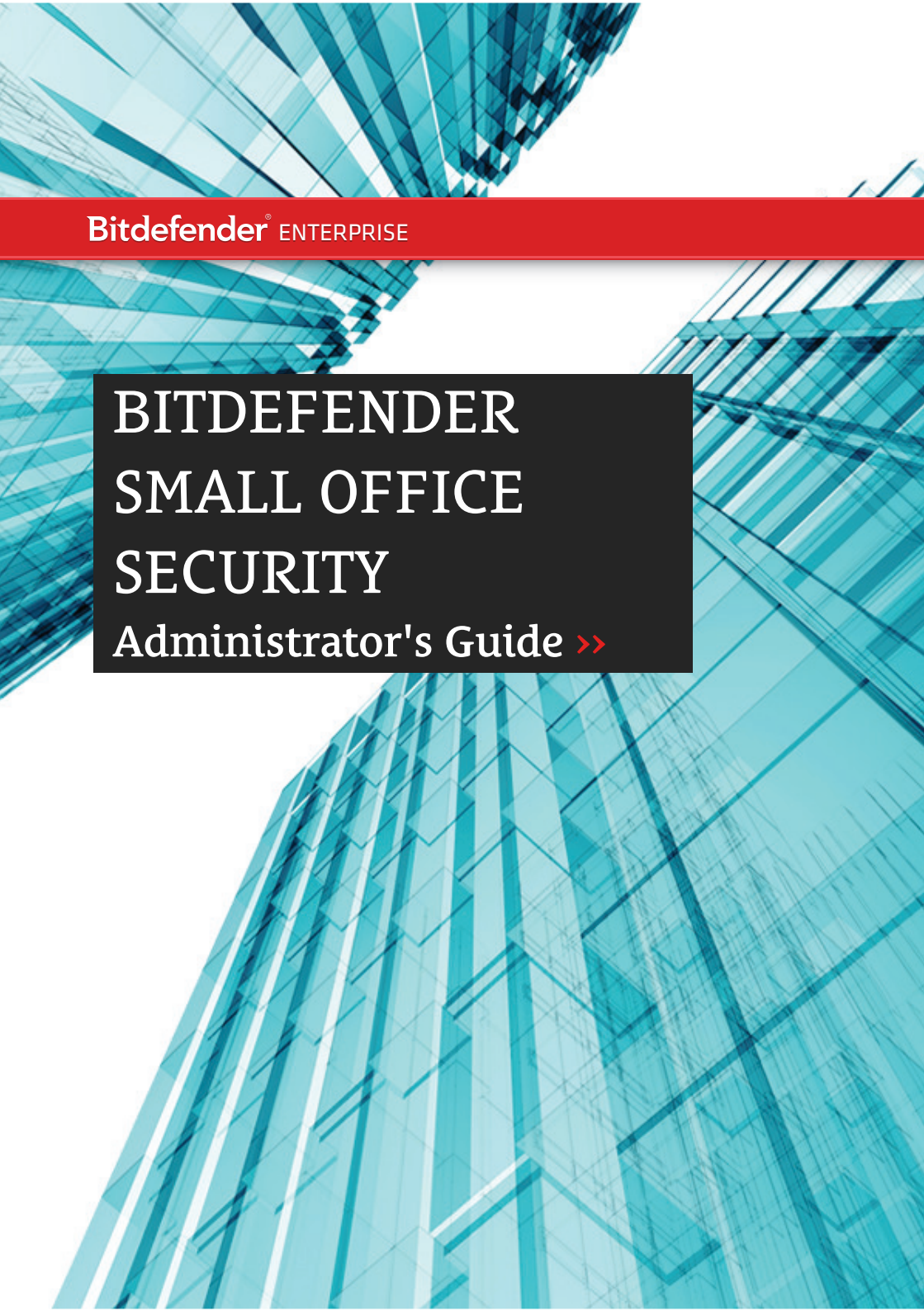

Bitdefender® ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Administrator's Guide ››

Bitdefender Small Office Security Administrator's Guide

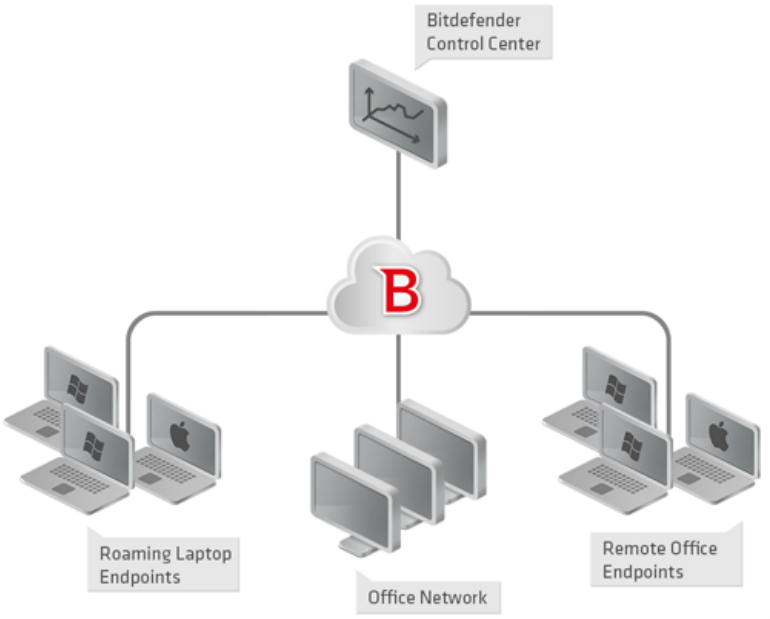
Publication date 2015.01.21


Bitdefender

Table of Contents

1. About Small Office Security

Small Office Security is a cloud-based malware protection service developed by Bitdefender for computers running Microsoft Windows and Macintosh operating systems. It uses a centralized Software-as-a-Service multiple deployment model suitable for enterprise customers, while leveraging field-proven malware protection technologies developed by Bitdefender for the consumer market.



Small Office Security Architecture

The security service is hosted on Bitdefender's public cloud. Subscribers have access to a Web-based management interface called **Control Center**. From this interface, administrators can remotely install and manage malware protection on all their Windows and Macintosh-based computers such as: servers and workstations within the internal network, roaming laptop endpoints or remote office endpoints.

A local application called **Endpoint Security** is installed on each protected computer. Local users have limited visibility and read-only access to the security settings, which are centrally managed by the administrator from the Control Center; while scans, updates and configuration changes are commonly performed in the background.

2. Getting Started

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

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

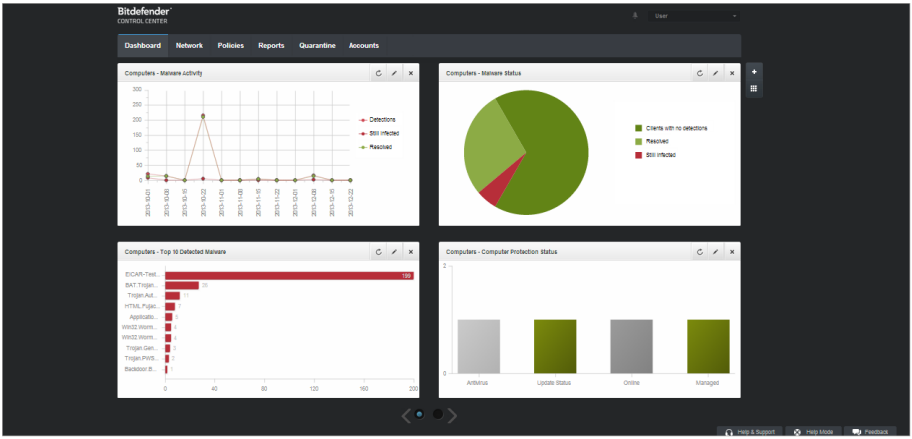
To connect to Control Center:

1. Open your web browser.
2. Go to the following address: https://gravityzone.bitdefender.com
3. Enter the email address and password of your account.
4. 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.

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. Available features depend on the type of user accessing the console.



The Dashboard

2.2.1. Control Center Overview

Users with company administrator role have full privileges over the Control Center configuration and network security settings, while users with administrator role have access to network security features, including users management.

According to their role, Small Office Security administrators can access the following sections from the menu bar:

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

Network
Install protection, apply policies to manage security settings, run tasks remotely and create quick reports.

Policies
Create and manage security policies.

Reports
Get security reports concerning the managed clients.

Quarantine
Remotely manage quarantined files.

Accounts

Manage the access to Control Center for other company employees.

Note

This menu is available only to users with Manage Users right.

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:

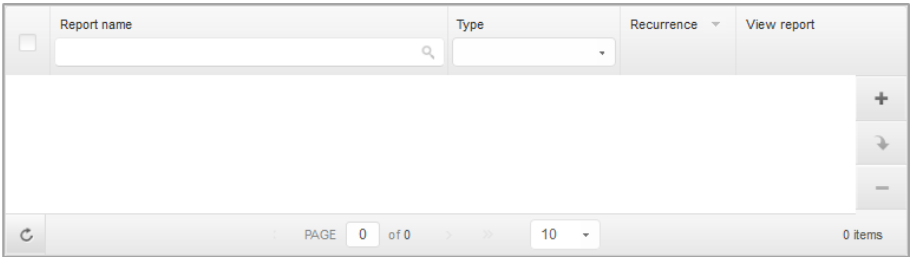
- **My Account**. Click this option to manage your user account details and preferences.
- **My Company**. Click this option to manage your company account details and preferences.
- **Credentials Manager**. Click this option to add and manage the authentication credentials required for remote installation tasks.
- **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 features.
- **Feedback**. Click this button to display a form allowing you to edit and send your feedback messages regarding your experience with Small Office Security.

2.2.2. 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.

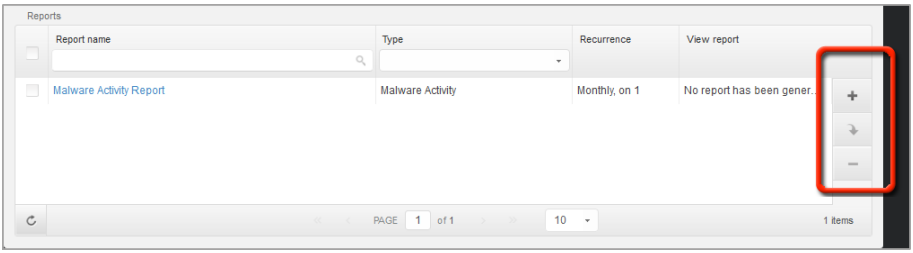
Refreshing Table Data

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

2.2.3. Action Toolbars

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

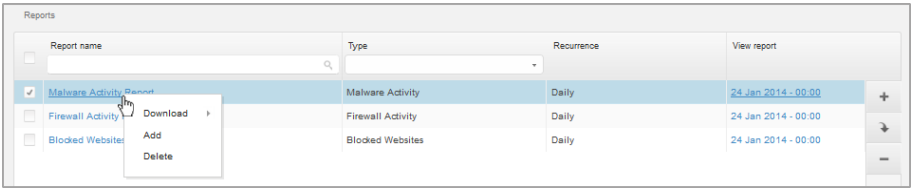
- Create a new report.
- Download reports generated by a scheduled report.
- Delete a scheduled report.



The Reports page - Action Toolbars

2.2.4. Contextual Menu

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

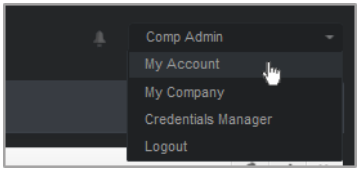


The Reports page - Contextual menu

2.3. 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

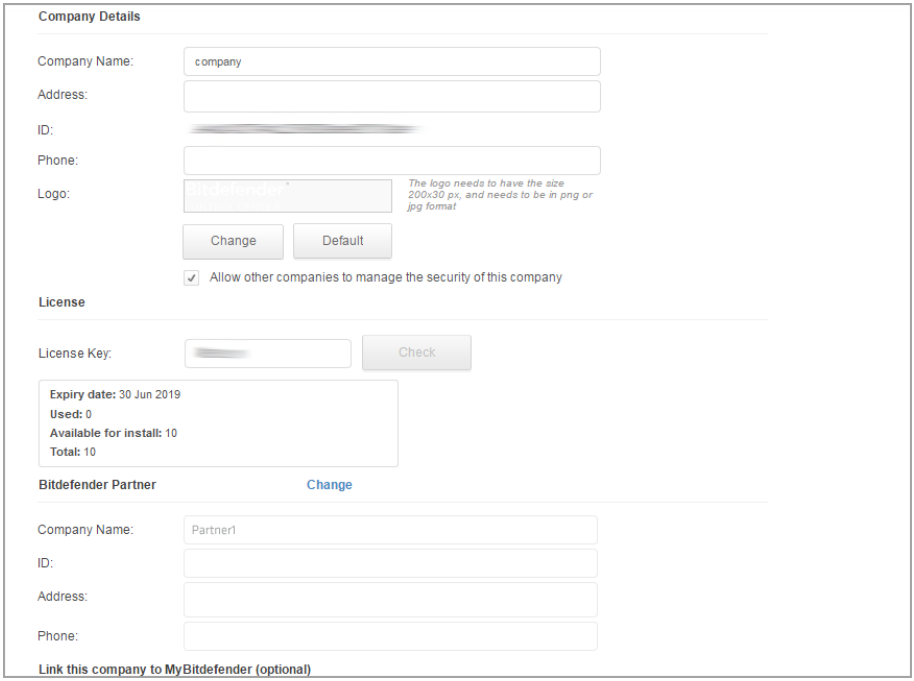
2. Under **Account Details**, correct or update your account details.
   - **Full name.** Enter your full name.
   - **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important 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 apply the changes.

Note
You cannot delete your own account.

2.4. Managing Your Company

As user with Company Administrator role, you can check or change your company details and license settings:

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



My Company Page

2. Under **Company Details**, fill in your company information, such as company name, address and phone.
3. You can change the logo displayed in Control Center and also in your company's reports and email notifications as follows:
   - Click **Change** to browse for the image logo on your computer. The image file format must be .png or .jpg and the image size must be 200x30 pixels.
   - Click **Default** to delete the image and reset to the image provided by Bitdefender.

4. By default, your company can be managed by other companies' partner accounts that may have your company listed in their Bitdefender Control Center. You can block the access of these companies to your network by disabling the option **Allow other companies to manage the security of this company**. As a result, your network will no longer be visible in other companies' Control Center and they will no longer be able to manage your subscription.
5. Under **License** section you can view and modify your license details.
   - To add a new license key:
     a. From the **Type menu**, choose a **License** subscription type.
     b. Enter the key in the **License key** field.
     c. Click the **Check** button and wait until Control Center retrieves information about the entered license key.
   - To check your license key's details, view the information displayed below the license key:
     – **Expiry date**: the date until the license key can be used.
     – **Used**: the number of used seats from the total amount of seats on the license key. A license seat is used when the Bitdefender client has been installed on an endpoint from the network under your management.
     – **Available for install**: the number of free seats from the total number of seats on a monthly license pool (excluding used seats).
     – **Total**: the total number of license seats available for your subscription.
6. Under **Bitdefender Partner** you can find information about your service provider company.
   To change your managed service provider:
   a. Click the **Change** button.
   b. Enter the partner's company ID code in the **Partner ID** field.

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

   c. Click **Save**.

   As a result, your company is automatically moved from the previous partner to the new partner's Control Center.
7. Optionally, you can link your company with your MyBitdefender account using the provided fields.
8. Click **Save** to apply the changes.

2.5. Changing Login Password

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

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

To change the login password:

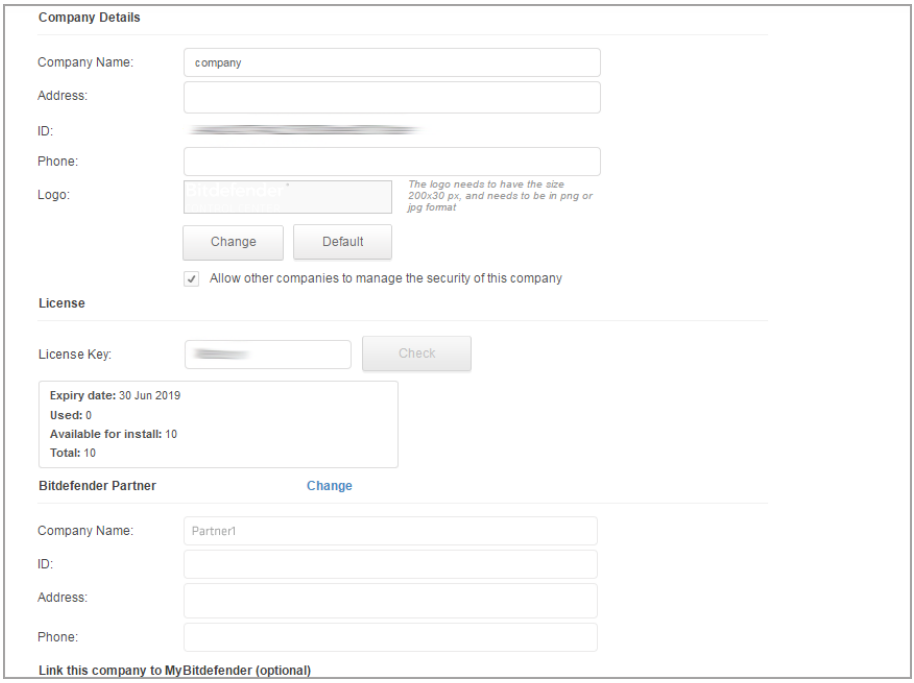
1. Point to your username in the upper-right corner of the console and choose **My Account**.
2. Under **Account Details**, click **Change password**.
3. Enter your current password and the new password in the corresponding fields.
4. Click **Save** to apply the changes.

3. Managing User Accounts

The Security for Endpoints service can be set up and managed from Control Center using the account received after subscribing to the service.

This is what you need to know about Small Office Security user accounts:

- To allow other employees of the company to access Control Center, you can create internal user accounts. You can assign user accounts with different roles, according to their access level in the company.
- For each user account, you can customize the access to Small Office Security features or to specific parts of the network it belongs to.
- All accounts with the **Manage Users** right can create, edit and delete other user accounts.
- You can only manage accounts with equal privileges as your account, or lesser.
- You can create and manage user accounts in the **Accounts** page.



The Accounts page

Existing accounts are displayed in the table. For each user account, you can view:

- The username of the account (used to log in to Control Center).
- Email address of the account (used as a contact address). Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
- User role (partner / company administrator / network administrator / reporter / custom).

3.1. User Roles

A user role consists in a specific combination of user rights. When creating a user account, you can choose one of the predefined roles or you can create a custom role, by selecting certain user rights only.

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

The following user roles are available:

1. **Company Administrator** - Suited for managers of customer companies that have purchased a Small Office Security license from a partner. A company administrator manages the license, the company's profile and its entire Small Office Security deployment, allowing top-level control over all security settings (unless overridden by its parent partner account in a security service provider scenario). Company administrators can share or delegate their operational responsibilities to subordinate administrator and reporter user accounts.
2. **Network Administrator** - Several accounts with Network Administrator role can be created for a company, with administrative privileges over the company's entire Security for Endpoints deployment or over a specific group of computers, including user management. Network Administrators are responsible for actively managing the network security settings.
3. **Reporter** - Reporter accounts are internal read-only accounts. They only allow access to reports and logs. Such accounts can be allocated to personnel with monitoring responsibilities or to other employees who must be kept up-to-date with security status.
4. **Custom** - Predefined user roles include a certain combination of user rights. If a predefined user role does not fit your needs, you can create a custom account by selecting only the rights that you are interested in.

The following table summarizes the relationships between different account roles and their rights. For detailed information, refer to “User Rights” (p. 12).

Account Role	Allowed Child Accounts	User Rights
Company Administrator	Company Administrators, Network Administrators, Reporters	Manage Company Manage Users Manage Networks Manage Reports
Network Administrator	Network Administrators, Reporters	Manage Users Manage Networks Manage Reports
Reporter	-	Manage Reports

3.2. User Rights

You can assign the following user rights to Small Office Security user accounts:

- **Manage Users**. Create, edit or delete user accounts.
- **Manage Company**. Users can manage their own Small Office Security license key and edit their company profile settings. This privilege is specific to company administrator accounts.
- **Manage Networks**. Provides administrative privileges over the network security settings (network inventory, policies, tasks, installation packages, quarantine). This privilege is specific to network administrator accounts.
- **Manage Reports**. Create, edit, delete reports and manage dashboard.

