



Bitdefender® ENTERPRISE

SECURITY FOR
VIRTUALIZED
ENVIRONMENTS
Reporter's Guide
(Multi-Platform) >>

Security for Virtualized Environments by Bitdefender Reporter's Guide (Multi-Platform)

Publication date 2012.12.18

Copyright© 2012 Bitdefender

Legal Notice

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

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

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

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



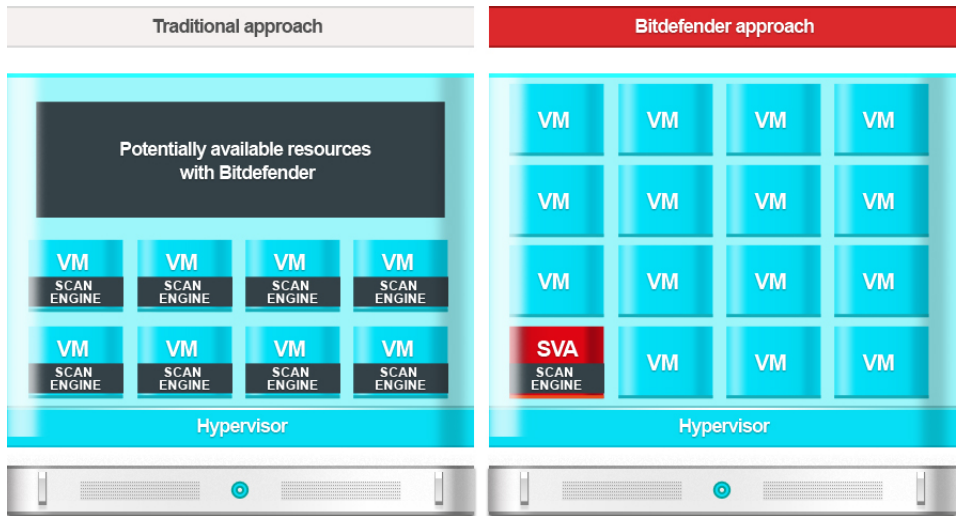
Table of Contents

1. About Security for Virtualized Environments	1
2. Getting Started	4
2.1. Connecting to Security Console	4
2.2. Security Console Overview	4
2.3. Guidelines	5
2.4. Changing Default Login Password	5
2.5. Managing Your Account	5
2.6. Working with Table Data	7
3. Monitoring Dashboard	8
3.1. Dashboard Portlets	8
3.2. Managing Portlets	10
4. Using Reports	11
4.1. Available Report Types	11
4.2. Creating Reports	13
4.3. Viewing and Managing Generated Reports	14
4.3.1. Viewing Reports	15
4.3.2. Searching Report Details	15
4.3.3. Saving Reports	15
4.3.4. Printing Reports	16
4.3.5. Emailing Reports	16
4.3.6. Automatic Deletion of Reports	16
4.3.7. Deleting Reports	16
4.4. Managing Scheduled Reports	16
4.4.1. Viewing Last Report Generated	17
4.4.2. Renaming Scheduled Reports	17
4.4.3. Editing Scheduled Reports	17
4.4.4. Deleting Scheduled Reports	18
5. User Activity Log	19
6. Getting Help	20
Glossary	21

1. About Security for Virtualized Environments

Organizations today look to virtualization technologies to increase the return on investment in datacenter infrastructure. Consolidation of server and end-user workloads onto shared infrastructure has led to cost reductions by deduplication of hardware resources. Virtualization also provides significant operational benefits through near-instant provisioning as organizations create and leverage private and public clouds.

To realize the full potential of virtualized datacenters, organizations must also look to consolidating elements of the workloads themselves, security being an element that must be present across all workloads. In gaining ever-higher consolidation ratios and operational benefits, organizations must not sacrifice security while their valuable brands become increasingly threatened by evermore dedicated, sophisticated, and focused attackers.



Bitdefender Approach

Security for Virtualized Environments (SVE) is the first comprehensive security solution for virtualized datacenters. SVE protects not only Windows servers and end-user systems, but also Linux and Solaris systems. Integrated with VMware vShield and VMware vCenter, its unique architecture also allows it to defend systems running on any system virtualization technology. As organizations increase consolidation ratios, Bitdefender security that has

been designed, from day one, to provide highly advanced, proactive, and reliable security in virtualized environments is a cornerstone of building and enhancing datacenter virtualization strategies.

