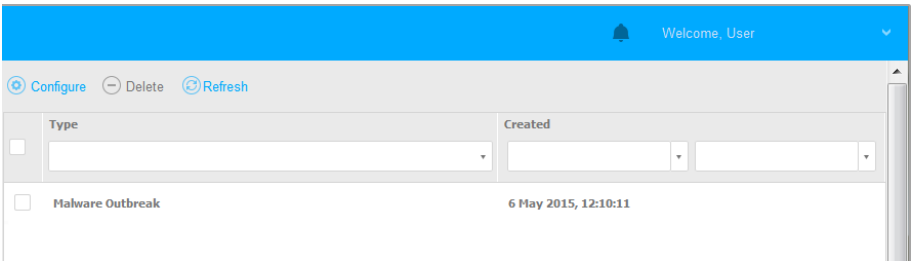
Password expiration reminder
This notification is sent daily, starting 10 days before your GravityZone password expires, to remind you that you need to change it. To quickly update the password, click the **My Account** button from the notification in Control Center.

Account Lockout Enabled
This notification informs you when the account lockout is enabled on your account.

Account Locked Out
This notification is sent via email to inform you that your account was locked out due to repeated login attempts with invalid passwords.

15.2. 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.

15.3. Deleting Notifications

To delete notifications:

1. Click the **Notification** 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.

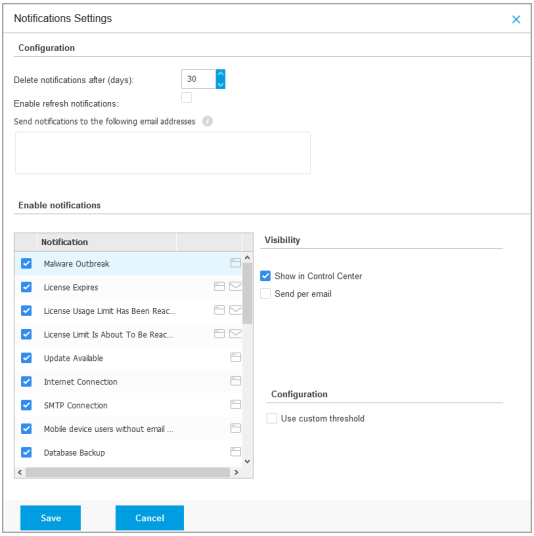
You can also configure notifications to be automatically deleted after a specified number of days. For more information, refer to "Configuring Notification Settings" (p. 515).

15.4. 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** 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. 504). 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** button.
- **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.

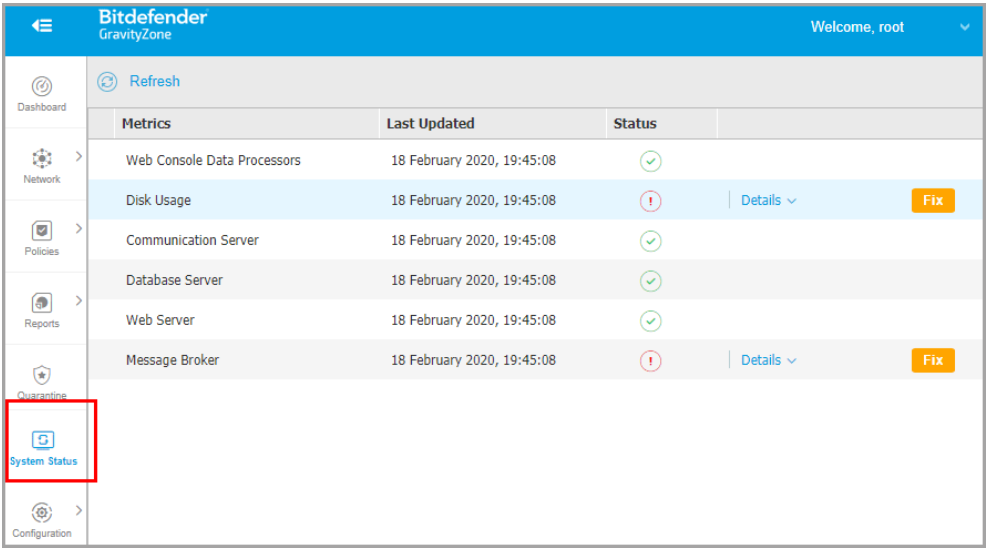
  For example, the Malware Outbreak notification is sent by default to users that have at least 5% of all their managed network objects infected by the same malware. To change the malware outbreak threshold value, enable the option **Use Custom Threshold**, then enter the value that you want in the **Malware 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**.

16. SYSTEM STATUS

The **System Status** page displays health status information of the GravityZone deployment, thus making it easier for you to view when something goes wrong. The page provides system metrics, their status and when they were last updated, all displayed in a grid formation.