3.3. Creating User Accounts

Before creating a user account, make sure you have the required email address at hand. This address is mandatory for creating the Small Office Security user account. Users will receive their Small Office Security login details at the supplied email address. Users will also use the email address to login to Small Office Security.

To create a user account:

1. Go to the **Accounts** page.
2. Click the + **Add** button at the right side of the table. A configuration window is displayed.
3. Under the **Details** section, fill in the account details.
    - **Email**. Enter the user's email address. Login information will be sent to this address immediately after creating the account.

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

- **Full Name**. Enter the full name of the account owner.

4. Under the **Settings and Privileges** section, configure the following settings:
   - **Timezone**. Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
   - **Language**. Choose from the menu the console display language.
   - **Role**. Select the user's role. For details regarding the user roles, refer to “User Roles” (p. 11).
   - **Rights**. Each predefined user role has a certain configuration of rights. However, you can select only the rights that you need. In this case, the user role changes to **Custom**. For details regarding the user rights, refer to “User Rights” (p. 12).
   - **Select Targets**. Scroll down the configuration window to display the targets section. Select the network groups the user will have access to. You can restrict the user access to specific network areas.
5. Click **Save** to add the user. The new account will appear in the user accounts list.

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

3.4. Editing Accounts

Edit accounts to keep account details up to date or to change account settings.

To edit a user account:

1. Log in to Control Center.
2. Go to the **Accounts** page.
3. Click the user's name.
4. Change account details and settings as needed.
5. Click **Save** to apply the changes.

Note
All accounts with the **Manage Users** right can create, edit and delete other user accounts. You can only manage accounts with equal privileges as your own account, or lesser.

3.5. Deleting Accounts

Delete accounts when they are no longer needed. For example, if the account owner is no longer with the company.

To delete an account:

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

3.6. Resetting Login Passwords

Accounts owners who forget their password can reset it by using the password recovery link on the login page. You can also reset a forgotten login password by editing the corresponding account from the console.

To reset the login password for a user:

1. Log in to Control Center.
2. Go to the **Accounts** page.
3. Click the user's name.
4. Type a new password in the corresponding fields (under **Details**).
5. Click **Save** to apply the changes. The account owner will receive an email with the new password.

4. Installing Security for Endpoints

Security for Endpoints is intended for computers and laptops running on Windows and Mac OS X operating systems and Windows servers. To protect your physical computers with Security for Endpoints, you must install Endpoint Security (the client software) on each of them. Endpoint Security manages protection on the local computer. It also communicates with Control Center to receive the administrator's commands and to send the results of its actions.

You can install Endpoint Security with one of the following roles (available in the installation wizard):

1. **Endpoint**, when the corresponding computer is a regular endpoint in the network.
2. **Endpoint Security Relay**, when the corresponding computer is used by other endpoints in the network to communicate with Control Center. Endpoint Security Relay role installs Endpoint Security together with an update server, which can be used to update all the other clients in the network. Endpoints in the same network can be configured via policy to communicate with Control Center through one or several computers with Endpoint Security Relay role. Thus, when an Endpoint Security Relay is unavailable, the next one is taken into account to assure the computer's communication with Control Center.

Warning

- The first computer on which you install protection must have Endpoint Security Relay role, otherwise you will not be able to deploy Endpoint Security on other computers in the network.
- The computer with Endpoint Security Relay role must be powered-on and online in order for the clients to communicate with Control Center.

You can install Endpoint Security on computers by running installation packages locally or by running installation tasks remotely from Control Center.

It is very important to carefully read and follow the instructions to prepare for installation.

Endpoint Security has a minimal user interface. It only allows users to check protection status and run basic security tasks (updates and scans), without providing access to settings.

By default, the display language of the user interface on protected computers is set at installation time based on the language of your account.

To install the user interface in another language on certain computers, you can create an installation package and set the preferred language in the package configuration options. For more information on creating installation packages, refer to “Creating Endpoint Security Installation Packages” (p. 19).

4.1. System Requirements

4.1.1. Supported Operating Systems

Security for Endpoints currently protects the following operating systems:

Workstation operating systems:

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista with Service Pack 1
- Windows XP with Service Pack 2 64 bit
- Windows XP with Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

Tablet and embedded operating systems:

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded with Service Pack 2*
- Windows XP Tablet PC Edition*

*Specific operating system modules must be installed for Security for Endpoints to work.

Server operating systems:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 with Service Pack 1
- Windows Home Server

4.1.2. Hardware Requirements

- Intel® Pentium compatible processor:

  Workstation Operating Systems
  - 1 GHz or faster for Microsoft Windows XP SP3, Windows XP SP2 64 bit and Windows 7 Enterprise (32 and 64 bit)
  - 2 GHz or faster for Microsoft Windows Vista SP1 or higher (32 and 64 bit), Microsoft Windows 7 (32 and 64 bit), Microsoft Windows 7 SP1 (32 and 64bit), Windows 8
  - 800 MHZ or faster for Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded with Service Pack 2, Microsoft Windows XP Tablet PC Edition

  Server Operating Systems
  - Minimum: 2.4 GHz single-core CPU
  - Recommended: 1.86 GHz or faster Intel Xeon multi-core CPU
- **Free RAM memory**:
  - For Windows: 512 MB minimum, 1 GB recommended
  - For Mac: 1 GB minimum
- **HDD space**:
  - 1.5 GB of free hard-disk space

Note
At least 6 GB free disk space is required for entities with Endpoint Security Relay role, as they will store all updates and installation packages.

4.1.3. Supported Browsers

Endpoint browser security is verified to be working with the following browsers:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

4.1.4. Small Office Security Communication Ports

The following table provides information on the ports used by the Small Office Security components:

Port	Usage
80 (HTTP) / 443 (HTTPS)	Port used to access the Control Center web console.

Port	Usage
80	Update Server port.
8443 (HTTPS)	Port used by client/agent software to connect to the Communication Server.
7074 (HTTP)	Communication with Endpoint Security Relay (if available)

For detailed information regarding Small Office Security ports, refer to this KB article.

4.2. Preparing for Installation

Before installation, follow these preparatory steps to make sure it goes smoothly:

1. Make sure the computers meet the minimum system requirements. For some computers, you may need to install the latest operating system service pack available or free up disk space. Compile a list of computers that do not meet the necessary requirements so that you can exclude them from management.
2. Uninstall (not just disable) any existing antimalware, firewall or Internet security software from computers. Running Endpoint Security simultaneously with other security software on a computer may affect their operation and cause major problems with the system.

   Many of the security programs that are incompatible with Endpoint Security are automatically detected and removed at installation time. To learn more and to check the list of detected security software, refer to this KB article.

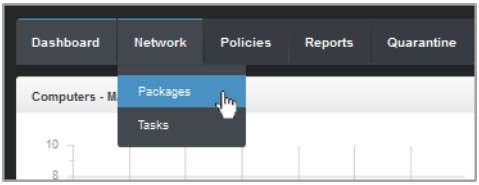
   Important
   No need to worry about Windows security features (Windows Defender, Windows Firewall), as they will be turned off automatically before installation is initiated.

3. The installation requires administrative privileges and Internet access. Make sure you have the necessary credentials at hand for all computers.
4. Computers must have connectivity to Control Center.

4.3. Local Installation

One way to install Endpoint Security on a computer is to locally run an installation package.

You can create and manage installation packages according to your needs in the **Network > Packages** page.



The Network > Packages menu

Warning

- The first computer on which you install protection must have Endpoint Security Relay role, otherwise you will not be able to deploy Endpoint Security on other computers in the network.
- The computer with Endpoint Security Relay role must be powered-on and online in order for the clients to communicate with Control Center.

Note

Once the first client has been installed, it will be used to detect other computers in the same network, based on the Network Discovery mechanism. For detailed information on network discovery, refer to "How Network Discovery Works" (p. 28).

To locally install Endpoint Security on a computer, follow the next steps:

1. Create an installation package according to your needs.

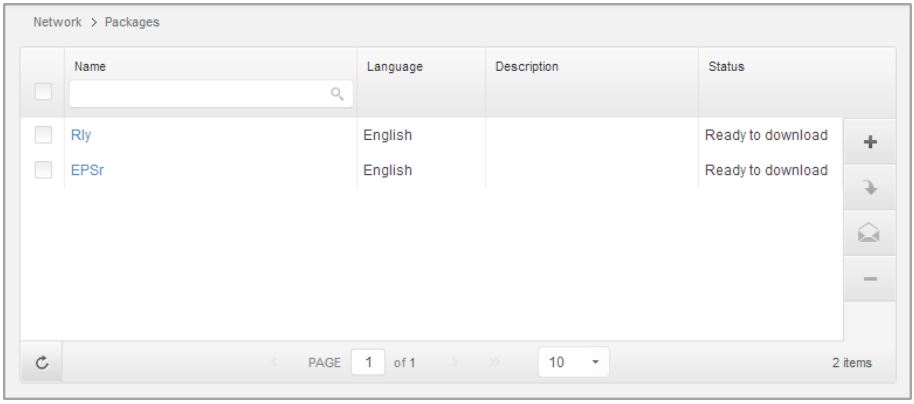
   Note
   This step is not mandatory if an installation package has already been created for the network under your account.

2. Download the installation package on the computer.
3. Run the installation package on the computer.

4.3.1. Creating Endpoint Security Installation Packages

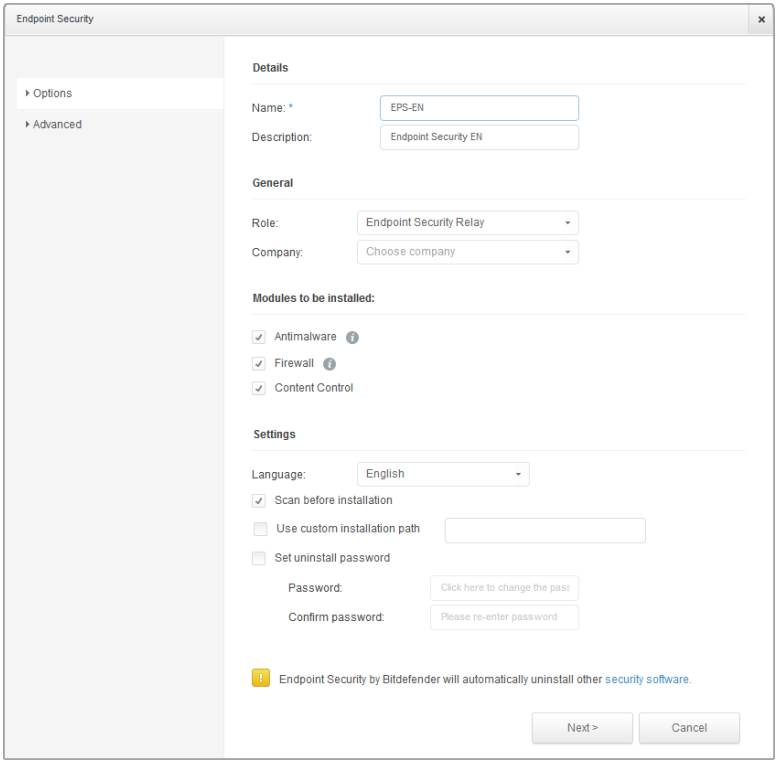
To create an Endpoint Security installation package:

1. Connect and log in to Control Center using your account.
2. Go to the **Network > Packages** page.



The Packages page

3. Click the + **Add** button at the right side of the table. A configuration window will appear.



Create Endpoint Security Packages - Options

4. Enter a suggestive name and description for the installation package you want to create.
5. Select the target computer role:
   - **Endpoint**. Select this option to create the package for a regular endpoint.
   - **Endpoint Security Relay**. Select this option to create the package for an endpoint with Endpoint Security Relay role. Endpoint Security Relay is a special role which installs an update server on the target machine along with Endpoint Security, which can be used to update all the other clients in the network, lowering the bandwidth usage between the client machines and Control Center.
6. Select the company where the installation package will be used.
7. Select the protection modules you want to install.
8. From the **Language** field, select the desired language for the client's interface.

9. Select **Scan before installation** if you want to make sure the computers are clean before installing the Endpoint Security on them. An on-the cloud quick scan will be performed on the corresponding computers before starting the installation.
10. Endpoint Security is installed in the default installation directory on the selected computers. Select **Use custom installation path** if you want to install the Endpoint Security in a different location. In this case, enter the desired path in the corresponding field. Use Windows conventions when entering the path (for example, `D:\folder`). If the specified folder does not exist, it will be created during the installation.
11. If you want to, you can set a password to prevent users from removing protection. Select **Set uninstall password** and enter the desired password in the corresponding fields.
12. Click **Next**.
13. Depending on the installation package role (Endpoint or Endpoint Security Relay), choose the entity to which the target computers will periodically connect to update the client:
    - **Bitdefender Cloud**, if you want to update the clients directly from the Internet.
    - **Endpoint Security Relay**, if you want to connect the endpoints to an Endpoint Security Relay installed in your network. All computers with Endpoint Security Relay role detected in your network will show-up in the table displayed below. Select the Endpoint Security Relay that you want. Connected endpoints will communicate with Control Center only via the specified Endpoint Security Relay.

      Important
      Port 7074 must be open for the deployment through Endpoint Security Relay to work.

14. Click **Save**.

The new installation package will appear in the list of packages of the target company.

4.3.2. Downloading Installation Packages

To download Endpoint Security installation packages:

1. Log in to Control Center from the computer on which you want to install protection.
2. Go to the **Network > Packages** page.
3. Select the Endpoint Security installation package you want to download.
4. Click the **Download** button at the right side of the table and select the type of installer you want to use. Two types of installation files are available:
    - **Downloader**. The downloader first downloads the full installation kit from the Bitdefender cloud servers and then starts the installation. It is small in size and it can be run both on 32-bit and 64-bit systems (which makes it easy to distribute). On the downside, it requires an active Internet connection.

- **Full Kit**. The full kit is to be used to install protection on computers with slow or no Internet connection. Download this file to an Internet-connected computer, then distribute it to other computers using external storage media or a network share.

Note
Available full kit versions:

– **Windows OS:** 32-bit and 64-bit systems

– **Mac OS X:** only 64-bit systems

Make sure to use the correct version for the computer you install on.

5. Save the file to the computer.

4.3.3. Running Installation Packages

For installation to work, the installation package must be run using administrator privileges or under an administrator account.

1. Connect and log in to Control Center.
2. Download or copy the installation file to the target computer or to a network share accessible from that computer.
3. Run the installation package.
4. Follow the on-screen instructions.

Once Endpoint Security has been installed, the computer will show up as managed in Control Center (**Network** page) within a few minutes.

4.4. Remote Installation

Once you have locally installed the first client with Endpoint Security Relay role, it may take a few minutes for the rest of the network computers to become visible in the Control Center. From this point, you can remotely install Endpoint Security on computers under your management by using installation tasks from Control Center.

Endpoint Security includes an automatic network discovery mechanism that allows detecting other computers in the same network. Detected computers are displayed as **unmanaged computers** in the **Network** page.

For detailed information on network discovery, refer to “How Network Discovery Works” (p. 28).

4.4.1. Remote Endpoint Security Installation Requirements

For remote installation to work:

- An Endpoint Security Relay must be installed in your network.

- Each target computer must have the admin$ administrative share enabled. Configure each target workstation to use advanced file sharing.
- Temporarily turn off User Account Control on all computers running Windows operating systems that include this security feature (Windows Vista, Windows 7, Windows Server 2008 etc.). If the computers are in a domain, you can use a group policy to turn off User Account Control remotely.
- Disable or shutdown firewall protection on computers. If the computers are in a domain, you can use a group policy to turn off Windows Firewall remotely.

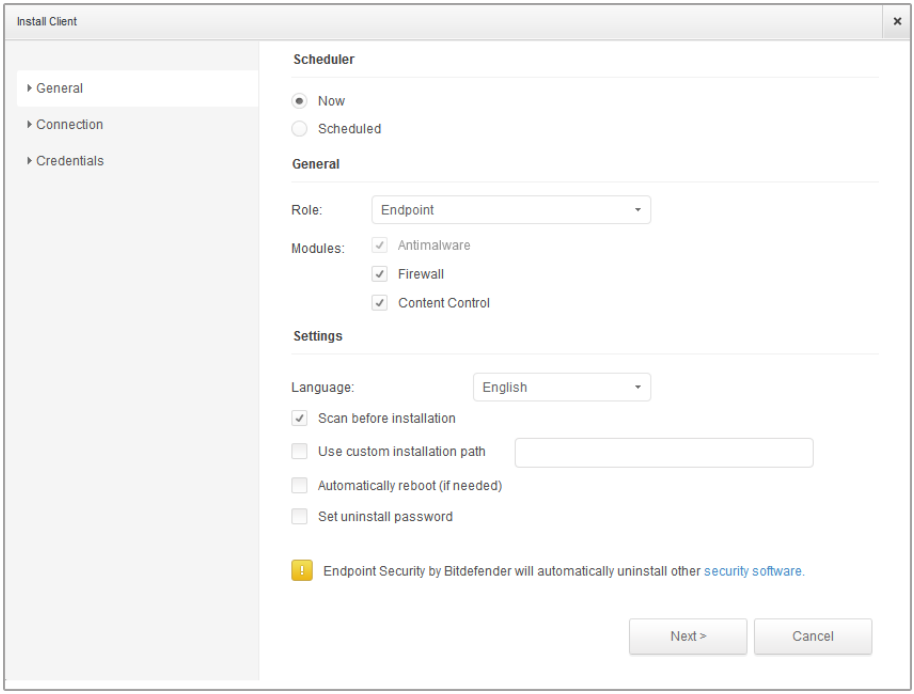
4.4.2. Running Remote Endpoint Security Installation Tasks

To run a remote installation task:

1. Connect and log in to Control Center.
2. Go to the **Network** page.
3. Select the desired network group from the left-side pane. The entities contained in the selected group are displayed in the right-side pane table.

Note
Optionally, you can apply filters to display unmanaged computers only. Click the **Filters** button and select the following options: **Unmanaged** from the **Security** category and **All items recursively** from the **Depth** category.

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



Installing Endpoint Security from the Tasks menu

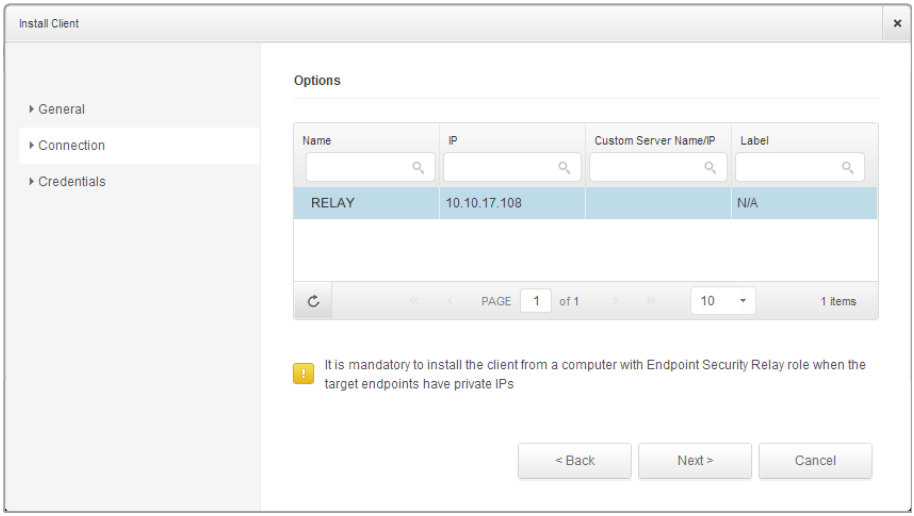
6. Configure the installation options:
   - Schedule the installation time:
     - **Now**, to launch the deployment immediately.
     - **Scheduled**, to set up the deployment recurrence interval. In this case, select the time interval that you want (hourly, daily or weekly) and configure it according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

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

   - Select the protection modules you want to install. Please note that only antimalware protection is available for server operating systems.
   - From the **Language** field, select the desired language for the client's interface.

