Bitdefender®

GravityZone

Bitdefender GravityZone
Partner's Guide

Publication date 2020.04.15

Copyright© 2020 Bitdefender

Table of Contents

Preface

This document aims to explain how to manage security of your customers' networks under your account using GravityZone Control Center. You will learn how to:

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

1. Conventions Used in This Guide

Typographical Conventions

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

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

Admonitions

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

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

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

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

1. ABOUT GRAVITYZONE

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

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

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

2. GRAVITYZONE PROTECTION LAYERS

GravityZone provides the following protection layers:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Advanced Anti-Exploit
- Firewall
- Content Control
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpoint Risk Analytics (ERA)
- Email Security

2.1. Antimalware

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

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

- First, a traditional scanning method is employed where scanned content is matched against the signature database. The signature database contains byte patterns specific to known threats and is regularly updated by Bitdefender. This scanning method is effective against confirmed threats that have been researched and documented. However, no matter how promptly the signature database is updated, there is always a vulnerability window between the time when a new threat is discovered and when a fix is released.

- Against brand-new, undocumented threats, a second layer of protection is provided by **B-HAVE**, Bitdefender's heuristic engine. Heuristic algorithms detect malware based on behavioral characteristics. B-HAVE runs suspicious files in a virtual environment to test their impact on the system and ensure they pose no threat. If a threat is detected, the program is prevented from running.

Scanning Engines

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

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

1. **Local Scan**, when the scanning is performed on the local endpoint. The local scanning mode is suited for powerful machines, having security content stored locally.

2. **Hybrid Scan with Light Engines (Public Cloud)**, with a medium footprint, using in-the-cloud scanning and, partially, the local security content. This scanning mode brings the benefit of better resources consumption, while involving off-premise scanning.

3. **Central Scan in Public or Private Cloud**, with a small footprint requiring a Security Server for scanning. In this case, no security content set is stored locally, and the scanning is offloaded on the Security Server.

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

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

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

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

2.2. Advanced Threat Control

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

Advanced Threat Control continuously monitors running processes and grades suspicious behaviors such as attempts to: disguise the type of process, execute code in another process's space (hijack process memory for privilege escalation),

replicate, drop files, hide from process enumeration applications, etc. Each suspicious behavior raises the process rating. When a threshold is reached, an alarm is triggered.

2.3. 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.

> **i** **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.

2.12. 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, analyze their behavior and report any subtle system changes that is indicative of malicious intent.

Sandbox Analyzer automatically submits suspicious files residing on the managed endpoints, yet hidden to signature-based antimalware services. Dedicated heuristics embedded in the Antimalware on-access module from Bitdefender Endpoint Security Tools trigger the submission process.

The Sandbox Analyzer service is able to prevent unknown threats from executing on the endpoint. It operates in either monitoring or blocking mode, allowing or denying access to the suspicious file until a verdict is received. Sandbox Analyzer automatically resolves discovered threats according to the remediation actions defined in the security policy for the affected systems.

Additionally, Sandbox Analyzer allows you to manually submit samples directly from Control Center, letting you decide what to do further with them.

> **Important**
> The manual submission is available to GravityZone users with **Manage Networks** right.

2.13. Endpoint Detection and Response (EDR)

Endpoint Detection and Response is an event correlation component, capable of identifying advanced threats or in-progress attacks. As part of our comprehensive and integrated Endpoint Protection Platform, EDR 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 EDR 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.

2.14. Endpoint Risk Analytics (ERA)

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

2.15. Email Security

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

2.16. GravityZone Protection Layers Availability

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

3. GRAVITYZONE ARCHITECTURE

The GravityZone solution includes the following components:

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

3.1. Web Console (GravityZone Control Center)

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

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

3.2. Security Server

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

> **Note**
> Your product license may not include this feature.

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

3.3. Security Agents

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

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

3.3.1. Bitdefender Endpoint Security Tools

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

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

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

Protection Layers

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

- Antimalware
- Advanced Threat Control
- HyperDetect
- Firewall
- Content Control
- Network Attack Defense
- Patch Management
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpoint Risk Analytics (ERA)

Endpoint Roles

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

Power User

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

> **Important**
> This module is available only for supported Windows desktop and server operating systems. For more information, refer to 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.

  This functionality is essential for the security agent deployment in a cloud GravityZone environment.
- Deploying the endpoint agent inside the local network.
- Updating protected endpoints in the network.
- Ensuring the communication between Control Center and connected endpoints.
- Acting as proxy server for protected endpoints.
- Optimizing the network traffic during updates, deployments, scanning and other resource-consuming tasks.

Patch Caching Server

Endpoints with Relay role may also act as a Patch Caching Server. With this role enabled, Relays serve for storing software patches downloaded from vendor's

websites, and distributing them to target endpoints in your network. Whenever a connected endpoint has software with missing patches, it takes them from the server and not from the vendor's website, thus optimizing the traffic generated and the network bandwidth load.

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

Exchange Protection

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

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

3.3.2. Endpoint Security for Mac

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

Protection Layers

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

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

3.4. 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 contains the following components:

- **Sandbox Analyzer Portal**. This component is a hosted communication server used for handling requests between endpoints and the Bitdefender sandbox cluster.

- **Sandbox Analyzer Cluster**. This component is 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.
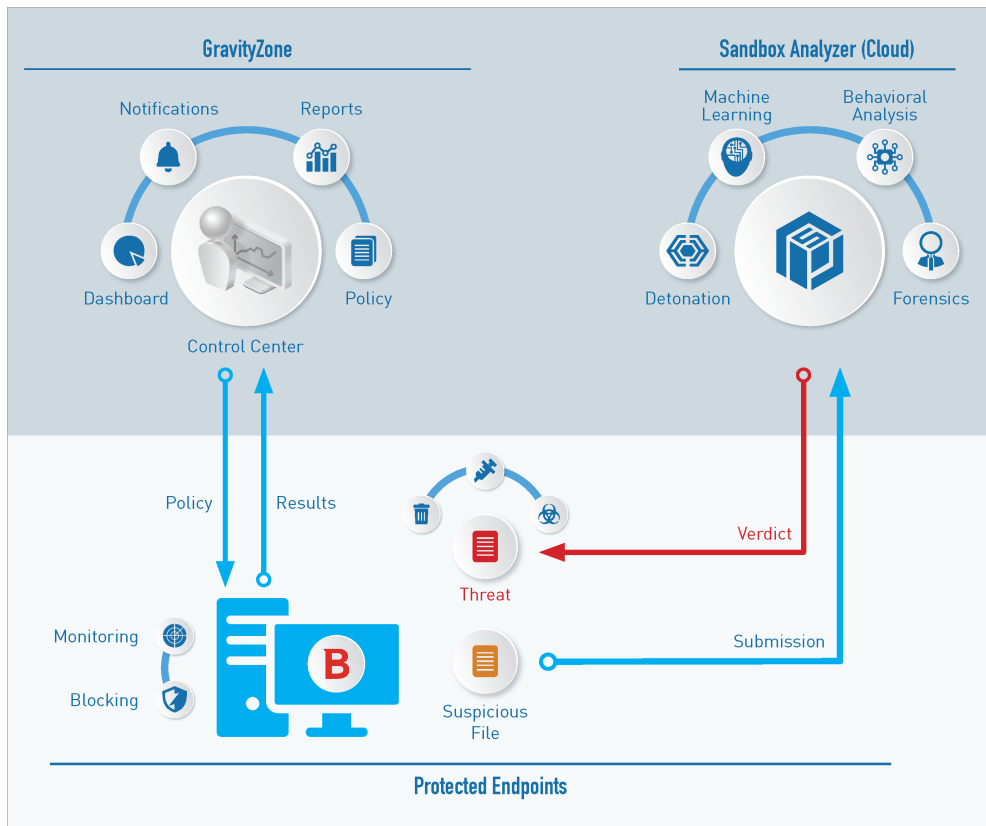
The Sandbox Analyzer architecture

Once the Sandbox Analyzer service is activated from Control Center on endpoints:

1. The Bitdefender security agent starts to submit suspicious files that match the protection rules set in the policy.

2. After the files are analyzed, a response is sent back to the Portal and further to the endpoint.

3. If a file is detected as dangerous, the user gets notified and a remediation action is taken.

The analysis results are preserved by file hash value in the Sandbox Analyzer database. When a previously analyzed file is submitted from a different endpoint,

a response is immediately sent back as the results are already available in the database.

3.5. EDR Architecture

To identify advanced threats and in-progress attacks, EDR requires hardware and operating system data. Some of the raw data is processed locally, while machine learning algorithms in the Security Analytics, perform more complex tasks.

EDR contains two major components:

- The Incidents Sensor, which collects process data, and reports endpoint and application behavior data.
- The Security Analytics, a back-end component part of the suite of Bitdefender technologies used to interpret metadata collected by the Incidents Sensor.
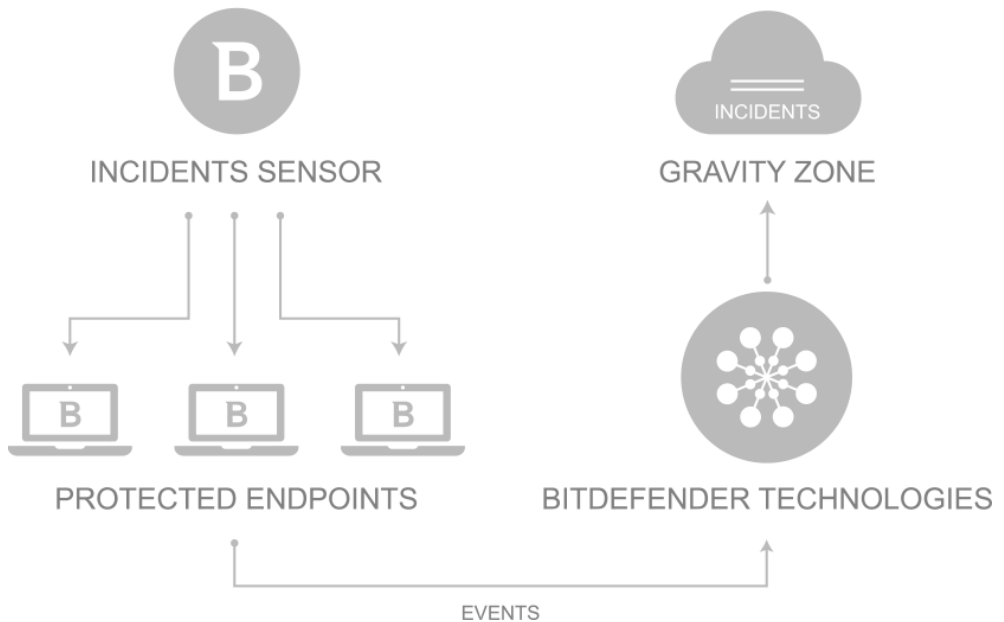
EDR flow from endpoint to Control Center

4. GETTING STARTED

GravityZone features 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. Open your web browser.
2. Go to the following address: https://gravityzone.bitdefender.com
3. If you use **GravityZone credentials**:
   a. Enter the email address of your account and click **Next**.
   b. Enter the password of your account and click **Next**.
   c. Enter the six-digit code from Google Authenticator as part of the two-factor authentification.
   d. Click **Continue** to log in.

   If you use **single sign-on**:
   a. When first logging in, enter the email address of your account and click **Next**.

      GravityZone will redirect you to the authentication page of your identity provider.
   b. Authenticate with the identity provider.

c. The identity provider will redirect you back to GravityZone and you will automatically log in to Control Center.

Next time, you will log in to Control Center with just your email address.

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.
>
> ● If your account uses single sign-on, but GravityZone asks you for a password, contact your administrator for assistance. In the meantime, log in with your previous password or use the password recovery link to receive a new password.

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.
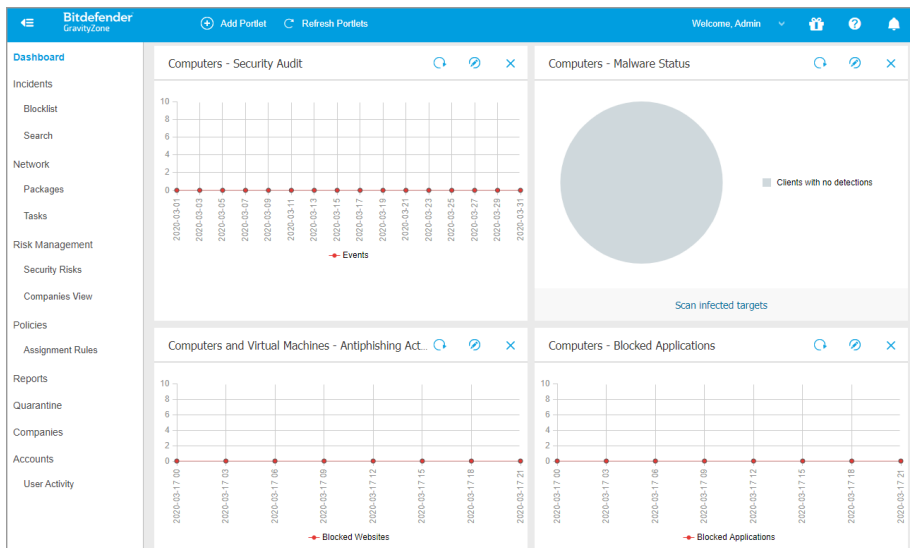
The Dashboard

4.2.1. Control Center Overview

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:

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
View your companies and networks, 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 computers and companies.

Quarantine
Remotely manage quarantined files.

Companies
Create and manage company accounts (partner companies and customer companies).

Accounts
Create and manage user accounts for your partners and customer companies you provide services to.

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

Configuration
Configure Control Center Network Inventory settings, including scheduled rules for automatic cleanup of unused virtual machines.

> **ⓘ** **Note**
> This menu is available only to users with the **Manage Networks** right.

> **ⓘ** **Note**
> Partner accounts without the **Manage Network** right can access only the monitoring and administrative menu options.

In the lower-left corner of Control Center, the 🕸 **Tools** section allows you to use more GravityZone resources, such as manual file submission to Sandbox Analyzer.

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.
- **My Company**. Click this option to manage your company account details and preferences.
- **Integrations**. Click this option to manage GravityZone integration with other management platforms.
- **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.
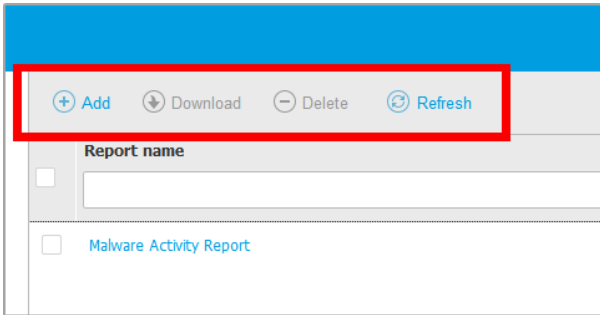
The Reports page - Action Toolbar

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.
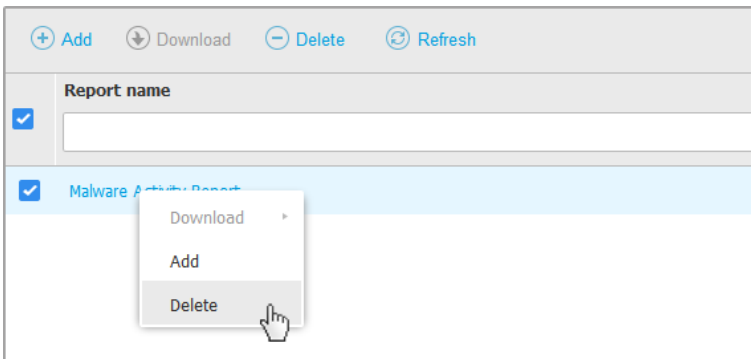
The Reports page - Contextual menu

4.3. 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**.
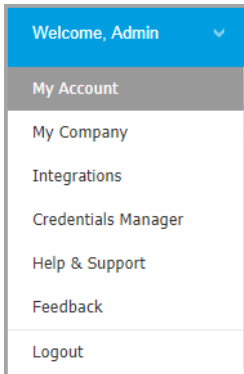
The User Account menu

2. Under **Account Details**, correct or update your account details.
   - **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. **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 logggin in to your GravityZone account you will be prompted to download and install the Google Authenticator app on a mobile device, link it to your GravityZone account, then use it with each Control Center login. Google Authenticator generates a six-digit code each 30 seconds. To complete the Control Center login, after entering the password, you will need to provide the Google Authenticator six-digit code.

> **ⓘ 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:

a. Go to **My account > Two-factor authentication** and click **Enable**.

b. A dialog box opens. Click the appropriate link to download and install Google Authenticator on your mobile device.

c. On your mobile device, open Google Authenticator.

d. 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 Google Authenticator on a new device and provide the secret key to link it to your GravityZone account.

e. Enter the six-digit code in the **Google Authenticator code** field.

f. 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.

5. In the **Control Center API** section, you can view your **Access URL**. You cannot edit this field.

For detailed information, please refer to Bitdefender Control Center API documentation.

6. The **API keys** section allows partners to generate API keys needed to perform calls to Bitdefender Control Center APIs. Partners can use Bitdefender Control Center APIs to build custom applications that automate repetitive and time consuming workflows.

   For detailed information, please refer to Bitdefender Control Center API documentation.

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

> **i** **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.

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.

4.5. Managing Your Company

4.5.1. Details and License Settings

To check or change your company details and license settings:

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

2. Under **Company Details**, fill in your company information, such as company name, address and phone.

   You can change the logo displayed in Control Center and also in your company's reports and email notifications as follows:

   - Click **Change** to browse for the image logo on your computer. The image file format must be .png or .jpg and the image size must be 200x30 pixels.

   - Click **Default** to delete the image and reset to the image provided by Bitdefender.

3. By default, your company can be managed by other companies' partner accounts that may have your company listed in their Bitdefender Control Center. You can block the access of these companies to your network by disabling the option **Allow your partner to assist with the security management of this company**. As a result, your network will not be visible in other companies' Control Center but they will be able to manage your subscription.

4. Under **License** section you can view and modify your license details and you can enter an add-on key.

   - To add a new license key:

     a. From the **Type menu**, choose a **License** subscription type.

     b. Enter the key in the **License key** field.

     c. Click the **Check** button and wait until Control Center retrieves information about the entered license key.

   - To check your license key's details, view the information displayed below the license key:

     – **Expiry date**: the date until the license key can be used.

     – **Used**: the number of used seats from the total amount of seats on the license key. A license seat is used when the Bitdefender client has been installed on an endpoint from the network under your management.

     – **Available for install**: the number of free seats from the total number of seats on a monthly license pool (excluding used and reserved seats).

     – **Reserved**: the total number of seats that you have reserved for other companies from your monthly license pool.

– **Total**: the total number of seats available on your license key or for your subscription.

Additionally, if you use a monthly subscription, you can generate the **Monthly License Usage** report for the current month. For more information, refer to **Monthly License Usage**.

- To enter an add-on key:
  – Fill in the key in the **Add-on key** field.
  – Click the **Add** button and wait until GravityZone checks the add-on key. If valid, Control Center retrieves the following information about the add-on: the type, the key and the option to remove it.

  > **Note**
  > The **Add-on key** field does not appear if you have a Trial or Monthly License.

5. Under **Bitdefender Partner** you can find information about your service provider company.

   To change your managed service provider:

   a. Click the **Change** button.

   b. Enter the partner's company ID code in the **Partner ID** field.

   > **Note**
   > Each company can find its ID in **My Company** page. Once you have made an agreement with a partner company, its representative must provide you with its Control Center ID.

   c. Click **Save**.

   As a result, your company is automatically moved from the previous partner to the new partner's Control Center.

6. Optionally, you can link your company with your MyBitdefender account using the provided fields.

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

4.5.2. Authentication Settings

To manage two-factor authentication and single sign-on for your company, go to the **Configuration > Authentication Settings** page.

Two-factor Authentication

The two-factor authentication (2FA) adds an extra layer of security to GravityZone accounts, by requiring an authentication code in addition to Control Center credentials.

This feature requires downloading and installing the Google Authenticator app on the user's mobile device, then linking the app to the GravityZone account and using it with each Control Center login. Google Authenticator generates a six-digit code each 30 seconds. To complete the Control Center login, after entering the password, the user will have to provide also the Google Authenticator six-digit code.

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

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

> **Note**
>
> - You can view the 2FA status for a user account in the **Accounts** page.
> - If a user with 2FA enabled cannot log in to GravityZone (because of new device or lost secret key), you can reset its two-factor authentication activation from the user account page, under **Two-factor authentication** section. For more details, refer to "Managing Two-factor Authentication" (p. 48).

Single Sign-on

GravityZone supports single sign-on (SSO) for Active Directory accounts as a simple and secure alternative to the classic login with username and password. This authentication method requires integration with an identity provider and SAML 2.0 as communication protocol between GravityZone and the identity provider.

To enable single sign-on in GravityZone:

1. Enable SSO for your company. To do this:

   a. Under the **Configure single sign-on using SAML** section, enter the identity provider metadata URL in the corresponding box.

      > ℹ️ **Note**
      > For AD FS, the identity provider metadata URL has the format: https://[:adfshost]/FederationMetadata/2007-06/FederationMetadata.xml, where [:adfshost] is the service FQDN.

   b. Click **Save**.

2. Configure the identity provider to use GravityZone as service provider. For details, refer to this KB article.

3. Configure GravityZone accounts to use SSO as authentication method. For details, refer to "Managing User Authentication Methods" (p. 47).

After enabling SSO, users will be required at the first login to authenticate with their identity provider to connect to GravityZone Control Center. After that, they will be able to log in only with their emails.

> ℹ️ **Note**
> Bitdefender operates two GravityZone cloud instances. In some cases, users may be required to choose one instance during the first login.

To disable single sign-on for your company:

1. Delete the identity provider metadata URL.

2. Click **Save** and confirm the action.

When disabling single sign-on for your company, users will automatically switch to log in with GravityZone credentials. Users can obtain new passwords by clicking the **Forgot password?** link on the Control Center login page and following the instructions.

When re-enabling SSO for your company, users will continue to log in to Control Center with GravityZone credentials. You need to configure manually each account to use SSO again.

5. COMPANY ACCOUNTS

As Bitdefender partner, you are in charge of managing subscriptions of your GravityZone clients, and of creating user accounts for them. Additionally, you can manage their network protection through the GravityZone security services.

Each client's subscription is associated with a company account in GravityZone. First of all, you have to create company accounts for your clients. You can do this from the **Companies** page.

The Companies page

5.1. Creating Company Accounts

To create a company account:

1. Go to the **Companies** page.
2. Click the ⊕ **Add** button at the upper side of the table. The configuration window is displayed.
3. Fill in the company details:
   - **Name**. Enter the name of the new company. The company name must be unique.
   - **Address**. Enter the physical address of the company's office. This information is optional.

