Bitdefender

GravityZone

REPORTER'S GUIDE

Bitdefender GravityZone
Reporter's Guide

Publication date 2015.05.27

Legal Notice

Table of Contents

1. ABOUT GRAVITYZONE

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

GravityZone is one product with a unified management console available in the cloud, hosted by Bitdefender, or as one virtual appliance to be installed on premise, 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, including Microsoft Exchange mail servers: antivirus and antimalware with behavioral monitoring, zero day threat protection, application control and sandboxing, firewall, device control, content control, anti-phishing and antispam.

1.1. GravityZone Security Services

GravityZone provides the following security services:

- Security for Endpoints
- Security for Virtualized Environments
- Security for Exchange
- Security for Mobile

1.1.1. Security for Endpoints

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

1.1.2. Security for Virtualized Environments

GravityZone provides the first platform-agnostic security solution for the dynamic datacenters of today. Compliant with any known hypervisor, from VMware ESXi to Citrix Xen or Microsoft Hyper-V, Bitdefender Security for Virtualized Environments leverages the pooled nature of virtualization by offloading major security processes onto a centralized virtual appliance. Powered by cutting-edge caching technologies, the solution drives significant performance gains and boosts server consolidation by up to 30% compared to traditional antimalware. On a management level, Security for Virtualized Environments integrates with third-party platforms such as VMware vCenter and XenServer to automate administrative tasks and reduce operational costs.

1.1.3. 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.

1.1.4. Security for Mobile

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

2. GETTING STARTED

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

2.1. Connecting to Control Center

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

Prerequisites:

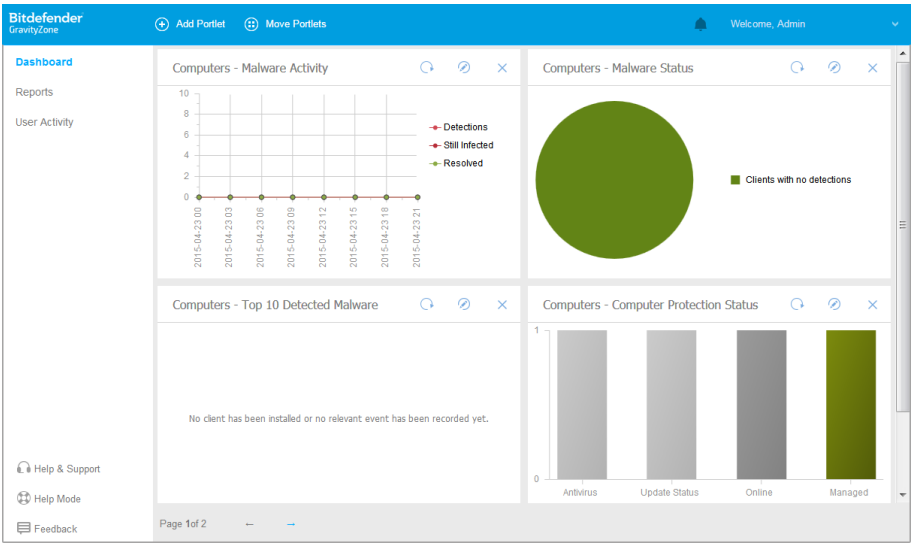
- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Recommended screen resolution: 1024x768 or higher

To connect to Control Center:

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

2.2. Control Center at a Glance

Control Center is organized so as to allow easy access to all the features. Use the menu bar in the upper area to navigate through the console.



The Dashboard

Reporters can access the following sections from the menu bar:

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

Reports
Get security reports concerning the managed clients.

User Activity
Check the user activity log.

Additionally, in the upper-right corner of the console, the **Notifications** icon provides easy access to notification messages and also to the **Notifications** page.

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

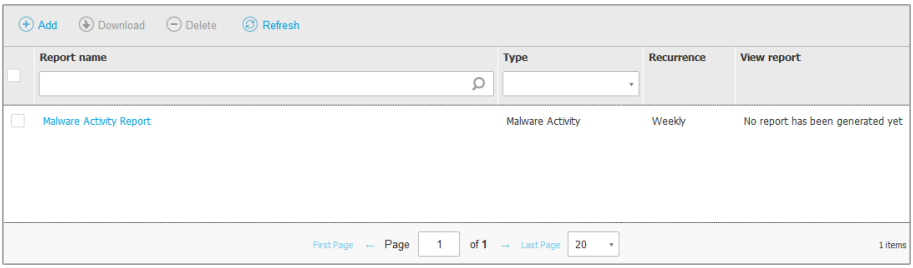
- **My Account**. Click this option to manage your user account details and preferences.
- **Logout**. Click this option to log out of your account.

On the lower-right corner of the console, the following links are available:

- **Help and Support**. Click this button to find help and support information.
- **Help Mode**. Click this button to enable a help feature providing expandable tooltips boxes placed on Control Center items. You will easily find out useful information regarding the Control Center functionalities.
- **Feedback**. Click this button to display a form allowing you to edit and send your feedback messages regarding your experience with GravityZone.