- Select **Scan before installation** if you want to make sure the computers are clean before installing the Endpoint Security on them. An on-the cloud quick scan will be performed on the corresponding computers before starting the installation.
- Endpoint Security is installed in the default installation directory on the selected computers. Select **Use custom installation path** if you want to install the Endpoint Security in a different location. In this case, enter the desired path in the corresponding field. Use Windows conventions when entering the path (for example, `D:\folder`). If the specified folder does not exist, it will be created during the installation.
- During the silent installation, the computer is scanned for malware. Sometimes, a system restart may be needed to complete malware removal.

  Select **Automatically reboot (if needed)** to make sure detected malware is completely removed before installation. Otherwise, installation may fail.
- If you want to, you can set a password to prevent users from removing protection. Select **Set uninstall password** and enter the desired password in the corresponding fields.
- Click **Next**.
- The **Connection** tab contains the list of endpoints with Endpoint Security Relay role installed in the network. Each new client must be connected to at least one Endpoint Security Relay from the same network, that will serve as communication and update server. Select the Endpoint Security Relay that you want to link with the new clients.

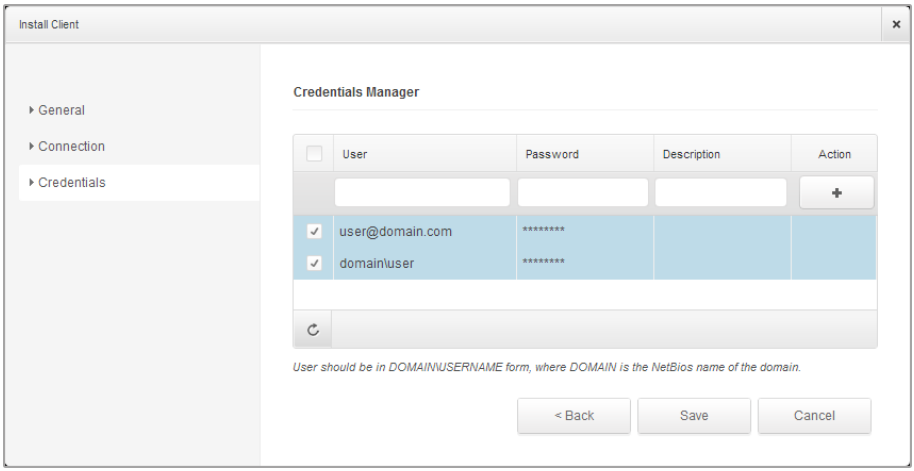


7. Click **Next**.

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

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

Note
A warning message is displayed as long as you have not selected any credentials. This step is mandatory to remotely install the Endpoint Security on computers.



To add the required OS credentials:

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

Use Windows conventions when entering the name of a domain user account, for example, `user@domain.com` or `domain\user`. To make sure that entered credentials will work, add them in both forms (`user@domain.com` and `domain\user`).

Note
Specified credentials are automatically saved to your Credentials Manager so that you do not have to enter them the next time.

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

c. Select the check box corresponding to the account you want to use.

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

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

4.5. How Network Discovery Works

Security for Endpoints includes an automatic network discovery mechanism intended to detect workgroup computers.

Security for Endpoints relies on the **Microsoft Computer Browser service** to perform network discovery. The Computer Browser service is a networking technology used by Windows-based computers to maintain updated lists of domains, workgroups, and the computers within them and to supply these lists to client computers upon request. Computers detected in the network by the Computer Browser service can be viewed by running the **net view** command in a command prompt window.

The Net view command

To enable network discovery, you must have Endpoint Security already installed on at least one computer in the network. This computer will be used to scan the network.

Important

Control Center does not use network information from Active Directory or from the network map feature available in Windows Vista and later. Network map relies on a different network discovery technology: the Link Layer Topology Discovery (LLTD) protocol.

Control Center is not actively involved in the Computer Browser service operation. Endpoint Security only queries the Computer Browser service for the list of workstations and servers currently visible in the network (known as the browse list) and then sends it to Control Center. Control Center processes the browse list, appending newly detected computers to its **Unmanaged Computers** list. Previously detected computers are not deleted after a new network discovery query, so you must manually exclude & delete computers that are no longer on the network.

The initial query for the browse list is carried out by the first Endpoint Security installed in the network.

- If Endpoint Security is installed on a workgroup computer, only computers from that workgroup will be visible in Control Center.
- If Endpoint Security is installed on a domain computer, only computers from that domain will be visible in Control Center. Computers from other domains can be detected if there is a trust relationship with the domain where Endpoint Security is installed.

Subsequent network discovery queries are performed regularly every hour. For each new query, Control Center divides the managed computers space into visibility areas and then designates one Endpoint Security in each area to perform the task. A visibility area is a group of computers that detect each other. Usually, a visibility area is defined by a workgroup or domain, but this depends on the network topology and configuration. In some cases, a visibility area might consist of multiple domains and workgroups.

If a selected Endpoint Security fails to perform the query, Control Center waits for the next scheduled query, without choosing another Endpoint Security to try again.

For full network visibility, Endpoint Security must be installed on at least one computer in each workgroup or domain in your network. Ideally, Endpoint Security should be installed on at least one computer in each subnetwork.

4.5.1. More about the Microsoft Computer Browser Service

Quick facts about the Computer Browser service:

- Works independent of Active Directory.
- Runs exclusively over IPv4 networks and operates independently within the boundaries of a LAN group (workgroup or domain). A browse list is compiled and maintained for each LAN group.
- Typically uses connectionless server broadcasts to communicate between nodes.
- Uses NetBIOS over TCP/IP (NetBT).
- Requires NetBIOS name resolution. It is recommended to have a Windows Internet Name Service (WINS) infrastructure up and running in the network.
- Is not enabled by default in Windows Server 2008 and 2008 R2.

For detailed information on the Computer Browser service, check the Computer Browser Service Technical Reference on Microsoft Technet.

4.5.2. Network Discovery Requirements

In order to successfully discover all the computers (servers and workstations) that will be managed from Control Center, the following are required:

- Computers must be joined in a workgroup or domain and connected via an IPv4 local network. Computer Browser service does not work over IPv6 networks.

- Several computers in each LAN group (workgroup or domain) must be running the Computer Browser service. Primary Domain Controllers must also run the service.
- NetBIOS over TCP/IP (NetBT) must be enabled on computers. Local firewall must allow NetBT traffic.
- File sharing must be enabled on computers. Local firewall must allow file sharing.
- A Windows Internet Name Service (WINS) infrastructure must be set up and working properly.
- For Windows Vista and later, network discovery must be turned on (**Control Panel > Network and Sharing Center > Change Advanced Sharing Settings**).

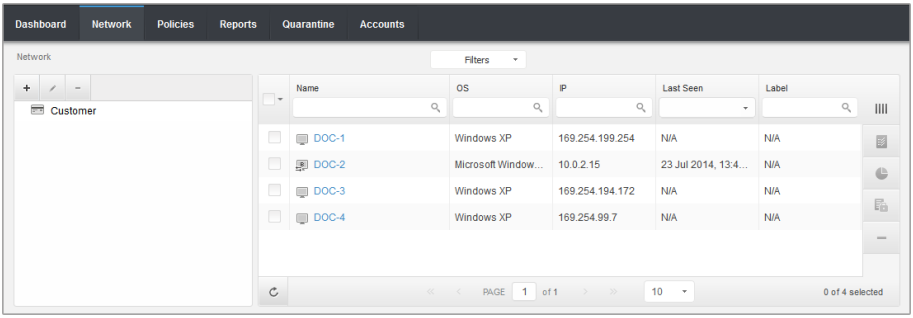
  To be able to turn on this feature, the following services must first be started:
  - DNS Client
  - Function Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- In environments with multiple domains, it is recommended to set up trust relationships between domains so that computers can access browse lists from other domains.

Computers from which Endpoint Security queries the Computer Browser service must be able to resolve NetBIOS names.

Note
The network discovery mechanism works for all supported operating systems, including Windows Embedded versions, provided the requirements are met.

5. Managing Computers

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



The Network Page

1. The left-side pane displays the available network tree structure.

   Note
   You can view and manage only the groups on which you have administrator rights.

2. The right-side pane displays the contents of the group that you have selected in the network tree. This pane consists of a grid, where the rows contain network objects and the columns display specific information for each type of object.

   From this pane, you can do the following:

   - View detailed information about each network object under your account. You can view the status of each object by checking the icon next to its name. Click the object's name to display a window containing more specific details.
   - Use the Action Toolbar at the right-side of the table to carry out specific operations for each network object (such as run tasks, create reports, assign policies and delete).
   - Refresh table data.

From the **Network** section you can also manage the installation packages and the list of tasks for each type of network object.

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

You can view the available computer network in the left-side pane and details about each computer in the right-side pane.

To customize the computer details displayed in the table:

1. Click the **Columns** button at the right-side of the table header.
2. Select the column names you want to view.
3. Click the **Reset** button to return to the default columns view.

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

- Check the computer status.
- Organize computers into groups.
- View computer details.
- Sort, filter and search for computers.
- Run tasks on computers.
- Create quick reports.
- Assign policies.
- Delete computers from network inventory.

5.1. Check the Computer Status

Each computer is represented in the network page by an icon specific to the computer's status. View the computer statuses and the corresponding icons in the following table:

Icon	Status
	Computer, Managed, No issues, Online
	Computer, Managed, With security issues, Online,
	Computer, Managed, No issues, Offline
	Computer, Managed, With security issues, Offline
	Unmanaged
	Deleted

For detailed information, refer to:

- “Managed, Unmanaged and Deleted Computers” (p. 32)
- “Online and Offline Computers” (p. 33)
- “Computers with security issues” (p. 34)

5.1.1. Managed, Unmanaged and Deleted Computers

Computers can have different management statuses:

- **Managed** - computers on which the Endpoint Security protection is installed.
- **Unmanaged** - detected computers on which the Endpoint Security protection has not been installed yet.
- **Deleted** - computers that you have deleted from Control Center. For more information, refer to "Deleting Computers from Network Inventory" (p. 56).

5.1.2. Online and Offline Computers

The connectivity status concerns only the managed computers. From this point of view, managed computers can be:

- **Online**. A blue icon indicates that the computer is online.
- **Offline**. A grey icon indicates that the computer is offline.

A computer is offline if Endpoint Security is inactive for more than 5 minutes. Possible reasons why computers appear offline:

- Computer is shut down, sleeping or hibernating.

  Note
  Computers normally appear online even when they are locked or the user is logged off.

- Endpoint Security does not have connectivity with Bitdefender Control Center or with the assigned Endpoint Security Relay:
  - Computer might be disconnected from the network.
  - A network firewall or router might block the communication between Endpoint Security and Bitdefender Control Center or the assigned Endpoint Security Relay.
- Endpoint Security has been manually uninstalled from the computer, while the computer did not have connectivity with Bitdefender Control Center or with the assigned Endpoint Security Relay. Normally, when Endpoint Security is being manually uninstalled from a computer, Control Center is being notified of this event, and the computer is flagged as unmanaged.
- Endpoint Security might not be working properly.

To find out for how long computers have been inactive:

1. Display only the managed computers. Click the **Filters** menu located above the table, select **Managed (Endpoints)** and **Managed (Endpoint Security Relay)** in the **Security** category and click **Save**.
2. Click the **Last Seen** column header to sort computers by inactivity period.

You can ignore shorter periods of inactivity (minutes, hours) as they are likely the result of a temporary condition. For example, the computer is currently shut down.

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

5.1.3. Computers with security issues

The security status concerns only the managed computers. Check the status icon displaying a warning symbol to identify computers with security issues:

- Computer managed, with issues, online.
- Computer managed, with issues, offline.

A computer has security issues provided at least one of the following situations applies:

- Antimalware protection is disabled.
- The license of Endpoint Security has expired.
- Endpoint Security is outdated.
- Signatures are outdated.
- Malware is detected.

If you notice a computer with security issues, click its name to display the **Computer Details** page. You can identify the security issues by icon. Check the icon's tooltip to find out more details. Further local investigations may be needed.

5.2. Organizing Computers into Groups

You can manage computer groups in the left-side pane of the **Network** page, in the **Network** groups.

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

Under **Network** group belonging to your company you can create, delete, rename and move computer groups within a custom-defined tree structure.

Important

Please note the following:

- A group can contain both computers and other groups.
- When selecting a group in the left-side pane, you can view all computers except those placed into its sub-groups. To view all computers included in the group and in its sub-groups, click the **Filters** menu located above the table and select **All items recursively** in the **Depth** section.

Creating Groups

Before you start creating groups, think of the reasons why you need them and come up with a grouping scheme. For example, you can group computers based on one or a mix of the following criteria:

- Organization structure (Sales, Marketing, Quality Assurance, Software Development, Management etc.).
- Security needs (Desktops, Laptops, Servers, etc.).
- Location (Headquarter, Local Offices, Remote Workers, Home Offices etc.).

To organize your network into groups:

1. Select **Network** group in the left-side pane.
2. Click the **Add group** button at the top of the left-side pane.
3. Enter a suggestive name for the group and click **OK**.

Renaming Groups

To rename a group:

1. Select the group in the left-side pane.
2. Click the **Edit group** button at the top of the left-side pane.
3. Enter the new name in the corresponding field.
4. Click **OK** to confirm.

Moving Groups and Computers

You can move groups and users anywhere in the **Network** group hierarchy. To move a group or a user, drag and drop it from the current location to the new one.

Note

The entity that is moved will inherit the policy settings of the new parent group, unless a different policy has been assigned to it. For more information about policy inheritance, refer to “Assigning Policies to Network Objects” (p. 70).

Deleting Groups

A group cannot be deleted if it contains at least one computer. Move all computers from the group you want to delete to another group. If the group includes sub-groups, you can choose to move all sub-groups rather than individual computers.

To delete a group:

1. Select the empty group in the right side pane of the **Network page**.
2. Click the **Remove group** button at the top of the left-side pane. You will have to confirm your action by clicking **Yes**.

5.3. Viewing Computer Details

You can obtain detailed information about each computer from the **Network** page, including OS, IP, last seen date and time, etc.

To find out details about a computer:

1. Go to the **Network** page.
2. Select the desired network group from the left-side pane.

   All computers from the selected group are displayed in the right-side pane table.
3. You can easily identify the computer status by checking the corresponding icon. For detailed information, refer to "Check the Computer Status" (p. 32).
4. Check the information displayed on columns for each computer:
   - **Name**: computer name.
   - **FQDN**: fully qualified domain name that includes the hostname and domain name.
   - **OS**: operating system installed on the computer.
   - **IP**: computer's IP address.
   - **Last Seen**: details about the computer's connectivity status.

     Note
     It is important to monitor the **Last Seen** field as long inactivity periods might indicate a communication issue or a disconnected computer.

   - **Label**: the label added to the computer in the **Computer Details** window.
5. Click the name of the managed computer you are interested in. The **Computer Details** window is displayed.
   - Go to **Overview** tab to find the following details:
     - General computer information, such as name, IP address, operating system, parent group and current status. You can also assign the computer with a label. You can therefore search and filter computers by label using the **Label** column search field from right-side table of the **Network** page.
     - Security details related to the Endpoint Security installed on the selected computer, such as installed modules, assigned policy, antimalware status, license status, last update, product and signature versions and detected malware in the last 24

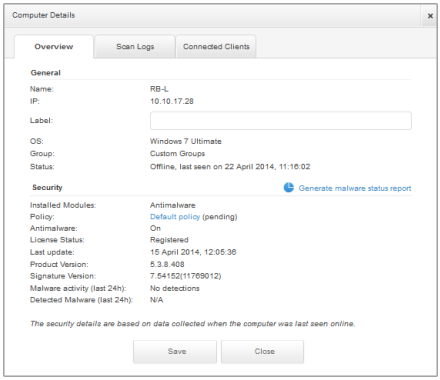
hours. You can also obtain a quick overview regarding the number of malware detections on computer in the current day.

– Click **Generate malware status report** to access the malware report options for the selected computer.

For more information, refer to “Creating Reports” (p. 121)

Note

Each property generating security issues is marked with icon. Check the icon's tooltip to find out more details. Further local investigations may be needed.



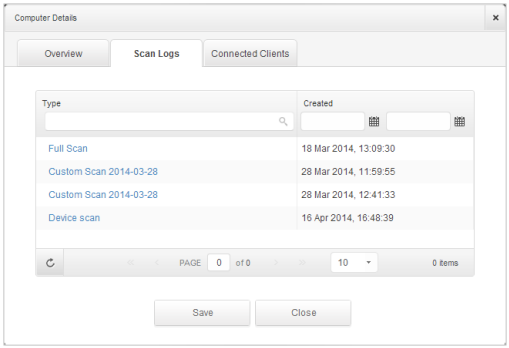
Computer Details - Overview

– The **Endpoint Security Relay** section (available for regular endpoint clients) displays information about the Endpoint Security Relay to which the current computer is connected.

- Click the **Scan logs** tab to view detailed information about all scan tasks performed on the computer. Click the scan report you are interested in to open it in a new page of the browser.

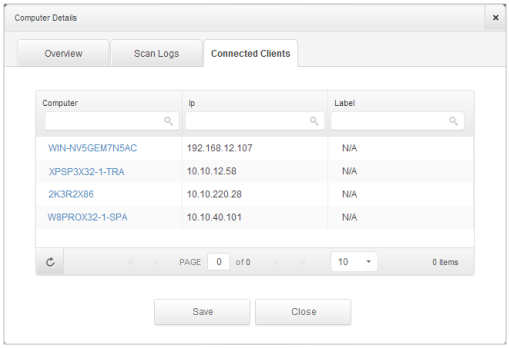
  To move through the pages, use the navigation options at the bottom of the table. If there are too many entries, you can use the filter options available at the top of the table.

  Click the **Refresh** button in the bottom-left corner of the table to update the scan logs list.



Computer Details - Scan Logs

- For computers with Endpoint Security Relay role, the **Connected Clients** tab is also available, where you can view the list of connected endpoints.



Computer Details - Connected Clients

5.4. Sorting, Filtering and Searching for Computers

Depending on the number of computers, the computers 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 **Filters** menu at the top of the table to filter displayed data. For example, you can search for a specific computer or choose to view only the managed computers.

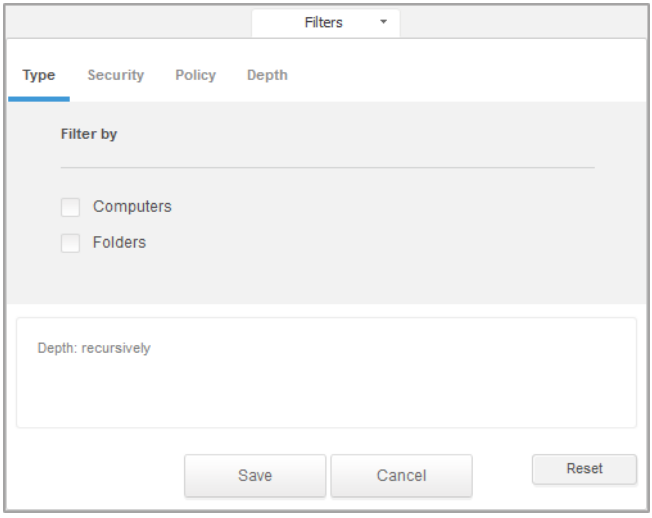
5.4.1. Sorting Computers

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

Sorting Computers

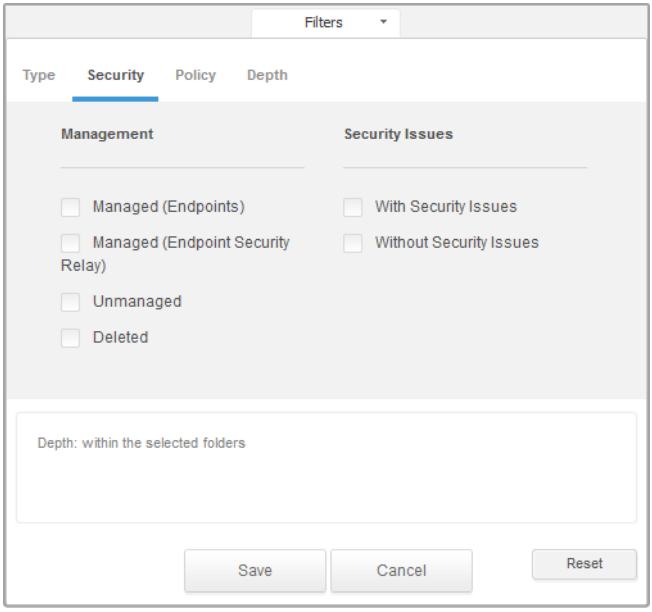
5.4.2. Filtering Computers

1. Select the desired group in the left-side pane.
2. Click the **Filters** menu located above the table.
3. Select the filter criteria as follows:
   - **Type**. Select the type of entities you want to display (computers, folders or both).