- **Phone**. You can add a phone number to contact the company.

- **Logo**. You can add the company's logo image. All reports and email notifications issued for this company will include the logo image.

  To add the company's logo:

  a. Click the **Change** button.

  b. Browse for the image logo on your computer.

  c. Click **Open**.

  To reset the logo to the image provided by Bitdefender, click the **Default** button.

- **Type**. Select the type of company account:

  – **Partner**, if the company is a security or service provider and uses GravityZone to protect its business clients, or it is local distributor of GravityZone.

  – **Customer**, if the company uses GravityZone to protect just its own network.

- **Manage Networks**. By default, this option grants the following permissions to the new company:

  – View the computer network

  – Install security agents

  – Create and manage security policies

  – Run tasks

  – Manage quarantine.

  For Customer companies, these permissions cannot be revoked because the Customer must have access to its own network.

  For Partner companies that are MSPs, this option must remain enabled, as they need these permissions to manage security of their clients' networks.

  Deselect the check box, if the Partner company is a service resellers only. In this case, the Partner can still create other company accounts, manage subscriptions and view reports.

- **Allow your partner to assist with the security management of this company**. By default, you can manage endpoint protection for this company. If the

company wants to manage protection by itself, then deselect this option. Consequently:

– The company will still appear in the **Network** page, but its network will be invisible to you.

– You will be able to manage its subscription further on.

– You will be able to enforce two-factor authentication even though you cannot manage its user accounts.

– You will be able to create only specific reports, which do not disclose network information.

> ⚠ **Important**
> Once disabled, this option cannot be restored.

4. Select **Link this company to MyBitdefender (optional)** and enter your MyBitdefender account credentials, if you want to monitor the subscription from your MyBitdefender account.

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

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

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

> **i** **Note**
> ● You can view the 2FA status for a user account in the **Accounts** page.
> ● If a user with 2FA enabled cannot log in to GravityZone (because of new device or lost secret key), you can reset its two-factor authentication activation from the user account page, under **Two-factor authentication** section. For more details, refer to "Managing Two-factor Authentication" (p. 48).

6. **Configure single sign-on using SAML**. GravityZone supports single sign-on (SSO) for Active Directory accounts as a simple and secure alternative to the classic login with username and password. This authentication method requires integration with an identity provider and SAML 2.0 as communication protocol between GravityZone and the identity provider.

To enable single sign-on for a company you manage, enter the identity provider metadata URL in the corresponding box.

> **i** **Note**
> For AD FS, the identity provider metadata URL has the format: https://[:adfshost]/FederationMetadata/2007-06/FederationMetadata.xml, where [:adfshost] is the service FQDN.

In addition, you need to make the following configurations:

● The identity provider uses GravityZone as service provider. For details, refer to this KB article.

● The GravityZone accounts use SSO as authentication method. For details, refer to "Managing User Authentication Methods" (p. 47).

After enabling SSO, users will be required at the first login to authenticate with their identity provider to connect to GravityZone Control Center. After that, they will be able to log in only with their emails.

> **i** **Note**
> Bitdefender operates two GravityZone cloud instances. In some cases, users may be required to choose one instance during the first login.

To disable single sign-on for a company you manage, delete the identity provider metadata URL.

When disabling single sign-on for a company, users will automatically switch to log in with GravityZone credentials. Users can obtain new passwords by

clicking the **Forgot password?** link on the Control Center login page and following the instructions.

When re-enabling SSO for a company, users will continue to log in to Control Center with GravityZone credentials. You need to configure manually each account to use SSO again.

7. Under **License**, configure the company's subscription settings. Choose the option that is in accordance with your business agreement:

- **Trial.** This option assigns an automatically generated trial license key to the new company. The trial is valid for 30 days and it is free. During trial, the company can test the GravityZone features.

  > **!** **Important**
  > The trial covers all features except Sandbox Analyzer, HyperDetect and EDR. Only demos are available for these features.

- **License.** This option is for prepaid subscriptions, valid for one or more years. Also, you have the option to enter and manage add-on keys.

  a. Enter the license key for the client's chosen subscription.

  b. Click the **Check** button and wait until GravityZone checks the license key. If valid, Control Center displays the expiry date and the seat capacity of the license.

  c. Enter an add-on key.

  d. Click the **Add** button and wait until GravityZone checks the add-on key. If valid, Control Center displays the add-on type, and the key.

  You can add different types of add-ons by repeating the steps above.

  If you want to remove an add-on, click the ⊗ **Delete** icon.

- **Monthly subscription.** This option assigns a subscription to the new company, which is invoiced monthly, based on the services usage. At 00:00 GMT of each first day of the month, all usages are reset to zero. For details about monthly usage, refer to this KB article.

  > **!** **Important**
  > This option is available only if you have a monthly license key from Bitdefender, or if you inherit a monthly license from your Bitdefender partner.

Configure the monthly subscription settings, if needed. You can find them described herein:

License Seats Allocation

This subscription type uses license seats for security agent deployments. Each security agent consumes one seat.

You can allocate license seats to the new company using one of these two methods:

Shared License Seats

When installed, the agent uses a seat from a pool of license seats shared with other companies, including your own company. The owner of the seats pool is the first Partner above the new company in the hierarchy of company accounts which uses reservation or, in its absence, Bitdefender.

No configuration is needed in this case.

This method ensures flexibility, but increases competition between companies for the same number of seats.

Reserved License Seats

With this method, the company has a limited number of seats at disposal.

> ⚠ **Important**
> This method requires you to use seat reservation yourself.

Choose this method in case:

- You deliberately want to limit the number of seats that the company can use.

- The company wants to have seats available at any time.

Any agent installation that exceeds the allocated number of seats enters in free trial until the end of the next month. If you do not extend the reservation, when trial ends, the agent expires and the endpoint is no longer protected.

To reserve seats for the new company:

a. Select the **Reserve seats** check box.

b. Enter the number of seats you want to reserve in the near field. Once the number has changed, you can view how many seats are still available to reserve.

Security Services
Select all security services you want to enable for the new company.

> **(!) Important**
> Each service comes with an additional fee based on usage. Enabling the service will add the fee to your monthly subscription.
> You can view the usage details in the Monthly License Usage report. Learn how to calculate the monthly usage from this KB article.

- **Monthly license trial.** This option is for Partner companies. The trial is valid for 45 days, 25 license seats and it is free. During this trial, all GravityZone features are available.

- **Monthly subscription trial.** This option is for companies under a Partner with monthly license trial or monthly subscription trial. These companies inherit the duration of the trial and the number of license seats from their parent company. During this trial, all GravityZone features are available.

8. Optionally, you can proceed with creating a user account by scrolling down the configuration window. However, if the company manages its own network protection exclusively (**Allow your partner to assist with the security management of this company** option is deselected), this step is mandatory.

   Enter the account details under **Add new Account** section. You can view and manage the user account afterwards in the **Accounts** page.

   For more details, refer to "User Accounts" (p. 42).

9. Click **Save** to create the company account. The new account will appear in the company accounts list.

   If you have also configured the user account linked to the new company, an email with the login details is instantly sent to the provided email address.

Once the company and user accounts have been created, your client can start using GravityZone.

5.2. Viewing Company Accounts

Once created, you can view the company accounts in the **Companies** page, together with information regarding the company type, and license usage and validity.

To quickly check license usage for a company (including client network for partner companies), view the details in the **License usage** column:

- **Licensed.** Shows the number of seats used from an active license. A license seat is used when the Bitdefender client has been installed on an endpoint.

- **Unlicensed.** Informs you about the number of Bitdefender client installations that exceed the license capacity or are in trial.

- **Reserved.** Shows the total number of seats that a partner company has reserved for its clients.

- **Total.** Shows the total number of seats, ensured either through reservation or a license key.

- **Mailboxes.** Informs you about the number of protected mailboxes, if the company's license also includes the Security for Exchange service.

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.

You can also view detailed information about licenses in the following reports:

- **License Status**
- **Monthly License Usage**
- **Exchange - Monthly License Usage**

5.3. Editing Company Accounts

You can adjust a company account settings at any time.

To edit a company account:

1. Go to the **Companies** page.

2. Search the company account you want to change and click its name.

3. Edit account details and settings as needed. For more information, refer to the section about creating company accounts.

Additionally, if the company uses a monthly subscription, you can generate the **Monthly License Usage** report for the current month. For more information, refer to **Monthly License Usage**.

4. Click **Save**. All changes apply immediately.

5.4. Suspending and Reactivating Company Accounts

If you are no longer doing business with a company, you can suspend their account. If that company has child accounts, you have the option to suspend them at the same time.

Suspending only one company account will not automatically affect the accounts created from the suspended account. Those accounts will continue to work as before.

Choosing to suspend a company account together with its child accounts will render all those accounts unavailable.

Suspending a company has the following consequences:

●   The company users cannot log into Bitdefender Control Center

●   The endpoints directly managed by the suspended company are expired.

> **i** **Note**
> Only the endpoints that have been protected with the Bitdefender security agent installed from a kit specifically created for the suspended company are expired. Bitdefender security agent is not uninstalled from the expired endpoints. Once the company is reactivated, all expired endpoints will be automatically registered.

When reactivating a company account, you have the option to activate all its child accounts at the same time.

To suspend a company account:

1. Go to the **Companies** page.

2. Select the company account from the list.

3. Click the ⊙ **Suspend** button at the upper side of the table.

4. Select the **Suspend also all companies under this account** check box if you want to do this. This action will suspend all child accounts under your company, including those managed by other child companies.

5. Click **OK** to confirm. The company account state will change immediately. Users linked to a suspended company will no longer be able to log in.

To reactivate a company account:

1. Go to the **Companies** page.

2. Select the suspended company account from the list.

3. Click the ⊙ **Activate** button at the upper side of the table.

4. Select the **Activate also all companies under this account** check box if you want to do this. This option will reactivate all companies, including those suspended by a child company that manages them.

5. Click **OK** to confirm. The company account state will change immediately. Users linked to a reactivated company will be able to log in again to Bitdefender Control Center.

5.5. Checking the Company Status

Each company is represented in the **Companies** page by an icon specific to its type and status, described herein:

- The icon shape informs you of the company account type:

Icon	Description
▢	Partner Company
▤	Customer Company

- Blue color shows who manages network security:

Icon	Description
▤	The company self manages its network security.
▤	The Partner manages the company's network security.

- The cross sign informs of the company account status:

Icon	Description
▤	Active

Icon	Description
📧✗	Suspended

- The exclamation mark informs you of the security issues in the company's network:

Icon	Description
🖥	Without issues
🖥❗	With issues

For example, from a quick view, the 📧✗ icon informs you that the company is a customer who self manages its network security and the account is suspended.

5.6. Deleting Company Accounts

Delete company accounts when they are no longer needed. For example, if a company no longer uses Bitdefender protection or a partnership ends.

To delete an account:

1. Log in to Control Center.

2. Go to the **Companies** page.

3. Select the company account from the list.

4. Click the ⊖ **Delete** button at the upper side of the table.

5. Click **Yes** to confirm. The company account, its linked user accounts and its license key are deleted from the database.

> ⓘ **Note**
> You cannot delete partner companies with subordinate company accounts.

5.7. Managing Custom Fields

Create, edit and delete custom fields and import associated custom data. Every custom field added will appear as a column in the Monthly License Usage report for storing third party data.

> **(i) Note**
> New custom fields will will not show up as columns in already existing reports. For this to happen you need to edit and save a report so the new fields can update.

To create a custom field:

1. Log in to Control Center.
2. Go to the **Companies** > **Custom Fields** page.
3. Click the ➕ **Add** button under the **Manage custom fields** section.
4. Type in the name of the field you want to create.
5. Click **Save**.

> **(i) Note**
> You can have up to five custom fields.

To delete or edit a field, use the buttons at the right side of each saved custom field.

> **(!) Important**
> Deleting the field will also delete the values associated to it for all the companies that you manage.

5.8. Importing Values for Custom Fields

To import values for your existing custom fields, use a GravityZone CSV file.

To import the data:

1. Log in to Control Center.
2. Go to the **Companies** > **Custom Fields** page.

3. Click the ✦ **Export CSV** button under the **Import values for custom fields** section to download the template.

4. Update the values for the custom fields in the downloaded document.

5. Click the ••• **Browse** button, select the updated document from your computer and click **Open**.

6. Click the **Import CSV** button.

> **i** **Note**
> If the import encounters errors, it will continue processing the document. You will be able to view the error messages in the current page. Fix them and try to import the file again.

6. USER ACCOUNTS

You can set up and manage GravityZone from Control Center, using the account received after subscribing to the service.

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

- For each user account, you can customize the access to GravityZone features, to certain companies 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.
- Email address of the account (used to log in to Control Center). 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 (partner / company administrator / network administrator / security analyst / custom).
- 2FA (two-factor authentication) status, which allows to quickly check if the user has enabled the two factor authentication.
- Authentication method, which indicates whether the user logs in with GravityZone credentials or with an Identity Provider for single sign-on (SSO).

- The company to which the user belongs.

6.1. 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.

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

The following user roles are available:

1. **Partner** - Suited for GravityZone distributors and resellers. Users with partner accounts can create and manage other companies. When expanding their distribution chain, they create subordinate partner company accounts. When selling directly to end-users, they create customer company accounts. Partner users can manage the licenses of their subordinate companies and also manage user accounts linked to these companies. Since partners can act as security service providers, they have administrative privileges over security settings for their children customer accounts. Partner user accounts can also manage the security of their own company.

2. **Company Administrator** - Suited for managers of customer companies that have purchased a GravityZone license from a partner. A company administrator manages the license, the company's profile and its entire GravityZone deployment, allowing top-level control over all security settings (unless overridden by its parent partner account in a security service provider scenario). Company administrators can share or delegate their operational responsibilities to subordinate administrator and security analyst user accounts.

3. **Network Administrator** - Several accounts with Network Administrator role can be created for each subordinate company, with administrative privileges over one or several companies' 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.

4. **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.

5. **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 .

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

6.2. User Rights

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

- **Manage Companies**. When expanding their distribution chain, partner users create subordinate partner company accounts. When selling directly to end-users, they create customer company accounts. Partner users can also edit, suspend or delete companies under their account. This privilege is specific to partner 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.

  Network Administrators from partner companies may have management privileges over the security of customer company networks.

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

6.3. Managing User Accounts

Before creating a user account, make sure you have the required email address at hand. This address is mandatory for creating the GravityZone user account. Users receive their GravityZone login details at the provisioned email address.

6.3.1. Managing User Accounts Individually

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

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:

   - – **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.

– **Company**. Select the company to which the new user account belongs.

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.

- **Authentication method**. This setting is available for accounts under a company with single sign-on enabled. Choose from the menu for the account to either log in using GravityZone credentials or an identity provider. For details regarding the available authentication methods, refer to "Managing User Authentication Methods" (p. 47).

- **Role**. Select the user's role. For details regarding the user roles, refer to "User Roles" (p. 43).

- **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. 44).

- **Select Targets**. Select the network groups the user will have access to.

  You can restrict the user access to specific network areas or to specific companies.

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

> **Note**
> The password for each user account is automatically generated once the account has been created, and sent to the user's email address along with the other account details.
> You can change the password after the account has been created. Click the account name in the **Accounts** page to edit its password. Once the password has been modified, the user is immediately notified via email.
> Users can change their login password from Control Center, accessing the **My Account** page.

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.

6.4. Managing User Authentication Methods

When creating or editing a user account under a company with single sign-on enabled, you can to choose the authentication method for that account. Under the **Settings and Privileges** section, you have the following options:

● **Login using GravityZone credentials**. Select this option for this account to log in to Control Center with username and password.

● **Login using your identity provider**. Select this option for this account to use single sign-on (SSO), provided the company has SSO enabled and a GravityZone integration with an identity provider is in place.

> ⓘ **Note**
> You can enable SSO individually, only for accounts under a company that uses SSO. You can also enable SSO only for certain accounts under such a company. The rest may continue to log in with GravityZone credentials.

For details on how to enable SSO for your company, refer to "Single Sign-on" (p. 27).
For details on how to enable SSO for companies under your management, refer to "Single Sign-on" (p. 27).

To check the SSO changes related to user accounts, go to **Accounts > User Activity** page and filter the activity logs by Area > Authentication settings.

6.5. 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.

6.6. 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**
> As a GravityZone partner, you may turn two-factor authentication mandatory for the companies that you want, in the company settings. For more information, refer to "Editing Company Accounts" (p. 36).

> **Important**
> Google Authenticator 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. 22)

7. MANAGING ENDPOINTS

The **Network** page provides several features for exploring and managing the available endpoints. The **Network** page consists of a two-pane interface displaying the real-time status of all endpoints:
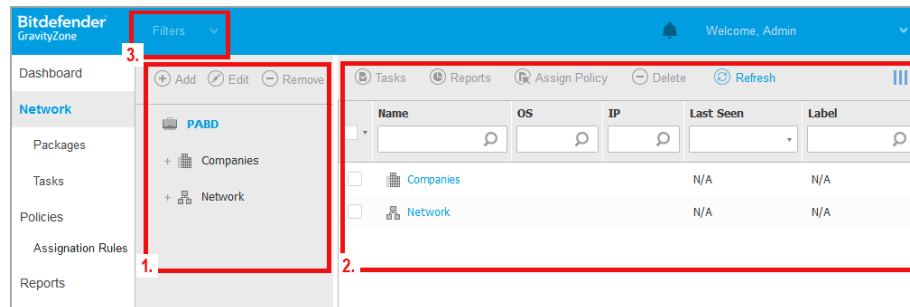
The Network Page

1. The left-side pane displays the available network tree structure. If you are logged on a partner account, you will see in this pane all networks managed from your account.

    All deleted endpoints are stored under the **Deleted** folder. To learn more, refer to .

    > **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 that you have selected in the network tree. 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. 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. 417).

● 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 **Filters** menu available at the upper side of the network panes helps you easily display only specific network objects, providing several filter criteria.

From the **Network** page you can also manage the installation packages and the tasks for your endpoints.

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

To view the endpoints under your account, go to the **Network** page and select the desired network group from the left side pane.

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 endpoint details displayed in the table:

1. Click the III **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 endpoints as follows:

● Check the endpoint status
● View endpoint details
● Organize endpoints into groups
● Sort, filter and search
● Manage patches
● Run tasks
● Define the Active Directory Integration
● Create quick reports
● Assign policies

- Delete endpoints from network inventory

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.

7.1. Checking the Endpoints Status

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

Refer to "Network Object Types and Statuses" (p. 417) for a list with all available icon types and statuses.

For detailed status information, refer to:

- Management Status
- Connectivity Status
- Security Status

7.1.1. Management Status

Endpoints can have the following management statuses:

- 🖥 **Managed** - endpoints on which the security agent is installed.

- 🗔 **Pending restart** - endpoints that require a system restart after installing or updating Bitdefender protection.

- 🖵 **Unmanaged** - detected endpoints on which the security agent has not been installed yet.

- ⊠ **Deleted** - endpoints that you have deleted from Control Center. For more information, refer to "Deleting Endpoints from Network Inventory" (p. 119).

7.1.2. Connectivity Status

The connectivity status concerns all virtual machines and only the managed computers. Managed endpoints can be:

- 🖥 **Online**. A blue icon indicates that the endpoint is online.

- 🖵 **Offline**. A grey icon indicates that the endpoint is offline.

An endpoint is offline if the security agent is inactive for more than 5 minutes. Possible reasons why endpoints appear offline:

- The endpoint is shut down, sleeping or hibernating.

  > **Note**
  > Endpoints appear online even when they are locked or the user is logged off.

- The security agent does not have connectivity with Bitdefender Control Center or with the assigned Endpoint Security Relay:
  - The endpoint 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 endpoint is behind a proxy server and the proxy settings have not been properly configured in the applied policy.

  > **Warning**
  > For endpoints behind a proxy server, the proxy settings must be properly configured in the security agent installation package, otherwise the endpoint 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 endpoint, while the endpoint 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 an endpoint, Control Center is notified of this event, and the endpoint is flagged as unmanaged.

- The security agent might not be working properly.

To find out for how long endpoints have been inactive:

1. Display only the managed endpoints. 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 endpoints 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 endpoint is currently shut down.

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

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

7.1.3. Security Status

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

● 🖥 Computer managed, with issues, online.

● 🖥 Computer managed, with issues, offline.

An endpoint 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:
  – 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 an endpoint 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.

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

7.2. Viewing Endpoint Details

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

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

7.2.1. Checking the Network page

To find out details about an endpoint, 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 **III Columns** button at the upper-right side of the pane.

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

2. 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.

3. You can easily identify the endpoint status by checking the corresponding icon. For detailed information, refer to "Checking the Endpoints Status" (p. 52).

4. Check the information displayed on columns for each endpoint.

   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.

     > **i** **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.

- **Company**: the company where the endpoint is located.

7.2.2. 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 endpoint 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 Endpoints" (p. 70).

- Protection layers information, including the list of security technologies acquired with your GravityZone solution and their license status, which can be:

  – **Not Licensed** - the GravityZone partner does not have a license key for this protection layer.

  – **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.

  > **i** **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.
- For endpoints with Active Directory Integrator role: the domain name and the last synchronization date and time.

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 security content 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. 54).

- 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. 365)

- 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. 117).

- Information on Security Analytics, as part of EDR:
  - Specific Agent Information indicates:
    - Events Provider - BEST reports endpoint and application behavior to the Security Analytics component.
    - Communication Status - BEST connects to Security Analytics.
    - Last Status Update - The most recent status.
  - Overview information on the Incidents Sensor activation status.
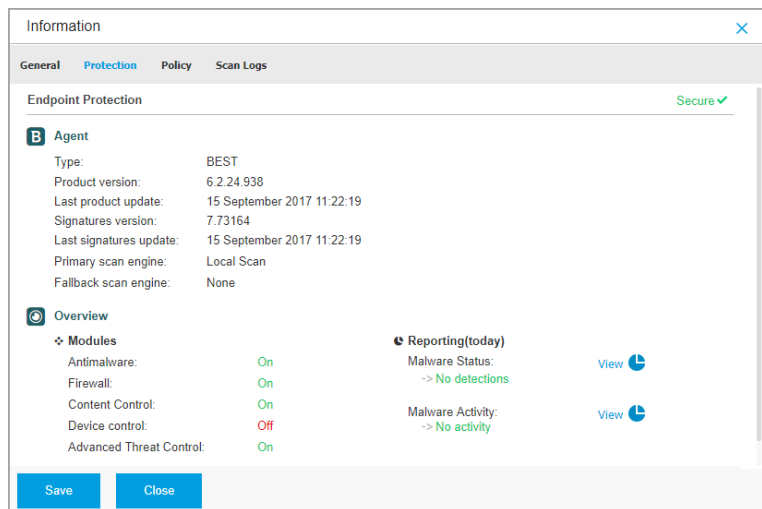
Information window - Protection tab

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. 139)

Relay tab

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

Information window - Relay tab

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 and Security Server Multi-Platform machines.