2.2.1. Table Data

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



The Reports page - Reports Table

Navigating through Pages

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

Searching for Specific Entries

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

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

Sorting Data

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

Refreshing Table Data

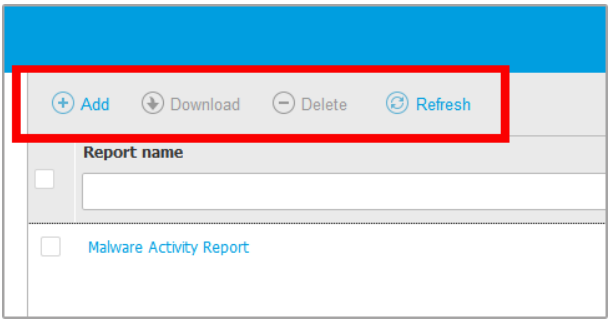
To make sure the console displays the latest information, click the **Refresh** button at the upper side of the table.

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

2.2.2. Action Toolbars

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

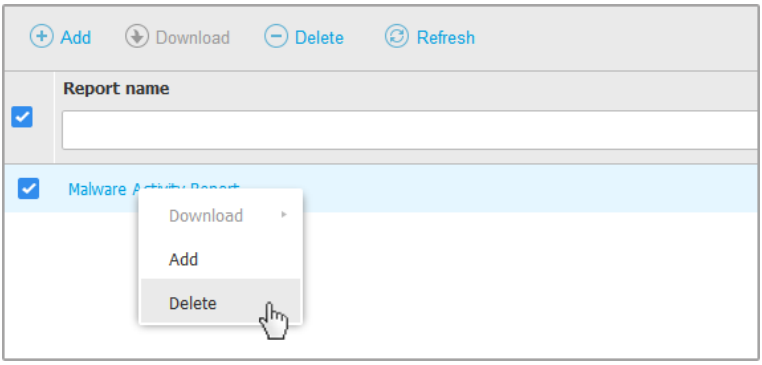
- Create a new report.
- Download a scheduled report.
- Delete a scheduled report.



The Reports page - Action Toolbar

2.2.3. Contextual Menu

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



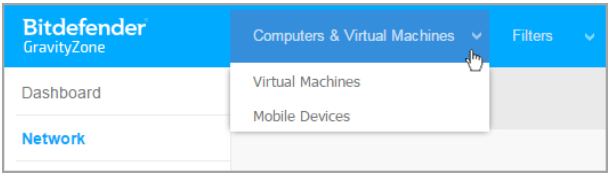
The Reports page - Contextual menu

2.2.4. Views Selector

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

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

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



The Views Selector

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

2.3. Changing Login Password

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

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

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

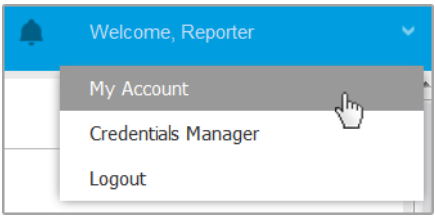
To change the login password:

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

2.4. Managing Your Account

To check or change your account details and settings:

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



The User Account menu

2. Under **Account Details**, correct or update your account details. If you use an Active Directory user account, you cannot change account details.
   - **Username.** The username is the unique identifier of a user account and cannot be changed.
   - **Full name.** Enter your full name.

- **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
- A **Change password** link allows you to change your login password.

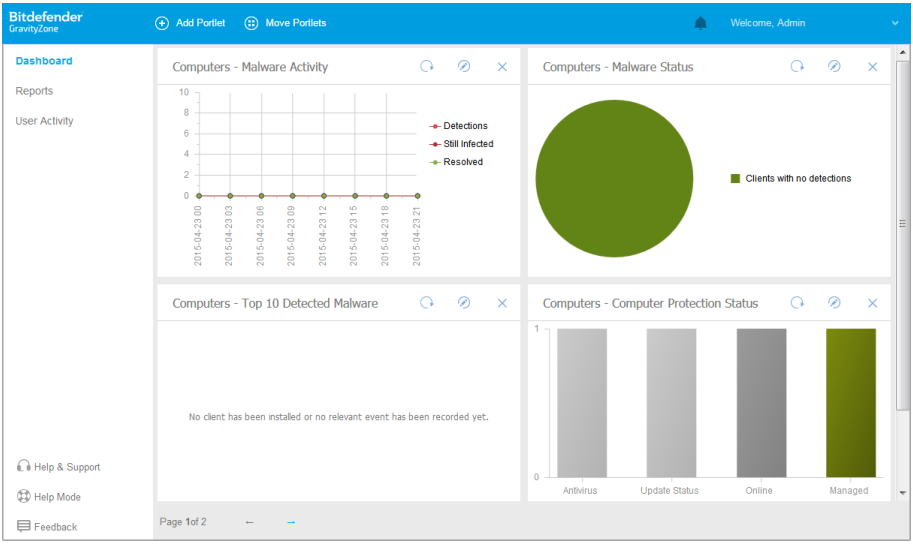
3. Under **Settings**, configure the account settings according to your preferences.
   - **Timezone.** Choose from the menu the timezone of your account. The console will display time information according to the selected timezone.
   - **Language.** Choose from the menu the console display language.
   - **Session Timeout.** Select the inactivity time interval before your user session will expire.
4. Click **Save** to apply the changes.

Note
You cannot delete your own account.

3. MONITORING DASHBOARD

The Control Center dashboard is a customizable visual display providing a quick security overview of all protected endpoints.

Dashboard portlets display various real-time security information using easy-to-read charts, thus allowing you to quickly identify any issues that might require your attention.