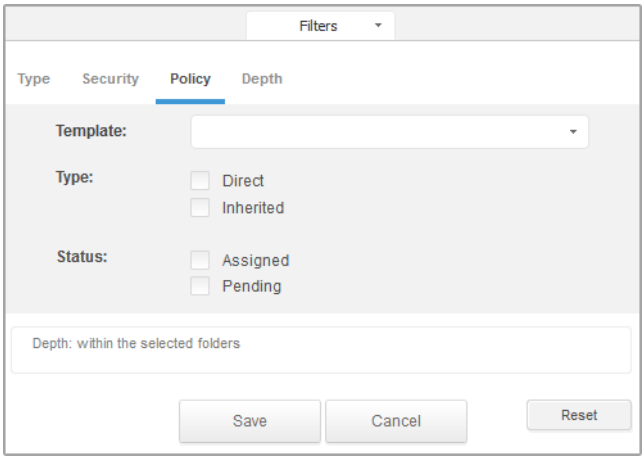
Computers - Filter by Type

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



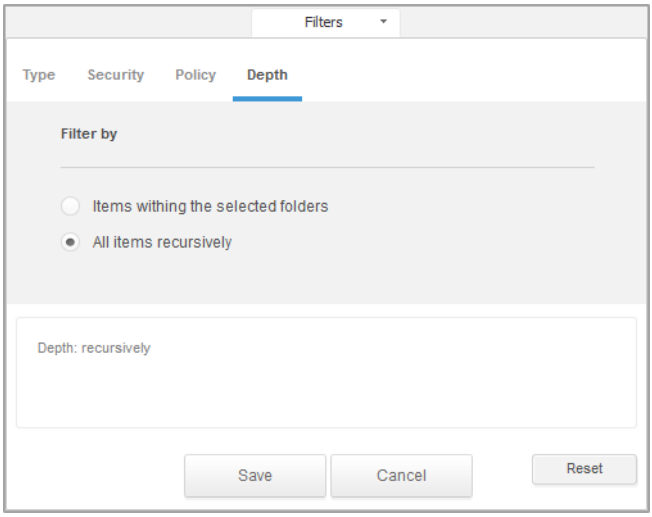
Computers - Filter by Security

- **Policy**. Select the policy template you want to filter the computers by, the policy assignment type (Direct or Inherited), as well as the policy assignment status (Assigned or Pending).



Computers - Filter by Policy

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



Computers - Filter by Depth

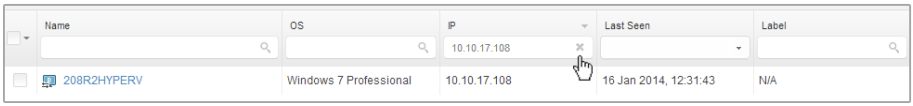
Note
You can view all selected filter criteria in the lower part of the **Filters** window. If you want to clear all filters, click the **Reset** button.

4. Click **Save** to filter the computers by the selected criteria. The filter remains active in the **Network** page until you log out or reset the filter.

5.4.3. Searching for Computers

1. Select the desired group in the left-side pane.
2. Enter the search term in the corresponding box under the column headers (Name, OS or IP) from the right-side pane. For example, enter the IP of the computer you are looking for in the **IP** field. Only the matching computer will appear in the table.

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



Search for computers

5.5. Running Tasks on Computers

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

This is what you can do:

- "Scan" (p. 42)
- "Install Client" (p. 49)
- "Modify Installer" (p. 52)
- "Uninstall Client" (p. 53)
- "Update" (p. 54)
- "Restart Computer" (p. 54)
- "Network Discovery" (p. 55)

You can choose to create tasks individually for each computer or for groups of computers. For example, you can remotely install the Endpoint Security on a group of unmanaged computers. At a later time, you can create a scan task for a certain computer from the same group.

For each computer, you can only run compatible tasks. For example, if you select an unmanaged computer, you can only choose to **Install client**, all the other tasks being disabled.

For a group, the selected task will be created only for compatible computers. If none of the computers in the group is compatible with the selected task, you will be notified that the task could not be created.

Once created, the task will start running immediately on online computers. If a computer is offline, the task will run as soon as it gets back online.

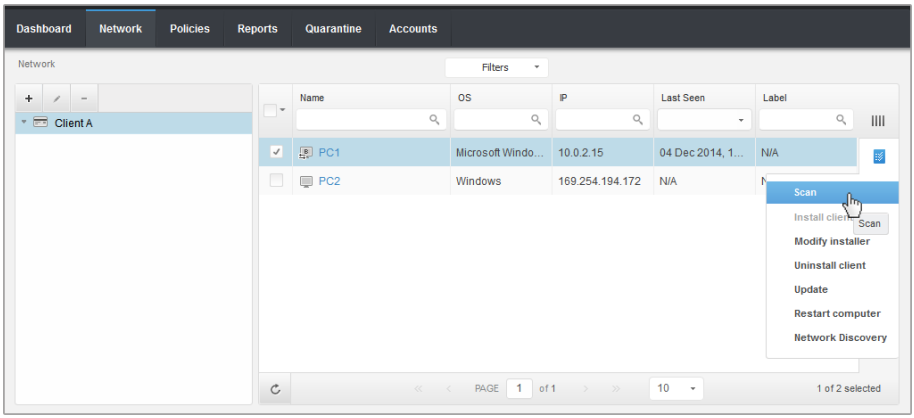
You can view and manage the task on the **Network > Tasks** page. For more information, refer to Viewing and Managing Tasks.

5.5.1. Scan

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

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.

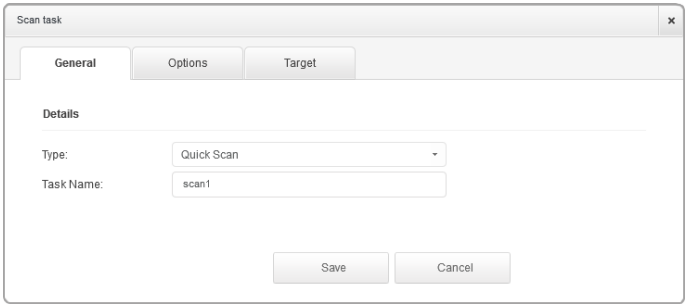
3. Select the check boxes corresponding to the computers you want to scan.
4. Click the **Task** button at the right-side of the table and choose **Scan**.



Computers Scan Task

A configuration window will appear.

5. Configure the scan options:
   - In the **General** tab, you can choose the type of scan and you can enter a name for the scan task. The scan task name is intended to help you easily identify the current scan in the **Tasks** page.



Computers Scan task - Configuring general settings

Select the type of scan from the **Type** menu:

- **Quick Scan** uses in-the-cloud scanning to detect malware running in the system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

Note

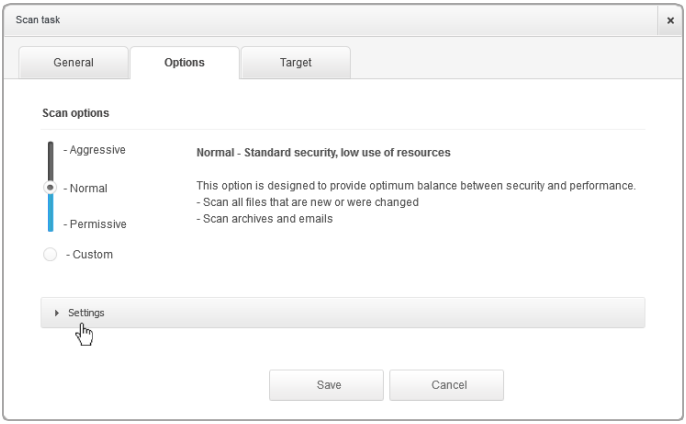
Quick Scan only detects existing malware, without taking any action. If malware is found during a Quick Scan, you must run a Full System Scan task to remove detected malware.

– **Full Scan** checks the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

– **Custom Scan** allows you to choose the locations to be scanned and to configure the scan options. To define a custom scan:

• Go to **Options** tab to set the scan options. Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right-side of the scale to guide your choice.

Based on the selected profile, the scan options in the **Settings** section are automatically configured. However, if you want to, you can configure them in detail. To do that, select the **Custom** check box and then go to the **Settings** section.



Computers Scan Task

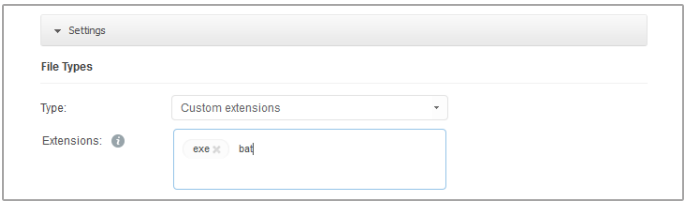
The following options are available:

– **File Types.** Use these options to specify which types of files you want to be scanned. You can set Endpoint Security to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

Note

Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "List of Application File Types" (p. 145).

If you want only specific extensions to be scanned, choose **Custom extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.



Computers scan task options - Adding custom extensions

– **Archives.** Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

Note

Scanning archived files increases the overall scanning time and requires more system resources.

- **Scan inside archives.** Select this option if you want to check archived files for malware. If you decide on using this option, you can configure the following optimization options:
  - **Limit archive size to (MB).** You can set a maximum accepted size limit of archives to be scanned. Select the corresponding check box and type the maximum archive size (in MB).
  - **Maximum archive depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.
- **Scan email archives.** Select this option if you want to enable scanning of email message files and email databases, including file formats such as .eml, .msg, .pst, .dbx, .mbx, .tbb and others.

Note
Email archive scanning is resource intensive and can impact system performance.

– **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.

  • **Scan boot sectors.** Scans the system's boot sector. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.

  • **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.

  • **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.

  • **Scan for keyloggers.** Select this option to scan for keylogger software.

  • **Scan memory.** Select this option to scan programs running in the system's memory.

  • **Scan cookies.** Select this option to scan the cookies stored by browsers on the computer.

  • **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.

  • **Scan for Potentially Unwanted Applications (PUA).** A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

– **Actions.** Depending on the type of detected file, the following actions are taken automatically:

  • **When an infected file is found.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Endpoint Security can normally remove the malware code from an

infected file and reconstruct the original file. This operation is known as disinfection.

If an infected file is detected, Endpoint Security will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

Important
For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- **When a suspect file is found.** Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Endpoint Security cannot be sure that the file is actually infected with malware. Suspect files cannot be disinfected, because no disinfection routine is available.

  Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine. Quarantined files are sent for analysis to Bitdefender Labs on a regular basis. If malware presence is confirmed, a signature is released to allow removing the malware.

- **When a rootkit is found.** Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

  Detected rootkits and hidden files are ignored by default.

Though not recommended, you can change the default actions. You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file. The following actions are available:

Disinfect
Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

Move to quarantine
Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

Delete
Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Ignore
No action will be taken on detected files. These files will only appear in the scan log.

- Go to **Target** tab to add the locations you want to be scanned on the target computers.

  In the **Scan target** section you can add a new file or folder to be scanned:

  a. Choose a predefined location from the drop-down menu or enter the **Specific paths** you want to scan.

  b. Specify the path to the object to be scanned in the edit field.

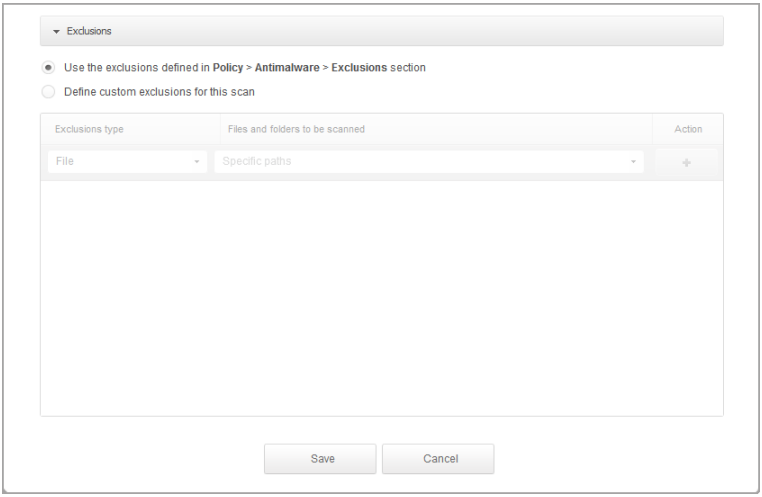
  – If you have chosen a predefined location, complete the path as needed. For example, to scan the entire `Program Files` folder, it suffices to select the corresponding predefined location from the drop-down menu. To scan a specific folder from `Program Files`, you must complete the path by adding a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

  – If you have chosen **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers. For more information regarding system variables, refer to "Using System Variables" (p. 145)

  c. Click the corresponding + **Add** button.

  To edit an existing location, click it. To remove a location from the list, move the cursor over it and click the corresponding – **Delete** button.

  Click the **Exclusions** sections if you want to define target exclusions.



Computers Scan Task - Defining Exclusions

You can either use the exclusions defined by policy or define explicit exclusions for the current scan task. For more details regarding exclusions, refer to “Exclusions” (p. 93).

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

5.5.2. Install Client

To protect your computers with Security for Endpoints, you must install Endpoint Security on each of them.

Warning

- The first computer on which you install protection must have Endpoint Security Relay role, otherwise you will not be able to deploy Endpoint Security on other computers in the network.
- The computer with Endpoint Security Relay role must be powered-on and online in order for the clients to communicate with Control Center.

Once you have installed an Endpoint Security client with Endpoint Security Relay role in a network, it will automatically detect unprotected computers in that network.

The Security for Endpoints protection can then be installed on those computers remotely from Control Center.

Remote installation is performed in the background, without the user knowing about it.

Warning

Before installation, be sure to uninstall existing antimalware and firewall software from computers. Installing Security for Endpoints over existing security software may affect their operation and cause major problems with the system. Windows Defender and Windows Firewall will be turned off automatically when installation starts.

To remotely install the Security for Endpoints protection on one or several computers:

1. Go to the **Network** page.
2. Select the desired network group from the left-side pane. The entities contained in the selected group are displayed in the right-side pane table.

Note

Optionally, you can apply filters to display unmanaged computers only. Click the **Filters** button and select the following options: **Unmanaged** from the **Security** category and **All items recursively** from the **Depth** category.

3. Select the entities (computers or groups of computers) on which you want to install protection.
4. Click the **Tasks** button at the right-side of the table and choose **Install client**. The **Install Client** wizard is displayed.
5. Configure the installation options:
   - Schedule the installation time:
     - **Now**, to launch the deployment immediately.
     - **Scheduled**, to set up the deployment recurrence interval. In this case, select the time interval that you want (hourly, daily or weekly) and configure it according to your needs.

Note

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

   - Select the role you want the client to have:
     - **Endpoint**. Select this option if you want to install the client on a regular endpoint.
     - **Endpoint Security Relay**. Select this option to install the client with Endpoint Security Relay role on the target computer. Endpoint Security Relay is a special role which installs an update server on the target machine along with Endpoint

Security, which can be used to update all the other clients in the network, lowering the bandwidth usage between the client machines and Control Center.

- Select the protection modules you want to install. Please note that only antimalware protection is available for server operating systems.
- From the **Language** field, select the desired language for the client's interface.
- Select **Scan before installation** if you want to make sure the computers are clean before installing the Endpoint Security on them. An on-the cloud quick scan will be performed on the corresponding computers before starting the installation.
- Endpoint Security is installed in the default installation directory on the selected computers. Select **Use custom installation path** if you want to install the Endpoint Security in a different location. In this case, enter the desired path in the corresponding field. Use Windows conventions when entering the path (for example, `D:\folder`). If the specified folder does not exist, it will be created during the installation.
- During the silent installation, the computer is scanned for malware. Sometimes, a system restart may be needed to complete malware removal.

  Select **Automatically reboot (if needed)** to make sure detected malware is completely removed before installation. Otherwise, installation may fail.
- If you want to, you can set a password to prevent users from removing protection. Select **Set uninstall password** and enter the desired password in the corresponding fields.
- Click **Next**.
- Depending on the client role (Endpoint or Endpoint Security Relay), choose the entity through which the clients will communicate:
  - **Bitdefender Cloud**, if you want to update the clients directly from the Internet.
  - **Endpoint Security Relay**, if you want to connect the endpoints to an Endpoint Security Relay installed in your network. All computers with Endpoint Security Relay role detected in your network will show-up in the table displayed below. Select the Endpoint Security Relay that you want. Connected endpoints will communicate with Control Center only via the specified Endpoint Security Relay.

    Important
    Port 7074 must be open for the deployment through Endpoint Security Relay to work.

6. Click **Next**.
7. Under the **Credentials Manager** section, specify the administrative credentials required for remote authentication on selected endpoints.

You can add the required credentials by entering the user and password of each target operating system.

Note
A warning message is displayed as long as you have not selected any credentials. This step is mandatory to remotely install the Endpoint Security on computers.

To add the required OS credentials:

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

   Use Windows conventions when entering the name of a domain user account, for example, `user@domain.com` or `domain\user`. To make sure that entered credentials will work, add them in both forms (`user@domain.com` and `domain\user`).

   Note
   Specified credentials are automatically saved to your Credentials Manager so that you do not have to enter them the next time.

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

c. Select the check box corresponding to the account you want to use.

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

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

5.5.3. Modify Installer

To change the protection modules installed on one or several computers:

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the check boxes corresponding to the managed computers on which you want to change the installed protection modules.
4. Click the **Task** button at the right-side of the table and choose **Modify installer**.
5. Select in the **Modules** section only the protection modules you want to be installed:

   Antimalware
   The Antimalware module protects the system against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on).

Firewall
The Firewall protects the computer from inbound and outbound unauthorized connection attempts.

Content Control
The Content Control module helps you control users' access to Internet and to applications. Please note that the configured Content Control settings will apply to all users who log on to the target computers.

Note
Please note that only antimalware protection is available for server operating systems.

6. Check **Reboot if needed** option to allow the computer to automatically reboot to complete the installation.
7. Click **Save**. A confirmation message will appear.

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

5.5.4. Uninstall Client

To remotely uninstall the Security for Endpoints protection from one or several computers:

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the check boxes corresponding to the computers from which you want uninstall Security for Endpoints protection.
4. Click the **Task** button at the right-side of the table and choose **Uninstall client**.
5. A configuration window is displayed, allowing you to opt for keeping the quarantined items on the client machine.
6. Click **Save** to create the task. A confirmation message will appear.

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

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

5.5.5. Update

Check the status of managed computers periodically. If you notice a computer with security issues, click its name to display the **Computer Details** page. For more information, refer to "Computers with security issues" (p. 34).

Outdated clients or outdated signatures represent a security issues. In these cases, you should run an update for the corresponding computer. This task can be done locally from the computer, or remotely from Control Center.

To remotely update the client and the signatures on managed computers:

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the check boxes of computers where you want to run a client update.
4. Click the **Task** button at the right-side of the table and choose **Update**. A configuration window will appear.
5. You can choose to update only the product, only the virus signatures or both.
6. Click **Update** to run the task. A confirmation message will appear.

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

5.5.6. Restart Computer

You can choose to remotely restart managed computers.

Note

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

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the check boxes corresponding to the computers you want to restart.
4. Click the **Task** button at the right-side of the table and choose **Restart computer**.
5. Choose the restart schedule option:
   - Select **Restart now** to restart computers immediately.
   - Select **Restart on** and use the fields below to schedule the restart at the desired date and time.

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

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

5.5.7. Network Discovery

Network discovery is automatically done each hour by Endpoint Security with Endpoint Security Relay role. However, you can manually run network discovery task from Control Center at any time you want, starting from any machine protected by Endpoint Security.

To run a network discovery task in your network:

1. Go to the **Network** page.
2. Select the desired computer group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the check boxes corresponding to the computers you want to perform network discovery with.
4. Click the **Task** button at the right-side of the table and choose **Network Discovery**.
5. A confirmation message will appear. Click **Yes**.