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.

   – **Bitdefender Cloud**: the logs archive is saved to a Bitdefender Cloud storage location where the Enterprise Support team can access the files. This option is available only for Windows machines.

   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, case ID) depending on the selected location.

4. Click the **Gather logs** button.

> **Note**
> If you choose **Bitdefender Cloud** as a storage option, consider the following:
>
> – The logs archive is saved with identical names both to **Bitdefender Cloud** and on the target machine. Click the troubleshooting event to view the archive's name in the details window.
>
> – After the archive is uploaded please provide Bitdefender Enterprise Support with the necessary information (name of the target machine, the archive name), on the opened case. Open a new case if none exists.

● **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 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 Security Servers:

Issue type	Use case
Antimalware (on-access and on-demand scanning)	Any unexpected behavior of the Security Server including:

Issue type	Use case
	– 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.

– **Bitdefender Cloud**: the logs archive is saved to a Bitdefender Cloud storage location where the Enterprise Support team can access the files. This option is available only for Windows machines.

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 with the necessary information (local path, credentials for the network share, path to the shared location, case ID) 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 cancelling 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.

7.3. Organizing Endpoints into Groups

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

You can manage endpoint groups in the left-side pane of the **Network** page, under **Computers and Groups** folder from the company you are interested in.

Under the **Computers and Groups** folder belonging to the company you want to manage, you can create, delete, rename and move computer groups within a custom-defined tree structure.

> **i Note**
>
> ● A group can contain both endpoints and other groups.
>
> ● When selecting a group in the left-side pane, you can view all endpoints except for those placed into its sub-groups. To view all endpoints 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 the **Computers and Groups** folder 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**.

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 Endpoints

You can move entities to **Computers and 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.

> **i** **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. 130).

Moving Endpoints between Companies

You can select multiple endpoints and move them between companies that are one level higher or lower in the Network Inventory hierarchy. To move endpoints to another company:

1. Select the endpoints you intend to move from the rights side of the **Network** page.
2. Drag and drop one of them into a folder under the destination company. A confirmation window will appear with the details of the move and any issues that might occur.

> **i** **Note**
> If you drop your selections directly under the company, the action will result in an error.

3. Confirm the task.

For more information on moving endpoints between companies refer to this kb article.

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**.

7.4. Sorting, Filtering and Searching for Endpoints

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 endpoint or choose to view only the managed endpoints.

7.4.1. Sorting Endpoints

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

Name	OS	IP	Last Seen	Label

Sorting Computers

7.4.2. Filtering Endpoints

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).

Endpoints - Filter by Type

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

Endpoints - Filter by Security

- **Policy**. Select the policy template you want to filter the endpoints 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.

Endpoints - Filter by Policy

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

Endpoints - 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 endpoints by the selected criteria. The filter remains active in the **Network** page until you log out or reset the filter.

7.4.3. Searching for Endpoints

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 endpoint you are looking for in the **IP** field. Only the matching endpoint will appear in the table.

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

	Name		OS		IP		Last Seen		Label	
		🔍		🔍	10.10.12.204	✕		▾		🔍
	🖥 BHARJOC-TEST		Windows		10.10.12.204		N/A		N/A	

Search for endpoints

7.5. 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

7.5.1. 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.

- **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.

- **Company**. The number of companies under your management where the patch is active or ignored, according to the selected view.

To customize the details displayed in the table:

1. Click the **III 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.

7.5.2. 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 them for the companies that you want. Filter patches by company, select the useless 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.

7.5.3. 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.

Moreover, you can choose to ignore some patches for specific companies under your management, while keeping them in the patch inventory for other companies.

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.

   > ⚠ **Important**
   > Selecting the root company does not automatically select subordinate companies, so make sure to select each company that you want.

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. 81)

● 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 and select the companies for which the patches will be restored.

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

7.5.4. 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. 110).

  – 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. 146).

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. 97).

   - 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.

7.5.5. 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.

> **ℹ 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.

   > **ℹ 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. 110).

– 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. 146).

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

You can select one or several endpoints from the same company. At first, select the company where the endpoints are located from the **Company** column. Then, you can use the other available filters to locate the endpoint that you want.

> **i** **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.

> **i** **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.

7.5.6. 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.

     – **Company Name**: the name of the company containing the target endpoint.

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

7.6. Running Tasks

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

This is what you can do:

- "Scan" (p. 83)
- "Scan for IOC" (p. 92)
- "Risk Scan" (p. 95)
- "Patch Tasks" (p. 96)
- "Exchange Scan" (p. 98)
- "Install" (p. 102)
- "Uninstall Client" (p. 107)
- "Update Client" (p. 108)
- "Reconfigure Client" (p. 109)
- "Restart Machine" (p. 110)
- "Network Discovery" (p. 111)
- "Update Security Server" (p. 111)

You can choose to create tasks individually for each endpoint or for groups of endpoints. For example, you can remotely install the security agent on a group of

unmanaged endpoints. At a later time, you can create a scan task for a certain endpoint from the same group.

For each endpoint, you can only run compatible tasks. For example, if you select an unmanaged endpoint, 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 endpoints. If none of the endpoints in the group is compatible with the selected task, you will be notified that the task could not be created.
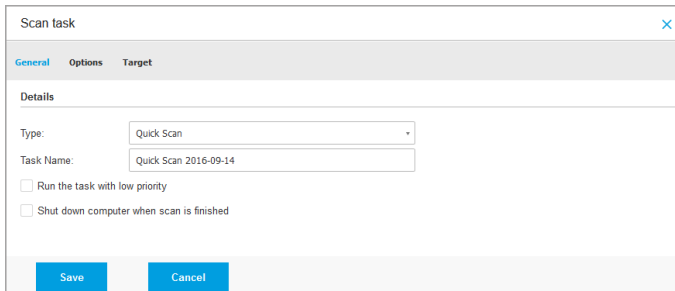
Once created, the task will start running immediately on the online endpoints. If an endpoint is offline, the task will run as soon as it gets back online.

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

7.6.1. Scan

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

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

2. 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.

3. Select the check boxes of endpoints or groups you want to scan.

4. Click the Ⓑ **Tasks** button at the upper side of the table and choose **Scan**.

   A configuration window will appear.

5. 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.

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 endpoint'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.

> **(i) 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.

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

> **(i) 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.
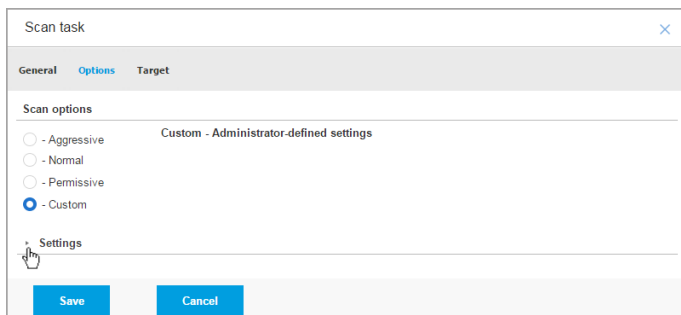
Scan Task - Configuring a Custom Scan

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. 418).

  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.

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 endpoint.

● **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 endpoints.

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. 420).

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.

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. 179).

6. 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.

> **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. 162).

7.6.2. Scan for IOC

At any time, you can choose to run on-demand scanning for known Indicators of Compromise (IOC) on selected endpoints, as follows:

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

2. Browse the containers and select the endpoints you want to scan.

3. Click the ⓑ **Tasks** button and choose **Scan for IOC**.

   A configuration page will appear, where you need to select the type of indicators taken into account for IOC scanning.

Configure Scan for IOC task

> **Note**
> You must select at least one type of Indicator of Compromise to create a valid task.

4. Select one or more IOC types you want to take into account for scanning and write the known IOC name in the newly added field.

Add IOCs

You may select from the following types:

- MD5
- SHA1
- SHA256
- SHA512
- File names
- Process names
- Registry values
- Registry keys

> **i** **Note**
> Content added inside each field must be valid. You will be prompted a warning sign and message if otherwise.

5. Click **Save** to create and run the **Scan for IOC** task. A confirmation message will appear.

You can check the task's progress in the **Network/Tasks** page.

Task Progress

6. Once the task has finished successfully you can click the ⬤ **Reports** button to read the generated report and determine the impact of the scanned-for IOC.

Valid file extensions for IOCs added to the task include: `exe`, `dll`, `com`, `scr`, `jar`, `msi`, `msc`, `bat`, `ps1`, `vbs`, `vbe`, `js`, `jse`, `wsf`, `wsh`, `psc1`, `lnk`, `doc`, `docx`, `docm`, `xls`, `xlsx`, `xlsm`, `ppt`, `pptx`, `pptm`, `eml`, `rtf`, `pdf`, `html`, `ppsx`, `pps`, `ppsm`, `pot`, `potx`, `potm`, `ocx`, `sys`, `fnr`, `fne`, and `pif`.

The **Scan for IOC** task will scan the following locations:

- `%Windows%\System32\Drivers`
- `%Windows%\System32\WindowsPowerShell\v1.0`
- `%Windows%\system32\config\systemprofile\AppData`
- `%Windows%\System32\Tasks`
- `%Windows%\System32\wbem`
- `%Windows%\SysWOW64\WindowsPowerShell\v1.0`
- `%Windows%\SysWOW64\config\systemprofile\AppData`
- `%Windows%\SysWOW64\sysprep`
- `%Windows%\Scripts`
- `%Windows%\System`
- `%Windows%\Web`
- `%Users%`

> **Important**
> The **Scan for IOC** 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 **EDR** module is not installed in the BEST client installed on the target endpoints.

- More than 100 **Scan for IOC** tasks are currently in queue.

- Invalid data is entered by user in the **Scan for IOC** task configuration page.

7.6.3. 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.

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

7.6.4. 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. 74).

> ⓘ **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. 221).

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 III **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 "Running Tasks" (p. 82).

> ℹ **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. 221).
>
> ● 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. 78).
>
> ● 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.

7.6.5. 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. 239).

To scan an Exchange Server database:

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

> ℹ️ **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.

3. Select the check box of the Exchange Server whose database you want to scan.
4. Click the **Tasks** button at the upper side of the table and choose **Exchange Scan**. A configuration window will appear.
5. 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. 418).

    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**.

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

7.6.6. Install

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

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

Once you have installed a Relay agent, it will automatically detect unprotected endpoints in the same network.

The Bitdefender protection can then be installed on endpoints 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:
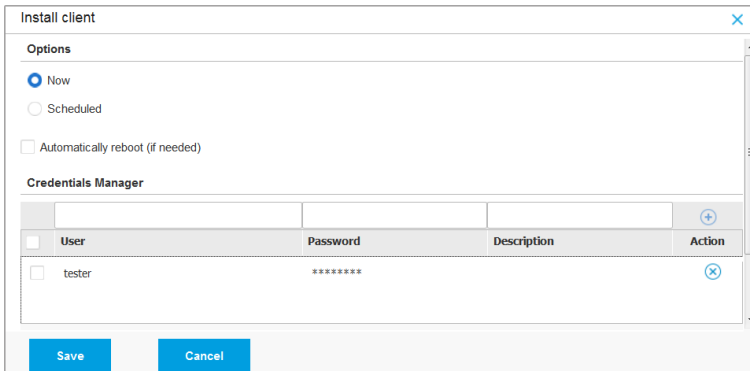
1. Connect and log in to Control Center.

2. Go to the **Network** page.

3. Select the desired group from the left-side pane. The entities contained in the selected group are displayed in the right-side pane table.

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

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

Installing Bitdefender Endpoint Security Tools from the Tasks menu

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

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

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

8. Under the **Credentials Manager** section, specify the administrative credentials required for remote authentication on target endpoints. You can add the credentials by entering the user and password for each target operating system.

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

To add the required OS credentials:

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

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

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

- For Active Directory machines use these syntaxes: `username@domain.com` and `domain\username`. To make sure that entered credentials will work, add them in both forms (`username@domain.com` and `domain\username`).

- For Workgroup machines, it suffices to enter only the user name, without the workgroup name.

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

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

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

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

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

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

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

- All machines with Relay role detected in your network will show-up in the table available under the **Deployer** section. Each new client must be connected to at least one Relay client from the same network, that will serve as communication and update server. Select the Relay that you want to link with the target endpoints. Connected endpoints will communicate with Control Center only via the specified Relay.

  > **(!) Important**
  > Port 7074 must be open, for the deployment through the Relay agent to work.

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

11. You need to select one installation package for the current deployment. Click the **Use package** list and select the installation package that you want. You can find here all the installation packages previously created for your account and also the default installation package available with Control Center.

12. If needed, you can modify some of the selected installation package's settings by clicking the button **Customize** next to the **Use package** field.

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

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

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

> **!** **Important**
> If using VMware Horizon View Persona Management, it is recommended to configure Active Directory Group Policy to exclude the following Bitdefender processes (without the full path):
> - `bdredline.exe`
> - `epag.exe`
> - `epconsole.exe`
> - `epintegrationservice.exe`
> - `epprotectedservice.exe`
> - `epsecurityservice.exe`
> - `epupdateservice.exe`
> - `epupdateserver.exe`
>
> These exclusions must apply as long as the security agent runs on endpoint. For details, refer to this VMware Horizon documentation page.

7.6.7. 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. 365).

7.6.8. Uninstall Client

To remotely uninstall the Bitdefender protection:

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

2. 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.

3. Select the check boxes of endpoints from which you want uninstall the Bitdefender security agent.

4. Click the ⓑ **Tasks** button at the upper side of the table and choose **Uninstall client**.

5. A configuration window is displayed, allowing you to opt for keeping the quarantined items on the client machine.

6. 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.

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

7.6.9. 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. 54).

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. 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.

3. Select the check boxes of endpoints where you want to run a client update.

4. Click the ⓑ **Tasks** button at the upper side of the table and choose **Update**. A configuration window will appear.

5. You can choose to update only the product, only the security content or both.

6. 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.

7.6.10. 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.

To change the installation settings for one or several endpoints:

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

2. 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.

3. Select the check boxes of endpoints for which you want to change the installation settings.

4. Click the ⓑ **Tasks** button at the upper side of the table and choose **Reconfigure client**.

5. 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.

6. 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.

7. 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.

8. 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**.

9. 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.

10. 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.

7.6.11. Restart Machine

You can choose to remotely restart managed endpoints.

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

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

2. 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.

3. Select the check boxes of endpoints you want to restart.

4. Click the ⓑ **Tasks** button at the upper side of the table and choose **Restart machine**.

5. Choose the restart schedule option:
   - Select **Restart now** to restart endpoints immediately.
   - Select **Restart on** and use the fields below to schedule the restart at the desired date and time.

6. 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.

7.6.12. Network Discovery

Network discovery is automatically done hourly by security agents with Relay role. However, you can manually run network discovery task from Control Center at any time, starting from any machine protected by Bitdefender Endpoint Security Tools.

To run a network discovery task in your network:

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

2. 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.

3. Select the check box of the relay endpoint you want to perform network discovery with.

4. Click the ⓑ **Tasks** button at the upper side of the table and choose **Network Discovery**.

5. 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.

7.6.13. Update Security Server

You can install a Security Server appliance only by downloading the Security Server installation package to a network share or to the local host and deploying it manually on the host. Once installed, the Security Server will appear under the **Custom Groups** folder belonging to its network. You can view Security Server details by clicking it and displaying the **Information** window. For details regarding the Security Server appliance installation, refer to the GravityZone Installation Guide.

> **ℹ Note**
> Your product license may not include this feature.

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

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

2. 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**.

3. Click the Ⓑ **Tasks** button at the upper side of the table and choose **Update Security Server**.

4. 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.

7.7. Integrating with Active Directory

The integration allows GravityZone to import the computer inventory from Active Directory on-premises and from Active Directory hosted in Microsoft Azure. This way, you can easily deploy and manage protection on Active Directory endpoints. Integration is performed through a managed endpoint called Active Directory Integrator.

To manage the Active Directory Integration, you can do the following:

- Set up the Active Directory Integrator
- Remove the Active Directory Integrator
- Remove the integration

7.7.1. Set up the Active Directory Integrator

You can define multiple Active Directory integrators for the same domain, and also for each available domain.

Prerequisites

The Active Directory Integrator must meet the following conditions:

- It runs Windows OS.

- It is joined in Active Directory.

- It is protected by Bitdefender Endpoint Security Tools.

- It is always online. If not, it may affect the synchronization with Active Directory.

> **!** **Important**
> It is recommended that endpoints joined in Active Directory to have the policy assigned directly to them. All the endpoints discovered in an Active Directory domain will be moved from their original folder to the Active Directory folder. In this case, if these endpoints have an inherited policy, they will be assigned with the policy set as default.

Setting Up the Active Directory Integrator

You can define multiple Active Directory integrators for the same domain, and also for each available domain.

To set an endpoint as Active Directory Integrator:

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

2. Navigate through the network inventory to the group where your endpoint is and select it.

> **i** **Note**
> If you want to define multiple integrators, you need to select one endpoint at a time.

3. Click the ⊚ **Integrations** button at the upper side of the table and choose **Set as Active Directory Integrator**.

4. Confirm your action by clicking **Yes**.

   You can notice the new 🖳 icon of the endpoint stating that it is an Active Directory Integrator. In a couple of minutes, you will be able to view the **Active Directory** tree next to **Computers and Groups**. For large Active Directory networks, the synchronization may take a longer time to complete. The endpoints joined in the same domain as the Active Directory Integrator will move from **Computers and Groups** to the Active Directory container.

Synchronizing with Active Directory

GravityZone automatically synchronizes with Active Directory every hour.

GravityZone is unable to synchronize with an Active Directory domain if the following situations occur:

- All Active Directory integrator roles have been removed
- Lost connection between Active Directory integrators and GravityZone for at least 2 hours.
- None of the Active Directory integrators from the same domain can communicate with the Domain Controller.

In any of these cases, an Active Directory issue will be triggered under the **Notifications Area**. For more information, refer to "Notifications" (p. 394).

7.7.2. Remove the Active Directory Integrator

To remove the role of Active Directory Integrator from an endpoint:

1. Go to the **Network** page.
2. Navigate through the network inventory to the group where the Active Directory Integrator is and select it.

   > **Note**
   > If you want to remove multiple integrators, you need to select one endpoint at a time.

3. Click the ⊚ **Integrations** button at the upper side of the table and choose **Remove Active Directory Integrator**.
4. A confirmation message will appear.

   - If there is not another endpoint with Active Directory Integrator role in the same domain, the confirmation message will also warn that the current domain will not be synchronized anymore with GravityZone.
   - If the endpoint is offline, the Active Directory Integrator role will be removed after it will be turned on.

You can check if any Active Directory integrator was removed from your managed network in the **User Activity** section, by filtering the user logs using the following criteria:

- **Area**: Active Directory
- **Action**: Removed AD Integrator

For more information, refer to "User Activity Log" (p. 391).

7.7.3. Remove the Active Directory integration

You can choose to remove one or several domains from the Active Directory folder, as follows:

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

2. Under the **Network** tree from the left pane, select the **Active Directory** folder.

3. Go to the right pane and select the folder of the domain you want to remove.

4. Click the ⊗ **Integrations** button at the upper side of the table and choose **Remove Active Directory Integration**.

5. A confirmation message will appear. An option available with this message allows you to choose whether you want to delete the unmanaged endpoints from the Network Inventory or not. Be careful, this option is enabled by default. Click **Confirm** to proceed.

6. All the endpoints under the selected domain will be placed under **Computer and Groups** folder (or their original groups), and the Active Directory integrator role will be removed from the assigned endpoints of this domain.

7.8. Creating Quick Reports

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

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

2. Select the group you want from the left-side pane. All endpoints 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 endpoints.

3. Select the check boxes of computers you want to include in the report.

4. 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. 351).

5. Configure the report options. For more information, refer to "Creating Reports" (p. 365).

6. Click **Generate**. The report is immediately displayed.

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

7.9. Assigning Policies

You can manage security settings on endpoints using policies.

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

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

To view the policy assigned to a particular endpoint:

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

2. Select the group that you want from the left-side pane. All endpoints from the selected group are displayed in the right-side pane table.

3. Click the name of the managed endpoint you are interested in. An information window will appear.

4. Under **General** tab, in the **Policy** section, click the name of the current policy to view its settings.

5. 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 endpoints assigned with the same policy.

   For more information about changing policy settings, refer to "Computer and Virtual Machines Policies" (p. 140).

To assign a policy to a computer or a group:

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

2. Select the group that you want from the left-side pane. All endpoints from the selected group are displayed in the right-side pane table.

3. Select the check box of the endpoint or group that you want. You can select one or several objects of the same type only from the same level.

4. Click the ⓡ **Assign Policy** button at the upper side of the table.

5. Make the necessary settings in the **Policy assignment** window. For more information, refer to "Assigning Policies" (p. 132).

7.10. 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. 259).

7.11. Assigning Security Servers

As a Service Provider, you can offer your clients with little resources the possibility to offload scanning from their endpoints, by sharing your Security Servers with them. These companies must have monthly license. You can share or assign one or more Security Servers to one or more companies at once.

To assign Security Servers:

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

2. Open the **Companies** folder in the left-side pane.

3. In the right-side pane, select the companies you want to share your Security Servers with.

4. Click the **Assign Security Servers** button at the upper side of the table. You can assign a Security Server also by right-clicking a target company and choosing this option from the contextual menu.

   A configuration window shows up, displaying the Security Servers installed in your network and the selected companies.

5. Select the Security Servers to assign.

   For each company, you can view the already assigned Security Servers. In case Security Servers were previously assigned and you want to continue using them, check that all selected targets have the same Security Servers assigned and then make sure to select those Security Servers too. If the assignment is inhomogeneous, you should reconsider making another target selection. The current assignment will overwrite all previous assignments on the selected targets. For example, you have the Security Servers SS1 and SS2, and companies C1 and C2. Security Server SS1 is assigned to company C1. You assign SS2 to both companies. After this new assignment, C1 will no longer have SS1 assigned.

6. Click **Finish**.

   Next, the target companies can start using the Security Servers shared with them, in installation packages and in antimalware policies.

To revoke a Security Server from a company, assign exact the same Security Servers, except the one you want to revoke.

> **!** **Important**
> Revoking a Security Server from a company will delete it also from the existing policies of that company.

7.12. 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.

The **Delete** action has the following effects:

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

To delete endpoints from the network inventory:

1. Go to the **Network** page.
2. In the left-side pane, select the network group that you are interested in.

> **i** **Note**
> You can only delete endpoints displayed under **Computer and Groups**, that are detected outside any integrated network infrastructure.

3. In the right-side pane, select the check box of to the endpoint 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**.

   If the deleted endpoint is managed, an **Uninstall client** task will be created on **Tasks** page, and the security agent will be uninstalled from the endpoint, releasing one license seat.
5. The endpoint is moved to the **Deleted** folder.

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

> **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.