The Dashboard

This is what you need to know about dashboard portlets:

- Control Center comes with several predefined dashboard portlets.
- Each dashboard portlet includes a detailed report in the background, accessible with just one click on the chart.
- There are several types of portlets that include various information about your endpoint protection, such as update status, malware status, firewall activity, etc. For more information on dashboard portlets types, refer to "Available Report Types" (p. 20).

- The information displayed via portlets refers to endpoints under your account only. You can customize each portlet's target and preferences using the **Edit Portlet** command.
- Click the chart legend entries, when available, to hide or display the corresponding variable on the graph.
- The portlets are displayed in groups of four. Use the arrows at the bottom of the page to navigate between portlet groups.
- For several report types, you have the option to instantly run specific tasks on target endpoints, without having to go to the **Network** page to run the task (for example, scan infected endpoints or update endpoints). Use the button at the lower side of the portlet to take the available action.

The dashboard is easy to configure, based on individual preferences. You can edit portlet settings, add additional portlets, remove or rearrange existing portlets.

3.1. Refreshing Portlet Data

To make sure the portlet displays the latest information, click the **Refresh** icon on its title bar.

3.2. 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.

3.3. Adding a New Portlet

You can add other portlets to obtain the information you need.

To add a new portlet:

1. Go to the **Dashboard** page.
2. Click the **Add Portlet** button at the upper side of the console. The configuration window is displayed.
3. Under the **Details** tab, configure the portlet details:
   - Endpoint type (**Computers**, **Virtual Machines** or **Mobile Devices**)
   - Type of background report
   - Suggestive portlet name
   - The time interval for the events to be reported

For more information on available report types, refer to "Available Report Types" (p. 20).

4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

3.4. 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.

3.5. Rearranging Portlets

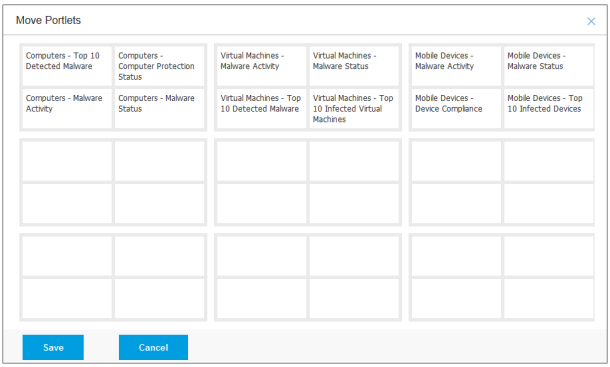
You can rearrange dashboard portlets to better suit your needs. To rearrange portlets:

1. Go to the **Dashboard** page.
2. Click the **Move Portlets** button at the upper side of the console. The portlet map window is displayed.
3. Drag and drop each portlet to the desired position. All other portlets between the new and old positions are moved preserving their order.

Note
You can move portlets only within the positions already taken.

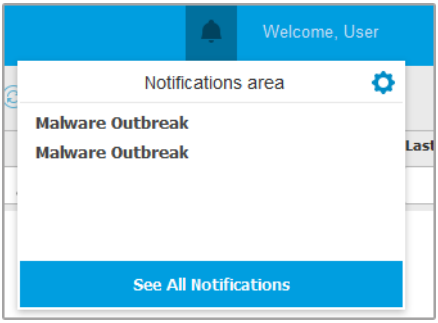
4. Click **Save**.

Move Portlets window


Move Portlets
Computers - Top 10 Detected Malware
Computers - Computer Protection Status
Computers - Malware Activity
Computers - Malware Status
Virtual Machines - Malware Activity
Virtual Machines - Malware Status
Virtual Machines - Top 10 Detected Malware
Virtual Machines - Top 10 Infected Virtual Machines
Mobile Devices - Malware Activity
Mobile Devices - Malware Status
Mobile Devices - Device Compliance
Mobile Devices - Top 10 Infected Devices
Save
Cancel

4. 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 upper right side of the Control Center interface.



Notification Area

When new events are detected in the network, the icon in the notification area will display the number of newly detected events. Clicking the icon displays the list of detected events.

4.1. Notification Types

This is the list of available notifications types:

Malware Outbreak

This notification is sent to the users that have at least 5% of all their managed network objects infected by the same malware.

You can configure the malware outbreak threshold in the **Notifications Settings** window. For more information, refer to “Configuring Notification Settings” (p. 16).

Antimalware event

This notification informs you when malware is detected on an endpoint in your network. This notification is created for each malware detection, providing details about the infected endpoint (name, IP, installed agent), detected malware and detection time.

Antiphishing event

This notification informs you each time the endpoint agent blocks a known phishing web page from being accessed. This notification also provides details such as the endpoint that attempted to access the unsafe website (name and IP), installed agent or blocked URL.

Firewall event

With this notification you are informed each time the firewall module of an installed agent has blocked a port scan or an application from accessing the network, according to applied policy.

AVC/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

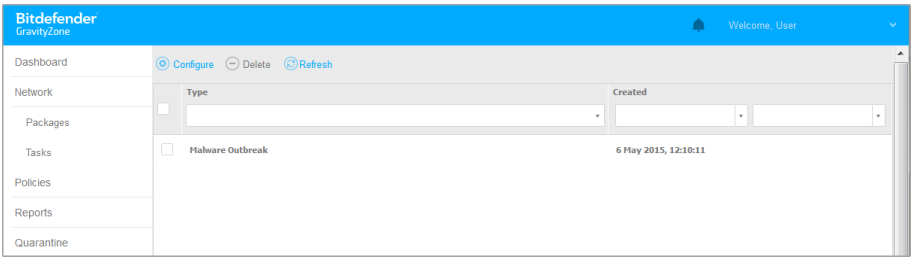
This notification is triggered each time a user activity such as web browsing or software application is blocked by the endpoint client according to applied policy.