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

5.6. Creating Quick Reports

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

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.

   Optionally, you can filter the contents of the selected group only by managed computers.
3. Select the check boxes corresponding to the computers to be included in the report.
4. Click the **Report** button at the right-side of the table and choose the report type from the menu. Activity reports will only include data from the last week. For more information, refer to “Available Report Types” (p. 118).
5. Configure the report options. For more information, refer to “Creating Reports” (p. 121)
6. Click **Generate**. The report is immediately displayed. The time required for reports to be created may vary depending on the number of selected computers.

5.7. Assigning Policies

Security settings on computers are managed using policies.

From the **Network** section you can view, change and assign policies for each computer or group of computers.

Note

You can view or change the security settings for managed computers or for groups. To make this task easier, you can filter the table contents only by managed computers.

To view the policy assigned to a particular computer:

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Click the name of the managed computer you are interested in. A details window will appear.
4. In the **Security** section, click the name of the current policy to view its settings.
5. You can change security settings as needed, provided the policy owner has allowed other users to make changes to that policy. Please note that any change you make will affect all the other computers assigned with the same policy.

   For more information about changing computer policies, refer to “Computer Policies” (p. 72).

To assign a policy to a computer or group:

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the check box of the desired computer or group. You can select one or several objects of the same type only from the same level.
4. Click the **Policy** button at the right side of the table.
5. Make the necessary settings in the **Policy assignment** window. For more information, refer to “Assigning Policies to Network Objects” (p. 70).

5.8. Deleting Computers from Network Inventory

If you do not plan to manage some of the detected computers, you can choose to exclude them from the network inventory. Furthermore, you can permanently delete excluded computers from the network inventory.

5.8.1. Excluding Computers from the Network Inventory

To exclude computers from the network inventory:

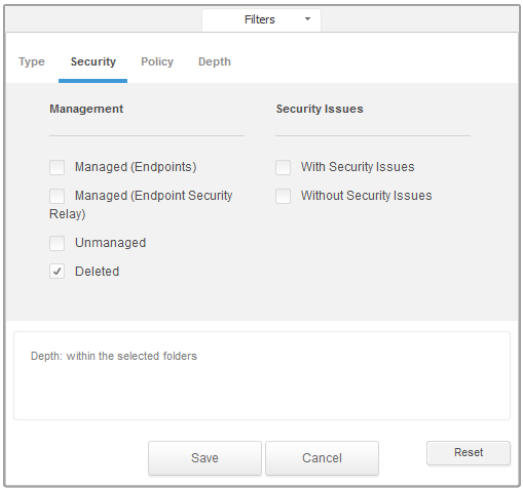
1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the check box corresponding to the computer you want to exclude.
4. Click the **– Delete** button at the right-side of the table. You will have to confirm your action by clicking **Yes**.

Note

If you delete a managed computer, the Endpoint Security will be automatically uninstalled from it.

Once you have deleted a computer, you can no longer view it in the table. Deleted computers still exist in the Small Office Security database, but they are no longer visible.

You may want to manage again some of the deleted computers. In this case, you have to display the deleted computers and install the Endpoint Security on the ones you are interested in. To display deleted computers, click the **Filters** menu located above the table, go to the **Security** tab, check the option **Deleted** then click **Save**.



Computers - Filter by Deleted Endpoints

Note
If you reinstall protection on an excluded computer, it will be detected as managed and restored in the table.

5.8.2. Deleting Computers Permanently

To permanently delete computers from network inventory:

1. Go to the **Network** page.
2. Select the desired group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Filter the table contents by **Deleted** computers.
4. Select the check box corresponding to the computers you want to delete.
5. Click the **– Delete** button at the right-side of the table. You will have to confirm your action by clicking **Yes**.

   The corresponding computers are permanently deleted from the Small Office Security database.

Warning
You cannot restore a permanently deleted computer in the Small Office Security database.

5.9. Installation Packages

The Small Office Security protection components can be installed on the target network objects either by deploying them from Control Center or by downloading the needed installation package and running it manually on the target network objects.

You can manage installation packages from the **Network > Packages** page.

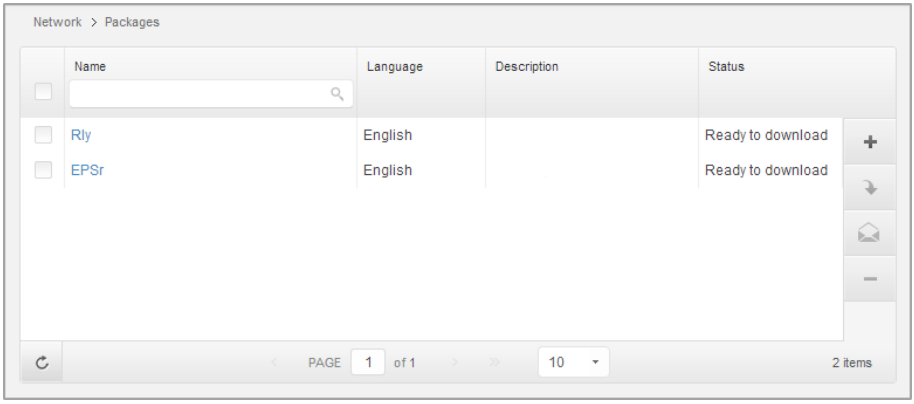
5.9.1. Creating Installation Packages

You might need to make certain customizations to the installation packages, to better fit the security needs.

Creating Endpoint Security Installation Packages

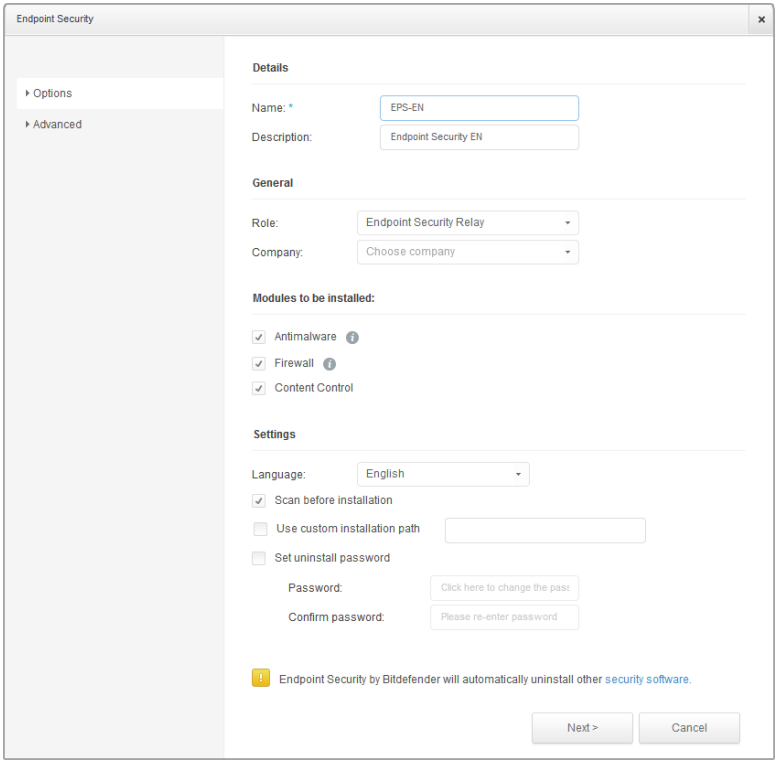
To create an Endpoint Security installation package:

1. Connect and log in to Control Center using your account.
2. Go to the **Network > Packages** page.



The Packages page

3. Click the + **Add** button at the right side of the table. A configuration window will appear.



Create Endpoint Security Packages - Options

4. Enter a suggestive name and description for the installation package you want to create.
5. Select the target computer role:
   - **Endpoint**. Select this option to create the package for a regular endpoint.
   - **Endpoint Security Relay**. Select this option to create the package for an endpoint with Endpoint Security Relay role. Endpoint Security Relay is a special role which installs an update server on the target machine along with Endpoint Security, which can be used to update all the other clients in the network, lowering the bandwidth usage between the client machines and Control Center.
6. Select the company where the installation package will be used.
7. Select the protection modules you want to install.
8. From the **Language** field, select the desired language for the client's interface.

9. Select **Scan before installation** if you want to make sure the computers are clean before installing the Endpoint Security on them. An on-the cloud quick scan will be performed on the corresponding computers before starting the installation.
10. Endpoint Security is installed in the default installation directory on the selected computers. Select **Use custom installation path** if you want to install the Endpoint Security in a different location. In this case, enter the desired path in the corresponding field. Use Windows conventions when entering the path (for example, `D:\folder`). If the specified folder does not exist, it will be created during the installation.
11. If you want to, you can set a password to prevent users from removing protection. Select **Set uninstall password** and enter the desired password in the corresponding fields.
12. Click **Next**.
13. Depending on the installation package role (Endpoint or Endpoint Security Relay), choose the entity to which the target computers will periodically connect to update the client:
    - **Bitdefender Cloud**, if you want to update the clients directly from the Internet.
    - **Endpoint Security Relay**, if you want to connect the endpoints to an Endpoint Security Relay installed in your network. All computers with Endpoint Security Relay role detected in your network will show-up in the table displayed below. Select the Endpoint Security Relay that you want. Connected endpoints will communicate with Control Center only via the specified Endpoint Security Relay.

      Important
      Port 7074 must be open for the deployment through Endpoint Security Relay to work.

14. Click **Save**.

The new installation package will appear in the list of packages of the target company.

5.9.2. Downloading Installation Packages

To download Endpoint Security installation packages:

1. Log in to Control Center from the computer on which you want to install protection.
2. Go to the **Network > Packages** page.
3. Select the Endpoint Security installation package you want to download.
4. Click the **Download** button at the right side of the table and select the type of installer you want to use. Two types of installation files are available:
    - **Downloader**. The downloader first downloads the full installation kit from the Bitdefender cloud servers and then starts the installation. It is small in size and it can be run both on 32-bit and 64-bit systems (which makes it easy to distribute). On the downside, it requires an active Internet connection.

- **Full Kit**. The full kit is to be used to install protection on computers with slow or no Internet connection. Download this file to an Internet-connected computer, then distribute it to other computers using external storage media or a network share.

  Note
  Available full kit versions:
  - **Windows OS:** 32-bit and 64-bit systems
  - **Mac OS X:** only 64-bit systems

  Make sure to use the correct version for the computer you install on.

5. Save the file to the computer.

5.9.3. Send Installation Packages Download Links by Email

You may need to quickly inform other users that an installation package is available to download. In this case, follow the steps described hereinafter:

1. Go to the **Network > Packages** page.
2. Select the installation package that you want.
3. Click the **Send download links** button at the right-side of the table. A configuration window will appear.
4. Enter the email of each user you want to receive the installation package download link. Press `Enter` after each email.

   Please make sure that each entered email address is valid.
5. If you want to view the download links before sending them by email, click the **View installation links** button.
6. Click **Send**. An email containing the installation link is sent to each specified email address.

5.10. Viewing and Managing Tasks

The **Network > Tasks** page allows you to view and manage all the tasks you have created.

Once you have created a task for one of several network objects, you can view it in the tasks table.

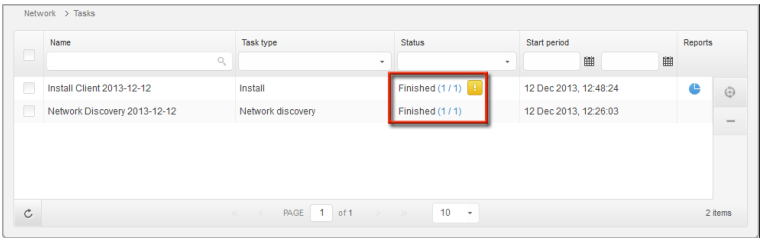
You can do the following from the **Network > Tasks** page:

- Check the task status
- View task reports
- Re-run tasks
- Delete tasks

5.10.1. Checking Task Status

Each time you create a task for one or several network objects, you will want to check its progress and get notified when errors occur.

Go to the **Network > Tasks** page and check the **Status** column for each task you are interested in. You can check the status of the main task, and you can also obtain detailed information about each sub-task.



The Tasks page

- **Checking the main task status**.

  The main task concerns the action launched on network objects (such as install client or scan) and contains a certain number of sub-tasks, one for each selected network object. For example, a main installation task created for eight computers contains eight sub-tasks. The numbers between brackets represent the sub-tasks completion ratio. For example, (2/8) means that two out of eight sub-tasks are finished.

  The main task status may be:
  - **Pending**, when none of the sub-tasks is started yet.
  - **In Progress**, when all sub-tasks are running. The main task status remains In Progress until the last sub-task is done.
  - **Finished**, when all sub-tasks are (successfully or unsuccessfully) finished. In case of unsuccessful sub-tasks, a warning symbol is displayed.

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

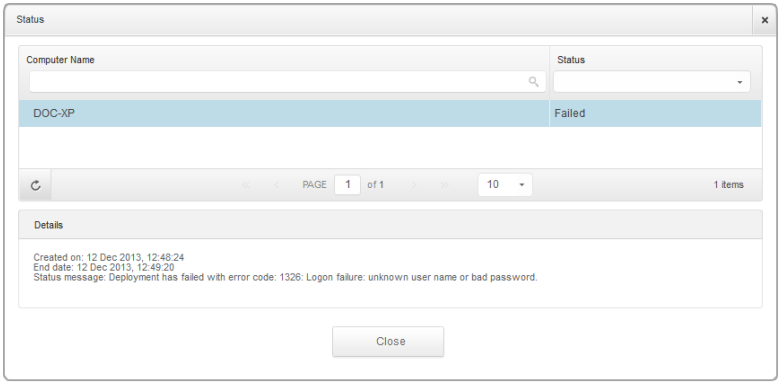
  Go to the task you are interested in and click the link available in the **Status** column to open the **Status** window. You can view the list of network objects assigned with the main task and the status of the corresponding sub-task. The sub-tasks status can be:

  - **In Progress,** when the sub-task is still running.
  - **Finished**, when the sub-task has finished successfully.
  - **Pending**, when the sub-task has not started yet. This can happen in the following situations:
    - The sub-task is waiting in a queue.

- There are connectivity issues between Control Center and the target network object.

– **Failed**, when the sub-task could not start or it had stopped due to errors, such as incorrect authentication credentials and low memory space.

To view the details of each sub-task, select it and check the **Details** section at the bottom of the table.



Tasks Status Details

You will obtain information regarding:

– Date and time when the task started.

– Date and time when the task ended.

– Description of encountered errors.

5.10.2. Viewing Task Reports

From the **Network > Tasks** page you have the option to view quick scan tasks reports.

1. Go to the **Network > Tasks** page.
2. Select the check box corresponding to the scan task you are interested in.
3. Click the corresponding button from the **Reports** column. Wait until the report is displayed. For more information, refer to “Using Reports” (p. 118).

5.10.3. Re-running Tasks

For various reasons, the client installation, uninstallation or update tasks may fail to complete. You can choose to re-run such failed tasks instead of creating new ones, following the next steps:

1. Go to the **Network > Tasks** page.
2. Select the check boxes corresponding to the failed tasks.
3. Click the **Run again** button at the right side of the table. The selected tasks will restart and the tasks status will change to **Retrying**.

Note
For tasks with multiple sub-tasks, **Run again** option is available only when all sub-tasks have finished and it will execute only the failed sub-tasks.

5.10.4. Deleting Tasks

To prevent the tasks list from getting cluttered, it is recommended to delete the tasks that you no longer need.

1. Go to the **Network > Tasks** page.
2. Select the check box corresponding to the task you want to delete.
3. Click the **Delete** button at the right side of the table. You will have to confirm your action by clicking **Yes**.

Warning
Deleting a pending task will also cancel the task.
If a task in progress is being deleted, any pending sub-tasks will be cancelled. In this case, all finished sub-tasks cannot be undone.

5.11. Credentials Manager

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

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

5.11.1. Adding Credentials to Credentials Manager

Credentials Manager

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

   Use Windows conventions when entering the name of a domain user account, for example, `user@domain.com` or `domain\user`. To make sure that entered credentials will work, add them in both forms (`user@domain.com` and `domain\user`).

2. Click the + **Add** button. The new set of credentials is added to the table.

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

5.11.2. Deleting Credentials from Credentials Manager

To delete obsolete credentials from the Credentials Manager:

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

6. Security Policies

Once installed, the Bitdefender protection can be configured and managed from Control Center using security policies. A policy specifies the security settings to be applied on computers.

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

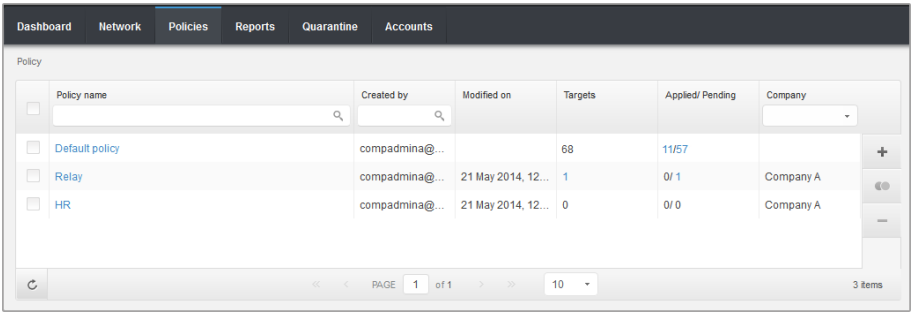
You can create as many policies as you need based on security requirements.

This is what you need to know about policies:

- Policies are created in the **Policies** page and assigned to network objects from the **Network** page.
- Network objects can have only one active policy at a time.
- Policies are pushed to target network objects immediately after creating or modifying them. Settings should be applied on network objects in less than a minute (provided they are online). If a network object is not online, settings will be applied as soon as it gets back online.
- The policy applies only to the installed protection modules. Please note that only antimalware protection is available for server operating systems.
- You cannot edit policies created by other users (unless the policy owners allow it from the policy settings), but you can override them by assigning the target objects a different policy.

6.1. Managing Policies

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



The Policies page

Existing policies are displayed in the table. For each policy, you can see:

- Policy name.
- User who created the policy.
- Date and time when the policy was last modified.
- The number of targets to which the policy was sent. Click the number to display in the network inventory the corresponding targets.
- The number of targets for which the policy was applied / is pending. Click the number that you want to display in the network inventory the corresponding targets.

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

6.1.1. Creating Policies

You can create policies by two methods: add a new one or duplicate (clone) an existing policy.

To create a new policy:

1. Go to the **Policies** page.
2. Choose the policy creation method:
   - **Add a new policy**.
     - Click the **Add** button at the right side of the table. This command creates a new policy starting from the default policy template.

- **Clone an existing policy**.
  a. Select the check box of the policy you want to duplicate.
  b. Click the **Clone** button at the right side of the table.

3. Configure the policy settings. For detailed information, refer to “Computer Policies” (p. 72).
4. Click **Save** to create the policy and return to the policies list.

6.1.2. Changing Policy Settings

Policy settings can be initially configured when creating the policy. Later on, you can change them as needed anytime you want.

Note
By default, only the user who created the policy can modify it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page.

To change the settings of an existing policy:

1. Go to the **Policies** page.
2. Find the policy you are looking for in the list and click its name to edit it.
3. Configure the policy settings as needed. For detailed information, refer to “Computer Policies” (p. 72).
4. Click **Save**.

   Policies are pushed to target network objects immediately after changing the policy assignments or after modifying the policy settings. Settings should be applied on network objects in less than a minute (provided they are online). If a network object is not online, settings will be applied as soon as it gets back online.

6.1.3. Renaming Policies

Policies should have suggestive names so that you or other administrator can quickly identify them.

To rename a policy:

1. Go to the **Policies** page.
2. Click the policy name. This will open the policy page.
3. Enter a new name for the policy.
4. Click **Save**.

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

6.1.4. Deleting Policies

If you no longer need a policy, delete it. Once the policy is deleted, the network objects to which it used to apply will be assigned the policy of the parent group. If no other policy applies, the default policy will be enforced eventually.

Note
By default, only the user who created the policy can delete it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page.

To delete a policy:

1. Go to the **Policies** page.
2. Select the corresponding check box.
3. Click the **Delete** button at the right side of the table. You will have to confirm your action by clicking **Yes**.

