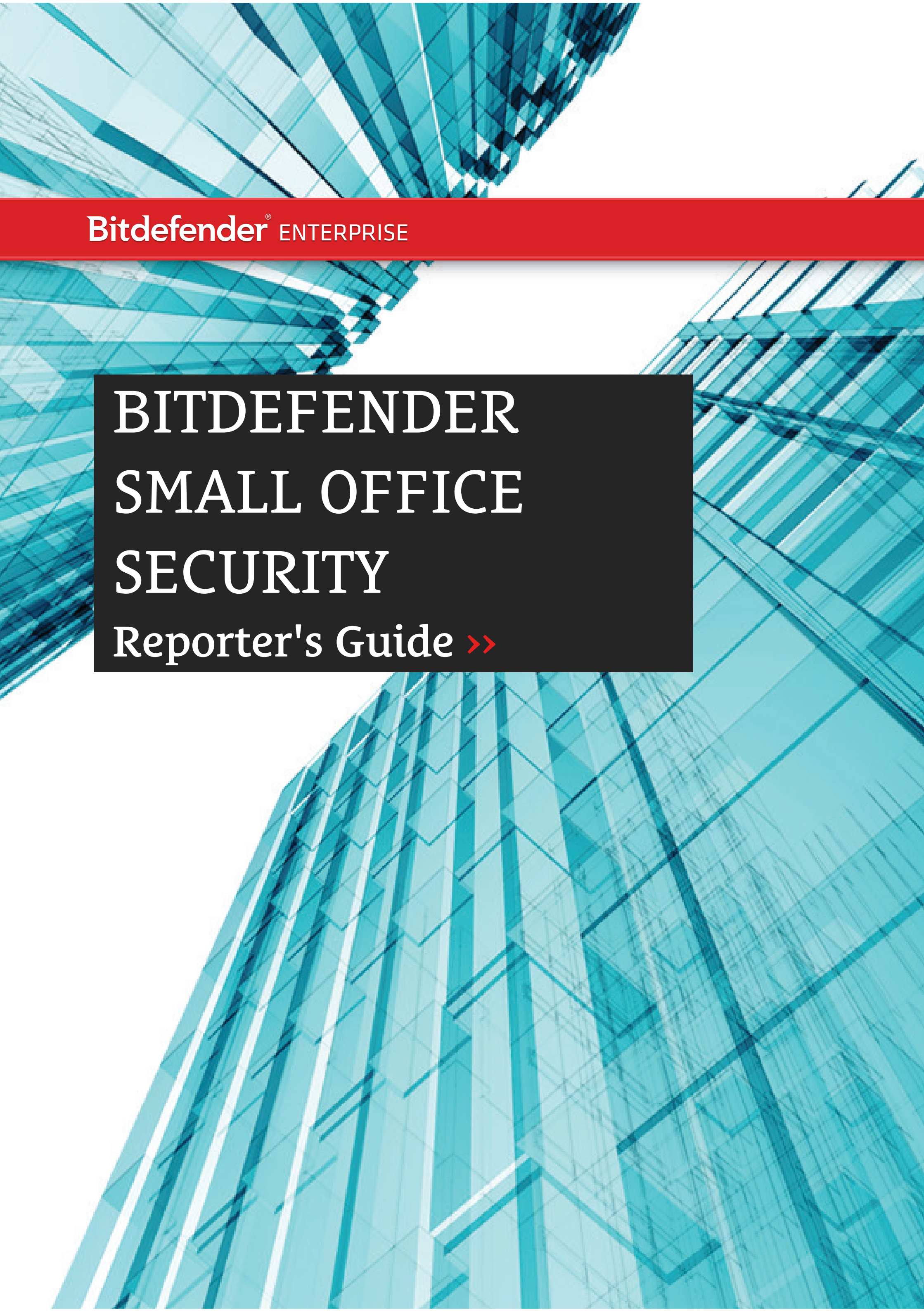


Bitdefender® ENTERPRISE

BITDEFENDER SMALL OFFICE SECURITY

Reporter's Guide ››

Bitdefender Small Office Security Reporter's Guide

Publication date 2014.06.10

Legal Notice

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.

Bitdefender®

Table of Contents

1. About Small Office Security

Small Office Security on-premise allows organizations to host security in their own infrastructure and easily deploy, administer and monitor protection for PC and Mac desktops and file servers, featuring leading antimalware detection as well as the latest administration console developed by Bitdefender.