Data Protection event

This notification is sent each time data traffic is blocked on an endpoint according to data protection rules.

4.2. Viewing Notifications

To view the notifications, click the **Notification Area** 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.

4.3. Deleting Notifications

To delete notifications:

1. Click the **Notification Area** button at the right side of the menu bar, then click **See All Notifications**. A table containing all the notifications is displayed.
2. Select the notifications you want to delete.
3. Click the **Delete** button at the upper side of the table.

You can also configure notifications to be automatically deleted after a specified number of days. For more information, refer to "Configuring Notification Settings" (p. 16).

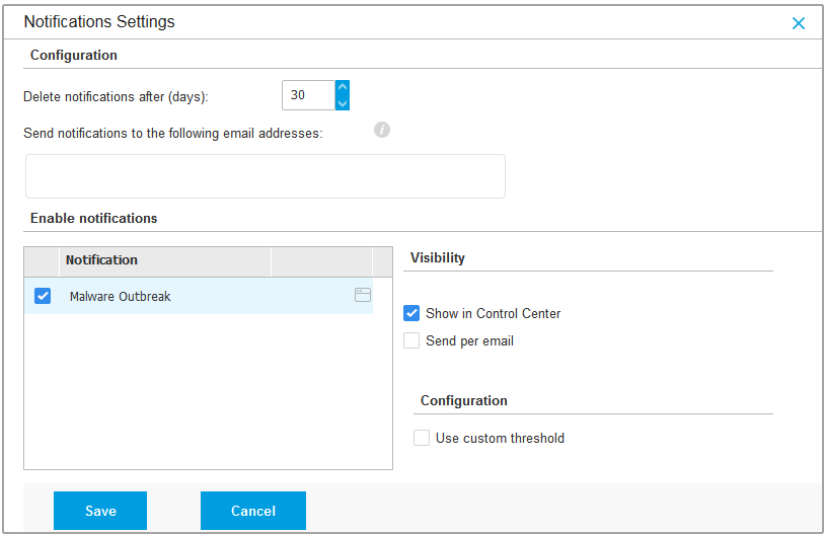
4.4. Configuring Notification Settings

The type of notifications to be sent and the email addresses they are sent to can be configured for each user.

To configure the notification settings:

1. Click the **Notification Area** button at the right side of the menu bar and then click **See All Notifications**. A table containing all the notifications is displayed.

2. Click the **Configure** button at the upper side of the table. The **Notification Settings** window is displayed.



Notifications Settings

Note
You may also access the **Notification Settings** window directly using the **Configure** icon from upper-right corner of the **Notification area** window.

3. Under **Configuration** section you can define the following settings:
   - You can configure notifications to be automatically deleted after a certain number of days. Enter the number of days that you want in the **Delete notifications after (days)** field.
   - Optionally, you can choose to send the notifications by email to specific email addresses. Type the email addresses in the dedicated field, pressing `Enter` 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. 14). While a notification type is selected, you can configure its specific options (when available) in the right-side area:

Visibility

- **Show in Control Center** specifies that this type of event is displayed in Control Center, with the help of **Notifications area** icon.
- **Log to server** specifies that this type of event is also sent to the `syslog` file, in the case when a syslog is configured.
- **Send per email** specifies that this type of event is also sent to certain email addresses. In this case, you are required to enter the email addresses in the dedicated field, pressing `Enter` after each address.

Configuration

- **Use custom threshold** - allows defining a threshold for the occurred events, from which the selected notification is being sent.

  For example, the Malware Outbreak notification is sent by default to users that have at least 5% of all their managed network objects infected by the same malware. To change the malware outbreak threshold value, enable the option **Use Custom Threshold**, then enter the value that you want in the **Malware Outbreak Threshold** field.
- For **Security Server Status event**, you can select the Security Server events that will trigger this type of notification:
  - **Out of date** - notifies each time a Security Server in your network is outdated.
  - **Powered off** - notifies each time a Security Server in your network has been shut down.
  - **Reboot required** - notifies each time a Security Server in your network requires a reboot.
- For **Task Status**, you can select the status type that will trigger this type of notification:
  - **Any status** - notifies each time a task sent from Control Center is done with any status.

- **Failed only** - notifies each time a task sent from Control Center has failed.

Note

5. Click **Save**.

5. USING REPORTS

Control Center allows you to create and view centralized reports on the security status of the managed network objects. The reports can be used for multiple purposes, such as:

- Monitoring and ensuring compliance with the organization's security policies.
- Checking and assessing the network security status.
- Identifying network security issues, threats and vulnerabilities.
- Monitoring security incidents and malware activity.
- Providing upper management with easy-to-interpret data on network security.

Several different report types are available so that you can easily get the information you need. The information is presented as easy-to-read interactive charts and tables, allowing you to quickly check the network security status and identify security issues.

Reports can consolidate data from the entire network of managed network objects or from specific groups only. In this way, from a single report, you can find out:

- Statistical data regarding all or groups of managed network objects.
- Detailed information for each managed network object.
- The list of computers that meet specific criteria (for example, those that have antimalware protection disabled).