6.1.5. Assigning Policies to Network Objects

Once you have defined the necessary policies in the **Policies** section, you can assign them to the network objects in the **Network** section.

All network objects are initially assigned with the default policy.

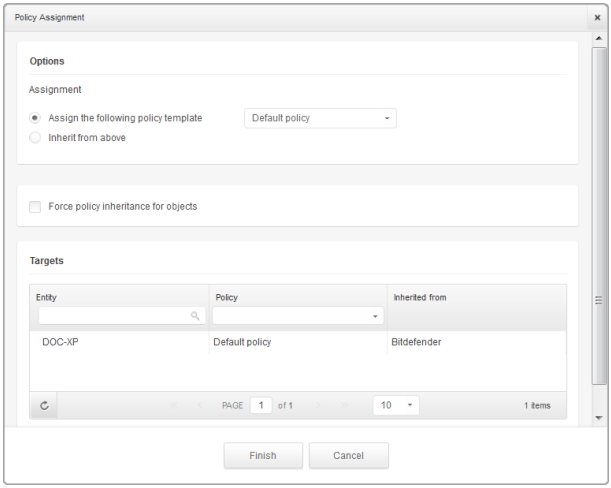
Note
You can assign only policies created by you. To assign a policy created by another user, you have to clone it first in the **Policies** page.

To assign a policy:

1. Go to the **Network** page.
2. Select the check box of the desired network object. You can select one or several objects only from the same level.
3. Click the **Assign Policy** button at the right side of the table.

   Note
   You can also right-click on a network tree group and choose **Assign Policy** from the context menu.

   The **Policy assignment** window is displayed:



Policy Assignment Settings

4. Configure the policy assignment settings for the selected objects:
   - View the current policy assignments for the selected objects in the table under the **Targets** section.
   - **Assign the following policy template**. Select this option to assign the target objects with one policy from the menu displayed at the right. Only the policies created from your user account are available in the menu.
   - **Inherit from above**. Select the **Inherit from above** option to assign the selected network objects with the parent group's policy.
   - **Force policy inheritance for objects**. By default, each network object inherits the policy of the parent group. If you change the group policy, all the group's children will be affected, excepting the group's members for which you have specifically assigned another policy.

     Select **Force policy inheritance for objects** option to apply the chosen policy to a group, including to the group's children assigned with a different policy. In this case, the table placed below will display the selected group's children that do not inherit the group policy.
5. Click **Finish** to save and apply changes.

Policies are pushed to target network objects immediately after changing the policy assignments or after modifying the policy settings. Settings should be applied on network objects in less than a minute (provided they are online). If a network objects is not online, settings will be applied as soon as it gets back online.

To check if the policy has been successfully assigned, go to the **Network** page and click the name of the object you are interested in to display the **Details** window. Check the **Policy** section to view the status of the current policy. If in pending state, the policy has not been applied yet to the target object.

6.2. Computer Policies

Policy settings can be initially configured when creating the policy. Later on, you can change them as needed anytime you want.

To configure the settings of a policy:

1. Go to the **Policies** page.
2. Click the policy name. This will open the policy settings page.
3. Configure the policy settings as needed. Settings are organized under the following categories:
   - General
   - Antimalware
   - Firewall
   - Content Control

   You can select the settings category using the menu on the left-side of the page.
4. Click **Save** to save changes and apply them to the target computers. To leave the policy page without saving changes, click **Cancel**.

Note
To learn how to work with policies, refer to "Managing Policies" (p. 68).

6.2.1. General

General settings help you manage user interface display options, communication options, update preferences, password protection and other settings of Endpoint Security.

The settings are organized into the following sections:

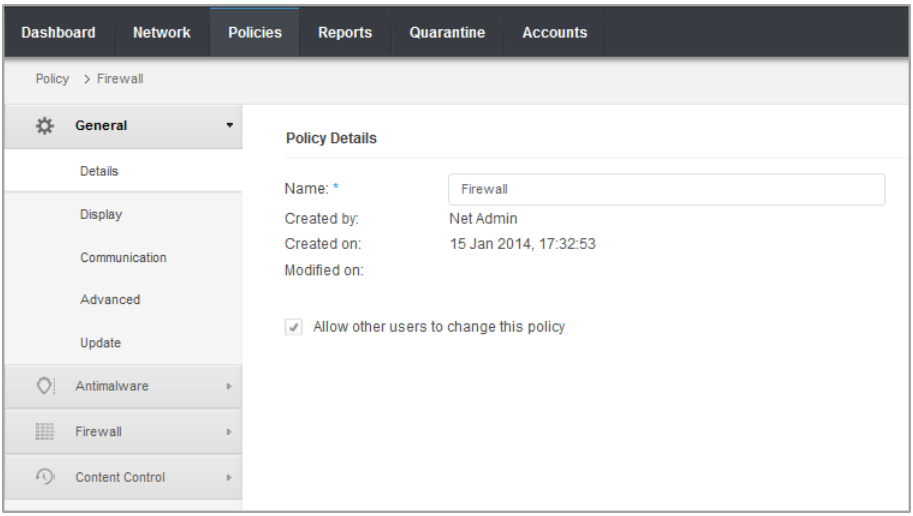
- Details
- Display
- Communication
- Advanced
- Update

Details

The Details page shows general policy details:

- Policy name

- User who created the policy
- Date and time when the policy was created
- Date and time when the policy was last modified



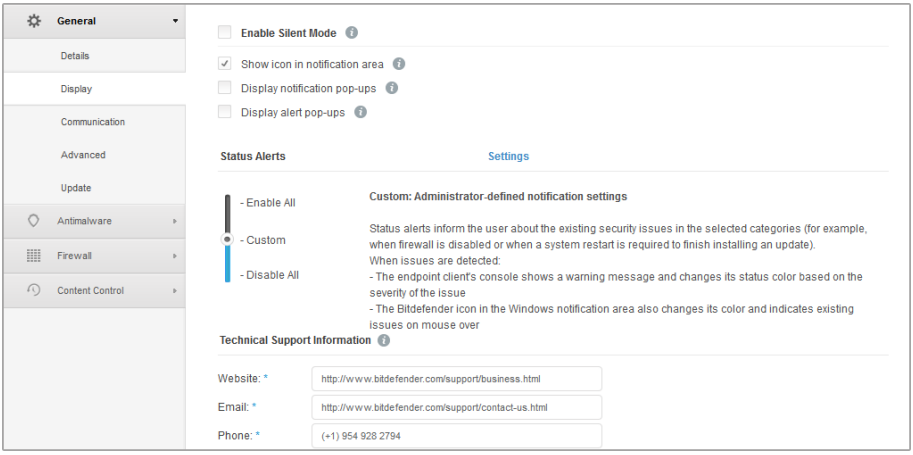
Computer Policies

You can rename the policy by entering the new name in the corresponding field and clicking **Save**. Policies should have suggestive names so that you or other administrator can quickly identify them.

Note
By default, only the user who created the policy can modify it. To change that, the policy owner must check the option **Allow other users to change this policy** from the policy's **Details** page.

Display

In this section you can configure the user interface display options.



Computer Policies - Display settings

- **Enable Silent Mode.** Use the checkbox to turn Silent Mode on or off. Silent Mode is designed to help you easily disable user interaction in Endpoint Security. When turning on Silent Mode, the following changes are made to the policy configuration:
  - The **Show icon in notification area**, **Display notification pop-ups** and **Display alert pop-ups** options in this section will be disabled.
  - If the firewall protection level was set to **Ruleset and ask** or **Ruleset, known files and ask** it will be changed to **Ruleset, known files and allow**. Otherwise, the protection level setting will remain unchanged.
- **Show icon in notification area.** Select this option to show the Bitdefender icon in the notification area (also known as the system tray). The icon informs users on their protection status by changing its appearance and displaying a corresponding notification pop-up. Additionally, users can right-click it to quickly open the Endpoint Security main window or **About** window. Opening the **About** window automatically initiates an on-demand update.
- **Display notification pop-ups.** Select this option to inform users about important security events such as the detection of malware and the action taken through small notification pop-ups. The pop-ups disappear automatically within a few seconds without user intervention.
- **Display alert pop-ups.** Different from notification pop-ups, alert pop-ups prompt users for action. If you choose not to display alert pop-ups, Endpoint Security automatically takes the recommended action. Alert pop-ups are generated in the following situations:
  - If the firewall is set to prompt the user for action whenever unknown applications request network or Internet access.

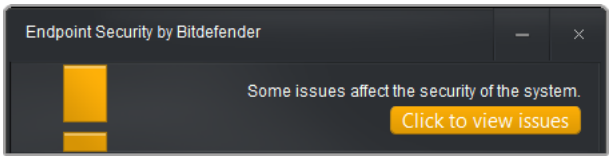
– If Active Virus Control / Intrusion Detection System is enabled, whenever a potentially dangerous application is detected.

– If device scanning is enabled, whenever an external storage device is connected to the computer. You can configure this setting in the **Antimalware > On-demand** section.

- **Status Alerts.** Users determine when their endpoint has security configuration issues or other security risks, based on status alerts. For example, users can view whenever there is a problem related to their antimalware protection, such as: On-Access scanning module is disabled or a full system scan is overdue.

  Users are informed about their protection status in two ways:

  – By the notification area of the main window, which displays an appropriate status message and changes its color depending on the severity of the security issues. Users have the possibility to view issues details as well, by clicking the available button.



Endpoint Security notification area

  – By the Bitdefender icon in the system tray, which changes its appearance when issues are detected.

  Endpoint Security uses the following color scheme for notification area:

  – Green: No issues are detected.

  – Orange: The endpoint has non-critical issues that affect its security. Users don't have to interrupt their current work for resolving these issues.

  – Red: The endpoint has critical issues that require user's immediate action.

  To configure the status alerts, select the alerting level that best suits your needs (**Enable All**, **Custom**, **Disable All**). Use the description on the right side of the scale to guide your choice.

  If you want to customize alerts:

  1. Select the **Custom** level of the scale.
  2. Click the **Settings** link to open the configuration window.
  3. Select the security aspects that you want to be monitored. The options are described herein:

- **General**. The status alert is generated whenever a system restart is required during or after a product maintenance operation. You may choose to show the alert as a warning or a critical issue.
- **Antimalware**. Status alerts are generated in the following situations:
  - On-Access scanning is enabled but many local files are skipped.
  - A certain number of days have passed since the last full system scan has been performed on the machine.

  You may select how to show the alerts and define the number of days from the last full system scan.
- **Firewall**. This status alert is generated when the Firewall module is disabled.
- **Content Control**. This status alert is generated when the Content Control module is disabled.
- **Update**. The status alert is generated whenever a system restart is required to complete an update operation. You may select to show the alert as a warning or a critical issue.

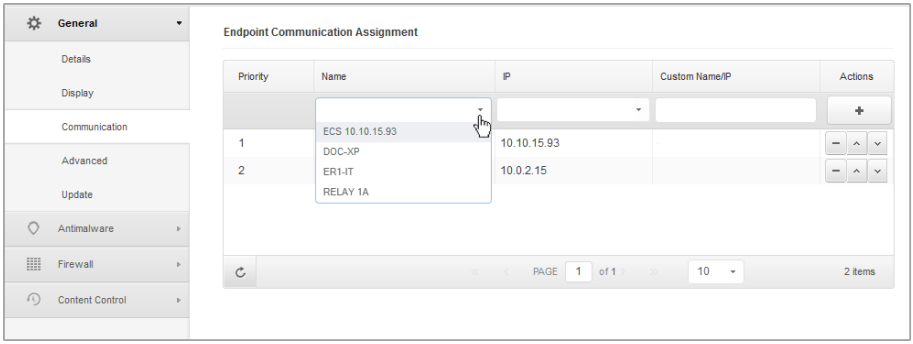
- **Technical Support Information.** You can customize the technical support and contact information available in Endpoint Security by filling in the corresponding fields. Users can access this information from the Endpoint Security window by clicking the icon in the lower-right corner or, alternatively, by right-clicking the Bitdefender icon in the system tray and selecting **About**.

Communication

When multiple Endpoint Security Relays are available in the target network, you can assign the selected computers with one or several Endpoint Security Relays via policy.

To assign an Endpoint Security Relay to target computers:

1. In the **Endpoint Communication Assignment** table, click the **Name** field. The list of Endpoint Security Relays detected in your network is displayed.
2. Select an entity.



Computer Polices - Communication settings

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

   The Endpoint Security Relay is added to the list. All target computers will communicate with Control Center via the specified Endpoint Security Relay.

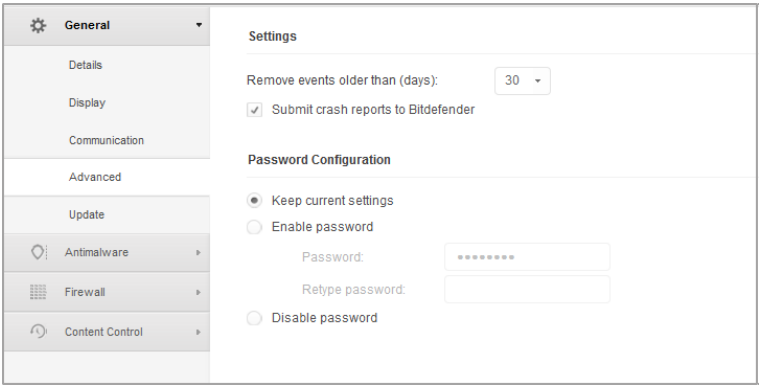
4. Follow the same steps to add several Endpoint Security Relays, if available.

5. You can configure the Endpoint Security Relays priority using the up and down arrows available at the right side of each entity. The communication with target computers will be carried out through the entity placed on top of the list. When the communication with this entity cannot be done, the next one will be taken into account.

6. To delete one entity from the list, click the corresponding − **Delete** button at the right side of the table.

Advanced

In this section you can configure general settings and the uninstall password.



Computer Policies - Advanced settings

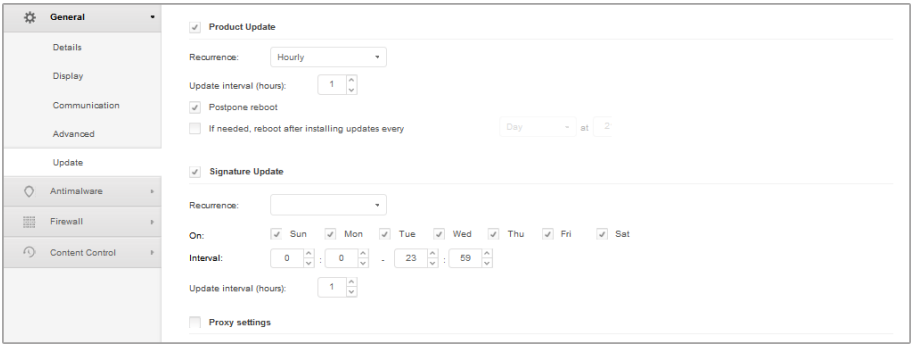
- **Remove events older than (days).** Endpoint Security keeps a detailed log of events concerning its activity on the computer (also including computer activities monitored by Content Control). By default, events are deleted from the log after 30 days. If you want to change this interval, choose a different option from the menu.
- **Submit crash reports to Bitdefender.** Select this option so that reports will be sent to Bitdefender Labs for analysis if Endpoint Security crashes. The reports will help our engineers find out what caused the problem and prevent it from occurring again. No personal information will be sent.
- **Password configuration.** To prevent users with administrative rights from uninstalling protection, you must set a password.

  The uninstall password can be configured before installation by customizing the installation package. If you have done so, select **Keep current settings** to keep the current password.

  To set the password, or to change the current password, select **Enable password** and enter the desired password. To remove password protection, select **Disable password**.

Update

In this section you can configure the Endpoint Security and virus signature update settings. Updates are very important as they allow countering the latest threats.



Computer Policies - Update options

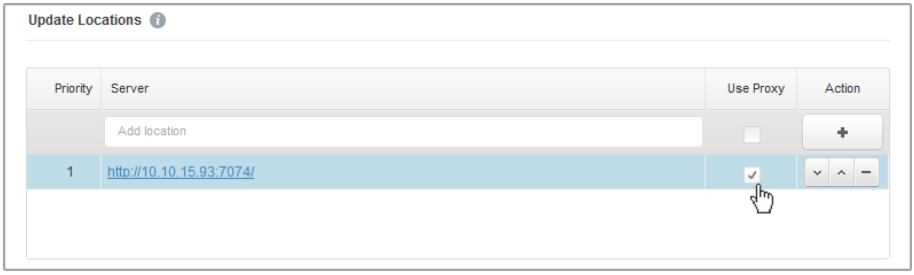
- **Product Update.** Endpoint Security automatically checks for, downloads and installs updates every hour (default setting). Automatic updates are performed silently in the background.
  - **Recurrence**. To change the automatic update recurrence, choose a different option from the menu and configure it according to your needs in the subsequent fields.
  - **Postpone reboot**. Some updates require a system restart to install and work properly. By selecting this option, the program will keep working with the old files until the computer is restarted, without informing the user. Otherwise, a notification in the user interface will prompt the user to restart the system whenever an update requires it.
  - If you choose to postpone reboot, you can set a convenient time when computers will reboot automatically if (still) needed. This can be very useful for servers. Select **If needed, reboot after installing updates** and specify when it is convenient to reboot (daily or weekly on a certain day, at a certain time of day).
- **Signature Update.** Endpoint Security automatically checks for signature update every hour (default setting). Automatic updates are performed silently in the background. To change the automatic update recurrence, choose a different option from the menu and configure it according to your needs in the subsequent fields.
- **Proxy Settings.** Select this option if computers connect to the Internet (or to the local update server) through a proxy server. There are three options to set the proxy settings:
  - **Import proxy settings from default browser.** Endpoint Security can import proxy settings from the most popular browsers, including the latest versions of Internet Explorer, Mozilla Firefox and Opera.
  - **Auto-detect network proxy.** Endpoint Security uses the Web Proxy Auto-Discovery (WPAD) protocol included in Windows to automatically retrieve proxy settings from a Proxy Auto-Configuration (PAC) file published on the local network. If no PAC file is available, updates will fail.

– **Use custom proxy settings.** If you know the proxy settings, select this option and then specify them:
  - **Server** - type in the IP of the proxy server.
  - **Port** - type in the port used to connect to the proxy server.
  - **Username** - type in a user name recognized by the proxy.
  - **Password** - type in the valid password of the previously specified user.

Note
Changing the proxy configuration option will overwrite existing proxy settings in Endpoint Security.

Additionally, you must select the **Use Proxy** check box corresponding to the update location to which the settings apply (the Internet or local update server address).

- **Update Locations**. To avoid overloading the outside network traffic, Endpoint Security is configured to update from http://upgrade.bitdefender.com. You can also add other local update server addresses to the list and configure their priority using the up and down buttons displayed on mouse-over. If the first update location is unavailable, the next one is checked and so on.



Computer Policies - Update Locations

To set the local update address:

1. Enter the address of the local update server in the **Add location** field. Use one of these syntaxes:
   – `update_server_ip:port`
   – `update_server_name:port`

   The default port is 7074.
2. If client computers connect to the local update server through a proxy server, select **Use Proxy**.
3. Click the **Add** button at the right side of the table.

4. Use the ^ Up / v Down arrows in the **Action** column to set the local update address the first one in the list. Place the mouse cursor over the corresponding row in order for the arrows to become visible.

To remove a location from the list, move the cursor over it and click the corresponding – **Delete** button. Although you can remove the default update location, this is not recommended.

6.2.2. Antimalware

The Antimalware module protects the system against all kinds of malware threats (viruses, Trojans, spyware, rootkits, adware and so on). The protection is divided in two categories:

- On-access scanning: prevents new malware threats from entering the system.
- On-demand scanning: allows detecting and removing malware already residing in the system.

When it detects a virus or other malware, Endpoint Security will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to isolate the infection. When a virus is in quarantine, it cannot do any harm because it cannot be executed or read.