7.13. 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

7.13.1. 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.
  - **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.
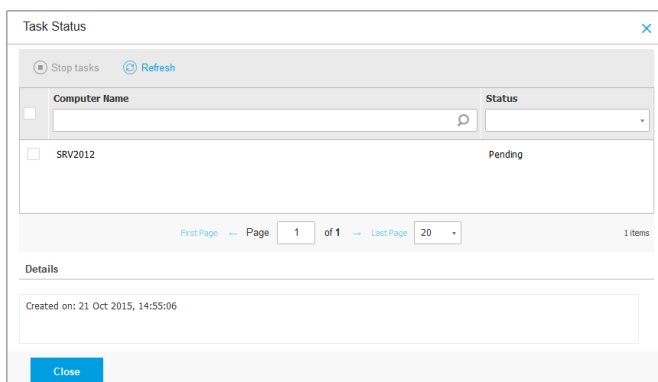
- **Checking the sub-tasks status**.

  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.

  – **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.

7.13.2. 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. Select the check box corresponding to the scan task you are interested in.

3. Click the corresponding ⊕ button from the **Reports** column. Wait until the report is displayed. For more information, refer to "Using Reports" (p. 350).

7.13.3. 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. Select the check boxes corresponding to the failed tasks.

3. Click the ⊛ **Restart** button at the upper side of the table. The selected tasks will restart and the tasks status will change to **Retrying**.

> **i** **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.

7.13.4. 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. Click the link in the **Status** column to open the **Task Status** window.

3. Select the check box corresponding to the pending or running sub-tasks you want to stop.

4. Click the ⊙ **Stop tasks** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

> **i** **Note**
> You can also stop an on-demand scan of the Exchange Store from the events area of Bitdefender Endpoint Security Tools.

7.13.5. 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. Select the check box corresponding to the task you want to delete.

3. 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.

7.14. 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

7.14.1. 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. 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**.

7.14.2. 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 (*).

      - The company where virtual machines are located - use the drop-down menu to make a selection.

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.

● Company name.

● 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.

The table displays existing rules for the selected company. To view the rules for another company, use the drop-down menu from the **Company** column to make a different selection.

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.

7.15. Credentials Manager

The Credentials Manager helps you define the credentials required for remote authentication on different operating systems in your network.

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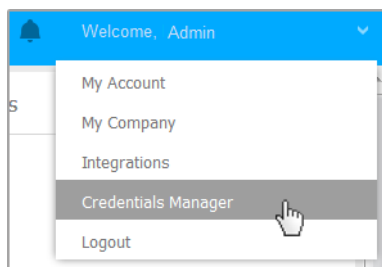
The Credentials Manager menu

7.15.1. Adding Credentials to the Credentials Manager

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

To add a set of credentials:
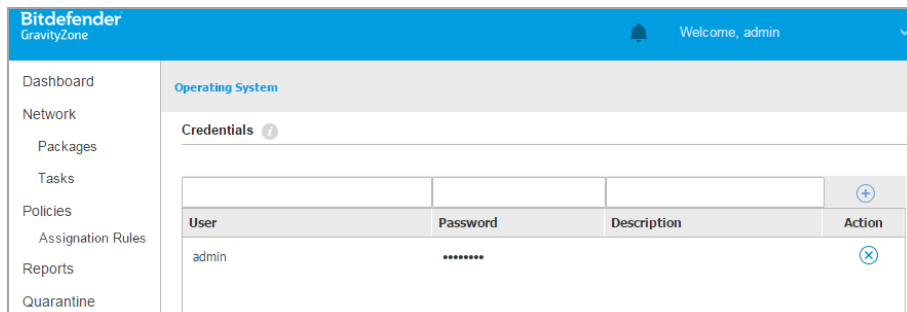
Credentials Manager

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

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

   - For Active Directory machines use these syntaxes: `username@domain.com` and `domain\username`. To make sure that entered credentials will work, add them in both forms (`username@domain.com` and `domain\username`).

   - For Workgroup machines, it suffices to enter only the user name, without the workgroup name.

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

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

7.15.2. Deleting Credentials from Credentials Manager

To delete obsolete credentials from the Credentials Manager:

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

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

8. 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 computers.

Immediately after installation, network inventory objects are assigned with the default policy, which is preconfigured with the recommended protection settings. You cannot modify or delete the default policy. You can only use it as a template for creating new policies.

You can create as many policies as you need based on security requirements. A different approach is to create separate policies for each of your customer networks.

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 at all times or only in certain conditions, based on the location of the endpoint. 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.
- Computers under a company account can be managed through policies both by the company administrator and by the partner who created the account.

Policies created from the partner account cannot be edited from the company account.

⊗ Warning
Only the supported policy modules will apply to target endpoints.
Please note that only Antimalware module is supported for server operating systems.

8.1. Managing Policies

You can view and manage policies in the **Policies** page.

The Policies page

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 company for which the policy is available.

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.

You can sort the available policies and also search for certain policies using the available criteria.

8.1.1. 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 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.

3. Configure the policy settings. For detailed information, refer to "Computer and Virtual Machines Policies" (p. 140).

4. Click **Save** to create the policy and return to the policies list.

8.1.2. 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.

You can assign 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.

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. Select the target endpoints. You can select one or several endpoints or groups of endpoints.

3. 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:

Target	Policy	Inherited from	Enforcement status
ENDPOINT3	MyPolicy	Group1	N/A

   Policy Assignment Settings

4. 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.

5. In case of warning, click the **Exclude these targets** link to continue.

6. 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.

7. 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.

8. 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**

Assigning Rule-Based Policies

The **Policies > Assignment Rules** page enables you to define assignment rules for policies, for a specific location. For example, you can apply more restrictive firewall rules if the user connects to the internet from outside the company or you can define different frequencies for on-demand tasks when outside the company.

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.

> **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 **Location 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 company to which the policy applies.

4. Select the policy for which you create the assignment rule.

5. Define the locations to which the rule applies.

   a. Select the type of the network settings from the menu at the upper side of the Locations table. These are the available types:

Type	Value
IP/network prefix	Specific IP addresses in a network or sub-networks. For sub-networks use the CIDR format. For example: `10.10.0.12` or `10.10.0.0/16`
Gateway address	IP address of the gateway
WINS server address	IP address of the WINS server **! Important** This option does not apply on Linux and Mac systems.
DNS server address	IP address of the DNS server
DHCP connection DNS suffix	DNS name without the hostname for a specific DHCP connection For example: `hq.company.biz`
Endpoint can resolve host	Hostname. For example: `fileserv.company.biz`

Type	Value
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.

6. You may want to exclude certain locations from the rule. To create an exclusion, define the locations to be excepted from the rule:

   a. Select the **Exclusions** check box under the Locations table.

   b. Select the type of the network settings from the menu at the upper side of the Exclusions table. For more information on the options, refer to the

   c. Enter the value for the selected type. You can enter multiple values in the dedicated field, separated by semicolon (;) and without additional spaces.

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

   The network settings on endpoints must match ALL conditions provided in the Exclusions table, for the exclusion to apply.

   Click the **Value** field to edit the existing criteria and then press `Enter` to save changes.

   To remove an exclusion, click the ⊗ **Delete** button at the right side of the table.

7. Click **Save** to save the assignment rule and apply it.

Once created, the location rule automatically applies to all target endpoints that are managed.

8.1.3. 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. Find the policy you are looking for in the list and click its name to edit it.

3. Configure the policy settings as needed. For detailed information, refer to "Computer and Virtual Machines Policies" (p. 140).

4. 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.

8.1.4. 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. Click the policy name. This will open the policy page.

3. Enter a new policy's name.

4. Click **Save**.

> **Note**
> The policy name is unique. You must enter a different name for each new policy.

8.1.5. 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 delete a policy:

1. Go to the **Policies** page.

2. Select the check box of the policy you want to delete.

3. Click the ⊖ **Delete** button at the upper side of the table. You will have to confirm your action by clicking **Yes**.

8.2. 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. Click the policy name. This will open the policy settings page.

3. Configure the policy settings as needed. Settings are organized under the following sections:
   - General
   - Antimalware
   - Sandbox Analyzer
   - Firewall
   - Network Protection
   - Patch Management

- Device Control
- Relay
- Exchange Protection
- Encryption
- Risk Management

Navigate through sections using the menu on the left-side of the page.

4. 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. 131).

8.2.1. 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
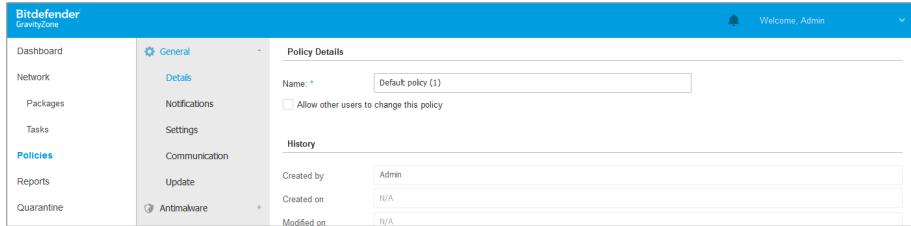
Computers and Virtual Machines Policies

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.

> **ℹ 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**.

As a Service Provider offering fully-managed services, customizing this information can help you direct end-user customer inquiries to your sales and support departments.

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.
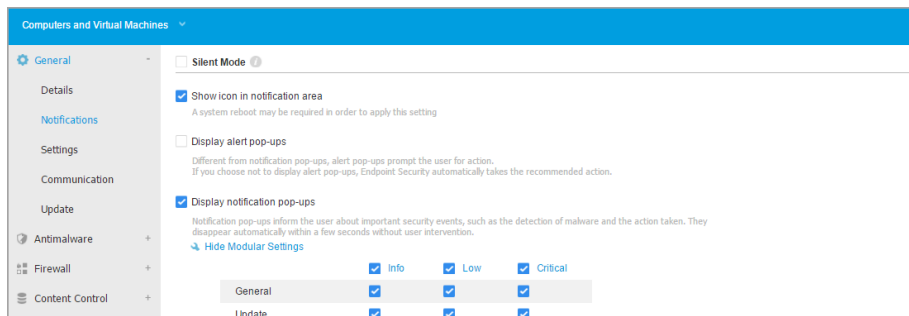
Policies - Display Settings

- **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.

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 **B** 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.

– **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 **B** 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.

> **i** **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.

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 relay agents are available in the target network, you can assign the selected computers with one or several relay endpoints via policy.

To assign relay endpoints to target computers:

1. In the **Endpoint Communication Assignment** table, click the **Name** field. The list of relay endpoints detected in your network is displayed.

2. Select an entity.

Policies - Communication settings

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

The relay endpoint is added to the list. All target computers will communicate with Control Center via the specified relay endpoint.

4. Follow the same steps to add several relays, if available.

5. You can configure the relay endpoints 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 GravityZone Control Center (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:

- **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.

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).

- **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 http://upgrade.bitdefender.com. 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.

       - **update.cloud.2d585.cdn.bitdefender.net**. This is the Bitdefender default update location, from where Bitdefender delivers updates. This update location should always remain the last option in the list.

– 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.

8.2.2. 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-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
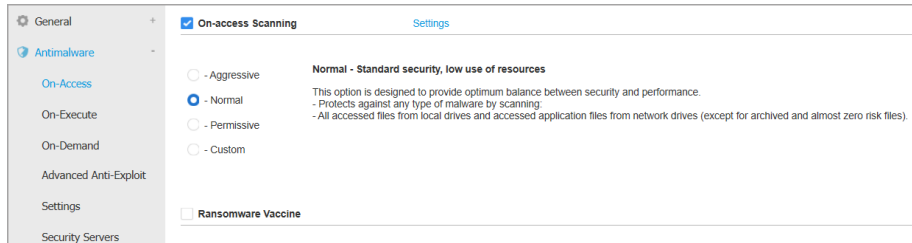
Policies - On Access Settings

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. 418).

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:

- Advanced Threat Control
- Fileless Attack Protection

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.
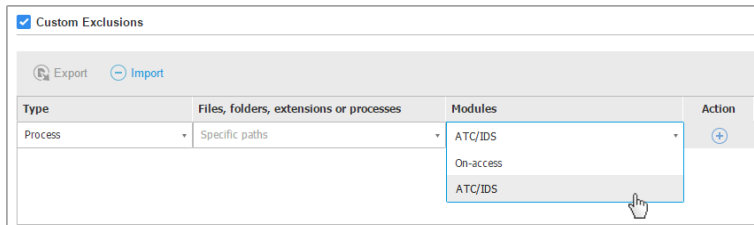
Policies - ATC/IDS process exclusion

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.

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.

> **i** **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:

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.
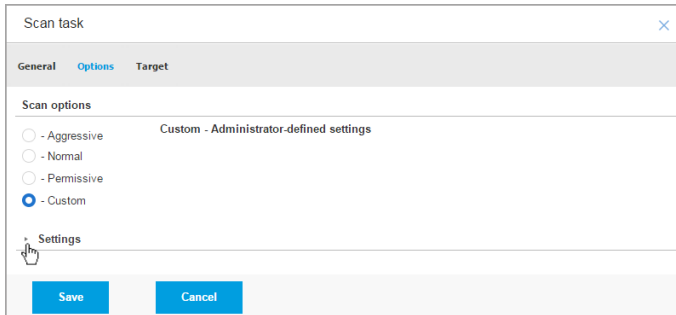
Scan Task - Configuring a Custom Scan

- **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. 418).

  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.

> **(i) 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. 179).

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

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. 175).

- **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. 175).

- **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. 175).

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.

Technique	Description
	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
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

Technique	Description
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 guarrantee 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.

- **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.

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:
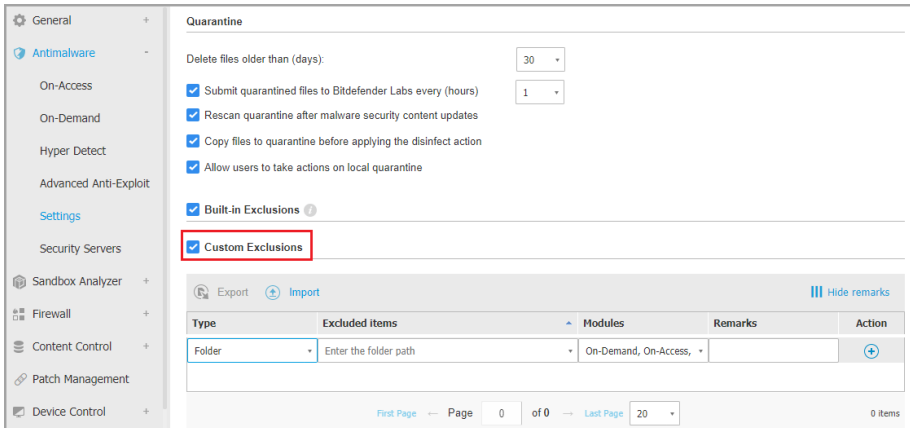
  – On-access scanning

  – On-execute scanning

  – On-demand scanning

  – Advanced Threat Control (ATC/IDS)

  > **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**: all files and processes inside the specified folder and 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 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.

For example:

File exclusions:

`C:\Test\*` – excludes all files from Test folder

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

Folder exclusion:

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

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

> **Note**
> Your product license may not include this feature.

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 regarding ports, 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.

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.

- **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.

8.2.3. Sandbox Analyzer
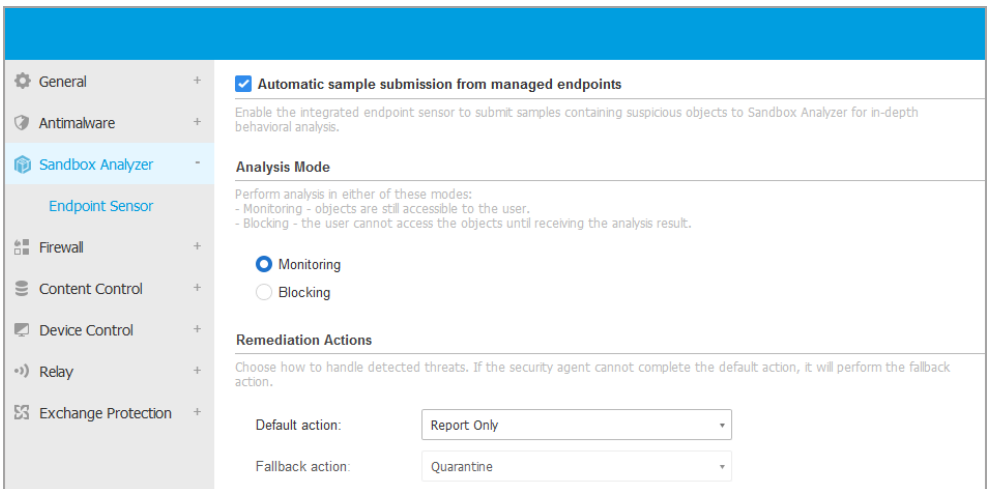
> **ℹ Note**
> This module is available for:
>
> - Windows for workstations
> - Windows for servers

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 Sandbox Analyzer settings for automatic submission via Bitdefender Endpoint Security Tools. For details about manual submission, refer to "Manual Submission" (p. 388).

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 the Sandbox Analyzer settings for automatic submission:

1. 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. 154).
> ● The upload limit for any file or archive is 50 MB.

2. 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.

3. 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:

   > **i** **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.

4. 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. 422).

   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 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.

5. **Connection Settings**. The endpoint sensor is configured to submit samples to a default Sandbox Analyzer instance hosted by Bitdefender, depending on your region.

- **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.

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. 229).

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

8.2.4. 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. 195).

> ⚠ **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.
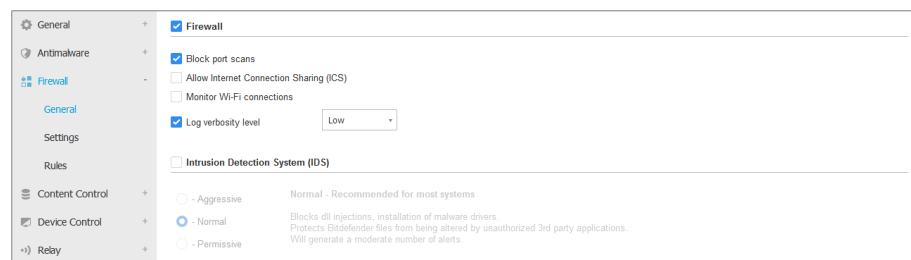
Policies - Firewall General Settings

- **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.
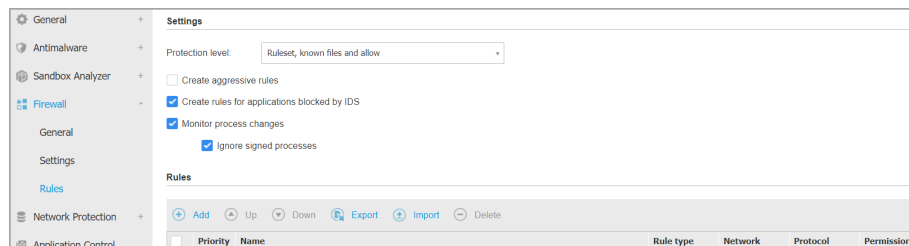
Policies - Firewall rules settings

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.

> **i** **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.

> **i** **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.

8.2.5. 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**
>
> For macOS, Content Control relies on a kernel extension. The installation of a kernel 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 kernel extension by whitelisting it using a Mobile Device Management tool. For details about Bitdefender kernel 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**

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:

    - 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 syntax samples for specifying web addresses (URLs).

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.

Syntax	Exception Applicability
`*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`.

> **i** **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.
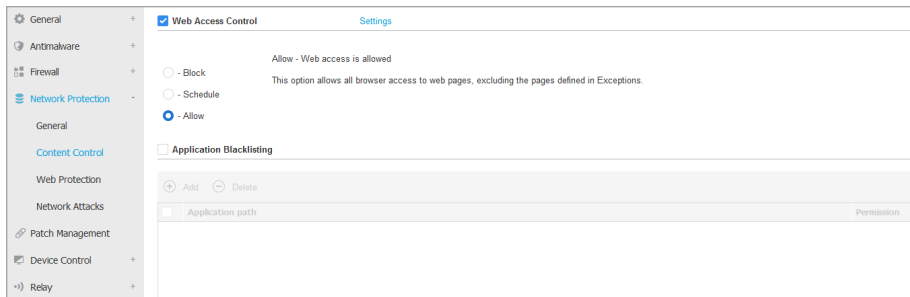
Policies - Content Control - Web

Use the switch to turn **Web Access Control** on or off.

You have three configuration options:

- Select **Allow** to always grant web access.

- Select **Block** to always deny web access.

- Select **Schedule** to enable time restrictions on web access upon a detailed schedule.

Either you choose to allow or block the web access, you can define exceptions to these actions for entire web categories or only for specific web addresses. Click **Settings** to configure your web access schedule and exceptions as follows:

Scheduler

To restrict the Internet access to certain times of the day on a weekly basis:

1. Select from the grid the time intervals during which you want Internet access to be blocked.

   You can click individual cells, or you can click and drag to cover longer periods. Click again in the cell to reverse the selection.

   To start a new selection, click **Allow All** or **Block all**, depending on the type of restriction you wish to implement.

2. Click **Save**.

> **i** **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.
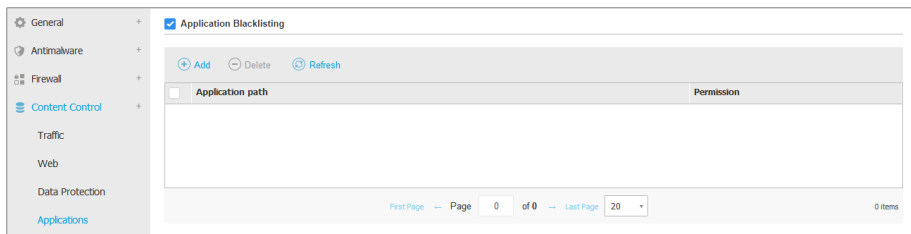
5. Click **Save**.

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.

General	+	☑ Application Blacklisting			
Antimalware	+				
Firewall	+	⊕ Add ⊖ Delete ⟳ Refresh			
Content Control	+	☐ **Application path**		**Permission**	
Traffic					
Web					
Data Protection					
Applications		First Page ← Page 0 of 0 → Last Page 20 ▾			0 items

Policies - Content Control - Applications

To configure Application Blacklisting:

1. Enable the **Application Blacklisting** option.
2. Specify the applications you want to restrict access to. To restrict access to an application:
   a. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.
   b. You must specify the path to the application executable file on the target computers. There are two ways to do this:
      - Choose from the menu a predefined location and complete the path as needed in the edit field. For example, for an application installed in the `Program Files` folder, select `%ProgramFiles` and complete the path by adding a backslash (\) and the name of the application folder.
      - Enter the full path in the edit field. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

    c. **Access Scheduler**. Schedule the applications access during certain times of day on a weekly basis:

- Select from the grid the time intervals during which you want to block access to the application. You can click individual cells, or you can click and drag to cover longer periods. Click again in the cell to reverse the selection.
- To start a new selection, click **Allow All** or **Block All**, depending on the type of restriction you wish to implement.
- Click **Save**. The new rule will be added to the list.