Some reports also allow you to quickly fix the issues found in your network. For example, you can effortless update all target network objects right from the report, without having to go and run an update task from the **Network** page.

All scheduled reports are available in Control Center but you can save them to your computer or email them.

Available formats include Portable Document Format (PDF) and comma-separated values (CSV).

5.1. Available Report Types

Different report types are available for each endpoint type:

- Computer and Virtual Machine Reports
- Mobile Device Reports

5.1.1. Computer & Virtual Machine Reports

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. 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 Application Control module of Bitdefender Endpoint Security Tools. You can see the number of blocked applications on the selected endpoints. For each target, by clicking the corresponding number, you can view additional information on the applications that have been blocked, the number of events triggered and the date and time of the last block event.

Blocked Applications By Behavior Scan

Informs you about the applications blocked by AVC (Active Virus Control) / IDS (Intrusion Detection System). You can view the number of applications blocked by AVC / IDS for each selected endpoint. Click the number of blocked applications for the endpoint you are interested in to view the list of blocked application and related information (application name, the reason for which it has been blocked, the number of blocked attempts and the date and time of the last blocked attempt).

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.

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.

Device Control Activity

Informs you about the events occurred when accessing the endpoints through the monitored devices. For each target endpoint, you can view the number of allowed / blocked access and read-only events. If events occurred, additional information is available by clicking the corresponding numbers. Details refer to:

- User logged on the machine
- Device type and ID
- Device vendor and product ID
- Date and time of the event.

Endpoint Modules Status

Provides a status overview of the Bitdefender Endpoint Security Tools protection modules for the selected endpoints. You can view which modules are active and which are disabled or not installed.

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.

Malware Activity

Provides you with overall information about the malware threats detected over a specific time period on selected endpoints. You can view:

- Number of detections (files that have been found infected with malware)

- Number of resolved infections (files that have been successfully disinfected or moved to quarantine)
- Number of unresolved infections (files that could not be disinfected, but to which access has been denied; for example, an infected file stored in some proprietary archive format)

For each detected threat, by clicking the links available in the disinfection result columns, you can view the list of the affected endpoints and file paths. For example, if you click the number from the **Resolved** column, you will view the files and endpoints from where the threat has been removed.

Malware Status

Helps you find out how many and which of the selected endpoints have been affected by malware over a specific time period and how the threats have been dealt with.

Endpoints are grouped based on these criteria:

- Endpoints with no detections (no malware threat has been detected over the specified time period)
- Endpoints with resolved malware (all detected files have been successfully disinfected or moved to quarantine)
- Endpoints still infected with malware (some of the detected files have been denied access to)

For each endpoint, by clicking the links available in the disinfection result columns, you can view the list of threats and paths to the affected files.

Network Status

Provides you with detailed information on the overall security status of selected endpoints. Endpoints are grouped based on these criteria:

- Issues status
- Management status
- Infection status
- Antimalware protection status
- Product update status
- Licensing status

- The network activity status of each endpoint(online/offline). If the endpoint is offline when the report is generated, you will see the date and time when it was last seen online by Control Center.

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:

- **Machine status**: informs which Security Server appliances are stopped
- **AV status**: points out whether the Antimalware module is enabled or disabled
- **Update status**: shows if the Security Server appliances are updated or whether the updates have been disabled.
- **Load status**: indicates the scan load level of a Security Server as described herein:
  - **Underloaded**, when less than 5% of its scanning capacity is used.
  - **Normal**, when the scan load is balanced.
  - **Overloaded**, when the scan load exceeds 90% of its capacity. In such case, check the security policies. If all the Security Servers allocated within a policy are overloaded, you need to add another Security Server to the list. Otherwise, check the network connection between the clients and the Security Servers without load issues.

Top 10 Detected Malware

Shows you the top 10 malware threats detected over a specific time period on selected endpoints.

Note
The details table displays all endpoints which were infected by the top 10 detected malware.

Top 10 Infected Endpoints

Shows you the top 10 most infected endpoints by the number of total detections over a specific time period out of the selected endpoints.

Note
The details table displays all malware detected on the top 10 infected endpoints.

Update Status

Shows you the update status of the Bitdefender Endpoint Security Tools protection installed on selected targets. The update status refers to product version and engines (signatures) version.

Using the available filters, you can easily find out which clients have updated and which have not in the last 24 hours.

Upgrade Status

Shows you the security agents installed on the selected targets and whether a more recent solution is available.

For endpoints with old security agents installed, you can quickly install the latest supported security agent by clicking the **Upgrade** button.

> **Note**
> This report is available only when a GravityZone solution upgrade has been made.

Virtual Machines Network Protection Status

Informs you which of the security agents is installed on the selected virtual machines:

- vShield Endpoint
- Bitdefender endpoint client
- Security Server (SVA).

Exchange - Blocked Content and Attachments

Provides you with information about emails or attachments that Content Control deleted from the selected servers over a specific time interval. The information includes:

- Email addresses of the sender and of the recipients.

  When the email has more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.
- Email subject.
- Detection type, indicating which Content Control filter detected the threat.
- The action taken on the detection.
- The server where the threat was detected.

Exchange - Email Scan Activity

Shows statistics on the actions taken by the Exchange Protection module over a specific time interval.

The actions are grouped by detection type (malware, spam, forbidden attachment and forbidden content) and by server.