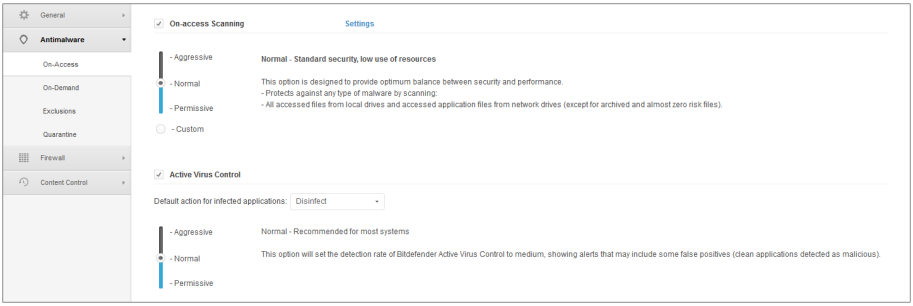
Advanced users can configure scan exclusions if they do not want specific files or file types to be scanned.

The settings are organized into the following sections:

- On-Access
- On-Demand
- Exclusions
- Quarantine

On-Access

In this section you can configure the two real-time antimalware protection components:



Computer Policies - On Access Settings

- On-access scanning
- Active Virus Control

On-access Scanning Settings

On-access scanning prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors and potentially unwanted applications (PUA).

To configure on-access scanning:

1. Use the checkbox to turn on-access scanning on or off. If you turn off on-access scanning, computers will be vulnerable to malware.
2. For a quick configuration, click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.
3. You can configure the scan settings in detail by selecting the **Custom** protection level and clicking the **Settings** link. The **On-access Scanning Settings** window will appear, containing the several options organized under two tabs, **General** and **Advanced**. Options are described hereinafter from the first tab to the last:

   - **Scan local files**. Use these options to specify which types of files you want to be scanned. Scan preferences can be configured separately for local files (stored on the local computer) or network files (stored on network shares). If antimalware protection is installed on all computers in the network, you may disable the network files scan to allow for a faster network access.

     You can set Endpoint Security to scan all accessed files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all accessed files provides best protection, while scanning applications only can be used for better system performance.

Note
Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "List of Application File Types" (p. 145).

If you want only specific extensions to be scanned, choose **User defined extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

For system performance reasons, you can also exclude large files from scanning. Select **Maximum size (MB)** checkbox and specify the size limit of the files which will be scanned. Use this option wisely because malware can affect larger files too.

- **Archives** Select **Scan inside archives** if you want to enable on-access scanning of archived files. Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having on-access scanning enabled.

  If you decide on using this option, you can configure the following optimization options:

  – **Archive maximum size (MB).** You can set a maximum accepted size limit of archives to be scanned on-access. Select the corresponding check box and type the maximum archive size (in MB).

  – **Archive maximum depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.

- **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.

  – **Scan boot sectors.** Scans the system's boot sector. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.

  – **Scan only new or changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.

  – **Scan for keyloggers.** Keyloggers record what you type on your keyboard and send reports over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

  – **Scan for Potentially Unwanted Applications (PUA).** A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express

installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

- **Scan Actions.** Depending on the type of detected file, the following actions are taken automatically:
  - **Default action for infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Endpoint Security can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

    If an infected file is detected, Endpoint Security will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

    Important

    For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

  - **Default action for suspect files.** Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Endpoint Security cannot be sure that the file is actually infected with malware. Suspect files cannot be disinfected, because no disinfection routine is available.

    When a suspect file is detected, users will be denied access to that file in order to prevent a potential infection.

Though not recommended, you can change the default actions. You can define two actions for each type of file. The following actions are available:

Deny access
Deny access to detected files.

Disinfect
Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

Delete
Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Move to quarantine
Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

Active Virus Control Settings

Bitdefender Active Virus Control is an innovative proactive detection technology which uses advanced heuristic methods to detect new potential threats in real time.

Active Virus Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful. Active Virus Control will automatically try to disinfect the detected file. If the disinfection routine fails, Active Virus Control will delete the file.

Note
Before applying the disinfect action, a copy of the file is sent to quarantine so as you can restore the file later, in the case of a false positive. This action can be configured using the **Copy files to quarantine before applying the disinfect action** option available in the **Quarantine** tab of the policy settings. This option is enabled by default in the policy templates.

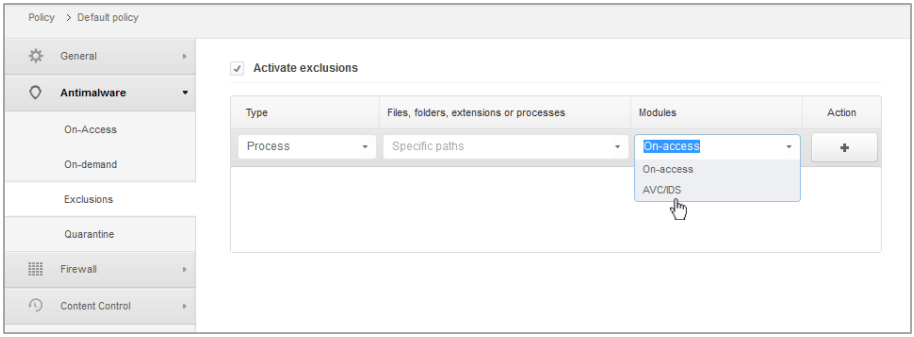
Note
For more information, go to our web site and check out the whitepaper on Active Virus Control.

To configure Active Virus Control:

1. Use the checkbox to turn Active Virus Control on or off. If you turn off Active Virus Control, computers will be vulnerable to unknown malware.
2. The default action for infected applications detected by Active Virus Control is disinfect. To set another default action, use the available menu.
3. Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.

   Note
   As you set the protection level higher, Active Virus Control will require fewer signs of malware-like behavior to report a process. This will lead to a higher number of applications being reported and, at the same time, to an increased likelihood of false positives (clean applications detected as malicious).

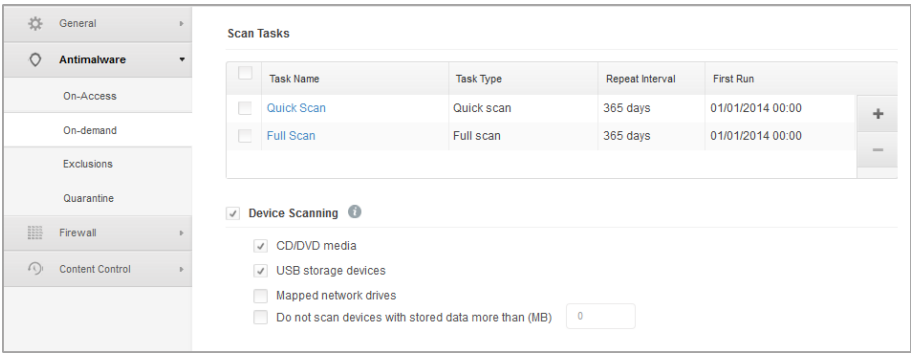
4. You should create exclusion rules for commonly used or known applications to prevent false positives (incorrect detection of legitimate applications). Go to the Exclusions tab and configure **AVC/IDS process exclusion rules** for trusted applications.



Computer policy - AVC/IDS process exclusion

On-Demand

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



Computer Policies - On Demand Scan Tasks

The scanning is performed silently in the background. The user is informed that a scanning process is running only through an icon that appears in the system tray.

Though not mandatory, it is recommended to schedule a comprehensive system scan to run weekly on all computers. Scanning computers regularly is a proactive security measure that can help detect and block malware that might evade real-time protection features.

Besides regular scans, you can also configure the automatic detection and scanning of external storage media.

Managing Scan Tasks

The Scan Tasks table informs you of the existing scan tasks, providing important information on each of them:

- Task name and type.
- Schedule based on which the task runs regularly (recurrence).
- Time when the task was first run.

There are two default system scan tasks which you can configure to run as needed:

- **Quick Scan** uses in-the-cloud scanning to detect malware running in the system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.
- **Full Scan** checks the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

The scan options of the default scan tasks are preconfigured and you cannot change them.

Besides the default scan tasks (which you cannot delete or duplicate), you can create as many custom scan tasks as you want. A custom scan task allows you to choose the specific locations to be scanned and to configure the scan options.

To create and configure a new custom scan task, click the + **Add** button at the right side of the table. To change the settings of an existing scan task, click the name of that task. Refer to the following topic to learn how to configure the task settings.

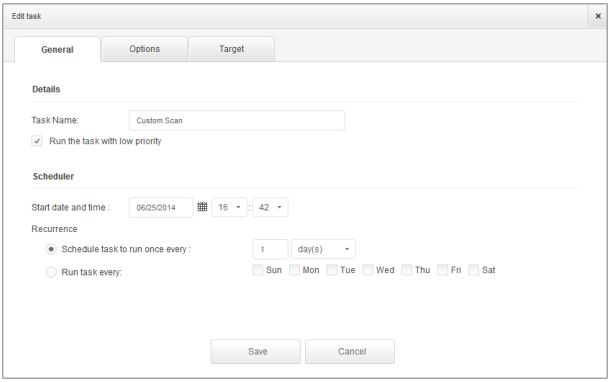
To remove a task from the list, select the task and click the − **Delete** button at the right side of the table.

Configuring Scan Tasks

The scan task settings are organized under three tabs:

- **General**: set task name and execution schedule.
- **Options**: choose a scan profile for quick configuration of the scan settings and define scan settings for a custom scan.
- **Target**: select the files and folders to be scanned.

Options are described hereinafter from the first tab to the last:



Computer Policies - Configuring On Demand Scan Tasks General Settings

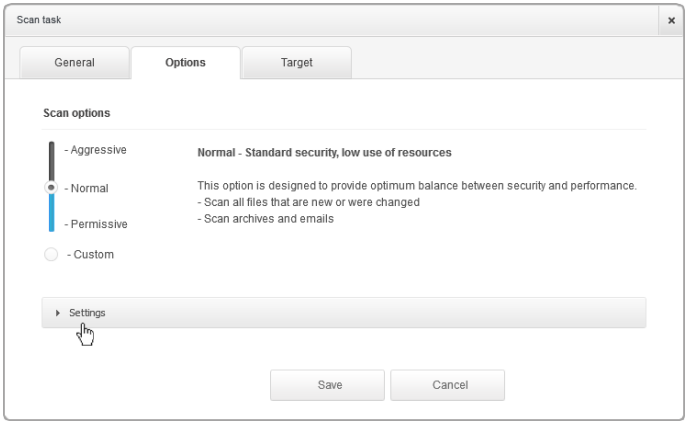
- **Details.** Choose a suggestive name for the task to help easily identify what it is about. When choosing a name, consider the scan task target and possibly the scan settings.
- **Scheduler.** Use the scheduling options to configure the scan schedule. You can set the scan to run every few hours, days or weeks, starting with a specified date and time.

  Please consider that computers must be on when the schedule is due. A scheduled scan will not run when due if the computer is turned off, hibernating or in sleep mode, or if no user is logged on. In such situations, the scan will be postponed until next time.

  Note
  The scheduled scan will run at the target endpoint local time. For example, if the scheduled scan is set to start at 6:00 PM and the endpoint is in a different timezone than Control Center, the scanning will start at 6:00 PM (endpoint time).

- **Scan Options.** Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.

  Based on the selected profile, the scan options in the **Settings** section are automatically configured. However, if you want to, you can configure them in detail. To do that, select the **Custom** check box and then go to the **Settings** section.



Computers Scan Task

- **File Types.** Use these options to specify which types of files you want to be scanned. You can set Endpoint Security to scan all files (regardless of their file extension), application files only or specific file extensions you consider to be dangerous. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Note

  Application files are far more vulnerable to malware attacks than other types of files. For more information, refer to "List of Application File Types" (p. 145).

  If you want only specific extensions to be scanned, choose **User Defined Extensions** from the menu and then enter the extensions in the edit field, pressing `Enter` after each extension.

- **Archives.** Archives containing infected files are not an immediate threat to system security. The malware can affect the system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

  Note

  Scanning archived files increases the overall scanning time and requires more system resources.

  – **Scan inside archives.** Select this option if you want to check archived files for malware. If you decide on using this option, you can configure the following optimization options:

- **Limit archive size to (MB).** You can set a maximum accepted size limit of archives to be scanned. Select the corresponding check box and type the maximum archive size (in MB).
- **Maximum archive depth (levels).** Select the corresponding check box and choose the maximum archive depth from the menu. For best performance choose the lowest value, for maximum protection choose the highest value.

– **Scan email archives.** Select this option if you want to enable scanning of email message files and email databases, including file formats such as .eml, .msg, .pst, .dbx, .mbx, .tbb and others.

Note
Email archive scanning is resource intensive and can impact system performance.

- **Miscellaneous.** Select the corresponding check boxes to enable the desired scan options.
  - **Scan boot sectors.** Scans the system's boot sector. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
  - **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.
  - **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.
  - **Scan for keyloggers.** Select this option to scan for keylogger software.
  - **Scan memory.** Select this option to scan programs running in the system's memory.
  - **Scan cookies.** Select this option to scan the cookies stored by browsers on the computer.
  - **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
  - **Scan for Potentially Unwanted Applications (PUA).** A Potentially Unwanted Application (PUA) is a program that may be unwanted on the PC and sometimes comes bundled with freeware software. Such programs can be installed without the user's consent (also called adware) or will be included by default in the express installation kit (ad-supported). Potential effects of these programs include the display of pop-ups, installing unwanted toolbars in the default browser or running several processes in the background and slowing down the PC performance.

- **Actions.** Depending on the type of detected file, the following actions are taken automatically:
  - **Default action for infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Endpoint Security can normally remove the malware code from an infected file and reconstruct the original file. This operation is known as disinfection.

    If an infected file is detected, Endpoint Security will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

    Important
    For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

  - **Default action for suspect files.** Files are detected as suspicious by the heuristic analysis. Because B-HAVE is a heuristic analysis technology, Endpoint Security cannot be sure that the file is actually infected with malware. Suspect files cannot be disinfected, because no disinfection routine is available.

    Scan tasks are configured by default to ignore suspect files. You may want to change the default action in order to move suspect files to quarantine. Quarantined files are sent for analysis to Bitdefender Labs on a regular basis. If malware presence is confirmed, a signature is released to allow removing the malware.
  - **Default action for rootkits.** Rootkits represent specialized software used to hide files from the operating system. Though not malicious in nature, rootkits are often used to hide malware or to conceal the presence of an intruder into the system.

    Detected rootkits and hidden files are ignored by default.

  Though not recommended, you can change the default actions. You can specify a second action to be taken if the first one fails and different actions for each category. Choose from the corresponding menus the first and the second action to be taken on each type of detected file. The following actions are available:

  Take no action
  No action will be taken on detected files. These files will only appear in the scan log.

  Disinfect
  Remove the malware code from infected files. It is recommended to always keep this as the first action to be taken on infected files.

  Delete
  Delete detected files from the disk, without any warning. It is advisable to avoid using this action.

Move to quarantine
Move detected files from their current location to the quarantine folder. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. You can manage quarantine files from the Quarantine page of the console.

- **Scan Target.** Add to the list all the locations you want to be scanned on the target computers.

  To add a new file or folder to be scanned:

  1. Choose a predefined location from the drop-down menu or enter the **Specific paths** you want to scan.
  2. Specify the path to the object to be scanned in the edit field.
     - If you have chosen a predefined location, complete the path as needed. For example, to scan the entire `Program Files` folder, it suffices to select the corresponding predefined location from the drop-down menu. To scan a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name.
     - If you have chosen **Specific paths**, enter the full path to the object to be scanned. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.
  3. Click the corresponding + **Add** button.

  To edit an existing location, click it. To remove a location from the list, move the cursor over it and click the corresponding − **Delete** button.

- **Exclusions.** You can either use the exclusions defined in the **Antimalware > Exclusions** section of the current policy, or you can define custom exclusions for the current scan task. For more details regarding exclusions, refer to "Exclusions" (p. 93).

Device Scanning

You can configure Endpoint Security to automatically detect and scan external storage devices when they are connected to the computer. Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- Mapped network drives
- Devices with more than a specified amount of stored data.

Device scans automatically attempt to disinfect files detected as infected or to move them to quarantine if disinfection is not possible. Take into account that no action can be taken on infected files detected on CDs/DVDs or on mapped network drives that allow read-only access.

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

If alert pop-ups are enabled in the **General > Display** section, the user is prompted whether or not to scan the detected device instead of the scan starting automatically.

When a device scan is started:

- A notification pop-up informs the user about the device scan, provided that notification pop-ups are enabled in the **General > Display** section.
- A scan icon appears in the system tray. The user can double-click this icon to open the scan window and check the scan progress.

Once the scan is completed, the user must check detected threats, if any.

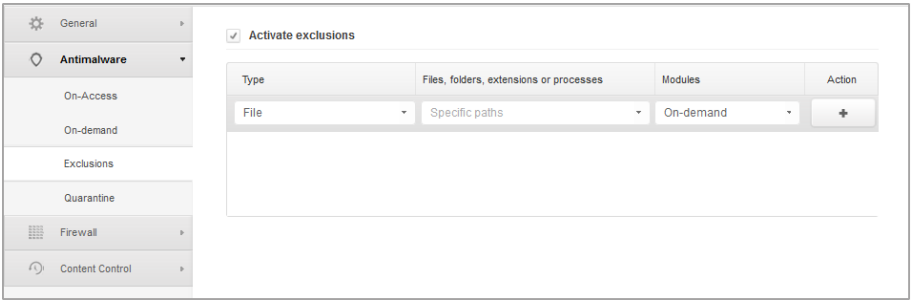
Select **Device Scanning** option to enable the automatic detection and scanning of storage devices. To configure device scanning individually for each type of device, use the following options:

- **CD/DVD media**
- **USB storage devices**
- **Mapped network drives**
- **Do not scan devices with stored data more than (MB)**. Use this option to automatically skip scanning of a detected device if the amount of stored data exceeds the specified size. Type the size limit (in megabytes) in the corresponding field. Zero means that no size restriction is imposed.

  Note
  This option applies only to CDs/DVDs and USB storage devices.

Exclusions

In this section you can configure scan exclusion rules. Exclusions can apply to on-access scanning or on-demand scanning, or to both. Based on the object of the exclusion, there are four types of exclusions:



Computer Policies - Antimalware Exclusions

- **File exclusions:** the specified file only is excluded from scanning.
- **Folder exclusions:** all files inside the specified folder and all of its subfolders are excluded from scanning.
- **Extension exclusions:** all files having the specified extension are excluded from scanning.
- **Process exclusions:** any object accessed by the excluded process is also excluded from scanning. You can also configure process exclusions for the Active Virus Control and Intrusion Detection System technologies.

Important

Scan exclusions are to be used in special circumstances or following Microsoft or Bitdefender recommendations. For an updated list of exclusions recommended by Microsoft, please refer to this article. If you have an EICAR test file that you use periodically to test antimalware protection, you should exclude it from on-access scanning.

Use the check box **Activate exclusions** to turn exclusions on or off.

To configure an exclusion rule:

1. Select the exclusion type from the menu.
2. Depending on the exclusion type, specify the object to be excluded as follows:
   - **Extension exclusions.** Specify one or more file extensions to be excluded from scanning, separating them with a semicolon ";". You can enter extensions with or without the preceding dot. For example, enter `txt` to exclude text files.

     ### Note

     Before you exclude extensions, document yourself to see which are commonly targeted by malware and which are not.

   - **File, folder and process exclusions.** You must specify the path to the excluded object on the target computers.

a. Choose from the menu either a predefined location or the **Specific paths** option.

b. If you have chosen a predefined location, complete the path as needed. For example, to exclude the entire `Program Files` folder, it suffices to select the corresponding predefined location from the menu. To exclude a specific folder from `Program Files`, you must complete the path by adding a backslash (\) and the folder name. For process exclusions, you must also add the name of the application's executable file.

c. If you have chosen **Specific paths**, enter the full path to the object to be excluded. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

3. Select the types of scanning the rule will apply to. Some exclusions may be relevant for on-access scanning only, some for on-demand scanning only, while others may be recommended for both. Process exclusions can be configured for on-access scanning and for the Active Virus Control and Intrusion Detection System technologies.