When installed in VMware environments, SVE takes advantage of vShield Endpoint. However, SVE is not dependent on the virtualization technology; it protects environments that are powered by any virtualization technology.

Components

Security Virtual Appliance

Security for Virtualized Environments deduplicates and centralizes much of the scanning functionality to a single, dedicated virtual appliance on each physical host. This hardened Linux scanning virtual appliance deals with the scanning and maintenance (updates, upgrades, RAM, IOPS, etc.) requirements of the antimalware clients.

Security Console

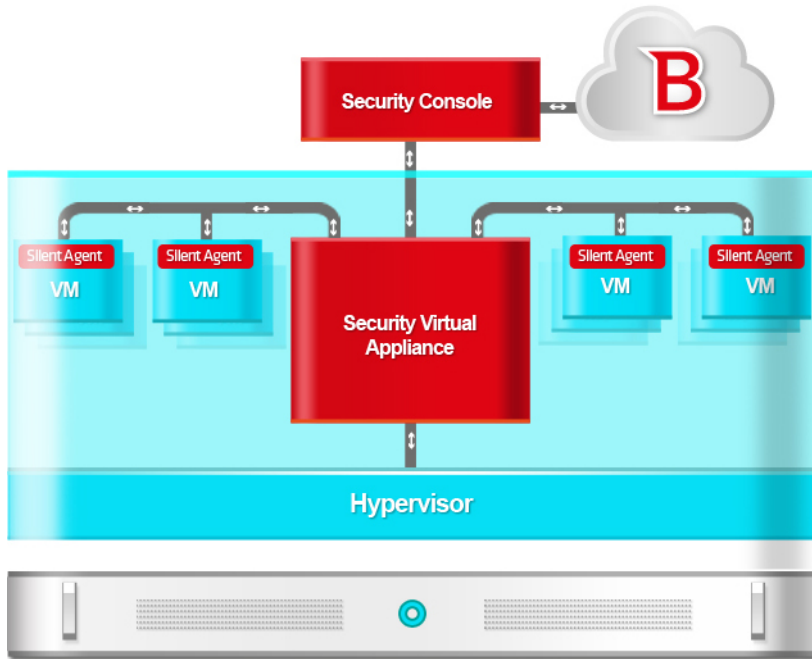
Security Console is a central web interface used for deploying, configuring, monitoring, and reporting on the security status of datacenters and end-user systems. Built on Bitdefender Gravity Architecture, a single Security Console and data store horizontally scale from the smallest to largest deployment with ease.

Security Console is delivered as a virtual appliance. The Security Console appliance also includes **Update Server**, the component handling all product upgrade and signature update tasks. Update Server is the only component that needs access to the Internet in order to communicate with the Bitdefender Cloud.

Silent Agent

Silent Agent is the guest side component that facilitates memory, on-access and on-demand scans. It is a thin application, which also has a secondary role of notifying the user on the local security status.

Silent Agent must be installed on each virtual machine to be protected (different from VMware environments where Security for Virtualized Environments is integrated with vShield Endpoint). The Silent Agent kit is accessible via Security Console.



Components and Operation

2. Getting Started

Security for Virtualized Environments can be configured and managed using Security Console, a central web-based interface. Installation, configuration and management tasks are performed by administrators.

As user of a reporter account, you can only monitor the Security for Virtualized Environments protection and create and view security reports.

2.1. Connecting to Security Console

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

To connect to Security Console:

1. Requirements:
 - The Security Console virtual appliance must be powered on, connected to Internet and accesible from your computer.
 - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari or Opera
 - Recommended screen resolution: 1024x768 or higher
2. Open your web browser.
3. Go to the IP address of the console host (using https).
4. Enter the email address and password of your account.
5. Click **Login**.



Note

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

The first time you log in to the console, you will be prompted to read and confirm that you agree with the terms of service. If you do not agree with these terms, you cannot use the service.

2.2. Security Console Overview

Security Console 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.

Dashboard

View easy-to-read charts providing key security information concerning your network. For more information, refer to “[Monitoring Dashboard](#)” (p. 8).

Reports

Get security reports concerning the managed computers. For more information, refer to “[Using Reports](#)” (p. 11).