The statistics refer to the following email statuses:

- **Quarantined.** These emails were moved to the Quarantine folder.
- **Deleted/Rejected.** These emails were deleted or rejected by the server.
- **Redirected.** These emails were redirected to the email address supplied in the policy.
- **Cleaned and delivered.** These emails had the threats removed and passed through the filters.

  An email is considered cleaned when all detected attachments have been disinfected, quarantined, deleted or replaced with text.
- **Modified and delivered.** Scan information was added to the emails headers and the emails passed through the filters.
- **Delivered without any other action.** These emails were ignored by Exchange Protection and passed through the filters.

Exchange - Malware Activity

Provides you with information about emails with malware threats, detected on the selected Exchange mail servers over a specific time period. The information refers to:

- Email addresses of the sender and of the recipients.

  When the email is sent to more recipients, instead of the email addresses, the report displays the recipients number with a link to a window containing the list of email addresses.
- Email subject.
- Email status after antimalware scan.

  By clicking the status link, you can view details about the detected malware and the action taken.
- Detection date and time.
- The server where the threat was detected.

Exchange - Top 10 Detected Malware

Informs you about the top 10 most detected malware threats in email attachments. You can generate two views containing different statistics. One view shows the number of detections by affected recipients and one by senders.

For example, GravityZone has detected one email with an infected attachment sent to five recipients.

- In the recipients view:
  - The report shows five detections.
  - The report details shows only the recipients, not the senders.
- In the senders view:
  - The report shows one detection.
  - The report details shows only the sender, not the recipients.

Besides the sender/recipients and the malware name, the report provides you with the following details:

- The malware type (virus, spyware, PUA, etc.)
- The server where the threat was detected.
- Measures that the antimalware module has taken.
- Date and time of the last detection.

Exchange - Top 10 Malware Recipients

Shows you the top 10 email recipients most targeted by malware over a specific time interval.

The report details provide you with the entire malware list that affected these recipients, together with the actions taken.

Exchange - Top 10 Spam Recipients

Shows you the top 10 email recipients by the number of spam or phishing emails detected over a specific time interval. The report provides information also on the actions applied to the respective emails.

5.1.2. Mobile Devices Reports

Note
Malware protection and related reports are only available for Android devices.

This is the list of available report types for mobile devices:

Malware Status

Helps you find out how many and which of the target mobile devices have been affected by malware over a specific time period and how the threats have been dealt with. Mobile devices are grouped based on these criteria:

- Mobile devices with no detections (no malware threat has been detected over the specified time period)
- Mobile devices with resolved malware (all detected files have been removed)
- Mobile devices with existing malware (some of the detected files have not been deleted)

Malware Activity

Provides you with details about the malware threats detected over a specific time period on target mobile devices. You can see:

- Number of detections (files that have been found infected with malware)
- Number of resolved infections (files that have been successfully removed from the device)
- Number of unresolved infections (files that have not been removed from the device)

Top 10 Infected Devices

Shows you the top 10 most infected mobile devices over a specific time period out of the target mobile devices.

Note
The details table displays all malware detected on the top 10 infected mobile devices.

Top 10 Detected Malware

Shows you the top 10 malware threats detected over a specific time period on the target mobile devices.

Note
The details table displays all mobile devices which were infected by the top 10 detected malware.

Device Compliance

Informs you of the compliance status of the target mobile devices. You can see the device name, status, operating system and the non-compliance reason.

Device Synchronization

Informs you of the synchronization status of the target mobile devices. You can view the device name, the user it is assigned to, as well as the synchronization status, the operating system and the time when the device was last seen online.

Blocked Websites

Informs you about the number of attempts of the target devices to access websites which are blocked by **Web Access** rules, over a certain time interval.

For each device with detections, click the number provided in the **Blocked Websites** column to view detailed information of each blocked web page, such as:

- Website URL
- Policy component that performed the action
- Number of blocked attempts
- Last time when the website was blocked

Web Security Activity

Informs you about the number of attempts of the target mobile devices to access websites with security threats (phishing, fraud, malware or untrusted websites), over a certain time interval. For each device with detections, click the number provided in the Blocked Websites column to view detailed information of each blocked web page, such as:

- Website URL
- Type of threat (phishing, malware, fraud, untrusted)
- Number of blocked attempts
- Last time when the website was blocked

Web Security is the policy component which detects and blocks websites with security issues.