Unlike the cloud-managed version which is hosted by Bitdefender and requires no onsite infrastructure, the Small Office Security version is deployed in the customer's own environment.

Small Office Security includes the following components:

- Control Center
- Security for Endpoints
- Security for Mobile Devices

Control Center

A web-based dashboard and unified management console that provides full visibility into organization's overall security posture, global security threats, and control over its security services that protects desktops and servers.

Control Center integrates with the existing system management and monitoring systems to make it simple to automatically apply protection to unmanaged desktops and servers.

Security for Endpoints

Bitdefender Security for Endpoints unobtrusively protects computers by using number-one-ranked antimalware technology combined with firewall, intrusion detection, web access control and filtering, sensitive data protection and application control. Security for Endpoints offers protection for computers and laptops running on Windows and Mac OS X operating systems and Windows servers. Employee productivity is ensured with low resource consumption, optimized system scanning and automated security that requires no end-user interaction.

Security for Mobile Devices

Manages and controls iPhone, iPad and Android devices with a unified enterprise-grade management that keeps the device safe with real-time scanning and enforces organization's security policies on mobile devices to lock screen, require authentication, encrypt removable media, locate lost devices and deny non-compliant or jailbroken devices accessing corporate services.

2. Getting Started

Bitdefender Small Office Security 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:

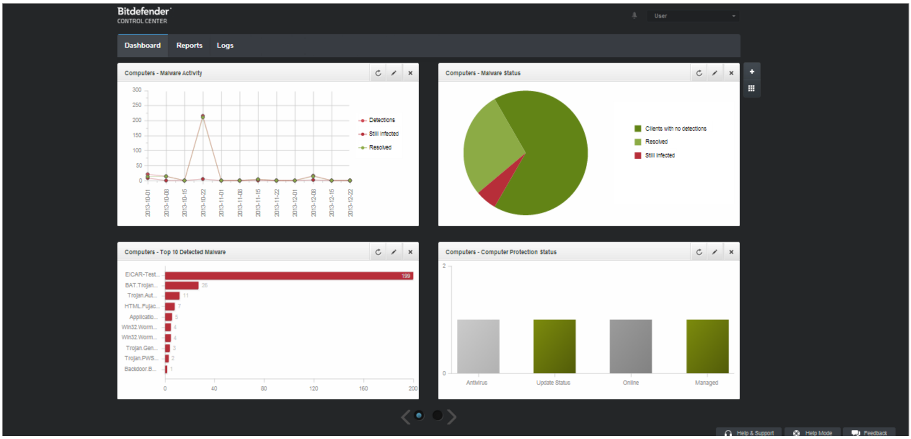
- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Recommended screen resolution: 1024x768 or higher

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.

Logs
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:

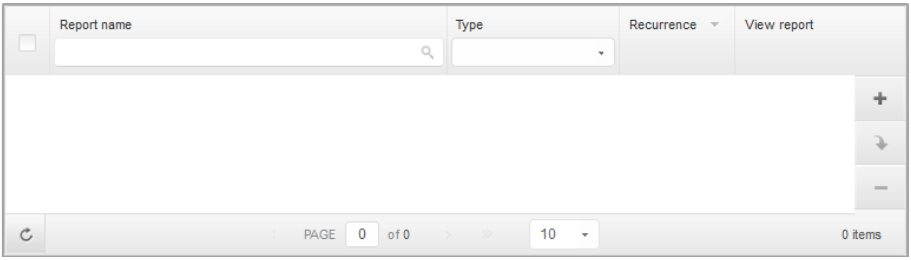
- **My Account**. Click this option to manage your user account details and preferences.
- **Logout**. Click this option to log out of your account.

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 Small Office Security.

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 10 entries span on several pages. By default, only 10 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.

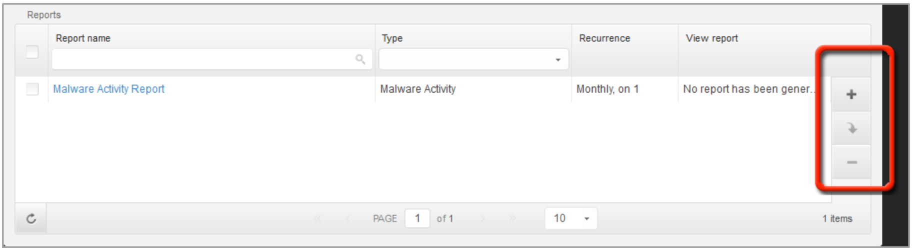
Refreshing Table Data

To make sure the console displays the latest information, click the ↻ **Refresh** button in the bottom-left corner of the table.