To remove a rule from the list, select it and click the ⊗ **Delete** button at the upper side of the table. To edit an existing rule, click it to open its configuration window.

Data Protection

Data Protection prevents unauthorized disclosure of sensitive data based on administrator-defined rules.

Note
This feature is not available for macOS.

Policies - Content Control - Data Protection

You can create rules to protect any piece of personal or confidential information, such as:

- Customer personal information
- Names and key details of in-development products and technologies
- Contact information of company executives

Protected information might include names, phone numbers, credit card and bank account information, email addresses and so on.

Based on the data protection rules you create, Bitdefender Endpoint Security Tools scans the web and outgoing email traffic for specific character strings (for example, a credit card number). If there is a match, the respective web page or email message is blocked in order to prevent protected data from being sent. The user is immediately informed about the action taken by Bitdefender Endpoint Security Tools through an alert web page or email.

To configure Data Protection:

1. Use the checkbox to turn on Data Protection.

2. Create data protection rules for all of the sensitive data you want to protect. To create a rule:

   a. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.

   b. Enter the name under which the rule will be listed in the rules table. Choose a suggestive name so that you or other administrator can easily identify what the rule is about.

   c. Select the type of data you want to protect.

   d. Enter the data you want to protect (for example, the phone number of a company executive or the internal name of a new product the company is working on). Any combination of words, numbers or strings consisting of alphanumerical and special characters (such as @, # or $) is accepted.

   Make sure to enter at least five characters in order to avoid the mistaken blocking of email messages and web pages.

   > ⚠ **Important**
   >
   > Provided data is stored in encrypted form on protected endpoints, but it can be seen on your Control Center account. For extra safety, do not enter all of the data you want to protect. In this case, you must clear the **Match whole words** option.

   e. Configure the traffic scan options as needed.

   - **Scan web (HTTP traffic)** - scans the HTTP (web) traffic and blocks the outgoing data that matches the rule data.

- **Scan email (SMTP traffic)** - scans the SMTP (mail) traffic and blocks the outgoing email messages that contain the rule data.

  You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.

  f. Click **Save**. The new rule will be added to the list.

3. Configure exclusions to data protection rules so that users can still send protected data to authorized websites and recipients. Exclusions can be applied globally (to all rules) or to specific rules only. To add an exclusion:
   a. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.
   b. Enter the web or email address that users are authorized to disclose protected data to.
   c. Select the type of exclusion (web or email address).
   d. From the **Rules** table, select the data protection rules(s) on which this exclusion should be applied.
   e. Click **Save**. The new exclusion rule will be added to the list.

ⓘ **Note**
If an email containing blocked data is addressed to multiple recipients, those for which exclusions have been defined will receive it.

To remove a rule or an exclusion from the list, click the corresponding ⊗ **Delete** button at the right side of the table.

Web Protection

In this page, the settings are organized under the following sections:

- Antiphishing
- Web Traffic Scan
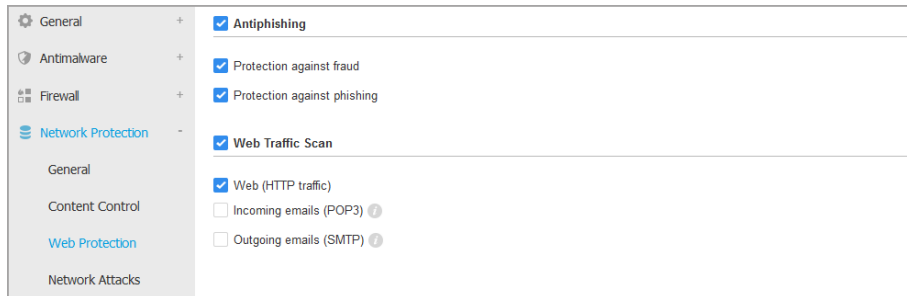
Policies - Network Protection - Web Protection

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. Click **Exclusions**.

2. Enter the web address and click the ⊕ **Add** button.

   If you want to exclude an entire website, write the domain name, such as `http://www.website.com`, and if you want to exclude only a webpage, write the exact web address of that page.

> **i** **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.
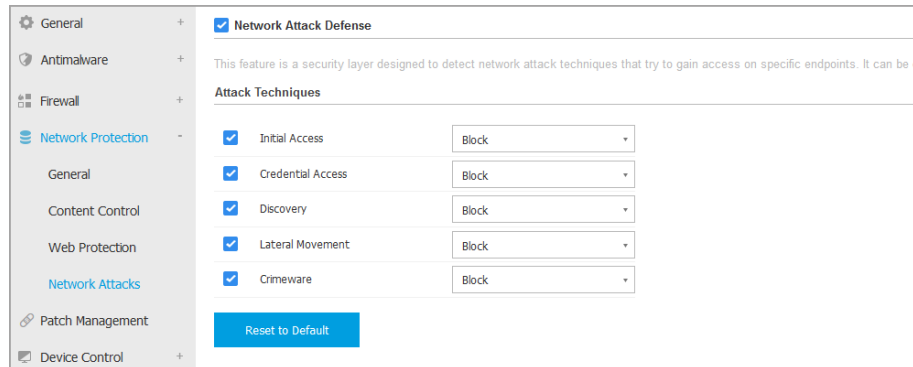
Though not recommended, you can disable email and web traffic scan to increase system performance. This is not a major threat as long as on-access scanning of local files remains enabled.

> **i** **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.

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 based 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.

Security Policies

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.

8.2.6. 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.

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

8.2.7. Device Control

> **i** **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**
> For macOS, Device Control relies on a kernel extension. The installation of a kernel 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 kernel extension by whitelisting it using a Mobile Device Management tool. For details about Bitdefender kernel 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	
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.

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**.

> **i** **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.

Policies - Device Control - Exclusions

8.2.8. 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.

- The default update location for relay agents is http://upgrade.bitdefender.com. You can specify other update locations by entering the IP or the local hostname of one or several relay machines 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.

8.2.9. 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 available at the company level, regardless of the policy or the user that created them.

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.

> **i** **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.

Settings

● **Delete quarantined files older than (days).** By default, quarantined files older than 15 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 .

    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.

> **i** **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

Hidden header with Bitdefender GravityZone logo

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. 418).

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. 246).
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. 244).

> ⚠️ **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. 248)

  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 .

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. 249).

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. 419).

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**.

8.2.10. Encryption

(i) **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. 262).

- **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.

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. 117).

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** ⊗.

8.2.11. Risk Management

ⓘ **Note**
This module is available for:

   - Windows for workstations
   - Windows for servers

The Endpoint Risk Analytics module helps you identify and remediate a large number of network and operating system risks at the endpoint level via risk scan tasks that can be configured in policy to run recurrently on target endpoints.

You can choose from a large list of indicators of risks for scanning your endpoints and determine if they are vulnerable. For more information about GravityZone indicators of risk, refer to this KB article.

To configure ERA:

- Check the box to enable the **Risk Management** features and start configuring policies that define how to run the **Risk Scan** task.
- **Scheduler**: define the risk scan schedule for target endpoints:
  1. Specify the start date and time for the scheduled risk scan.
  2. Choose the scan recurrence type:
     - Periodically, by a specified number of hours / days / weeks.
     - By weekday.

     > **Important**
     > 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.
     > 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).

  3. Optionally, you can specify what happens when the scan task could not start at the scheduled time (endpoint was offline or shutdown).

     Use the **If scheduled run time is missed, run task as soon as possible** option 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.

Risk scan tasks run with all the indicators of risk activated by default.

After a risk scan 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 of risk and their description, refer to this KB article.

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.
- **Search**: provides options for querying the security events database.

9.1. The Incidents Page

Use the **Incidents** page to filter and manage security events.

Incidents page overview

This page contains the following areas:

1. **Investigate** and **Review** tabs, containing corresponding incident categories.
2. **Overview** bar, listing the open incidents, top alerts, used attack techniques, and affected devices.
3. **Filters**, providing multiple filtering criteria for security events.
4. **List of security event cards**, displaying the list of events according to the applied filters.

> ℹ️ **Note**
> This feature no longer provides support for Internet Explorer.

This is what you can do from the **Incidents** page:

- Filter security events
- View the list of security events
- Change the incidents investigation status
- Open and investigate a security event

9.1.1. Filtering Security Events

Use filters to refine your search when analyzing security events.

Security events filtering options

1. GravityZone groups security events under two categories, available as tabs in the **Incidents** page. Click the tab you want for viewing the appropriate list of security events:

   - 🧭 **Investigate**: displays all suspicious incidents requiring investigation, upon which no action was taken yet. Here you can find all reported endpoint activity that may represent a threat and needs your attention.

   - 🛡️ **Review**: includes security events identified as threats by GravityZone prevention modules and applied with the predefined policy actions. In certain cases, these incidents require taking an action, or you may want to review them for further analysis.

2. Fully customizable grid with multiple filtering options.

The Filters Grid

The **Incidents** page allows you to choose what incidents to display by customizing the filters grid.
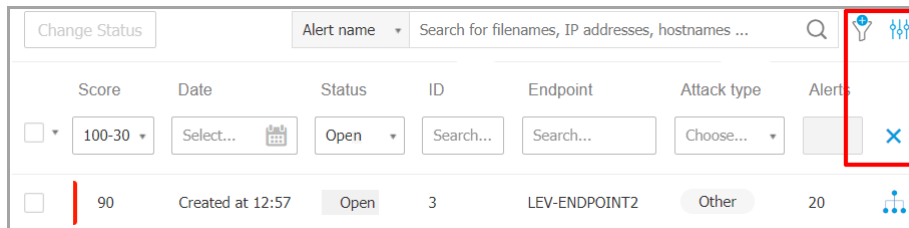
Filters Grid

- 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. It provides context based on the attack indicators, and ATT&CK Techniques, if applicable.
	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.
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:

Filtering Option	Details
	● Click the **From** and **To** tabs to select the dates defining the time interval. ℹ️ **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 (the last 7 up-to 90 days). 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.
Company	Filter the incidents by the name of the company where the security events were triggered. By default, the **Incidents** page displays incidents from all companies under your management. ℹ️ **Note** Only companies under your management with a valid EDR license will appear in the list.
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.

Filtering Option	Details
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.

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.
- **ATT&CK Technique** - 100 maximum 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. For a more granular search, you can create search queries in the Search page.

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 EDR triggers new events.

! **Important**
All security events older than 90 days are automatically deleted from both **Investigate** and **Review** sections, 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).

| 90 | Created at 12:57 | Open | 3 | LEV-ENDPOINT2 | Other | 20 | |

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.

| | 90 | Created at 12:57 | Open | 3 | LEV-ENDPOINT2 | Other | 20 | |

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.
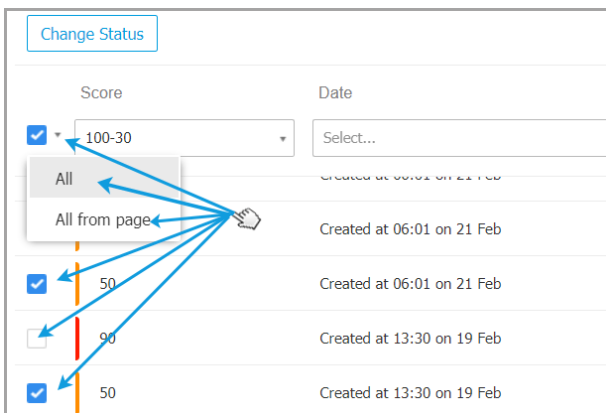
Selecting Security Event Cards

You can select them individually or by using the bulk selection options in the drop-down menu.

> **i** **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:
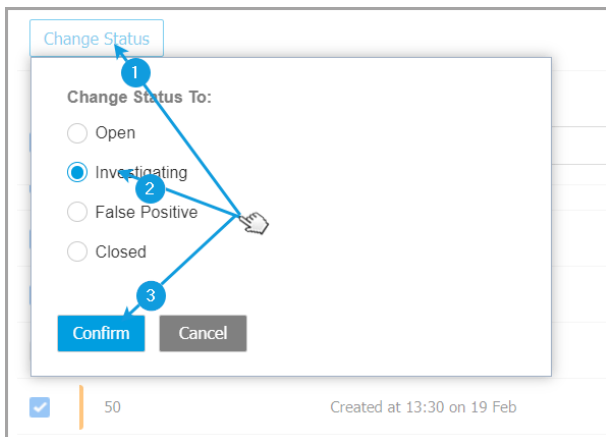
Changing the Status of Security Event

- **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.
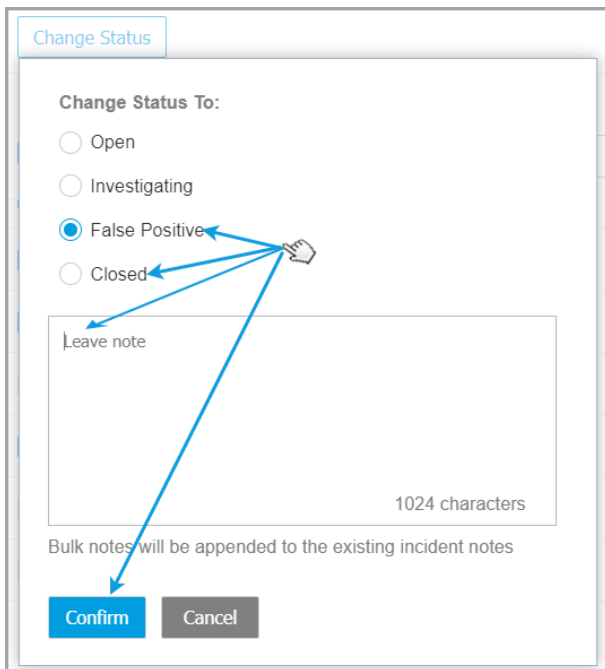
Leaving Note for False Positive and Closed events

> **ⓘ 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. Investigating a Security Event

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.

Security Incident Page

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.
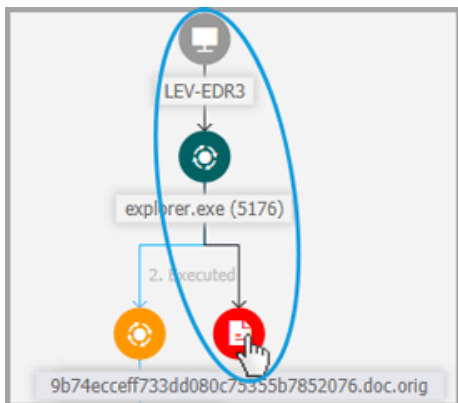
- Three or more same action type event nodes spawning from a parent node are grouped into an expandable cluster-node.
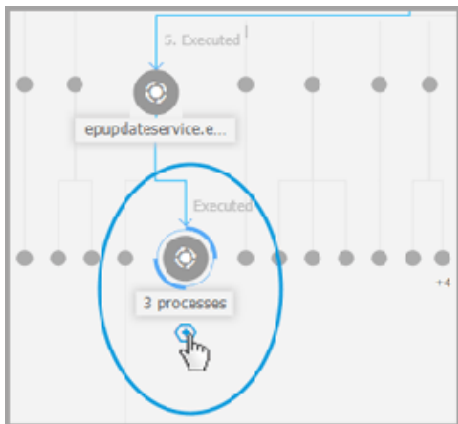
- Only nodes without child elements will be hidden from the incident graph when the cluster-node is collapsed.
- Nodes where suspicious activity has been detected will not be added to the cluster-node.
- Clicking a node will display the following details:

– 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. 291) 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 complex incidents that evolve over time, the graphic displays every single stage of the attack.
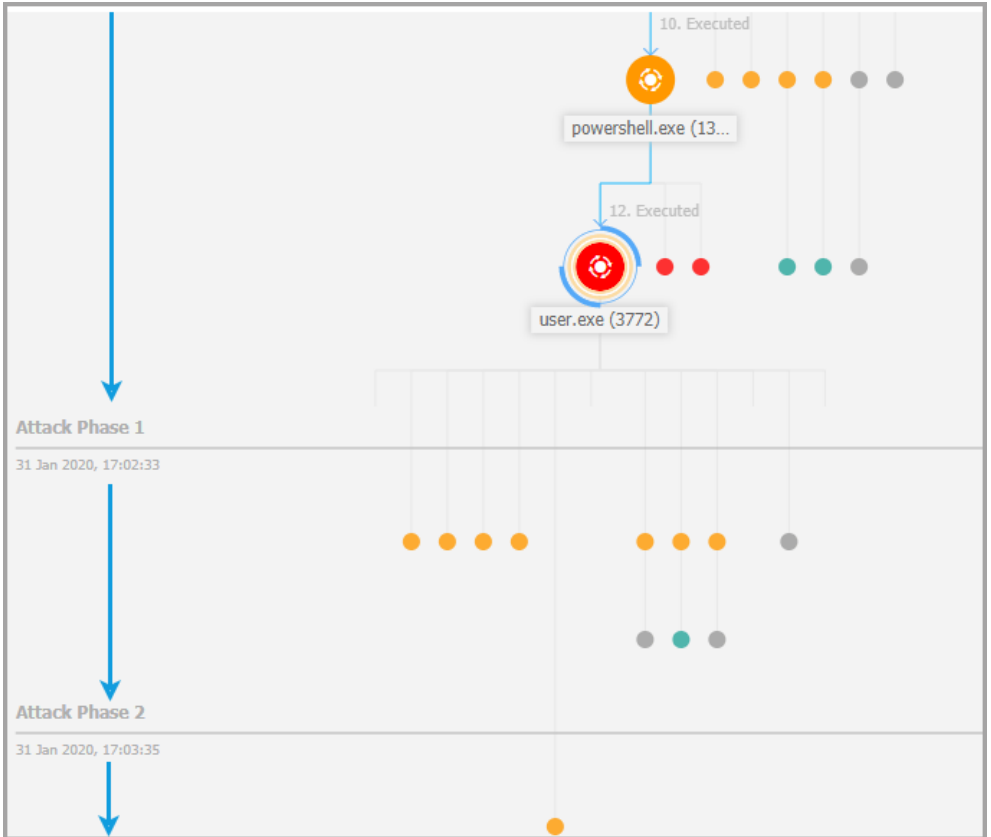
Staged Attack

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.
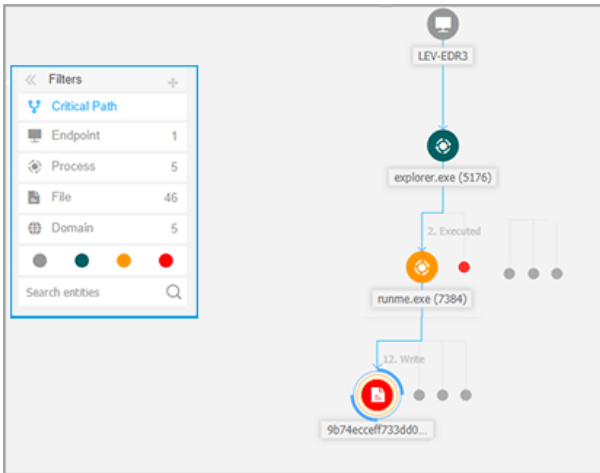
Incident Graph Filters

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.
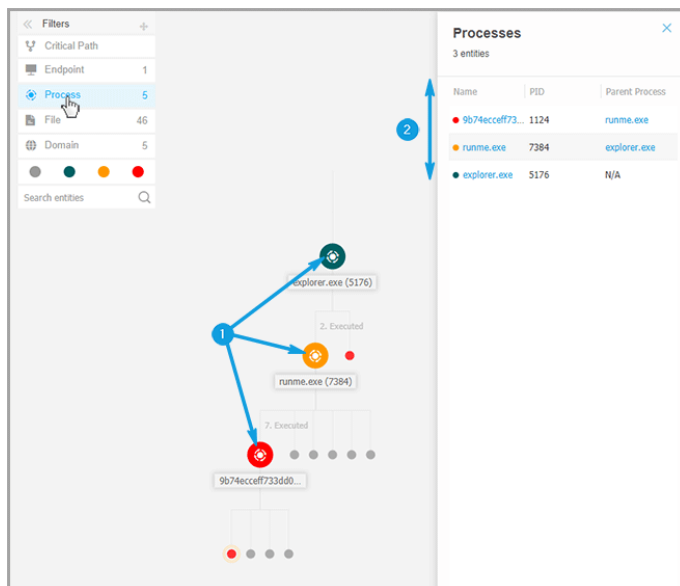
> **i** **Note**
> Selecting an element from the displayed list will highlight it in the incident graphic, and open a details panel with information related to that element.
> Only one filter can be applied at a time.

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.
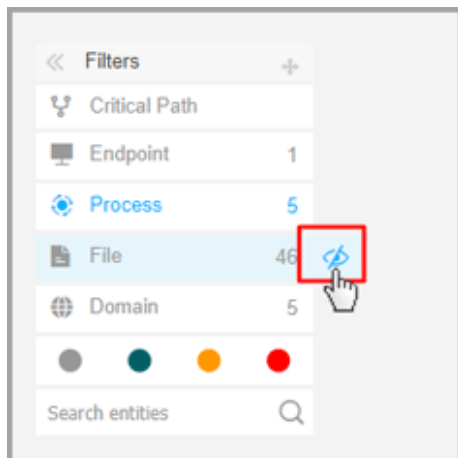
Hiding an element type redraws the incident graph by removing all corresponding elements, even if they are zoomed out, excepting the trigger node and nodes with child elements.