System Status Page

The **Metrics** column displays all the indicators monitored by the GravityZone Control Center. For more details on every metric and status messages, refer to "Data Processors" (p. 542).

The **Last Updated** column displays the date and time of the latest status check of the metric.

The **Status** column displays the state of each metric: **OK** or **Attention**. The **Status** of a metric is updated every 15 minutes or every time you click the **Refresh** button.

16.1. OK Status

The OK status indicates that the metric is behaving normal. No additional details are displayed in this case.

16.2. Attention Status

The Attention status indicates that the metric is not running within normal parameters.

In this case you need to investigate further to see what happened and fix the current issues:

1. Click the **Details** button to expand the additional information related to the metric under scrutiny.

Metric Details

- Under **Appliance** you can find the IP addresses of the affected machines
- Under **Details** you can view the information specific to each metric.

2. Click the **Fix** to repair the metric and GravityZone will take care of the rest.

Metric Details

The status of the metric will turn back to **OK** once it has been fixed.

Note
For any other metric related issues contact Enterprise Support Team.

16.3. Metrics

The **System Status** page contains details about the following metrics:

- Web Console Data Processors
- Disk Usage
- Communication Server
- Database Server
- Web Server
- Message Broker

Web Console Data Processors

This metric monitors the state of the data processors that are used for compiling the data displayed in Control Center.

Attention Status Message	Details
`Processors that failed on this appliance: <array of data processors> .`	One or more data processors are stopped.
`The virtual appliance is down`	The virtual appliance using Web Console services is shut down.

For a complete list of processors used by Control Center, refer to "Data Processors" (p. 542).

Disk Usage

This metric monitors the amount of disk space used on each virtual appliance, how much free space is left, as well as total space on disk. If any of the disks is used above 80%, the metric displays the ⓘ **Attention** status.

Attention Status Message	Details
`Used space on disk (disk name)`	One or more disks are used above 80% of their maximum capacity.

Attention Status Message	Details
`The virtual appliance is down`	The reported virtual appliance is shut down.

Communication Server

This metric monitors the link between the security agents installed on your endpoints and the Database Server.

Attention Status Message	Details
`The service is inactive since <timestamp>`	The service has stopped running.

Database Server

This metric monitors the status of the GravityZone database.

Attention Status Message	Details
`The service is inactive since <timestamp>`	The service has stopped running on one of the appliances.
`The virtual appliance is down`	The virtual appliance using the Database Server is shut down.

Web Server

This metric monitors the state of the web server that hosts the GravityZone Control Center.

Attention Status Message	Details
`The service is inactive since <timestamp>`	The server has stopped running on one of the appliances.
`The virtual appliance is down`	The virtual appliance using this server is shut down.

Message Broker

This metric monitors the state of the message broker service on appliances with Web Console and Communication Server roles.

Attention Status Message	Details
`The message broker service is down on these appliances`	The service has stopped running on one of the appliances.
`The network connection between appliances has failed`	The connection between two appliances is broken.
`The virtual appliance is down`	The virtual appliance using this service is shut down.

17. 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.

17.1. 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.

17.2. Asking for Assistance

You can ask for assistance through our online Support Center. Fill in the contact form and submit it.

17.3. 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.

17.3.1. Using Support Tool on Windows Operating Systems

Running the Support Tool application

To generate the log on the affected computer, use one of these methods:

- Command-line

  For any issues with BEST, installed on the computer.

- Installation issues

  For situations where BEST is not installed on the computer and the installation fails.

Command-line method

Using command line you can collect logs directly from the affected computer. This method is useful in situations where you do not have access to GravityZone Control Center or the computer does not communicate with the console.

1. Open Command Prompt with administrative privileges.
2. Go to the product installation folder. The default path is:

   `C:\Program Files\Bitdefender\Endpoint Security`
3. Collect and save the logs by running this command:

   ```
   Product.Support.Tool.exe collect
   ```

   The logs are saved by default to `C:\Windows\Temp`.

   Optionally, if you want to save the Support Tool log in a custom location, use the option path:

   ```
   Product.Support.Tool.exe collect [path="<path-to-file>"]
   ```

   Example:

   ```
   Product.Support.Tool.exe collect path="D:\Test"
   ```

While the command is executing, you can notice a progress bar on the screen. When the process is complete, the output displays the name of the archive containing the logs and its location.

To submit the logs to Bitdefender Enterprise Support access `C:\Windows\Temp` or the custom location and find the archive file named `ST_[computername]_[currentdate]`. Attach the archive to your support ticket for further troubleshooting.

Installation issues

1. To download BEST Support Tool click here.
2. Run the executable file as administrator. A window will be prompted.
3. Choose a location to save the logs archive.

   While the logs are collected, you will notice a progress bar on the screen. When the process is complete, the output displays the name of the archive and its location.