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 to the right 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 reports generated by a scheduled report.
- Delete a scheduled report.



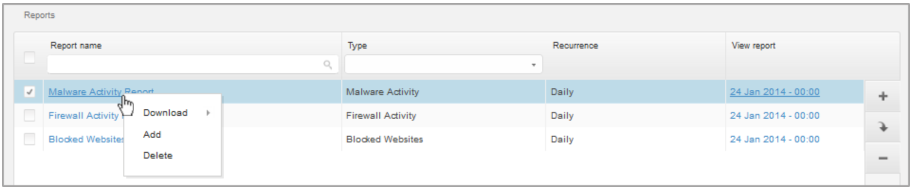
Reports

Report name	Type	Recurrence	View report
Malware Activity Report	Malware Activity	Monthly, on 1	No report has been gener...

The Reports page - Action Toolbars

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.



Reports

Report name	Type	Recurrence	View report
Malware Activity Report	Malware Activity	Daily	24 Jan 2014 - 00:00
Firewall Activity	Firewall Activity	Daily	24 Jan 2014 - 00:00
Blocked Websites	Blocked Websites	Daily	24 Jan 2014 - 00:00

The Reports page - Contextual menu

2.2.4. Service Selector

As administrator or reporter, you can manage the Control Center services one at a time. Select the service you want to work with from the **services menu** in the upper-right corner of the page.

Note

The services menu is available only in the pages where it makes sense to filter data by service type.

The services menu contains the following options:

- **Computers** (Security for Endpoints)
- **Mobile Devices** (Security for Mobile Devices)

Note
You will see only the services 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.

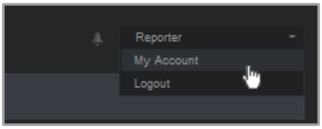
To change the login password:

1. Point to 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 save the changes.

2.4. Managing Your Account

To check or change your account details and settings:

1. Point to 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.
   - **Password.** A **Change password** link allows you to change your login password.

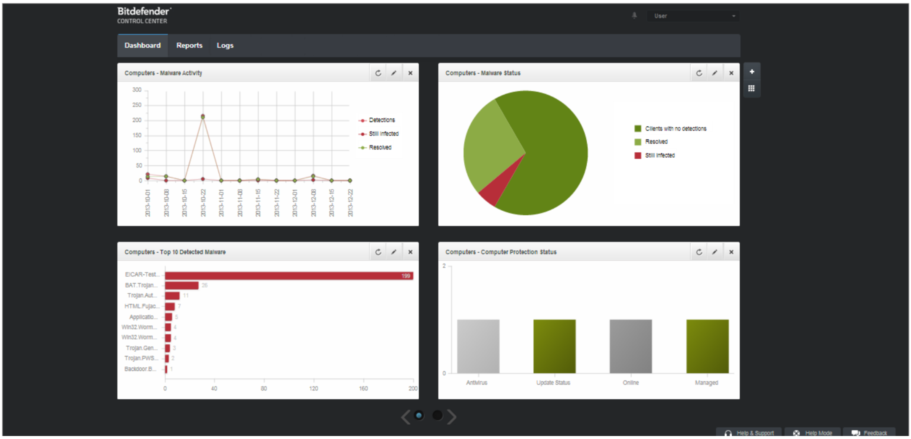
3. Under **Settings**, configure the account settings according to your preferences.
   - **Timezone.** Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
   - **Language.** Choose from the menu the console display language.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

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 for each Small Office Security security service.
- 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 network objects protection, such as update status, malware status, firewall activity etc. For more information on dashboard portlets types, refer to "Available Report Types" (p. 16).
- The information displayed by portlets refers only to the network objects under your account. You can customize the target of each portlet 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 slider at the bottom of the page to navigate between portlet groups.