Log

Check the user activity log. For more information, refer to “[User Activity Log](#)” (p. 19).

In the upper-right corner of the console, you can find the following links:

- **User name.** Click your user name to manage your account details and preferences.
- **Help and Support.** Click this link to find help and support information.
- **Logout.** Click this link to log out of your account.

2.3. Guidelines

Here are some guidelines to help you get started:

1. [Change your default password.](#)
2. Go to the **Dashboard** page to see real-time information on the Security for Virtualized Environments protection.
3. Go to the **Reports > New Report** page to create the reports you need. It is recommended to create scheduled reports for the report types you need regularly. To view a generated report, go to the **Reports > View Reports** page and click the report name.

2.4. Changing Default Login Password

It is recommended that you change the default login password. It is also advisable to change your login password periodically.

To change the login password:

1. Click your user name in the upper-right corner of the console.
2. Type a new password in the corresponding fields (under **Account Details**).
3. Click **Submit** to save the changes.

2.5. Managing Your Account

To check and change your account details and settings:

1. Click your user name in the upper-right corner of the console.
2. Under **Account Details**, correct or update your account details.

- **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.
 - **Roles and Group.** These fields represent your account type and the computer group you are in charge of.
 - **Password.** To change your login password, type a new one in the corresponding fields.
3. **Company account only!** Under **Proxy Settings**, select **Use Proxy** if the Security Console machine connects to the Internet via a proxy server. The following settings must be specified:
- Address of the proxy server.
 - Port number used by the proxy server.
 - Username recognized by the proxy.
 - Valid password for the previously specified username.
4. **Company account only!** Under **SMTP Settings**, you can configure Security Console to send email reports and notifications using an external mail server instead of the built-in postfix mail server. If you do not specify any settings, Security Console uses the built-in mail server.
- **IP/ Hostname.** Enter the IP address or hostname of the mail server that is going to send the emails.
 - **Port.** Enter the port used to connect to the mail server.
 - **Username.** If the SMTP server requires authentication, enter a recognized username / email address.
 - **Password.** If the SMTP server requires authentication, enter the password of the previously specified user.
 - **Encryption.** If the SMTP server requires an encrypted connection, choose the appropriate type from the menu (SSL or TLS).
 - **From Name.** Enter the name that you want to appear in the From field of the email (sender's name).
 - **From Email.** Enter the email address that you want to appear in the From field of the email (sender's email address).
5. Under **Settings**, configure the account settings according to your preferences.
- **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.

6. Click **Submit** to save the changes.

2.6. Working with Table Data

Tables are frequently used throughout the console to organize data into an easy-to-use format. You may find this information useful:

- Tables can span several pages (only 10 entries are displayed per page by default). To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.
- To easily find what you are looking for, use the search boxes or the filtering options below the column headers.
- You can also click column headers to sort data by a specific column. Click the column header again to change the sorting order.


To make sure the latest information is being displayed, click the **Refresh** button in the bottom-left corner of the table.

3. Monitoring Dashboard

Each time you connect to Security Console, the **Dashboard** page is displayed automatically. The dashboard is a status page consisting of 7 portlets, which provide you with a quick security overview of all protected virtual machines.

Dashboard portlets display various security information using easy-to-read charts, thus allowing you to quickly identify any issues that might require your attention. Each dashboard portlet includes a detailed report in the background, accessible with just one click on the chart.

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  button on its title bar.

3.1. Dashboard Portlets

The dashboard consists of the following portlets:

Network Status

Provides you with detailed information on the overall network security status. Computers are grouped based on these criteria:

- Unmanaged computers do not have Security for Virtualized Environments protection installed and their security status cannot be assessed. Unmanaged computers are detected automatically by the Security for Virtualized Environments agents installed on protected virtual machines. They can represent not only virtual machines, but also physical computers (if they are connected to the virtual network).
- Offline computers normally have Security for Virtualized Environments protection installed, but there is no recent activity from Silent Agent. The security status of offline computers cannot be accurately assessed because status information is not current.
- Protected computers have Security for Virtualized Environments protection installed and no security risks have been detected.
- Vulnerable computers have Security for Virtualized Environments protection installed, but specific conditions prevent proper protection of the system. The report details show you which security aspects need to be addressed.