To submit the logs to Bitdefender Enterprise Support, access the selected location and find the archive file named `ST_[computername]_[currentdate]`. Attach the archive to your support ticket for further troubleshooting.

17.3.2. Using Support Tool on Linux Operating Systems

For Linux operating systems, the Support Tool is integrated with the Bitdefender security agent.

To gather Linux system information using Support Tool, run the following command:

```
# /opt/BitDefender/bin/bdconfigure
```

using the following available options:

- `--help` to list all Support Tool commands
- `enablelogs` to enable product and communication module logs (all services will be automatically restarted)
- `disablelogs` to disable product and communication module logs (all services will be automatically restarted)

- `deliverall` to create:
  - An archive containing the product and communication module logs, delivered to the `/tmp` folder in the following format: `bitdefender_machineName_timeStamp.tar.gz`.

  After the archive is created:

  1. You will be prompted if you want to disable logs. If needed, the services are automatically restarted.
  2. You will be prompted if you want to delete logs.
- `deliverall -default` delivers the same information as with the previous option, but default actions will be taken on logs, without the user to be prompted (the logs are disabled and deleted).

You can also run the `/bdconfigure` command right from the BEST package (full or downloader) without having the product installed.

To report a GravityZone issue affecting your Linux systems, follow the next steps, using the options previously described:

1. Enable product and communication module logs.
2. Try to reproduce the issue.
3. Disable logs.
4. Create the logs archive.
5. Open an email support ticket using the form available on the **Help & Support** page of Control Center, with a description of the issue and having the logs archive attached.

The Support Tool for Linux delivers the following information:

- The `etc`, `var/log`, `/var/crash` (if available) and `var/epag` folders from `/opt/BitDefender`, containing the Bitdefender logs and settings
- The `/var/log/BitDefender/bdinstall.log` file, containing installation information
- The `network.txt` file, containing network settings / machine connectivity information

- The `product.txt` file, including the content of all `update.txt` files from `/opt/BitDefender/var/lib/scan` and a recursive full listing of all files from `/opt/BitDefender`
- The `system.txt` file, containing general system information (distribution and kernel versions, available RAM and free hard-disk space)
- The `users.txt` file, containing user information
- Other information concerning the product related to the system, such as external connections of processes and CPU usage
- System logs

17.3.3. 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.

17.4. Contact Information

Efficient communication is the key to a successful business. During the past 18 years Bitdefender has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

17.4.1. 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

17.4.2. 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.

17.4.3. Bitdefender Offices

The Bitdefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

United States

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Phone (sales&technical support): 1-954-776-6262
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Support Center: http://www.bitdefender.com/support/business.html

France

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Phone: +33 (0)1 47 35 72 73
Email: b2b@bitdefender.fr
Website: http://www.bitdefender.fr
Support Center: http://www.bitdefender.fr/support/business.html

Spain

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España

Fax: (+34) 93 217 91 28
Phone (office&sales): (+34) 93 218 96 15
Phone (technical support): (+34) 93 502 69 10
Sales: comercial@bitdefender.es
Website: http://www.bitdefender.es
Support Center: http://www.bitdefender.es/support/business.html

Germany

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Phone (office&sales): +49 (0) 2304 94 51 60
Phone (technical support): +49 (0) 2304 99 93 004
Sales: firmenkunden@bitdefender.de
Website: http://www.bitdefender.de
Support Center: http://www.bitdefender.de/support/business.html

UK and Ireland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Phone (sales&technical support): (+44) 203 695 3415
Email: info@bitdefender.co.uk
Sales: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Support Center: http://www.bitdefender.co.uk/support/business.html

Romania

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470

Sales: sales@bitdefender.ro
Website: http://www.bitdefender.ro
Support Center: http://www.bitdefender.ro/support/business.html

United Arab Emirates

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Phone (sales&technical support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Support Center: http://www.bitdefender.com/support/business.html

A. Appendices

A.1. Supported File Types

The antimalware scanning engines included in the Bitdefender security solutions can scan all types of files that may contain threats. The list below includes the most common types of files that are being analyzed.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

```
xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo
```

A.2. Network Object Types and Statuses

A.2.1. 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
	Golden image
	Exchange Server virtual machine
	Relay Exchange Server virtual machine
	Virtual machine with vShield
	Relay virtual machine with vShield
	Nutanix inventory
	Nutanix Prism
	Nutanix cluster
	VMware inventory
	VMware vCenter
	VMware Datacenter
	VMware resource pool

Icon	Type
	VMware cluster
	Citrix inventory
	Xen Server
	Xen Pool
	Amazon EC2 inventory
	Amazon EC2 integration
	Amazon EC2 / Microsoft Azure Region
	Amazon EC2 / Microsoft Azure Availability Zone
	Microsoft Azure inventory
	Microsoft Azure integration
	Security Server
	Security Server with vShield
	Host without Security Server
	Host with Security Server
	VMware vApp
	Mobile device user
	Mobile device

A.2.2. 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

Icon	Status
	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.3. 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.4. 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.5. 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:

  `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`.