5.2. Creating Reports

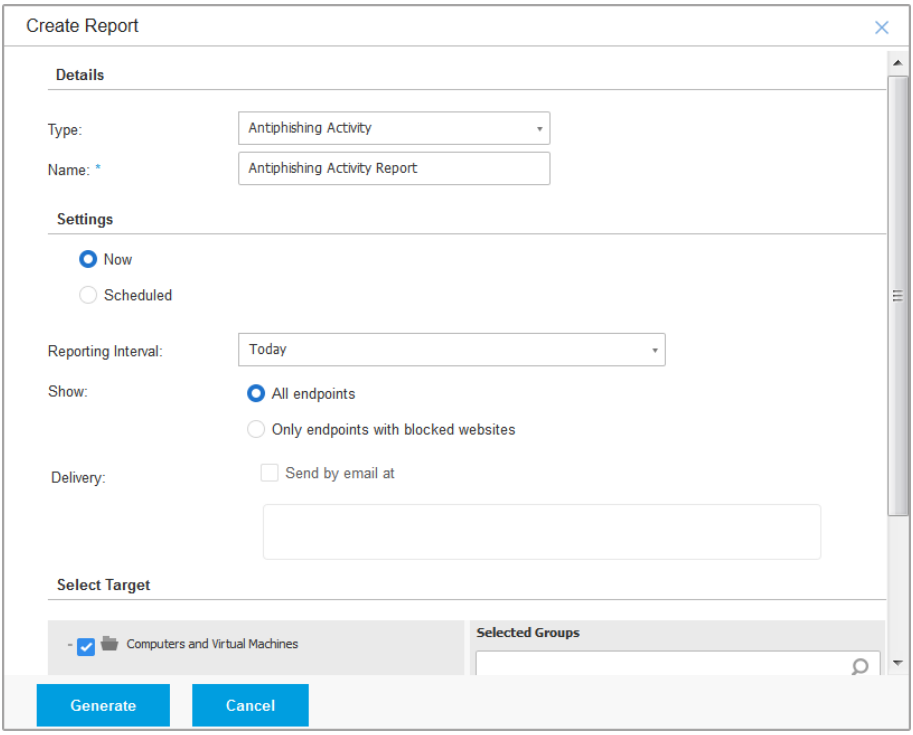
You can create two categories of reports:

- **Instant reports.** Instant reports are automatically displayed after you generate them.
- **Scheduled reports.** Scheduled reports can be configured to run periodically, at a specified time and date. A list of all the scheduled reports is displayed in the **Reports** page.

Important
Instant reports are automatically deleted when you close the report page. Scheduled reports are saved and displayed in the **Reports** page.

To create a report:

1. Go to the **Reports** page.
2. Choose the network objects type from the views selector.
3. Click the ⊕ **Add** button at the upper side of the table. A configuration window is displayed.



Computers and Virtual Machines Report Options

4. Select the desired report type from the menu. For more information, refer to "Available Report Types" (p. 20)
5. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
6. Configure the report recurrence:
   - Select **Now** to create an instant report.
   - Select **Scheduled** to configure the report to be automatically generated at the time interval that you want:
     - Hourly, at the specified interval between hours.
     - Daily. In this case, you can also set the start time (hour and minutes).

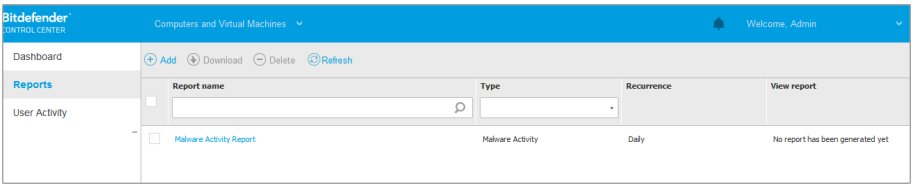
- Weekly, in the specified days of the week and at the selected start time (hour and minutes).
- Monthly, at each specified day on the month and at the selected start time (hour and minutes).

7. For most report types you must specify the time interval to which the contained data is referring. The report will only display data from the selected time period.
8. Several report types provide filtering options to help you easily find the information you are interested in. Use the filtering options under **Show** section to obtain only the desired information.

   For example, for an **Update Status** report you can choose to view only the list of network objects that have not updated, or the ones that need to be restarted to complete the update.
9. **Delivery**. To receive a scheduled report by email, select the corresponding checkbox. Enter the email addresses that you want in the field below.
10. **Select Target**. Scroll down to configure the report target. Select one or several groups of endpoints you want to include in the report.
11. Depending on the selected recurrence, click **Generate** to create an instant report or **Save** to create a scheduled report.
    - The instant report will be displayed immediately after clicking **Generate**. The time required for reports to be created may vary depending on the number of managed network objects. Please wait for the requested report to be created.
    - The scheduled report will be displayed in the list on the **Reports** page. Once a report instance has been generated, you can view the report by clicking the corresponding link in the **View report** column on the **Reports** page.

5.3. 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.

5.3.1. 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. 36)

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.

5.3.2. 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.

5.3.3. 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.

5.4. 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:

Update Status

- **Refresh**. Updates the information displayed in the table.
- **Update**. Updates the target clients to their latest available versions.

Malware Status

- **Scan infected targets**. Runs a preconfigured Full Scan task on the targets showing as still infected.
- **Delete**. Deletes the infected files from the targets.
- **Refresh**. Updates the information displayed in the table.

Upgrade Status

- **Upgrade**. Replaces old endpoint clients with the latest generation of products available.
- **Refresh**. Updates the information displayed in the table.

5.5. 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

5.5.1. Exporting Reports

To export the report to your computer:

1. Click the **Export** button in the lower-left corner of the report page.

2. Select the desired format of the report:
   - Portable Document Format (PDF) or
   - Comma Separated Values (CSV)
3. Depending on your browser settings, the file may be downloaded automatically to a default download location, or a download window will appear, where you must specify the destination folder.

5.5.2. 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.

5.6. Emailing Reports

You can send reports by email using the following options:

1. To email the report you are viewing, click the **Email** button in the lower-left corner of the report page. The report will be sent to the email address associated with your account.
2. To configure the desired scheduled reports delivery by email:
   a. Go to the **Reports** page.
   b. Click the desired report name.
   c. Under **Options > Delivery**, select **Send by email at**.
   d. Provide the desired email address in the field below. You can add as many email addresses as you want.
   e. Click **Save**.

Note
Only the report summary and the chart will be included in the PDF file sent by email. Report details will be available in the CSV file.