Computer Status

Provides you with various status information concerning the computers on which the Security for Virtualized Environments protection is installed.

- Protection update status
- Antimalware protection status
- License status
- Network activity status (online/offline)

You can apply filters by security aspect and status to find the information you are looking for.

Top 10 Most Infected Computers

Shows you the top 10 most infected computers in the network over a specific time period.

Top 10 Detected Malware

Shows you the top 10 malware threats detected in the network over a specific time period.

Malware Activity

Provides you with overall and per computer details about the malware threats detected in the network over a specific time period. You can see:

- Number of detections (files that have been found infected with malware)
- Number of infections solved (files that have been successfully disinfected or isolated in the local quarantine folder)
- Number of infections blocked (files that could not be disinfected, but to which access has been denied; for example, an infected file stored in some proprietary archive format)

Computer Malware Status

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

- Computers with no detections (no malware threat has been detected over the specified time period)
- Computers with resolved malware (all detected files have been successfully disinfected or isolated in the local quarantine folder)
- Computers with blocked malware (some of the detected files have been denied access to)

Notifications





This portlet, which by default is minimized, informs you of existing security risks in the virtualized environment. Notifications are also sent to you by email.

3.2. Managing Portlets

The dashboard is easy to configure based on individual preferences.

You can minimize portlets to focus on the information you are interested in. When you minimize a portlet, it is removed from the dashboard and its title bar appears at the bottom of the page. The remaining portlets are automatically resized to fit the screen. All minimized portlets can be restored at any time.

To manage a portlet, use the buttons on its title bar:

-  The refresh option will re-load data for each portlet.
-  Click this button to configure portlet options. Some portlets include data from a specific time period.
-  Minimize the portlet to the bottom of the page.
-  Restore a minimized portlet.

4. Using Reports

Security Console allows you to create and view centralized reports on the security status of the protected virtual machines. The reports can be used for multiple purposes, such as:

- Monitoring and ensuring compliance with the organization's security policies.
- Checking and assessing the security status of the virtual network.
- Identifying security issues, threats and vulnerabilities.
- Monitoring security incidents and malware activity.
- Providing upper management with easy-to-interpret data on VM 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 pie charts, tables and graphics, allowing you to quickly check the virtual network security status and identify security issues.

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

- Statistical data regarding all or groups of protected virtual machines.
- Detailed information for each protected virtual machine.
- The list of VMs that meet specific criteria (for example, those that have antimalware protection disabled).

All generated reports are available in Security Console for a default period of 90 days, but you can save them to your computer or email them. Available formats include Portable Document Format (PDF) and comma-separated values (CSV).

4.1. Available Report Types

This is the list of available report types:

Update Status

Shows you the update status of the Security for Virtualized Environments protection installed on selected computers. Using the available filters, you can easily find out which clients have updated or have not updated in a specific time period.

Computer Status

Provides you with various status information concerning selected computers on which Security for Virtualized Environments protection is installed.

- Protection update status
- License status

- Network activity status (online/offline)
- Antimalware protection status

You can apply filters by security aspect and status to find the information you are looking for.

Malware Activity

Provides you with overall and per computer details about the malware threats detected over a specific time period on selected computers. You can see:

- Number of detections (files that have been found infected with malware)
- Number of infections solved (files that have been successfully disinfected or isolated in the local quarantine folder)
- Number of infections blocked (files that could not be disinfected, but to which access has been denied; for example, an infected file stored in some proprietary archive format)

Protection Module Status

Informs you of the status of the antimalware protection on selected computers. The protection status can be Enabled or Disabled. The report details also provide information on the update status.

You can apply filters by status to find the information you are looking for.

Top 10 Most Infected Computers

Shows you the top 10 most infected computers over a specific time period from selected computers.

Top 10 Detected Malware

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

Network Status

Provides you with detailed information on the overall network security status. Computers are grouped based on these criteria:

- Unmanaged computers do not have Security for Virtualized Environments protection installed and their security status cannot be assessed. Unmanaged computers are detected automatically by the Security for Virtualized Environments agents installed on protected virtual machines. They can represent not only virtual machines, but also physical computers (if they are connected to the virtual network).
- Offline computers normally have Security for Virtualized Environments protection installed, but there is no recent activity from Silent Agent. The security status of offline computers cannot be accurately assessed because status information is not current.
- Protected computers have Security for Virtualized Environments protection installed and no security risks have been detected.