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 additional 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 right side of the dashboard. The configuration window is displayed.
3. Under the **Details** tab, configure the portlet details:
   - Security service (**Computers** or **Mobile Devices**)
   - Type of background report
   - Suggestive portlet name
   - Update interval

   For more information on available report types, refer to "Available Report Types" (p. 16).
4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

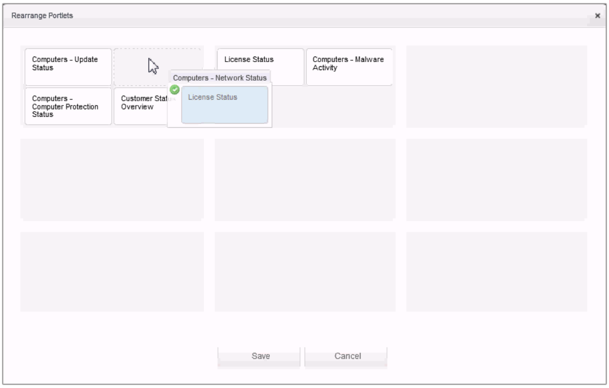
3.4. Removing a Portlet

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:

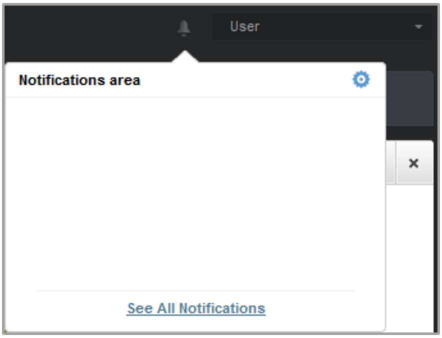
1. Go to the **Dashboard** page.
2. Click the **Rearrange Portlets** button at the right side of the dashboard. The portlet map window is displayed.
3. Drag and drop each portlet to the desired position.
4. Click **Save**.


Rearrange Portlets
×
Computers - Update Status
License Status
Computers - Malware Activity
Computers - Network Status
Computers - Computer Protection Status
Customer Stat Overview
License Status
Save
Cancel

Rearrange dashboard portlets

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 a new event is detected in the network, the notification area will display a 🔔5 red icon indicating 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.

Update Available
Informs you of the availability of a new Small Office Security update.

License Expires
This notification is sent 30 and 7 days before the license expires, as well as the day the license expires.

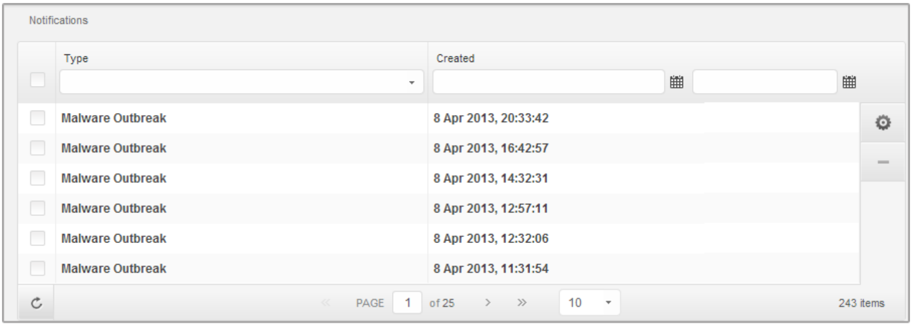
License Limit Is About To Be Reached
This notification is sent when 90% of the available licenses have been used.

License Usage Limit Has Been Reached

This notification is sent when all of the available licenses have been used.

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.



Notifications

□	Type	Created
□	Malware Outbreak	8 Apr 2013, 20:33:42
□	Malware Outbreak	8 Apr 2013, 16:42:57
□	Malware Outbreak	8 Apr 2013, 14:32:31
□	Malware Outbreak	8 Apr 2013, 12:57:11
□	Malware Outbreak	8 Apr 2013, 12:32:06
□	Malware Outbreak	8 Apr 2013, 11:31:54

PAGE 1 of 25 10 243 items

The Notifications page

Depending on the number of notifications, the notifications table 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.

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. For example, you can search for a specific type of notification or choose to view only the notifications generated in a specific time interval.