5.7. Printing Reports

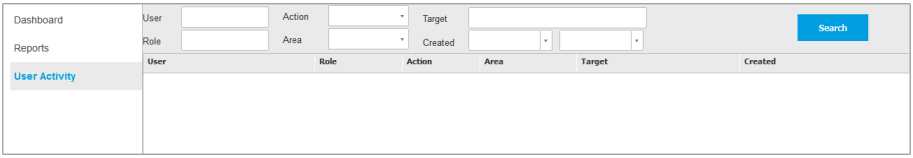
Control Center does not currently support print button functionality. To print a report, you must first save it to your computer.

6. 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

To examine the user activity records, go to the **User Activity** page and choose the network view that you want from the views selector.



The User Activity Page

To display recorded events that you are interested in, you have to define a search. Fill in the available fields with the search criteria and click the **Search** button. All the records matching your criteria will be displayed in the table.

The table columns provide you with useful information about the listed events:

- The username of who performed the action.
- User role.
- Action that caused the event.
- Type of console object affected by the action.
- Specific console object affected by the action.
- Time when the event occurred.

To sort events by a specific column, simply click the header of that column. Click the column header again to reverse the sorting order.

To view detailed information about an event, select it and check the section under the table.

7. GETTING HELP

For any problems or questions concerning Control Center, contact an administrator.

7.1. 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.

7.1.1. Using Support Tool on Windows Operating Systems

1. Download the Support Tool and distribute it to the affected computers. To download the Support Tool:
   a. Connect to Control Center using your account.
   b. Click the **Help and Support** link in the lower-left corner of the console.
   c. The download links are available in the **Support** section. Two versions are available: one for 32-bit systems and the other for 64-bit systems. Make sure to use the correct version when running the Support Tool on a computer.
2. Run the Support Tool locally on each of the affected computers.
   a. Select the agreement check box and click **Next**.
   b. Complete the submission form with the necessary data:
      i. Enter your email address.
      ii. Enter your name.
      iii. Choose your country from the corresponding menu.
      iv. Enter a description of the issue you encountered.
      v. Optionally, you can try to reproduce the issue before starting to collect data. In this case, proceed as follows:
         A. Enable the option **Try to reproduce the issue before submitting**.
         B. Click **Next**.
         C. Select the type of issue you have experienced.
         D. Click **Next**.

E. Reproduce the issue on your computer. When done, return to Support Tool and select the option **I have reproduced the issue**.

c. Click **Next**. The Support Tool gathers product information, information related to other applications installed on the machine and the software and hardware configuration.

d. Wait for the process to complete.

e. Click **Finish** to close the window. A zip archive has been created on your desktop.

Send the zip archive together with your request to the Bitdefender support representative using the email support ticket form available in the **Help and Support** page of the console.

7.1.2. Using Support Tool on Linux Operating Systems

For Linux operating systems, the Support Tool is integrated with the Bitdefender security agent.

To gather Linux system information using Support Tool, run the following command:

```
# /opt/BitDefender/bin/bdconfigure
```

using the following available options:

- `--help` to list all Support Tool commands
- `enablelogs` to enable product and communication module logs (all services will be automatically restarted)
- `disablelogs` to disable product and communication module logs (all services will be automatically restarted)
- `deliverall` to create an archive containing the product and communication module logs, delivered to the `/tmp` folder in the following format: `bitdefender_machineName_timeStamp.tar.gz`.

  1. You will be prompted if you want to disable logs. If needed, the services are automatically restarted.
  2. You will be prompted if you want to delete logs.

- `deliverall -default` delivers the same information as with the previous option, but default actions will be taken on logs, without the user to be prompted (the logs are disabled and deleted).

To report a GravityZone issue affecting your Linux systems, follow the next steps, using the options previously described:

1. Enable product and communication module logs.
2. Try to reproduce the issue.
3. Disable logs.
4. Create the logs archive.
5. Open an email support ticket using the form available on the **Help & Support** page of Control Center, with a description of the issue and having the logs archive attached.

The Support Tool for Linux delivers the following information:

- The `etc`, `var/log`, `/var/crash` (if available) and `var/epag` folders from `/opt/BitDefender`, containing the Bitdefender logs and settings
- The `/tmp/bdinstall.log` file, containing installation information
- The `network.txt` file, containing network settings / machine connectivity information
- The `system.txt` file, containing general system information (distribution and kernel versions, available RAM and free hard-disk space)
- The `users.txt` file, containing user information
- Other information concerning the product related to the system, such as external connections of processes and CPU usage
- System logs

Glossary

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Antivirus storm

An intensive use of system resources that occurs when antivirus software simultaneously scans multiple virtual machines on a single physical host.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. The two most popular browsers are Netscape Navigator and Microsoft Internet Explorer. Both of these are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

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.

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.

Heuristic

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP

Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Keylogger

A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Malware

Malware is the generic term for software that is designed to do harm - a contraction of 'malicious software'. It is not yet in universal usage, but its popularity as a general term for viruses, Trojan Horses, worms, and malicious mobile code is growing.

Malware signature

Malware signatures are snippets of code extracted from actual malware samples. They are used by antivirus programs to perform pattern-matching

and detect malware. Signatures are also used to remove the malware code from infected files.

The Bitdefender Malware Signature Database is a collection of malware signatures updated hourly by the Bitdefender malware researchers.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

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.

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.

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.

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.