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.
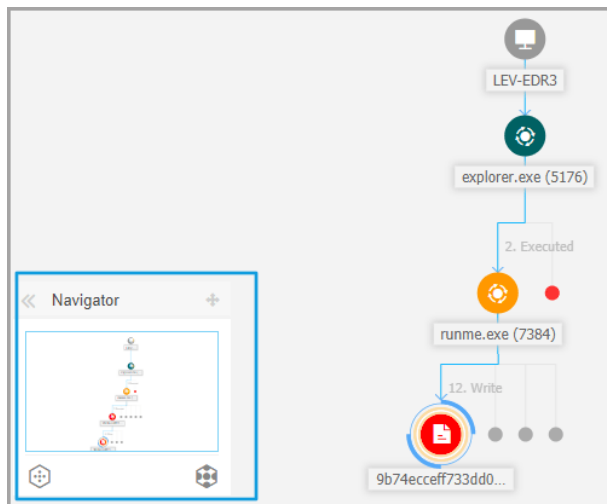
Navigator

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.
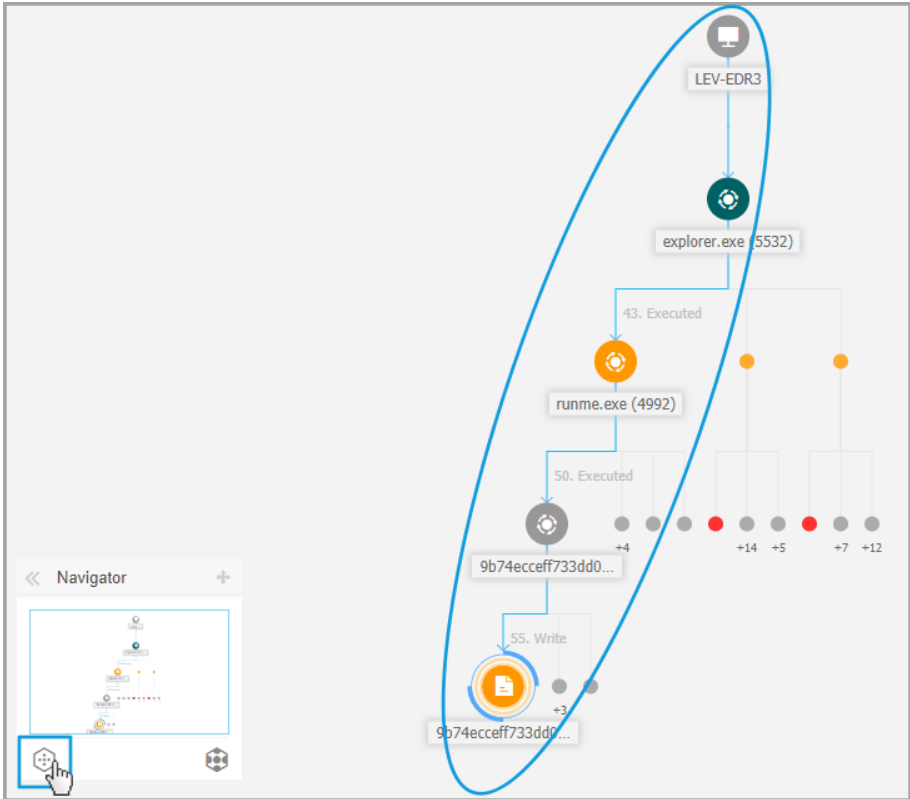
Overview Visualization

When you click the ⊞ **More Details** button, all the incident graph elements are expanded, highlighting every node and node clusters.
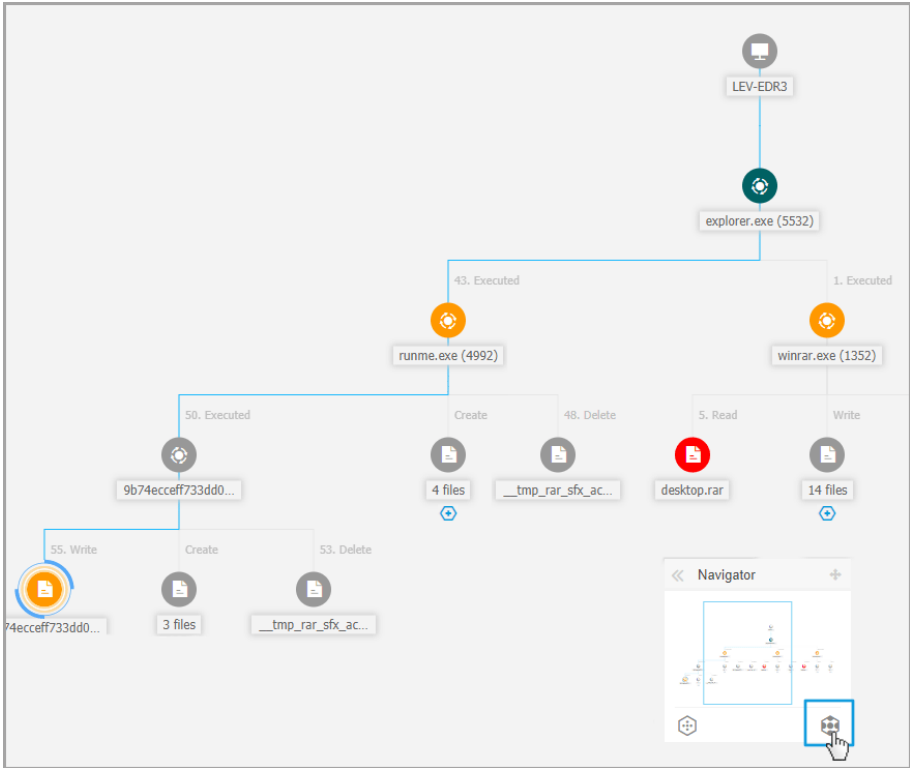
Zoomed-in Visualization

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.
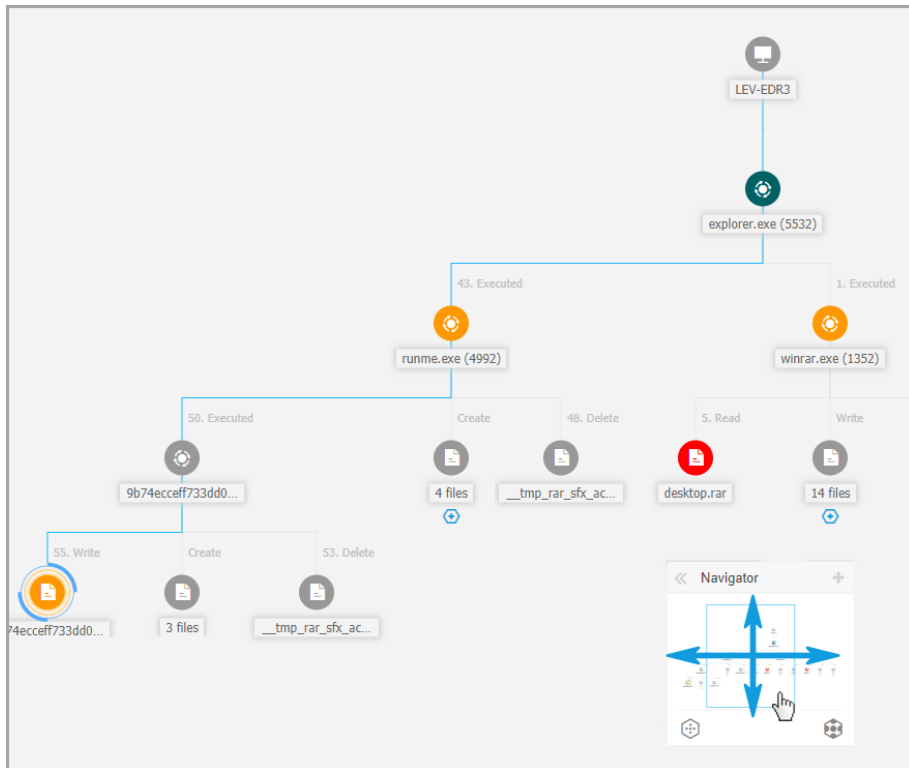
Mini-map Selector

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.
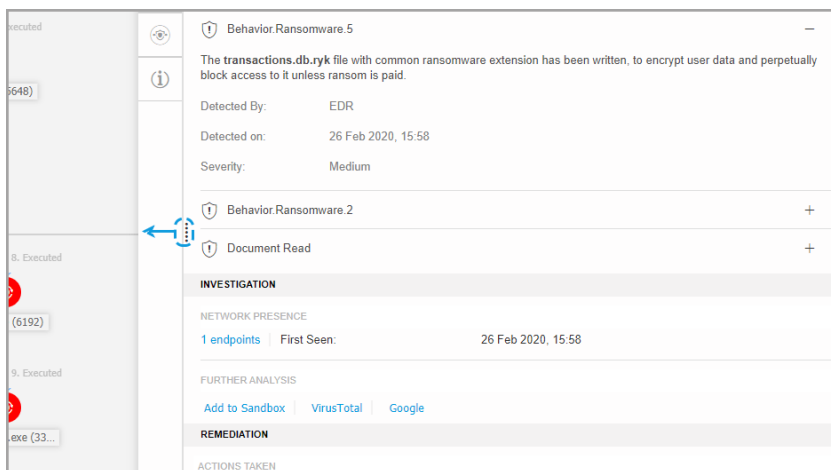
Expanded Panel

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:
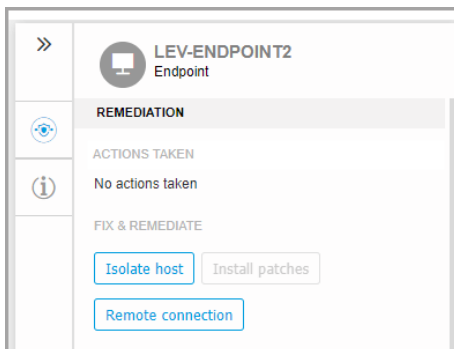
- **Isolate host** - Use this remediation solution to isolate the endpoint from the network.

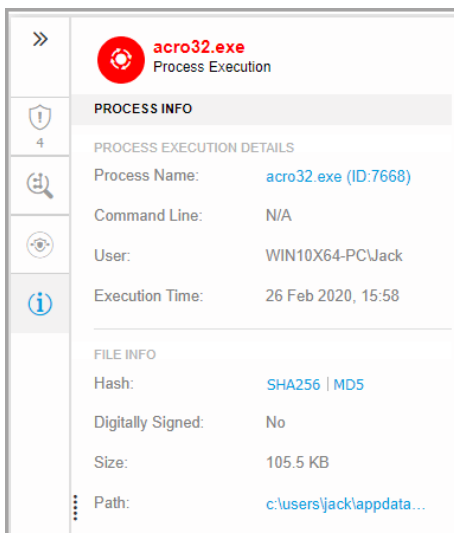- **Install patches** - Use this action to install a missing security patch on the target endpoint. This option is visible only with the Patch Management module, an add-on available with a separate license key. Refer to Patch Install for more information.

- **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**.

It 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:

– **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**.

It 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**

Displays details about the selected file node, including file origin and path, hash value, or digital signature.
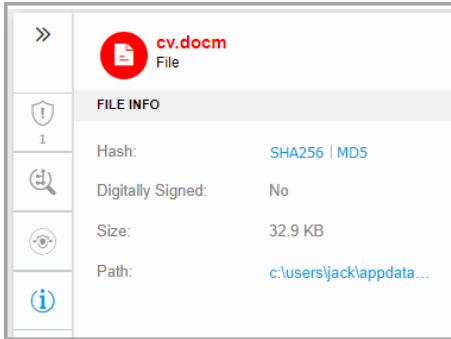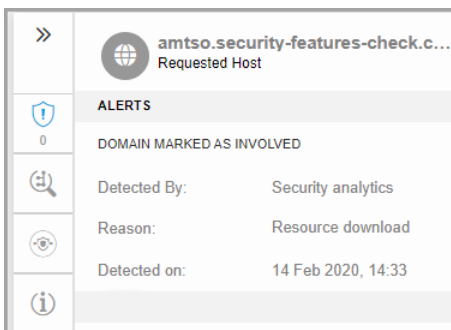
You can copy the hash value to clipboard by clicking the available hashing algorithms within the **Hash** field and then **Copy to Clipboard**, and use it to add a file hash value to **Blocklist**. For more information, refer to **Blocklisting Files**.

Details Panel for 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**

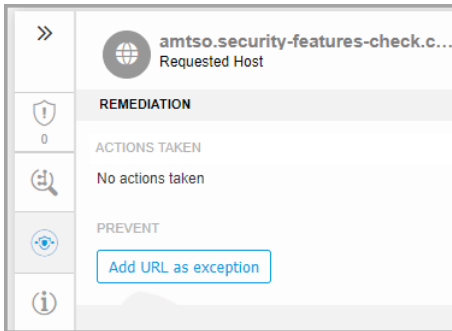Displays date stamps for the initial detection and all the endpoints where this element was spotted.

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.
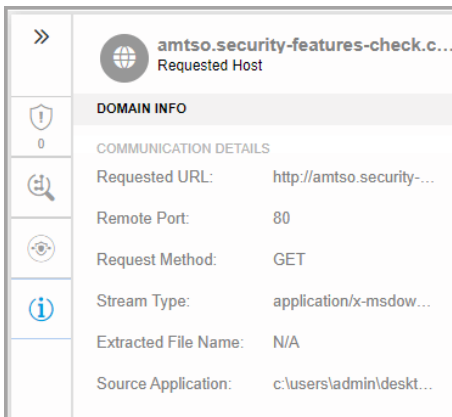
Details Panel for Registry Nodes

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.
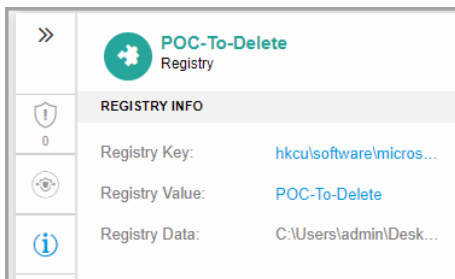
You can click the registry key and value to copy it to clipboard for further analysis purposes.

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 EDR, 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 attack info.

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.

> **i** **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 1024 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 cancelling the threat instantly or collecting data for further investigation.
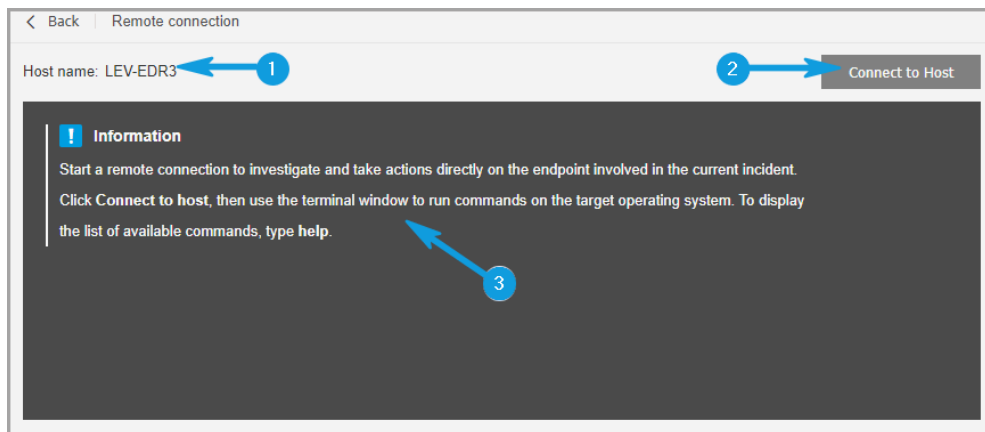
Remote Connection tab

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.

> **i** **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.

9.3. Searching Security Events

The **Search** page allows you to go through past events based on complex criteria.

Search page overview

To view the events you are interested in, you must build queries using the query language available in GravityZone.

The **Search** page provides the following options:

- A search bar for entering queries, displaying the list of query terms by categories when clicked, and an autocomplete assistant.
- Saving favorite searches for later use.
- Filtering options by date and time and by company.
- A **Get Started** section with a link to the query language Syntax Help.
- Predefined queries, designed for useful security event search cases.

9.3.1. The Query Language

The query language provides the vocabulary (fields and operators) and the syntax with which you can build queries. You can find them described herein.

Click the **Syntax Help** link and select the **Query Language** tab to view its contents.

Fields

The query field is the same with the field in GravityZone database. Fields stand for entities such as file paths, file hashes, hostnames, or domain names.

Any field may have one or more values, representing the state of the field at a specific time. Values are of different types of data, depending on the meaning of the field.

Operators

Operators allow you to create relationships between fields to build searching criteria. You can use the following operators:

Operator	Example	Description
:	`fieldCategory.option:` `value1`	Compares the query field value with values of the same field in the database.
" "	`fieldCategory.option:` `"value1 value2"`	Strings enclosed in quotation marks are treated together, as a phrase.
( )	`fieldCategory1.option:` `value1 AND` `(fieldCategory2.option:` `value2 OR`	Groups query terms.

Operator	Example	Description
	`fieldCategory3.option:` `value3)`	

AND	`fieldCategory1.option:`
	`value1 AND`
	`fieldCategory2.option:`
	`value2`
		Retrieves results that match all your query conditions.

OR	`fieldCategory1.option:`
	`value1 OR`
	`fieldCategory2.option:`
	`value2`
		Retrieves results that match any of your query conditions.

AND NOT	`fieldCategory1.option:`
	`value1 AND NOT`
	`fieldCategory2.option:`
	`value2`
		This operator is useful in complex queries and returns results not matching the specified term, apart from all the other conditions.

exists	`_exists_:` `fieldCategory.option`	Returns results that contain the specified field.
-	`fieldCategory.option:` `-value`	Use the minus sign (-) when the value must be excluded from the results.
?	`fieldCategory.option:` `???_file.path`	Use a question mark (?) to match any single character in your field value.
*	`fieldCategory.option:` `file.*`	Use an asterisk (*) to match any field value.

Query Syntax

A query is a logical condition, or a series of conditions bound by operators, which have as results events from the EDR database.

All conditions must relate to fields. Some conditions require you to provide a value, while others not. For example, you don't need a value when you only ask if the field exists in the event details.

Queries may be from simple to complex. Complex queries may have nested queries (query in another query).

A valid field syntax consists of the field category followed by one of options in the **Query Language** section, and its corresponding value: `fieldCategory.option:` `value`.

For example, `file.path: "%system32%\com\svchost.exe"` is a rather simple query that searches all events that include `%system32%\com\svchost.exe`, and it consists in:

- A mandatory field category and related option (separated by a period): `file.path`

- An operator: the colon (:) - to compare the field's value

- The searched value: `%system32%\com\svchost.exe`

- Quotation marks (" "), because the value contains special characters such as <\> and <.>

9.3.2. Running Queries

To run a query:

1. Type the query string in the field.

   Clicking the **Search** field will display the list of search terms grouped by category. Select the term that you want to start creating your query.

   As you type, Control Center assists you with autocomplete suggestions. Use the arrow keys to select a suggested option and then press **Enter** to add it to the query.

   If you need more help, click the **Syntax Help** link.

   > **i** **Note**
   > You can use nested queries to build complex searches.

2. To filter the events within a time frame, click the time field. You have several options to define it:

   - Only specific date.

     Select a date in the **From** tab of the calendar.

- An exact time interval.
    a. Select the start date in the **From** tab of the calendar.
    b. Select the end date in the **To** tab.
- A recent time interval from the available options.
- Click **OK**.

3. Select the company for which you want to view events. Type the name of the company or choose one from the drop-down list.

   You can search only through one company at a time.

4. Click **Search**, or press **Enter**.

   You can view the matching events, together with their details, below your query.

> **Important**
> When you search the `detections.detection_type` query in the *Search* field, Control Center requires you complete it with an integer value ranging from 1 to 15 (i.e `detections.detection_type:1`).
> Each value you put in corresponds to a certain detection type, as follows:
>
> a. `detections.detection_type:1` - Advanced Threat Control detection
> b. `detections.detection_type:2` - Antimalware static engines detection
> c. `detections.detection_type:3` - HyperDetect detection
> d. `detections.detection_type:4` - Advanced Threat Control suspicious event notification
> e. `detections.detection_type:5` - HyperDetect reported attack types detection
> f. `detections.detection_type:6` - Antimalware CMDLine Scanner detection
> g. `detections.detection_type:7` - Cross Technologies Correlation detection
> h. `detections.detection_name:8` - Network Attack Defense detection
> i. `detections.detection_type:9` - HyperDetect unreported attack types detection
> j. `detections.detection_type:10` - Sandbox Analyzer contained dynamic analysis detection

k. `detections.detection_type:11` - Memory Buffer Register Scan detection

l. `detections.detection_type:12` - URL detection

m. `detections.detection_type:13` - Advanced Anti-Exploit detection

n. `detections.detection_type:14` - User Behavior Analysis detection

o. `detections.detection_type:15` - Antimalware Scan Interface detection

Control Center can display up to 10,000 events. If the query results contain more than 10,000 events, a message will appear on the screen. In this case, you need to refine your search.

9.3.3. Favourite Searches

As most queries are long, some are even hard to build or to remember. Instead of saving them into a file and copy-pasting them in GravityZone, you can save them directly in GravityZone, to have them at hand.

To save your query:

1. Enter the string in the **Search** field.

2. Click the ☆ icon at the right-end of the **Search** field.

3. When prompted to name it, type the name you want for your query.

4. Click **Add**.

Click the **Favourite Searches** link under the **Query** field to view your saved queries.

Further on, you have three options:

● Run the query.

● Edit the query name.

● Delete the query.

To run a saved query:

1. Click the **Favourite Searches** link.

2. Select your preferred query.
   The saved string will be added to the **Search** field.

> **i** **Note**
> If needed, edit the query string. Additionally, you can save the new search query to your Favourite Searches.

3. Use the company and calendar filters to refine the search.

4. Click **Search**.

When your list of queries needs adjustments, place the mouse over the saved query to reveal the inline options.

- Click the ⊘ **Edit** icon to rename the query.
- Click the ⊗ **Delete** icon if you no longer need the query.

9.3.4. Predefined queries

The **Search** page provides a few example of complex query searches, specific to security events investigations.

Predefined queries are grouped by security investigation category.

To launch a predefined query:

- Click the ⊕ icon next to the predefined query description.
- The query phrase will appear automatically in the **Search** bar. Fill in the specific details for the query terms.
- Click the **Search** button to run the query.

> **i** **Note**
> You can anytime return to the **Get Started** options from the **Search** page, by clicking the **Get Started** link at the top-right side of the page.

10. MANAGING ENDPOINT RISKS

Endpoint Risk Analytics (ERA) helps you assess and harden your endpoints security configurations against industry best practices, to minimize the attack surface.

> **! Important**
> Endpoint Risk Analytics module is available only for supported Windows desktop and server operating systems.

ERA gathers and analyzes data through risk scan tasks run on selected devices in your network.

To do so you must first make sure the ERA module is activated from the policy applied to the selected devices:

1. Go to the **Policies** page.

2. Click the **Add** button and configure the **General** settings.

3. Scroll to and select the **Risk Management** policy.

4. Select the check box to enable the **Risk Management** features and start configuring policies that define how to run the **Risk Scan** task.

> **i Note**
> For more information about GravityZone indicators of risk, refer to this KB article. For more information about known application vulnerabilities, refer to the CVE Details website.

Follow these steps to run risk scan tasks and assess the results:

1. You can run risk scan tasks on endpoints in two ways:

   a. On demand - by selecting the endpoints from the **Network** page and sending a **Risk Scan** task from the **Tasks** menu.

   b. Scheduled - by configuring from policy a risk scan task that runs automatically on target endpoints at a defined interval.

   After the risk scan has finished successfully, GravityZone calculates a risk score for each endpoint.

2. Access the **Risk Management** dashboard to obtain the following information:

   - The company risk score and score evolution

- Risk scores and statistics broken down into misconfigurations, vulnerable applications, and affected devices

- The description of each indicator of risk and the recommended remediation actions

3. Access the Security Risks page to analyze and mitigate the discovered misconfigurations and application vulnerabilities.