- 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:

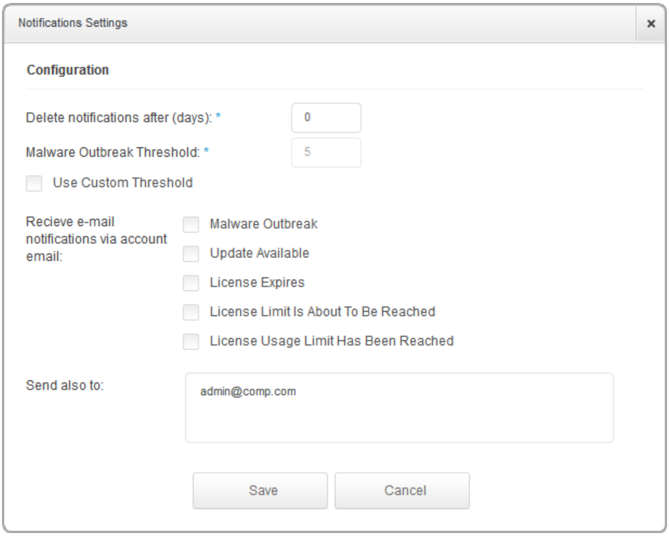
1. Click the 🔔 **Notification Area** button at the right side of the menu bar and then click **See All Notifications**. A table containing all the notifications is displayed.
2. Select the notifications you want to delete.
3. Click the − **Delete** button at the right side of the table.

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 right side of the table. The **Notification Settings** window is displayed.



Delete notifications after (days): * 0

Malware Outbreak Threshold: * 5

□ Use Custom Threshold

Recieve e-mail notifications via account email:
□ Malware Outbreak
□ Update Available
□ License Expires
□ License Limit Is About To Be Reached
□ License Usage Limit Has Been Reached

Send also to: admin@comp.com

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. Select the desired notification types from the list. For more information, refer to "Notification Types" (p. 12)

4. 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.
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).

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 security service:

- Computer Reports
- Mobile Device Reports

5.1.1. Computer Reports

This is the list of available report types for computers:

Update Status

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

Using the available filters, you can easily find out which clients have updated or have not updated in a specific time period.

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 moved to quarantine)
- Computers still infected with malware (some of the detected files have been denied access to)

Malware Activity

Provides you with overall information 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 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)

Network Status

Provides you with detailed information on the overall security status of selected computers. Computers 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 computer(online/offline). If the computer is offline when the report is generated, you will see the date and time when it was last seen online by Control Center.

Computer Protection Status

Provides you with various status information concerning selected computers from your network.

- Antimalware protection status
- Endpoint Security 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.

Top 10 Infected Computers

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

> **Note**
> The details table displays all malware detected on the top 10 infected computers.

Top 10 Detected Malware

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

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

Firewall Activity

Informs you about the status of the Firewall module of Endpoint Security. You can see the number of blocked traffic attempts and blocked port scans on the selected computers.

Blocked Websites

Informs you about the status of the Web Control module of Endpoint Security. You can see the number of blocked websites on the selected computers.

Blocked Applications

Informs you about the status of the Application Control module of Endpoint Security. You can see the number of blocked applications on the selected computers.

Data Protection

Informs you about the status of the Data Protection module of Endpoint Security. You can see the number of blocked emails and websites on the selected computers.

Antiphishing Activity

Informs you about the status of the Antiphishing module of the Endpoint Security. You can see the number of blocked websites on the selected computers.

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 computer. Click the number of blocked applications for the computer 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).

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

5.2. Creating Reports

You can create two categories of reports:

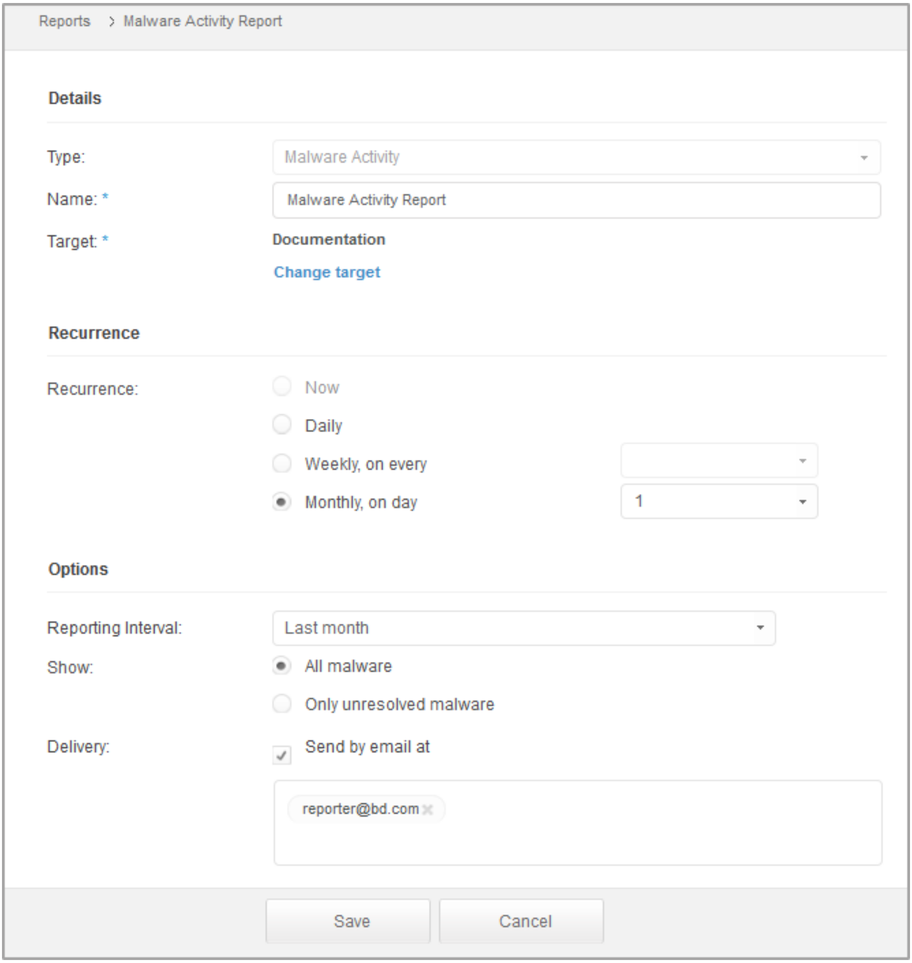
- **Instant reports.** Instant reports are automatically displayed after you generate them.
- **Scheduled reports.** Scheduled reports can be configured to run at a specified time and date and a list of all the scheduled reports is displayed in the **Reports** page.

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 desired network objects type from the service selector.
3. Click the + **Add** button at the right side of the table.



Reports > Malware Activity Report

Details

Type: Malware Activity

Name: * Malware Activity Report

Target: * **Documentation**

Change target

Recurrence

Recurrence:
○ Now
○ Daily
○ Weekly, on every
● Monthly, on day 1

Options

Reporting Interval: Last month

Show:
● All malware
○ Only unresolved malware

Delivery: ☑ Send by email at

reporter@bd.com

Computer Reports Options

4. Select the desired report type from the menu.
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 target by clicking the **Change target** link. Select the group you want to run the report on.
7. Configure report recurrence (schedule). You can choose to create the report immediately (instant report), or schedule it to run daily, weekly (on a specific day of the week) or monthly (on a specific day of the month).

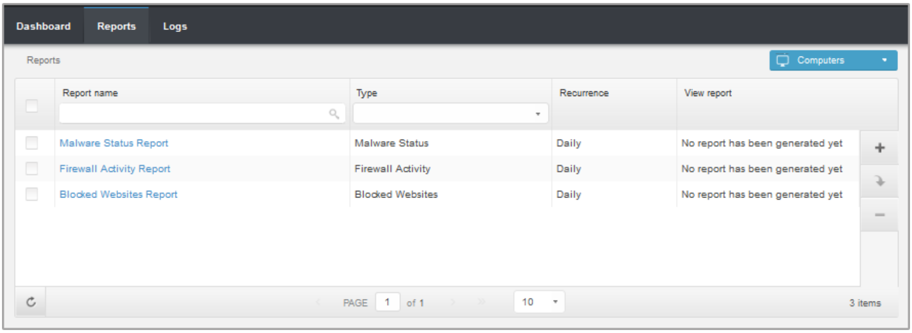
   Note
   Scheduled reports are generated on the due date immediately after 00:00 UTC (default timezone of the GravityZone appliance).

8. Configure the report options.
   a. For most report types you must specify the update interval. 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 computers that have updated (or, on the contrary, that have not updated) in the selected time period or the ones that need to be restarted to complete the update.
   c. To receive a scheduled report by email, select the corresponding option.
9. Click **Generate** to create an instant report or **Save** to create a scheduled report. The **Save** button will change to **Generate** if you choose to create an instant report.
   - If you have chosen to create an instant report, it will be displayed immediately after clicking **Generate**. The time required for reports to be created may vary depending on the number of managed computers. Please wait for the requested report to be created.
   - If you have chosen to create a scheduled report, it will be displayed in the list on the **Reports** page. Once the report has been created, you can view the report by clicking its 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.