- Vulnerable computers have Security for Virtualized Environments protection installed, but specific conditions prevent proper protection of the system. The report details show you which security aspects need to be addressed.

Computer Malware Status

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

- Computers with no detections (no malware threat has been detected over the specified time period)
- Computers with resolved malware (all detected files have been successfully disinfected or isolated in the local quarantine folder)
- Computers with blocked malware (some of the detected files have been denied access to)

Executive

Allows you to export the charts from the dashboard portlets to a PDF file.

4.2. Creating Reports

To create a report:

1. Go to the **Reports > New Report** page.



Note

If you are on the **View Reports** or **Scheduled Reports** page, just click the **New** button located above the table.

2. Select the desired report type from the menu. For more information, refer to [“Available Report Types”](#) (p. 11).
3. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
4. Configure the report target. Select one of the available options and click the corresponding link to choose the groups or the individual virtual machines to be included in the report.
5. Configure report recurrence (schedule). You can choose to create the report immediately, daily, weekly (on a specific day of the week) or monthly (on a specific day of the month).
6. Configure the report options.
 - a. For most report types, when you create an immediate report, you must specify the reporting period. The report will only include data from the selected time period.
 - b. Several report types provide filtering options to help you easily find the information you are interested in. Use the filtering options to obtain only the desired information. For example, for an **Update Status** report you can choose to view only the list of

protected VMs that have updated (or, on the contrary, that have not updated) in the selected time period.



Note

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 selected information will be included in the PDF file. Full report details will only be available in CSV format.

- c. To receive the report by email, select the corresponding option.
7. Click **Generate** to create the report.
- If you have chosen to create an immediate report, it will be displayed on the [View Reports](#) page. The time required for reports to be created may vary depending on the number of managed VMs. Please wait for the requested report to be created. Once the report has been created, you can view the report by clicking its name.
 - If you have chosen to create a scheduled report, it will be displayed on the [Scheduled Reports](#) page.

4.3. Viewing and Managing Generated Reports

To view and manage generated reports, go to the **Reports > View Reports** page. This page is automatically displayed after creating an immediate report.



Note

Scheduled reports can be managed on the [Reports > Scheduled Reports](#) page.

You can see the generated reports and useful information about them:

- Report name and type.
- When the report was generated.

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

Each report is marked with one of the following icons to inform you whether the report is scheduled or not:

Indicates a one-time only report.

Indicates a scheduled report.

To make sure the latest information is being displayed, click the **Refresh** button in the bottom-left corner of the table.

4.3.1. Viewing Reports

To view a report:

1. Go to the **Reports > View Reports** page.
2. Click the name of the report you want to view. To easily find the report you are looking for, you can sort reports by name, type or creation time.

All reports consist of a Summary page and a Details page.

- The Summary page provides you with statistical data (pie charts and graphics) for all target VMs or groups. At the bottom of the page, you can see general information about the report, such as the reporting period (if applicable), report target etc.
- The Details page provides you with detailed information for each managed VM. For some reports, you may need to click a pie chart area on the Summary page in order to see details.

Use the tabs in the upper-left corner of the report to view the desired page.

4.3.2. Searching Report Details

The report details are displayed in a table that consists of several columns providing various information. The table can span several pages (only 10 entries are displayed per page by default). To browse through the details pages, use the buttons at the bottom of the table.

To easily find what you are looking for, use the search boxes or the filtering options below the column headers.

To sort report details by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

4.3.3. Saving Reports

By default, generated reports are available in Security Console for 90 days. After this period, they are deleted automatically.

If you need reports to be available for longer time periods, you can save them to your computer. The report summary and selected report information will be available in PDF format, whereas full report details will be available in CSV format.

To save the report you are viewing to your computer:

1. Click the **Export** button in the upper-right corner of the report page. A download window will appear.
2. Download the `.zip` archive to your computer. Depending on your browser settings, the file may be downloaded automatically to a default download location.

4.3.4. Printing Reports

To print a report, you must first save it to your computer.

4.3.5. Emailing Reports

To email the report you are viewing:

1. Click the **Email** button in the upper-right corner of the report page. A window will appear.
2. If you want to, you can change the report name.
3. Enter the email addresses of the people you want to send the report to, separating them by semicolons (;).
4. Click **Send Email**.