4. Access the Companies View page for an overview of the risk score of all the companies under your management.

10.1. The Risk Management Dashboard

The **Risk Management** page provides an overview of your network security and risk assessment information.
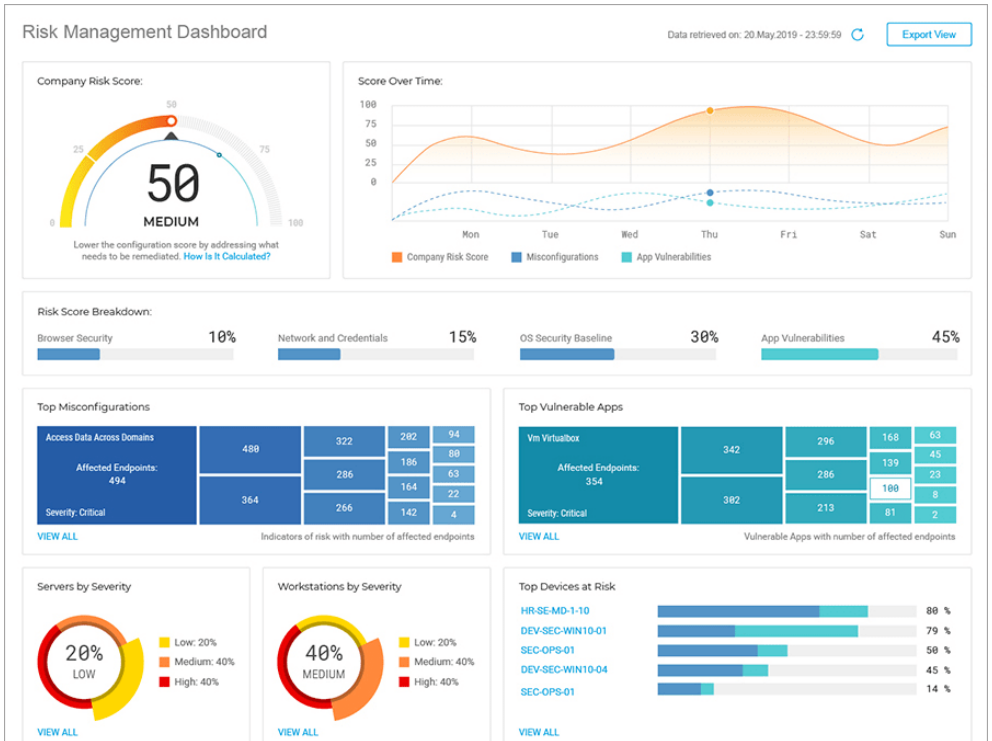
Risk Management Dashboard

1. Company Risk Score
2. Score Over Time
3. Risk Score Breakdown
4. Top Misconfigurations
5. Top Vulnerable Apps
6. Servers by Severity
7. Workstations by Severity
8. Top Devices at Risk

The data displayed on this page is organized in several widgets:

Company Risk Score

The overall risk score displays the level of risk your organization is exposed to by misconfigured system settings and known vulnerabilities of currently installed applications. The score reflects the severity of indicators of risk enabled through policy.

The score represents an average of the two major risk categories **Misconfiguration** and **App Vulnerabilities**.

Company Risk Score Widget

Click the widget and a details panel will open where you can see details of how the overall risk is being calculated and broken down into subcategories.
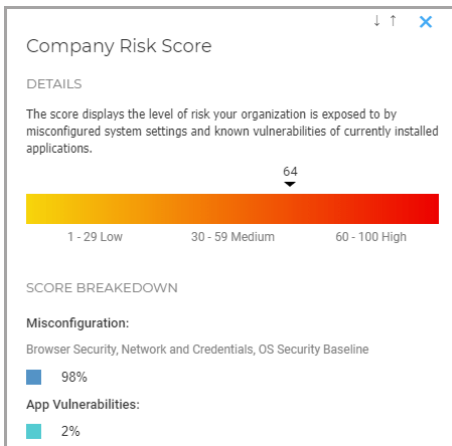
Company Risk Score Details Panel

> **ℹ Note**
> Running an on-demand Risk Scan on a new target device will influence the overall score. The results will be kept for 90 days, or until the next scan.

Score Over Time

This widget is a histogram that displays the weekly evolution of the number of affected devices detected as vulnerable after risk scans. The histogram data represents the number of devices affected by risk indicators from the last seven days, until 12 AM (server time) of the current day.
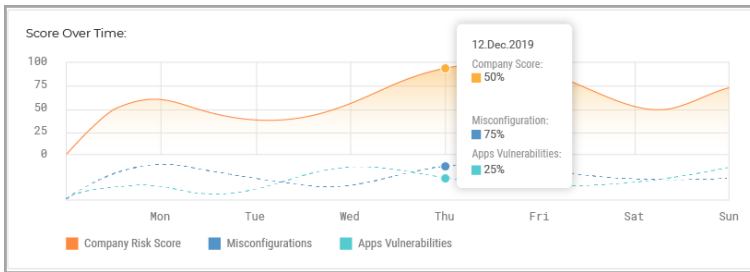
Score Over Time Widget

Risk Score Breakdown

This widget displays the impact of each risk category in the overall company score. The indicators of risk are grouped in the following categories:

- Misconfiguration
    - Browser Security
    - Network and Credentials
    - OS Security Baseline
- Application Vulnerabilities
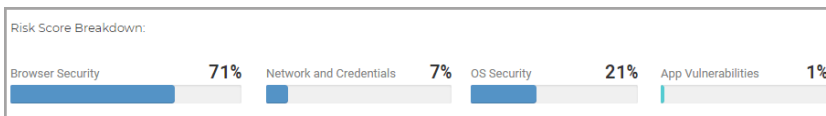
Risk Score Breakdown Widget

Top Misconfigurations

This widget displays the top 15 results for indicators that triggered a risk alert after scanning the devices, ordered by the number of affected devices. Each card represents one indicator that has triggered a risk alert for at least one device.
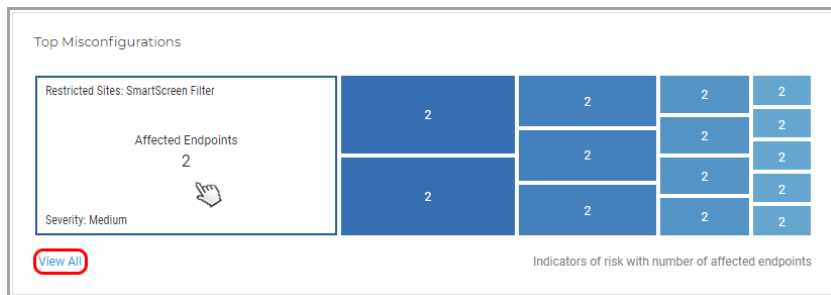
Top Misconfigurations Widget

Each card displays the following elements:

- The indicator's name.
- The number of devices detected as vulnerable for this indicator.
- The severity for the current indicator of risk.

If you click the **View All** button you will view the entire list of discovered misconfigurations in the Misconfigurations tab of the **Security Risks** page.

> **Note**
> You can find the indicators severity types also in the policy, under the **Risk Management** section. For more details, refer to this KB article.

Top Vulnerable Apps

This widget displays the top 15 results for known application vulnerabilities that triggered a risk alert after scanning the devices, ordered by the number of affected devices. Each card represents one vulnerable application that raised a risk alert for at least one device.
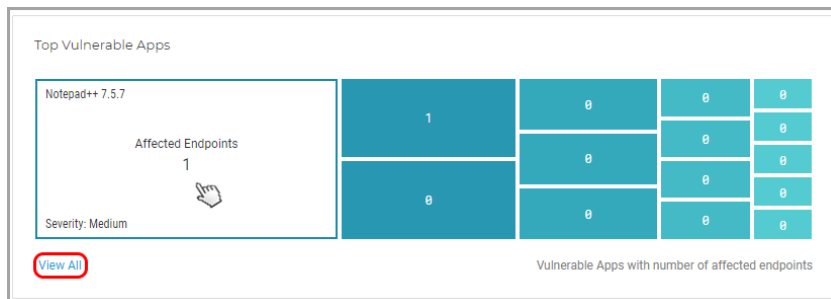
Top Vulnerable Apps Widget

Each card displays the following elements:

● The application's name.

● The number of devices made vulnerable by this application.

● The severity for the vulnerable application.

If you click the **View All** button you will view the entire list of discovered application vulnerabilities in the App Vulnerabilities tab of the **Security Risks** page.

> **Note**
> You can find details about known application vulnerabilities on the CVE Details website.

Servers by Severity

This widget shows the severity of the risks threatening the servers in your environment. The impact of the discovered misconfigurations and application vulnerabilities is displayed as a percentage.
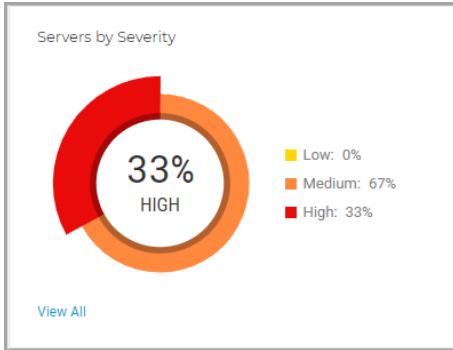
Servers by Severity Widget

Workstations by Severity

This widget shows the severity of the risks threatening the workstations in your environment. The impact of the discovered misconfigurations and application vulnerabilities is displayed as a percentage.
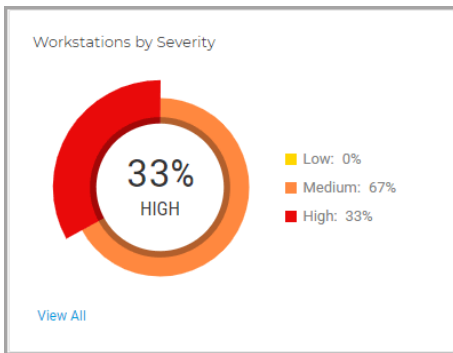
Workstations by Severity Widget

Top Devices at Risk

This widget displays the most vulnerable servers and workstations in your environment, according to the overall score calculated after scanning for misconfigurations and vulnerabilities.
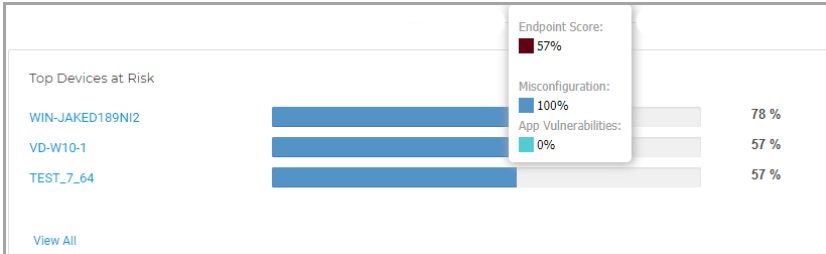
Top Devices at Risk Widget

10.2. Security Risks

This page displays all the risks and affected devices discovered in your environment after running a **Risk Scan** task.

The Security Risks page

The indicators of risk are displayed in a fully customizable grid formation with complex filtering options:

1. Select the company under your management to analyze and mitigate the risks impacting it.

2. Select which category to investigate:

   ● Misconfigurations

   ● App Vulnerabilities

   ● Devices

3. Use these action buttons to customize your grid:

   ● Click the ⁙ **Show/Hide Columns** button to add or remove filter columns.

     The page will update automatically, loading the indicator of risk cards with information matching the added columns.

     You can always reset the filter columns from the **Reset** button inside the **Show/Hide Columns** drop-down menu.

   ● Click the 🔽 **Show/Hide Filters** button to show or hide the filters bar.

   ● Click the ⟳ **Refresh** button to refresh the list.

Each indicator entry is listed in a rich card format, providing an overview of each indicator of risk, with information based on the selected filters.

Misconfigurations

The **Misconfigurations** tab displays by default all the GravityZone indicators of risk. It provides detailed info of their severity, number of affected devices, the misconfiguration type, mitigation type (manual or automatic), and status (active or ignored).
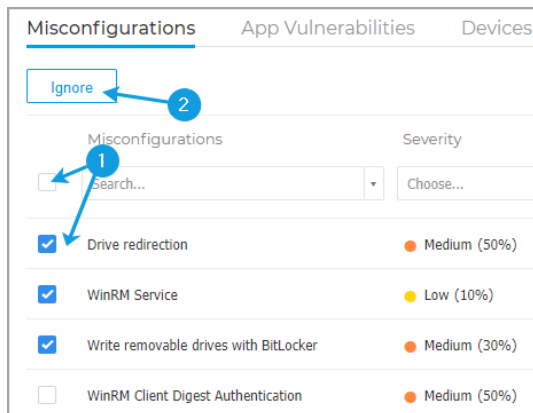
Misconfigurations tab

To change the status of misconfigurations:

1. Select the master check box or individual boxes of indicators of risk to select them for status change.

2. Click the **Ignore/Restore** button to change the status from **Active** to **Ignored**, or vice-versa.

> ℹ️ **Note**
> The **Ignore** action applies to all the selected devices, and influences the overall company risk score upon performing a new risk scan. We strongly recommend you to assess how disregarded indicators of risk may impact your organization's security.

You can customize the information displayed in cards and filter misconfigurations by using these options:

Filtering Option	Details
Misconfiguration	This column includes a searchable drop-down menu that allows you to filter the list of indicators by name.
Severity	This column allows you to filter the list of indicators by the level of severity of each indicator of risk. You may select between Low, Medium, and High.

Filtering Option	Details
Affected Devices	This column shows the number of servers and workstations that may be exposed to threats by a specific indicator of risk.
Type	This column allows you to filter the list of indicators of risk by their type: ● Browser Security ● Network and Credentials ● OS Security
Mitigation Type	This column allows you to filter the list of indicators of risk that can be mitigated manually or automatically.
Status	This column allows you to filter the list of indicators of risk by their status, Active or Ignored.

Click the misconfiguration you want to analyze to expand its specific side panel.
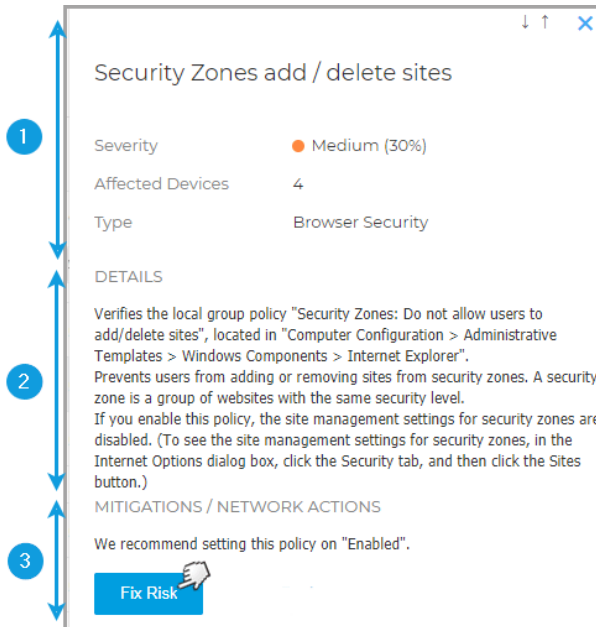
Details Panel for Misconfigurations

Each panel contains:

1. An info section with the name of the risk indicator, its level of severity, number of affected devices, and type.

2. A **Details** section that thoroughly describes the setting, and configuration guidelines.

3. A **Mitigations** section that includes recommendations that minimize the risk on the affected devices, as well as available actions:

   a. Click **Fix Risk** button to properly configure this setting.

      A new window pops up where you need to confirm the action, or cancel it.

   b. A new task is created to apply the recommended setting on all affected devices.

      ### Note
      You may check the progress of the task in the **Network** > **Tasks** page.

If the indicator of risk can be mitigated only manually, you need to access the affected devices yourself and apply the recommended configuration.

App Vulnerabilities

The **App Vulnerabilities** tab displays all the vulnerable applications discovered on devices in your environment during scanning. It provides detailed info of their level of severity, number of known CVEs per application, and number of affected devices.

You can customize the information displayed in cards and filter vulnerable applications by using these options:

Filtering Option	Details
Applications	This column includes a searchable drop-down menu that allows you to filter the list of vulnerable applications by name.
Severity	This column allows you to filter the list of vulnerable applications by the level of severity of each app. You may select between Low, Medium, and High.
CVE	This column shows the number of Common Vulnerabilities and Exposures (CVEs) for applications currently installed in your environment.
Affected Devices	This column shows the number of servers and workstations that may be exposed to threats by a specific indicator of risk.

Click the vulnerable app you want to analyze to expand its specific side panel.
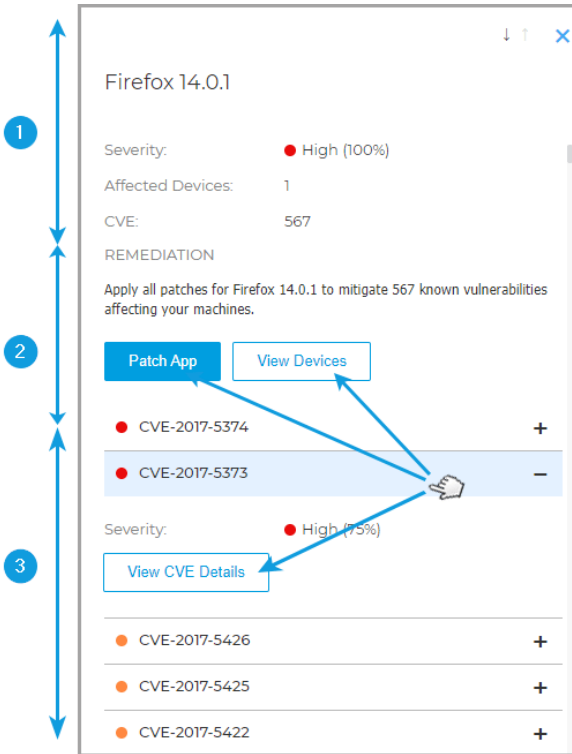
Details Panel for Vulnerable Applications

Each panel contains:

1. An info section with the name of the application, level of severity, how many devices it affects, and how many exploits were allowed to corrupt your environment.

2. A **Remediation** section with mitigation actions and list of discovered CVEs:

   a. Click **Patch App** button to apply available patches for the vulnerable application.

      ⚠ **Important**
      The **Patch App** functionality works only for scanned devices that have the Patch Management module installed.

A new window pops up where you need to confirm the action, or cancel it.

b. A new task will be created to apply the patches to vulnerable applications on all affected devices.

Note
You may check the progress of the task in the **Network** > **Tasks** page.

3. Expand listed CVEs and click the **View CVE Details** button to access the database with specific info.

Devices

The **Devices** tab displays all the scanned servers and workstations under your management. It provides detailed info of their name, level of severity, device type, and number of risks affecting them.

You can customize the information displayed in cards and filter devices by using these options:

Filtering Option	Details
Device	This column includes a searchable drop-down menu that allows you to filter the list of affected servers and workstations by name.
Severity	This column allows you to filter the list of vulnerable applications by the level of severity of each app. You may select between Low, Medium, and High.
Misconfigurations	This column shows the number of misconfigurations discovered per device.
CVEs	This column shows the number of Common Vulnerabilities and Exposures (CVE) discovered per device.
Device Type	This column allows you to filter the list of devices by their type. You may select between Server, and Workstation.

Click the device you want to investigate to expand its specific side panel.

Details Panel for Devices

Each panel contains:

1. An info section with the name of the device, level of severity, and number of misconfigurations and common vulnerabilities and exposures affecting it.

2. A risks section displaying in detail each misconfiguration and vulnerable application discovered on the device, grouped in two tabs.

   - The **Misconfigurations** tab includes all the misconfigurations discovered on the device, grouped into indicators of risk that can be fixed automatically, and indicators of risk that may be resolved only manually.

- The **App Vulnerabilities** tab includes all the vulnerable applications discovered on the device, and number of CVEs impacting each application.

10.3. Companies View

The **Companies View** page provides an overview of the overall risk for all the companies under your management.

Companies with the highest exposure to threats make the top of the list hierarchy, so you can access them easily and take fast actions to harden their security.
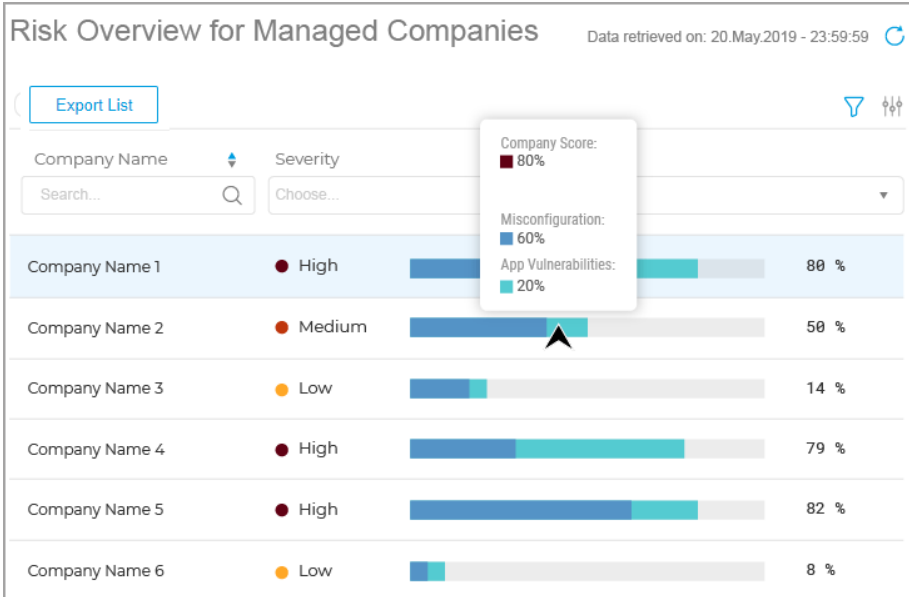
The Companies View page

Customize the list of managed companies by using these options:

Filtering Option	Details
Company Name	This column includes a searchable drop-down menu that allows you to filter the list of companies by name.
Severity	This column allows you to filter the list of companies by the level of severity of the risk impacting them. You may select between Low, Medium, and High.

After customizing the list with companies it's easy to access each one, analyze the risks that make them vulnerable to potential threats and take actions:

1. Click a company in the list and it will take you to the dashboard area populated with specific data.

2. When you select a company from the list to take you to its dashboard area it also populates the Security Risks page, where you can investigate the misconfigurations, vulnerable applications, and affected devices within the company.

3. You can also export the list of companies under your management in `.csv` format.

> **Note**
> The **Companies View** page will be empty if no **Risk Scan** task is deployed beforehand for the companies under your management.

11. MONITORING DASHBOARD

The Control Center dashboard is a customizable visual display providing a quick security overview of all protected endpoints and network status.