`%USERPROFILE%`
: The path to the user's profile folder. Typical path:

  `C:\Users\{username}`

  On macOS, the user's profile folder corresponds to the Home folder. Use `$HOME` or `~` when configuring exclusions.

A.6. 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. 316).

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. 316).

A.7. Sandbox Analyzer Objects

A.7.1. Supported File Types and Extensions for Manual Submission

The following file extensions are supported and can be manually detonated in Sandbox Analyzer:

`Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.`

Sandbox Analyzer is able to detect the above-mentioned file types also if they are included in archives of the following types: `7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.`

A.7.2. File Types Supported by Content Prefiltering at Automatic Submission

Content prefiltering will determine a particular file type through a combination which implies the object content and extension. That means that an executable having the `.tmp` extension will be recognized as an application and, if found suspicious, it will be sent to Sandbox Analyzer.

- Applications - files having the PE32 format, including but not limited to the following extensions: `exe, dll, com.`

- Documents - files having the document format, including but not limited to the following extensions: `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf`.
- Scripts: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe`.
- Archives: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00`.
- Emails (saved in the file system): `eml, tnef`.

A.7.3. Default Exclusions at Automatic Submission

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt`.

A.7.4. Recommended Applications for Detonation VMs

Sandbox Analyzer On-Premises requires certain applications to be installed on the detonation virtual machines so that they open the submitted samples.

Applications	File Types
Microsoft Office suite	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Windows default	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp

Applications	File Types
Mozilla Thunderbird Microsoft Outlook	eml

A.8. Data Processors

Name	Details
Processor Request Forwarder	Forwards processor requests in distributed environments
VMware Hypervision Integrator	Synchronizes VMware inventory and other information with GravityZone
Xen Hypervision Integrator	Synchronizes Xen inventory and other information with GravityZone
Generic Virtualization Integrator	Synchronizes Nutanix, Amazon EC2 and Azure inventory with GravityZone
NTSA Integrator	Synchronizes Network Traffic Security Analytics (NTSA) integration status and sends license updates to NTSA appliance
Active Directory Computer Inventory Syncer	Synchronizes the Active Directory computer inventory with GravityZone
Active Directory Groups Inventory Syncer	Synchronizes the Active Directory groups inventory with GravityZone
Active Directory Users Import Syncer	Synchronizes the Active Directory users accounts with GravityZone (used for linking AD accounts to GravityZone accounts)
Active Directory Users Inventory Syncer	Synchronizes the Active Directory users inventory with GravityZone
Email Processor	Queues emails for sending from GravityZone
Reports Processor	Processes reports and portlets
Windows Security Agent Deployer	Deploys Bitdefender security agent to Windows devices
Security Server Deployer	Deploys Security Virtual Appliances

Name	Details
License Manager	Manages licenses of installed endpoints
Mobile Push Notifications Processor	Sends push notifications to protected mobile devices
Linux and macOS Security Agent Deployer	Deploys the Bitdefender GravityZone Enterprise Security for Virtualized Environments (SVE) agent on Linux and macOS devices
Endpoint Kits and Product Updater	Downloads and publishes Bitdefender endpoint kits and product updates
GravityZone Updater	Automatically updates GravityZone when configured. Updates version for GravityZone Virtual Appliances
Package Cleaner	Cleans up unused package files
Security Issues Processor	Processes security issues for the items in the Network section
Backup Processor	Performs backups of the GravityZone database
Notifications Processor	Sends notifications to users
System Events Processor	Handles events from the infrastructure (Application Control, Sandbox Analyzer, Serenity, SVA) or integrations (Exchange, Nutanix, NSX)
HVI Supplemental Pack Deployer	Handles the installation, update and removal of HVI supplemental pack for XEN hosts
HVI Reboot Task Processor	Manages reboot tasks on HVI hosts
Power and Online Status Processor	Computes the power state and the connectivity status of computers and virtual machines
Offline Machines Cleanup Processor	Cleans up offline machines from the network
Background Task Runner	Handles and runs background tasks and processes

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.

Antimalware Scanning 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.

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.

Protection layers

GravityZone provides protection through a series of modules and roles, collectively referred to as protection layers, which are divided into Endpoint Protection (EPP), or core protection, and various add-ons. Endpoint Protection includes Antimalware, Advanced Threat Control, Advanced Anti-Exploit, Firewall, Content Control, Device Control, Network Attack Defense, Power User, and Relay. Add-ons include protection layers such as Security for Exchange and Sandbox Analyzer.

For details about protection layers available with your GravityZone solution, refer to "GravityZone Protection Layers" (p. 2).

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.