	Report name	Type	Recurrence	View report
□	Malware Status Report	Malware Status	Daily	No report has been generated yet
□	Firewall Activity Report	Firewall Activity	Daily	No report has been generated yet
□	Blocked Websites Report	Blocked Websites	Daily	No report has been generated yet

The Reports page

All scheduled reports are displayed in a table. You can see the generated scheduled reports and useful information about them:

- Report name and type.
- When the report will be generated.

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.

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.

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** icon in the bottom-left corner 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.

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 or groups as well as general information about the report, such as the reporting period (if applicable), report target etc.
- The details section provides you with detailed information for each managed 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 you are interested in to view related details in the table placed below the chart.

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 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.
   - **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.** The report will only include data from the selected update interval. You can change the interval starting with the next recurrence. 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 the selected information will be included in the PDF file. Report details will only be available in CSV format.

4. Click **Save** to save 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 reports 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 right side of the table.

5.4. 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.

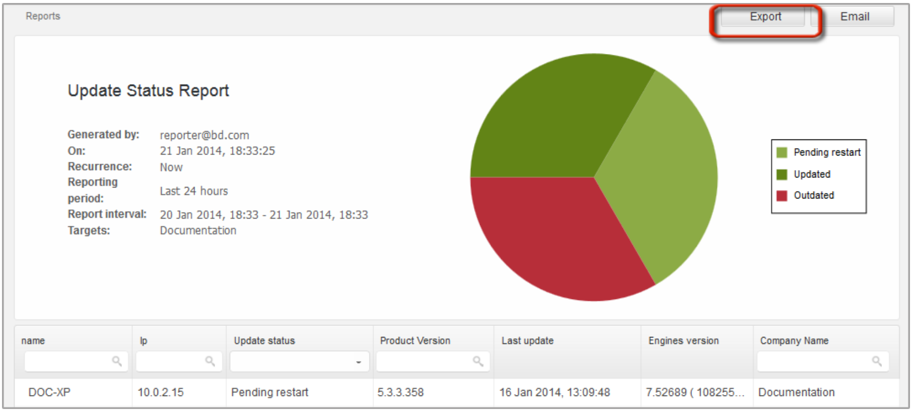
You have two ways of saving reports:

- Export
- Download

5.4.1. Exporting Reports

To export the report to your computer:

1. Click the **Export** button in the upper-right corner of the report page.



Update Status Report

Generated by:	reporter@bd.com
On:	21 Jan 2014, 18:33:25
Recurrence:	Now
Reporting period:	Last 24 hours
Report interval:	20 Jan 2014, 18:33 - 21 Jan 2014, 18:33
Targets:	Documentation

name	Ip	Update status	Product Version	Last update	Engines version	Company Name
DOC-XP	10.0.2.15	Pending restart	5.3.3.358	16 Jan 2014, 13:09:48	7.52689 (108255...	Documentation

Reports - Export option

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.

5.4.2. 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.

5.5. 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 upper-right 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.

5.6. Printing Reports

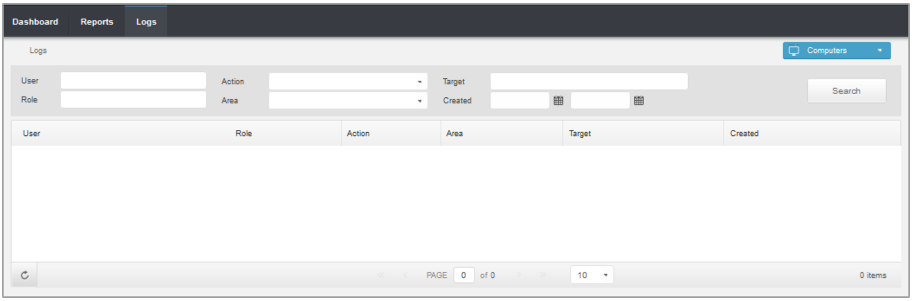
Control Center does not currently support print button functionality. To print a report, you must first save it to your computer.

6. User Activity Log

Control Center logs all the operations and actions performed by users. Logs list include 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 **Logs** page and choose the desired network object from the service selector.



The Logs 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.

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

7. Getting Help

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

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.