It is composed of two sections:

- Dashboard network status bar
- Dashboard portlets

The Dashboard network status bar updates you with the number of opened or in-progress incidents, threatened assets (endpoints) and detected threats in your network. Use this information to glance over unresolved network items. Click **View** to access the **Incidents** page. For more information, refer to "Investigating Incidents" (p. 267).

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.
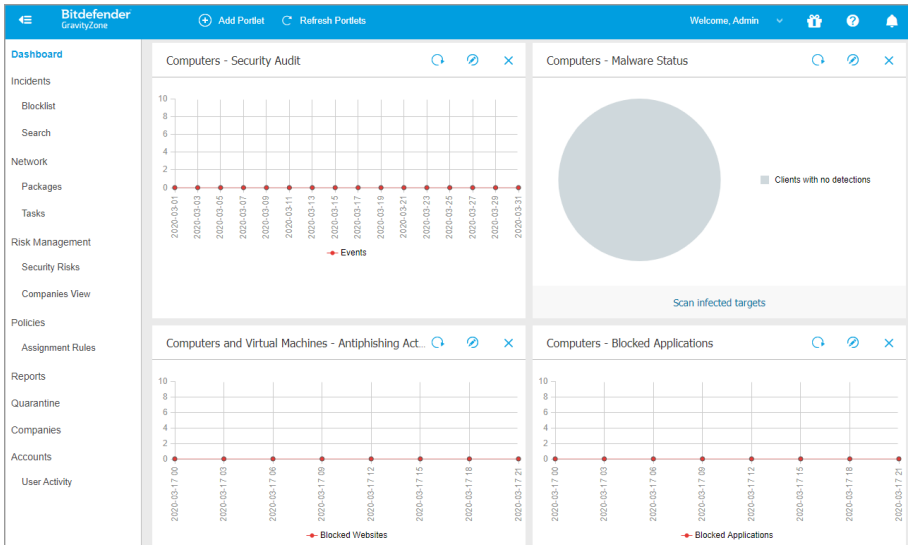
The Dashboard

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.

> **ℹ 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.
- Specific portlets are available for users in Partner companies (**License Status**, **Customer Status Overview** and **Top 10 Infected Companies**).
- 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.

11.1. 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.

11.2. 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.

11.3. 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:
   - 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. 350).
4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

11.4. 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.

11.5. 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.

12. USING REPORTS

Control Center allows you to create and view centralized reports on the security status of the managed network objects. The reports can be used for multiple purposes, such as:

* Monitoring and ensuring compliance with the organization's security policies.
* Checking and assessing the network security status.
* Identifying network security issues, threats and vulnerabilities.
* Monitoring security incidents.
* 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).

12.1. Report Types

Different report types are available for each endpoint type:

* Computer and Virtual Machine Reports
* Exchange Reports

12.1.1. 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, Advanced Anti-Exploit and ATC/IDS. 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 and Firewall. A confirmation window will show up, informing you of the new rule that will modify the existing policy for that specific endpoint.

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.

Customer Status Overview

Helps you find out protection issues within your customer companies. A company has issues whether malware is detected, the antimalware is outdated or the license has expired. The company name is a link to a new window, where you can find company details.

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.

- Company name.

Endpoint Modules Status

Provides an overview of the protection modules coverage over the selected targets. In the report details, for each target endpoint you can view which modules are active, disabled or not installed, and also the scanning engine in use. Clicking the endpoint name will show up the **Information** window with details about the endpoint and installed protection layers.

Endpoint Protection Status

Provides you with various status information concerning selected endpoints from your network.

- Antimalware protection status

- Bitdefender Endpoint Security Tools update status

- Network activity status (online/offline)

- Management status

You can apply filters by security aspect and status to find the information you are looking for.

Firewall Activity

Informs you about the activity of the Firewall module of Bitdefender Endpoint Security Tools. You can see the number of blocked traffic attempts and blocked port scans on the selected endpoints, as well as the user that was logged in at the time of the last detection.

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.

> **i** **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.

> **i** **Note**
> You can find these exceptions in the following sections of the selected policies: **Antimalware > Settings** for files, and **Content Control > Traffic** for URLs.

License Status

Informs you of the Bitdefender protection coverage in your network. You are provided with details regarding the licenses type, usage and lifetime for the selected companies.

By clicking the number in the **Usage** column, which corresponds to a company with monthly license, you can also view usage details, such as the total number of license seats and the number of the remaining seats available for installation.

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.

Monthly License Usage

Provides detailed information about the license usage in each month, over a specified time period and for the selected companies that use monthly subscription. To view the hierarchy of a child company, click the plus sign in front of the company name. If needed, you can easily adjust license details by clicking the company name.

The report includes information regarding:
- Company types
- License keys
- Licensed endpoints
- Endpoint usage
- Encryption usage
- Patch Management usage
- Security for Virtualized Environments usage (virtual servers and virtual desktops)
- Advanced Threat Security usage (HyperDetect and Sandbox Analyzer)
- EDR usage
- Reserved seats.

Click the numbers in each column to view details regarding each module and add-on available. You can easily customize the report by clicking the **Show/Hide Columns** button.

Email Security - Monthly License Usage

This report provides license usage for the Email Security service. All report intervals retrieve license usage information until the end of the previous day. For example, you generate a report on Monday, at 12 pm and set the interval to **This month**. The report will provide license usage information until the end of Sunday.

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.
- The name of the company containing the target machine.

Network Protection Status

Provides detailed information on the overall security status of the target endpoints. For example, you can view information about:

- Available protection layers
- Managed and unmanaged endpoints
- License type and status (additional license related columns are hidden by default)
- Infection status
- 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. 421).

- 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
- 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.

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.

> **i** **Note**
> The details table displays all endpoints which were infected by the top 10 detected malware.

Top 10 Infected Companies

Shows you the top 10 most infected companies, based on your selection, by the number of total detections over a specific time period.

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.

> **i** **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. This operation is possible only if all targets are from the same company.

> **i** **Note**
> This report is available only when a GravityZone solution upgrade has been made.

12.1.2. 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.

- The company that owns the mail server.

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.

- The company that owns the mail server.

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.

- The company that owns the mail server.

Exchange - Monthly License Usage

Provides detailed information regarding the Security for Exchange license usage for your managed companies over a specific time period.

The table below the graphic provides details regarding the company name, license keys, month and number of protected mailboxes belonging to each of your managed companies.

The license usage number for a company links to a new window, where you can find detailed usage information, such as domains licensed on that company and the belonging mailboxes.

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.

12.2. 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. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.

Report Options

3. Select the desired report type from the menu. For more information, refer to "Report Types" (p. 350)

4. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.

5. 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).

6. 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.

7. 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.

8. **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.

9. **Select Target**. Scroll down to configure the report target. Select one or several groups of endpoints you want to include in the report.

10. 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.

12.3. Viewing and Managing Scheduled Reports

To view and manage scheduled reports, go to the **Reports** page.

The Reports page

All scheduled reports are displayed in a table together with useful information about them:

- Report name and type
- Report reccurence
- Last generated instance.

> **Note**
> Scheduled reports are available only for the user who has created them.

To sort reports by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

To easily find what you are looking for, use the search boxes or the filtering options below the column headers.

To clear a search box, place the cursor over it and click the × **Delete** icon.

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

12.3.1. 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. 371)

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.

12.3.2. 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.

12.3.3. 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.

12.4. 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:

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.

12.5. 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

12.5.1. 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.

12.5.2. 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.

12.6. 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**.

   > **i** **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.

12.7. Printing Reports

Control Center does not currently support print button functionality. To print a report, you must first save it to your computer.
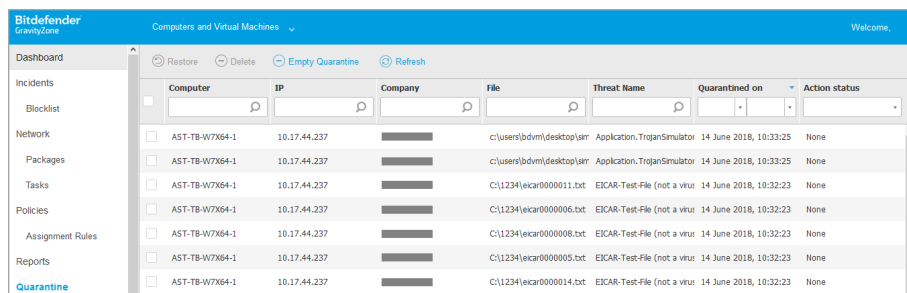
13. QUARANTINE

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.

13.1. 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.

13.2. 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 .

13.2.1. Viewing the Quarantine Details

The Quarantine table provides you with the following information:

- The name of endpoint the threat was detected on.
- The company where the endpoint is located.
- 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.

13.2.2. 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.

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.

> **i** **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. Select the check boxes corresponding to the quarantined files you want to restore.
3. Click the ⟳ **Restore** button at the upper side of the table.
4. 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.
5. 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.
6. Click **Save** to request the file restore action. You can notice the pending status in the **Action** column.
7. 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.

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 the check boxes corresponding to the quarantined files you want to delete.
3. 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. Click the **Empty Quarantine** button.

    In the confirmation window, select the option **Include sub-companies quarantine** to also delete the quarantined objects for your child companies, and click **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.

13.3. 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.

13.3.1. 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.

*   **Company.** The company in whose environment the email or attachment was detected and quarantined.

*   **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.

> **i 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.

13.3.2. 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 ⑧ **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. 179).

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 15 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.

   In the confirmation window, select the option **Include sub-companies quarantine** to also delete the quarantined objects for your child companies, and click **Yes**.

All the entries from the Quarantine table are cleared. The requested action is sent to the target network objects immediately.

14. 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 and MITRE's ATT&CK techniques.

2. The **submission cards area** displays all submissions in a compact format with detailed information about each one.

> **i** **Note**
> As MSP, you can view only your company's submissions to Sandbox Analyzer. The Customer companies' submissions are available in the **Sandbox Analyzer Results (Deprecated)** report.

In the Sandbox Analyzer page, you can do the following:

- Filter submission cards
- View the list of submissions and the analysis details
- Delete submission cards
- Make manual submissions

14.1. 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. 421).

- **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.
- **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.
- **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.

14.2. 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.

14.3. 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.

14.4. 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. 16).

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 submit only one URL per session.

2. Under **Detonation settings**, configure the analysis parameters for the current session:

   • **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.

15. 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, renaming, assigning and deleting policies

To examine the user activity records, go to the **Accounts > User Activity** page.

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.

16. USING TOOLS

17. NOTIFICATIONS

Depending on the events that might occur throughout your network, Control Center will show various notifications to inform you of the security status of your environment. The notifications will be displayed in the **Notification Area**, located in the right side of the Control Center.
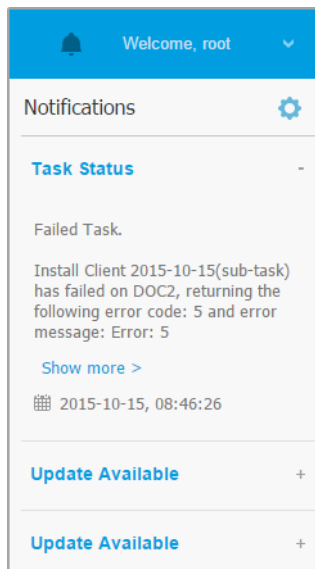
Notification Area

When new events are detected in the network, the [11] icon in the upper right corner of Control Center will display the number of newly detected events. Clicking the icon displays the Notification Area containing the list of detected events.

17.1. 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.

Thus, for partner companies, the notification is generated when the same malware is cumulatively detected on endpoints from their own network and the child companies' networks.

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. 401).

Threats detected by HyperDetect are out of the scope of this notification.

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.

License Usage Limit Has Been Reached
This notification is sent when all of the available licenses have been used.

You must have **Manage Company** right to view this notification.
The notification informs you which of your managed companies has used all available licenses.

License Limit Is About To Be Reached
This notification is sent when 90% of the available licenses have been used.

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.

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.

Exchange License Usage Limit Has Been Reached
This notification is triggered each time the number of protected mailboxes from your Exchange servers reaches the limit specified on your license key.

Invalid Exchange user credentials
This notification is sent when an on-demand scan task could not start on the target Exchange server due to invalid Exchange user credentials.

Upgrade Status

This notification is triggered weekly, if old product versions are found in your network.

Advanced Anti-Exploit

This notification informs you when Advanced Anti-Exploit has detected exploit attempts in your network.

Antiphishing event

This notification informs you each time the endpoint agent blocks a known phishing web page from being accessed. This notification also provides details such as the endpoint that attempted to access the unsafe website (name and IP), installed agent or blocked URL.

Firewall event

With this notification you are informed each time the firewall module of an installed agent has blocked a port scan or an application from accessing the network, according to applied policy.

ATC/IDS event

This notification is sent each time a potentially dangerous application is detected and blocked on an endpoint in your network. You will also find details about the dangerous application type, name and path.

User Control event

This notification is triggered each time a user activity such as web browsing or software application is blocked by the endpoint client according to applied policy.

Data Protection event

This notification is sent each time data traffic is blocked on an endpoint according to data protection rules.

Product Modules event

This notification is sent each time a security module of an installed agent gets enabled or disabled.

Security Server Status event

This type of notification provides information about the status changes of a certain Security Server installed in your network. The Security Server status changes refer to the following events: powered off / powered on, product update, security content update and reboot required.

Overloaded Security Server event

This notification is sent when the scan load on a Security Server in your network exceeds the defined threshold.

Product Registration event

This notification informs you when the registration status of an agent installed in your network has changed.

Authentication Audit

This notification informs you when another GravityZone account from your company, except your own, was used to log in to Control Center from an unrecognized device. If you select the **Receive notification for child companies** check box, notifications will be sent also for GravityZone accounts belonging to your managed companies.

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.

Task Status

This notification informs you either each time a task status changes, or only when a task finishes, according to your preferences.

Outdated Update Server

This notification is sent when an update server in your network has outdated security content.

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.

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 company name, 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.

> **i** **Note**
> You will not receive notifications for clean analyzed samples. Information on samples submitted by your company is available in the **Sandbox Analyzer Results (Deprecated)** report. Information on samples submitted by your company is also available in the **Sandbox Analyzer** section, in the main menu of Control Center. You will not receive notifications for clean analyzed samples. Information on samples submitted by your company and, if configured, by your child companies is available in the **Sandbox Analyzer Results (Deprecated)** report. Information on samples submitted by your company is also available in the **Sandbox Analyzer** section, in the main menu of Control Center.

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

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. 365).

5. Click **Generate**.

> **i** **Note**
> To avoid spamming, you will receive maximum one notification per hour.

Active Directory Integration Issue
This notification informs you of issues that affect the synchronization with Active Directory.

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. The notification is sent to all your user accounts.

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.
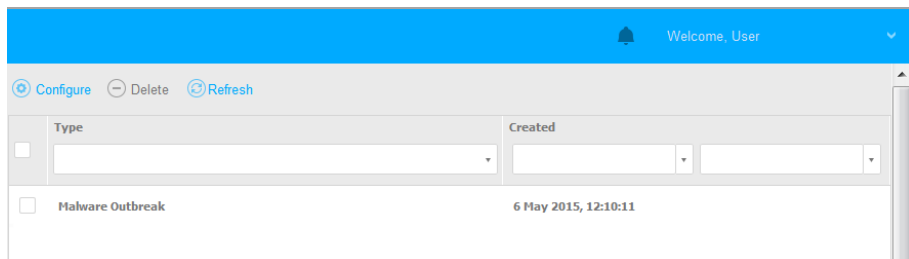
New Incident
This notification informs you when EDR creates an Incident. View the incident by clicking the **Incident Name**.

17.2. 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.

17.3. 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. 401).

17.4. Configuring Notification Settings

The type of notifications to be sent and the email addresses they are sent to can be configured for each user.
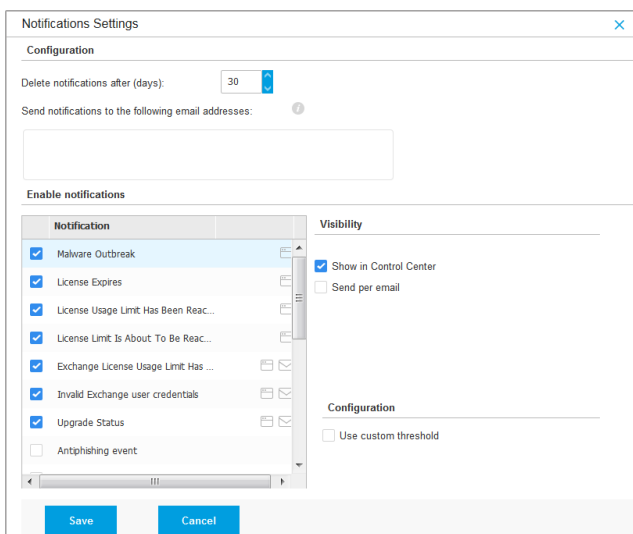
To configure the notification settings:

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

> ℹ️ **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 1 and 365 in the **Delete notifications after (days)** field.

- 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. 394). 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 ▲11 **Notifications** button.
- **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.

- **Receive notifications for child companies** - available for all events, referring by default to your network. Enable this option if you want to be notified when an event occurs on one of your managed companies.

- 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.

– **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**.

18. INTEGRATIONS

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

You can configure your third-party solutions integration in the **Integrations** page, which you can access by pointing to your username in the upper-right corner of the console and choosing **Integrations**.
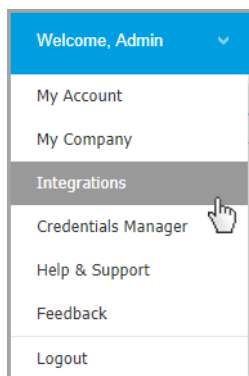
From this page, you can add, edit or remove the integrations according to your needs.

18.1. Integrating with ConnectWise Automate

With this integration, you have access to GravityZone features such as deployment, quarantine management, alerts, and notifications within the Automate Control Center. For more information, refer to the ConnectWise Automate Integration Guide.

18.2. Integrating with ConnectWise Manage

Control Center provides a specific integration functionality for partners with ConnectWise accounts, allowing to efficiently monitor Bitdefender security services delivered to customer companies via ConnectWise platform, based on automated ticketing and billing procedures.

For a complete guidance on how to integrate GravityZone Control Center with ConnectWise Manage, refer to the ConnectWise Manage Integration Guide.

18.3. Integrating with Amazon EC2

As Managed Service Provider (MSP) with Partner account in GravityZone Control Center, you have the possibility to integrate Control Center with Amazon EC2 and centrally deploy, manage and monitor Bitdefender security on their instance inventory. Proprietary scanning servers are hosted by Bitdefender in the AWS Cloud to ensure an optimal footprint on the protected instances and to eliminate the scanning overhead occurring with traditional security software.

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

18.4. Integrating with Splunk

Partners with Splunk accounts are able send data from GravityZone to Splunk via HTTP Event Collector. This integration uses GravityZone APIs and, for configuration, it requires simultaneous access to Control Center and to Splunk platform.

For a complete guidance on how to integrate GravityZone with Splunk, refer to this KB article.

18.5. Integrating with Kaseya VSA

Through this integration you can manage GravityZone security within Kaseya VSA. For more information, refer to the Bitdefender Kaseya VSA Integration Guide.

18.6. Integrating with Datto RMM

Through this integration, you can deploy the Bitdefender security agent to individual or multiple targets. For more information, refer to the Bitdefender Kaseya VSA Integration Guide.

19. 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.

19.1. 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.

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.

19.2. Asking for Assistance

You can ask for assistance through our online Support Center. Fill in the contact form and submit it.

19.3. 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.

19.3.1. 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.

19.3.2. 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

19.3.3. 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.

19.4. 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.

19.4.1. 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

19.4.2. 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.

19.4.3. 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) 231 98 92 80 16
Sales: firmenkunden@Bitdefender.de
Website: http://www.bitdefender.de
Support Center: http://www.bitdefender.de/support/business.html

UK and Ireland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Phone (sales&technical support): (+44) 203 695 3415
Email: info@bitdefender.co.uk
Sales: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Support Center: http://www.bitdefender.co.uk/support/business.html

Romania

BITDEFENDER SRL
rsOrhideea Towe
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470

Sales: sales@bitdefender.ro
Website: http://www.bitdefender.ro
Support Center: http://www.bitdefender.ro/support/business.html

United Arab Emirates

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Phone (sales&technical support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Support Center: http://www.bitdefender.com/support/business.html

A. Appendices

A.1. Supported File Types

The antimalware scanning engines included in the Bitdefender security solutions can scan all types of files that may contain threats. The list below includes the most common types of files that are being analyzed.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

```
xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo
```

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
	Partner company
	Customer company
	Companies collection
	Company network
	Network group
	Computer
	Relay computer
	Active Directory integrator computer
	Exchange Server computer
	Relay Exchange Server computer
	Virtual machine
	Relay virtual machine
	Golden image
	Exchange Server virtual machine
	Relay Exchange Server virtual machine
	Security Server

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
	Customer Company, Active, Self Managed
	Customer Company, Active, Managed by Partner
	Customer Company, Suspended, Self Managed
	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. Sandbox Analyzer Objects

A.6.1. 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.6.2. 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.6.3. Default Exclusions at Automatic Submission

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt`.

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".

IOR

Indicator of Risk - refers to a registry key value or data of a specific system setting, or a known application vulnerability.

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Keylogger

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Malware

Malware is the generic term for software that is designed to do harm - a contraction of 'malicious software'. It is not yet in universal usage, but its popularity as a general term for viruses, Trojan Horses, worms, and malicious mobile code is growing.

Malware signature

Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching and detect malware. Signatures are also used to remove the malware code from infected files.

The Bitdefender Malware Signature Database is a collection of malware signatures updated hourly by the Bitdefender malware researchers.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Password stealer

A password stealer collects pieces of data that can be account names and associated passwords. These stolen credentials are then used for malicious purposes, like account takeovers.

Phishing
> The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Polymorphic virus
> A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port
> An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

> In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Ransomware
> A malware that locks you out of your computer or blocks access to your files and applications. Ransomware will demand that you pay a certain fee (ransom payment) in return for a decryption key that allows you to regain access to your computer or files.

Report file
> A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit
> A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing

them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited email.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the

applications running in the background can lead to system crashes or general system instability.

Suspicious files and network traffic

Suspicious files are those with a doubtful reputation. This ranking is given by many factors, among which to name: existence of the digital signature, number of occurrences in computer networks, packer used, etc. Network traffic is considered suspicious when it deviates from the pattern. For example, unreliable source, connection requests to unusual ports, increased bandwidth usage, random connection times, etc.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

Targeted attacks

Cyber-attacks that mainly aim financial advantages or denigration of reputation. The target can be an individual, a company, a software or a system, well studied before the attack takes place. These attacks are rolled out over a long period of time and in stages, using one or more infiltration points. They are hardly noticed, most times when the damage has already been done.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak

out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.