4.3.6. Automatic Deletion of Reports

By default, generated reports are available in Security Console for 90 days. After this period, they are deleted automatically.

To change the automatic deletion period for generated reports:

1. Go to the **Reports > View Reports** page.
2. Click the link at the bottom of the table.
3. Select the new period from the menu.
4. Click **OK**.

4.3.7. Deleting Reports

To delete a report:

1. Go to the **Reports > View Reports** page.
2. Select the report.
3. Click the **Delete** button located above the table.

4.4. Managing Scheduled Reports

When creating a report, you can choose to configure a schedule based on which the report will be automatically generated (at regular time intervals). Such reports are referred to as scheduled reports.

Generated reports will be available on the **Reports > View Reports** page for a default period of 90 days. They will also be emailed to you if you have selected this option.

To manage scheduled reports, go to the **Reports > Scheduled Reports** page. You can see all scheduled reports and useful information about them:

- Report name and type.
- Schedule based on which the report is automatically generated.
- When the report was last generated.

4.4.1. Viewing Last Report Generated

From the **Reports > Scheduled Reports** page, you can easily view the most recently generated report by clicking the link in the **Last Report Generated** column.

4.4.2. Renaming Scheduled Reports

Reports generated by a scheduled report are named after it. Renaming a scheduled report will not affect the reports generated previously.

To rename a scheduled report:

1. Go to the **Reports > Scheduled Reports** page.
2. Click the report name.
3. Change the report name in the corresponding field. 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.
4. Click **Submit** to save changes.

4.4.3. Editing Scheduled Reports

To change the settings of a scheduled report:

1. Go to the **Reports > Scheduled 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 target.** The selected option indicates the type of the current report target (either groups or individual virtual machines). Click the corresponding link to view the current report target. To change it, click any of the two links and select the groups or VMs to be included in the report.
 - **Report recurrence (schedule).** You can set the report to be automatically generated daily, weekly (on a specific day of the week) or monthly (on a specific day of the

month). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.

- **Report options.** You can choose to receive the report by email. 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 selected information will be included in the PDF file. Full report details will only be available in CSV format.

4. Click **Submit** to save changes.

4.4.4. Deleting Scheduled Reports

When a scheduled report is no longer needed, it is best to delete it. Deleting a scheduled report will not delete the reports it has generated automatically to that point.

To delete a scheduled report:

1. Go to the **Reports > Scheduled Reports** page.
2. Select the report.
3. Click the **Delete** button located above the table.

5. User Activity Log

Security Console logs all the operations and actions performed by users. Logged events include the following:

- Logging in and logging out
- Creating, editing, renaming, deleting user accounts
- Creating, editing, renaming, deleting policies
- Creating, editing, renaming, deleting reports
- Deleting, restoring quarantined files
- Deleting or moving computers between groups
- Creating, moving, renaming, deleting groups


To examine the user activity records, go to the **Log** page.

Recorded events are displayed in a table. The table columns provide you with useful information about the listed events:

- Name of the user who performed the action.
- Type of user account.
- Action that caused the event.
- Type of console object affected by the action.
- Specific object affected by the action.
- IP address the user connected from.
- Time when the event occurred.

To easily find what you are looking for, use the search boxes or the filtering options below the column headers. To sort events by a specific column, simply click the header of that column. Click the column header again to change the sorting order.

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

To make sure the latest information is being displayed, click the  **Refresh** button in the bottom-left corner of the table.

6. Getting Help

For any problems or questions concerning Security Console, contact an administrator.

Glossary

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

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.

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.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

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.

Guest Operating System

An isolated operating system that runs inside another operating system (the host) within a virtualized environment.

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".

Host Operating System

An operating system inside of which other operating systems (the guests) run by virtualization.

Hypervisor

A program that allows multiple operating systems to run concurrently on a single computer.

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.

Java applet

A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

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.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

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.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

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.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an e-mail 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 e-mail 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 e-mail.

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 e-mail 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.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

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.

Virtual appliance

A virtual machine image containing a pre-configured operating system and an application packaged together to facilitate the installation and configuration of the application in a virtualized environment.

Virtual machine

An isolated software environment that emulates a physical computer on which an operating system and applications can run.

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.

Virus definition

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.