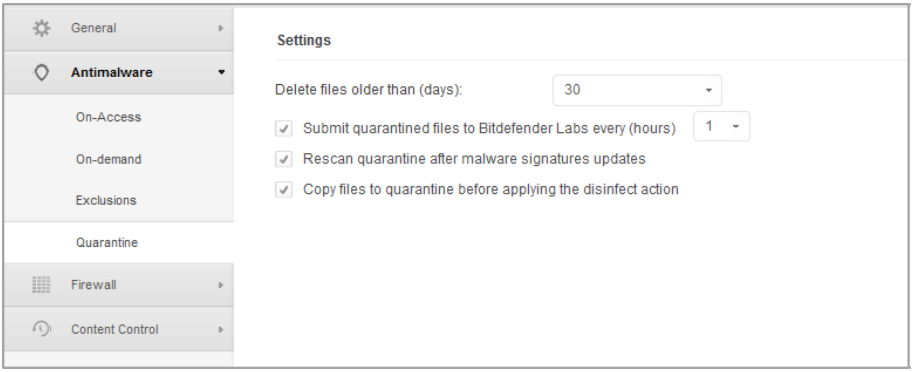
> **Note**
>
> Please note that on-demand scanning exclusions will NOT apply to contextual scanning. Contextual scanning is initiated by right-clicking a file or folder and selecting **Scan with Endpoint Security by Bitdefender**.

4. Click the **+ Add** button. The new rule will be added to the list.

To remove a rule from the list, click the corresponding **– Delete** button.

Quarantine

In this section you can configure the quarantine settings.



Computer Policies - Quarantine

You can set Endpoint Security to automatically perform the following actions:

- **Delete files older than (days).** By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, choose a different option from the menu.
- **Submit quarantined files to Bitdefender Labs every (hours).** Keep this option selected to automatically send quarantined files to Bitdefender Labs. You can edit the time interval between quarantined files are being sent (one hour by default). The sample files will be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

  By default, quarantined files are automatically sent to Bitdefender Labs every hour. If you want to change this interval, choose a different option from the menu.
- **Rescan quarantine after malware signatures updates.** Keep this option selected to automatically scan quarantined files after each malware signatures update. Cleaned files are automatically moved back to their original location.
- **Copy files to quarantine before applying the disinfect action.** Select this option to prevent data loss in case of false positives and copy each file detected as infected to quarantine before applying the disinfect action. You can afterwards restore legitimate files from the **Quarantine** page.

6.2.3. Firewall

The Firewall protects the computer from inbound and outbound unauthorized connection attempts.

The Firewall's functionality relies on network profiles. The profiles are based on trust levels, which have to be defined for each network.

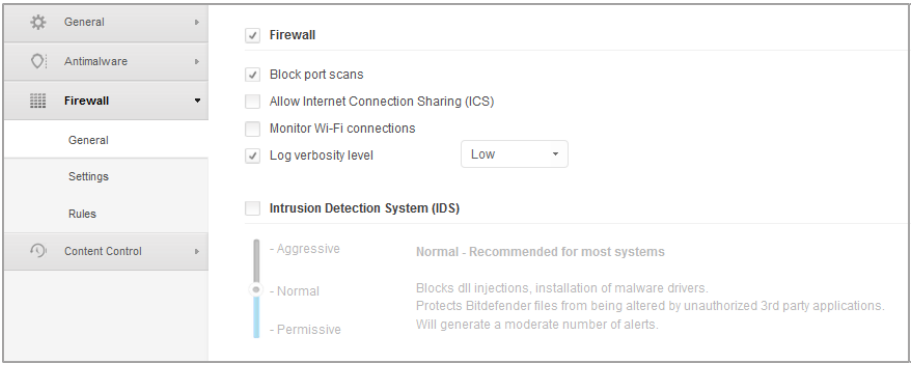
Each time a new connection is created, the Firewall detects it and compares the connection's adapter information with the information from the existing profiles, applying the correct profile. For detailed information on how the profiles are applied, see networks settings.

The settings are organized into the following sections:

- General
- Settings
- Rules

General

In this section you can enable or disable the Bitdefender Firewall and configure the general settings.



Computer Policies - Firewall General Settings

- **Firewall.** Use the checkbox to turn Firewall on or off. If you turn off firewall protection, computers will be vulnerable to network and Internet attacks.
- **Block port scans.** Port scans are frequently used by hackers to find out which ports are open on a computer. They might then break into the computer if they find a less secure or vulnerable port.
- **Allow Internet Connection Sharing (ICS).** Select this option to set the firewall to allow Internet Connection Sharing traffic.

  Note
  This option does not automatically enable ICS on the user's system.

- **Monitor Wi-Fi connections.** Endpoint Security can inform users connected to a Wi-Fi network when a new computer joins the network. To display such notifications on the user's screen, select this option.
- **Log verbosity level.** Endpoint Security maintains a log of events regarding the Firewall module usage (enabling/disabling firewall, traffic blocking, modifying settings) or generated by the activities detected by this module (scanning ports, blocking connection attempts or traffic according to the rules). Choose an option from the **Log verbosity level** to specify how much information the log should include.
- **Intrusion Detection System.** Intrusion Detection System monitors the system for suspicious activities (for example, unauthorized attempts to alter the Bitdefender files, DLL injections, keylogging attempts etc.).

  To configure Intrusion Detection System:

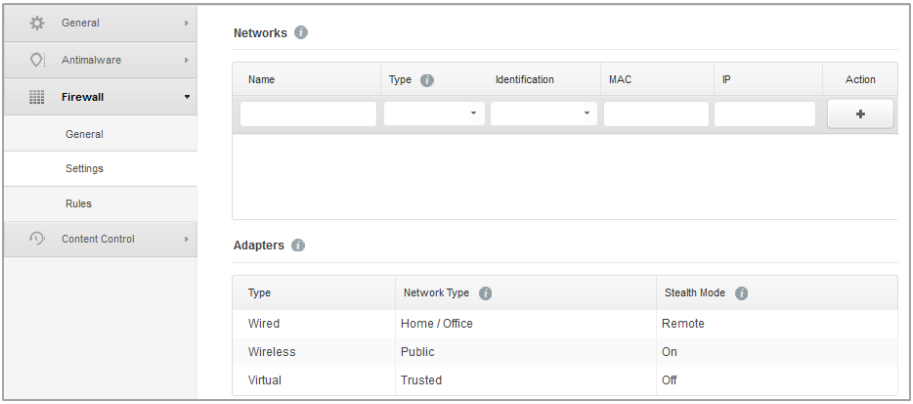
  1. Use the checkbox to turn Intrusion Detection System on or off.
  2. Click the security level that best suits your needs (Aggressive, Normal or Permissive). Use the description on the right side of the scale to guide your choice.

To prevent a legitimate application from being detected by Intrusion Detection System, add an **AVC/IDS process exclusion rule** for that application in the **Antimalware > Exclusions** section.

Settings

The firewall automatically applies a profile based on the network type. You can specify the generic profiles to be applied depending on the adapter type and also specify profiles individually for your company's networks. The settings are organized under the following tables:

- Networks
- Adapters



Computer Policies - Firewall Settings

Networks Settings

For the firewall to function properly, the administrator has to define the networks that will be managed in the **Networks** table. The fields from the **Networks** table are described as follows:

- **Name.** A name by which the administrator can recognize the network in the list.
- **Type.** Select from the menu the profile type assigned to the network.

  Endpoint Security automatically applies one of four firewall profiles to each detected network connection to define the basic traffic filtering options. The firewall profiles are:

  - **Trusted** network. Disable the firewall for the respective adapter.
  - **Home/Office** network. Allow all traffic to and from computers in the local network.
  - **Public** network. All traffic is filtered.

  - **Untrusted** network. Completely block network and Internet traffic through the respective adapter.

- **Identification.** Select from the menu the method through which the network will be identified by Endpoint Security. The networks can be identified by three methods: **DNS**, **Gateway** and **Network**.
- **MAC.** Use this field to specify the MAC address of a specific DNS server.

Note
This field is mandatory if the DNS identification method is selected.

- **IP.** Use this field to define specific IP addresses in a network. You can also use a mask to define an entire sub-network.

After you defined a network, click the **Add** button at the right side of the table to add it to the list.

Adapters Settings

If a network that is not defined in the **Networks** table is detected, Endpoint Security detects the type of the network adapter and applies a corresponding profile to the connection. The fields from the **Adapters** table are described as follows:

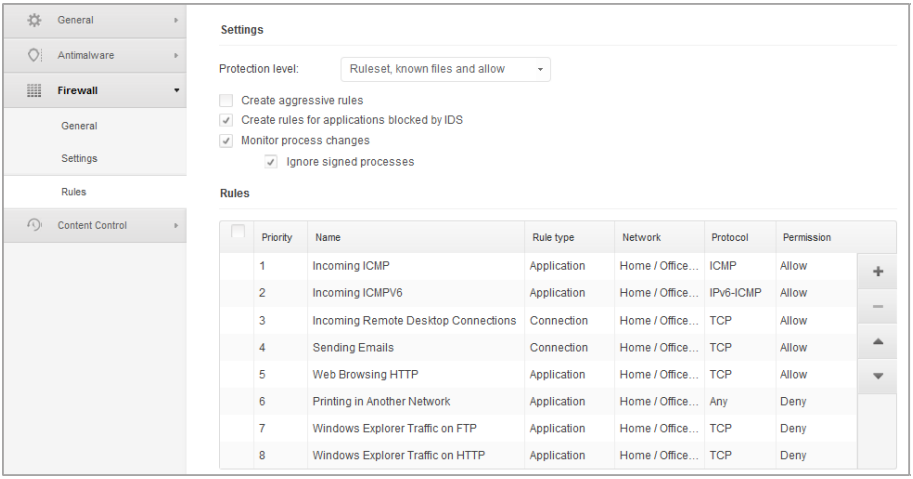
- **Type.** Displays the type of the network adapters. Endpoint Security can detect three predefined adapter types: **Wired**, **Wireless** and **Virtual** (Virtual Private Network).
- **Network Type.** Describes the network profile assigned to a specific adapter type. The network types are described in the network settings section. Clicking the network type field allows you to change the setting. If you select **Let Windows decide**, for any new network connection detected after the policy is applied, Endpoint Security applies a firewall profile based on the network classification in Windows, ignoring the settings from the **Adapters** table.

  If the detection based on Windows Network Manager fails, a basic detection is attempted. A generic profile is used in which the network type is considered **Public** and the stealth settings are set to **On**. If the IP address of the domain the computer is found in is in one of the networks associated with the adapter, then the trust level is considered **Home/Office** and the stealth settings are set to **Remote On**. If the computer is not in a domain, this condition is not applicable.
- **Stealth Mode.** Hides the computer from malicious software and hackers in the network or the Internet. Configure Stealth Mode as needed for each adapter type by selecting one of the following options:
  - **On.** The computer is invisible from both the local network and the Internet.
  - **Off.** Anyone from the local network or the Internet can ping and detect the computer.

– **Remote.** The computer cannot be detected from the Internet. Anyone from the local network can ping and detect the computer.

Rules

In this section you can configure the application network access and data traffic rules enforced by the firewall. Note that available settings apply only to the **Home/Office** and **Public** firewall profiles.



Computers policies - Firewall rules settings

Settings

You can configure the following settings:

- **Protection level.** The selected protection level defines the firewall decision-making logic used when applications request access to network and Internet services. The following options are available:

  Ruleset and allow

  Apply existing firewall rules and automatically allow all other connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

  Ruleset and ask

  Apply existing firewall rules and prompt the user for action for all other connection attempts. An alert window with detailed information about the unknown connection attempt is displayed on the user's screen. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset and deny
Apply existing firewall rules and automatically deny all other connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset, known files and allow
Apply existing firewall rules, automatically allow connection attempts made by known applications and automatically allow all other unknown connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset, known files and ask
Apply existing firewall rules, automatically allow connection attempts made by known applications and prompt the user for action for all other unknown connection attempts. An alert window with detailed information about the unknown connection attempt is displayed on the user's screen. For each new connection attempt, a rule is created and added to the ruleset.

Ruleset, known files and deny
Apply existing firewall rules, automatically allow connection attempts made by known applications and automatically deny all other unknown connection attempts. For each new connection attempt, a rule is created and added to the ruleset.

Note
Known files represent a large collection of safe, trustworthy applications, which is compiled and continuously maintained by Bitdefender.

- **Create aggressive rules.** With this option selected, the firewall will create rules for each different process that opens the application requesting network or Internet access.
- **Create rules for applications blocked by IDS.** With this option selected, the firewall will automatically create a **Deny** rule each time the Intrusion Detection System blocks an application.
- **Monitor process changes.** Select this option if you want each application attempting to connect to the Internet to be checked whether it has been changed since the addition of the rule controlling its Internet access. If the application has been changed, a new rule will be created according to the existing protection level.

Note
Usually, applications are changed by updates. But there is a risk that they might be changed by malware applications, with the purpose of infecting the local computer and other computers in the network.

Signed applications are supposed to be trusted and have a higher degree of security. You can select **Ignore signed processes** to automatically allow changed signed applications to connect to the Internet.

Rules

The Rules table lists the existing firewall rules, providing important information on each of them:

- Rule name or application it refers to.
- Protocol the rule applies to.
- Rule action (allow or deny packets).
- Actions you can take on the rule.
- Rule priority.

Note

These are the firewall rules explicitly enforced by the policy. Additional rules may be configured on computers as a result of applying firewall settings.

A number of default firewall rules help you easily allow or deny popular traffic types. Choose the desired option from the **Permission** menu.

Incoming ICMP / ICMPv6
Allow or deny ICMP / ICMPv6 messages. ICMP messages are often used by hackers to carry out attacks against computer networks. By default, this type of traffic is denied.

Incoming Remote Desktop Connections
Allow or deny other computers' access over Remote Desktop Connections. By default, this type of traffic is allowed.

Sending Emails
Allow or deny sending emails over SMTP. By default, this type of traffic is allowed.

Web Browsing HTTP
Allow or deny HTTP web browsing. By default, this type of traffic is allowed.

Printing in Another Network
Allow or deny access to printers in another local area network. By default, this type of traffic is denied.

Windows Explorer traffic on HTTP / FTP
Allow or deny HTTP and FTP traffic from Windows Explorer. By default, this type of traffic is denied.

Besides the default rules, you can create additional firewall rules for other applications installed on computers. This configuration however is reserved for administrators with strong networking skills.

To create and configure a new rule, click the + **Add** button at the right side of the table. Refer to the following topic for more information.

To remove a rule from the list, click the corresponding − **Delete** button at the right side of the table.

Note
You can neither delete nor modify the default firewall rules.

Configuring Custom Rules

You can configure two types of firewall rules:

- **Application-based rules.** Such rules apply to specific software found on the client computers.
- **Connection-based rules.** Such rules apply to any application or service that uses a specific connection.

To create and configure a new rule, click the + **Add** button at the right side of the table and select the desired rule type from the menu. To edit an existing rule, click the rule name.

The following settings can be configured:

- **Rule name.** Enter the name under which the rule will be listed in the rules table (for example, the name of the application the rule applies to).
- **Application path** (only for application-based rules). You must specify the path to the application executable file on the target computers.
  - Choose from the menu a predefined location and complete the path as needed. For example, for an application installed in the `Program Files` folder, select `%ProgramFiles%` and complete the path by adding a backslash (\) and the name of the application folder.
  - Enter the full path in the edit field. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.
- **Command line** (only for application-based rules). If you want the rule to apply only when the specified application is opened with a specific command in the Windows command line interface, type the respective command in the edit field. Otherwise, leave it blank.
- **Application MD5** (only for application-based rules). If you want the rule to check the application's file data integrity based on its MD5 hash code, enter it in the edit field. Otherwise, leave the field blank.
- **Local Address.** Specify the local IP address and port the rule applies to. If you have more than one network adapter, you can clear the **Any** check box and type a specific IP address. Likewise, to filter connections on a specific port or port range, clear the **Any** check box and enter the desired port or port range in the corresponding field.

- **Remote Address.** Specify the remote IP address and port the rule applies to. To filter the traffic to and from a specific computer, clear the **Any** check box and type its IP address.
- **Apply rule only for directly connected computers.** You can filter access based on Mac address.
- **Protocol.** Select the IP protocol the rule applies to.
  - If you want the rule to apply to all protocols, select **Any**.
  - If you want the rule to apply to TCP, select **TCP**.
  - If you want the rule to apply to UDP, select **UDP**.
  - If you want the rule to apply to a specific protocol, select that protocol from the **Other** menu.

Note

IP protocol numbers are assigned by the Internet Assigned Numbers Authority (IANA). You can find the complete list of assigned IP protocol numbers at http://www.iana.org/assignments/protocol-numbers.

- **Direction.** Select the traffic direction the rule applies to.

Direction	Description
Outbound	The rule applies only for the outgoing traffic.
Inbound	The rule applies only for the incoming traffic.
Both	The rule applies in both directions.

- **IP version.** Select the IP version (IPv4, IPv6 or any) the rule applies to.
- **Network.** Select the type of network the rule applies to.
- **Permission.** Select one of the available permissions:

Permission	Description
Allow	The specified application will be allowed network / Internet access under the specified circumstances.
Deny	The specified application will be denied network / Internet access under the specified circumstances.

Click **Save** to add the rule.

For the rules you created, use the arrows at the right side of the table to set each rule priority. The rule with higher priority is closer to the top of the list.

6.2.4. Content Control

Use the Content Control module to configure your preferences regarding content filtering and data protection for user activity including web browsing, email and software applications. You can restrict or allow web access and application usage, configure traffic scan, antiphishing and data protection rules. Please note that the configured Content Control settings will apply to all users who log on to the target computers.

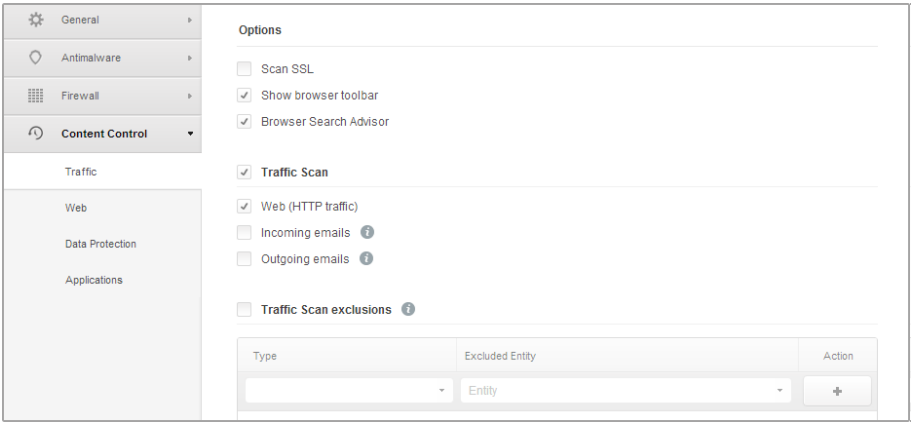
The settings are organized into the following sections:

- Traffic
- Web
- Data Protection
- Applications

Traffic

Configure the traffic security preferences using the settings under the following sections:

- Options
- Traffic Scan
- Traffic Scan Exclusions



Computer Policies - Content Control - Traffic

Options

- **Scan SSL**. Select this option if you want the Secure Sockets Layer (SSL) web traffic to be inspected by the Endpoint Security protection modules.
- **Show browser toolbar**. The Bitdefender toolbar informs users about the rating of the web pages they are viewing. The Bitdefender toolbar is not your typical browser toolbar.

The only thing it ads to the browser is a small dragger  at the top of every web page. Clicking the dragger opens the toolbar.

Depending on how Bitdefender classifies the web page, one of the following ratings is displayed on the left side of the toolbar:

- The message "This page is not safe" appears on a red background.
- The message "Caution is advised" appears on an orange background.
- The message "This page is safe" appears on a green background.

- **Browser Search Advisor.** Search advisor rates the results of Google, Bing and Yahoo! searches, as well as links from Facebook and Twitter, by placing an icon in front of every result. Icons used and their meaning:

  You should not visit this web page.

  This web page may contain dangerous content. Exercise caution if you decide to visit it.

  This is a safe page to visit.

Traffic Scan

Incoming emails and web traffic are scanned in real time to prevent malware from being downloaded to the computer. Outgoing emails are scanned to prevent malware from infecting other computers. Scanning the web traffic may slow down web browsing a little, but it will block malware coming from the Internet, including drive-by downloads.

When an email is found infected, it is replaced automatically with a standard email informing the receiver of the original infected email. If a web page contains or distributes malware, it is automatically blocked. A special warning page is displayed instead to inform the user that the requested web page is dangerous.

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

Traffic Scan Exclusions

You can choose to skip certain traffic of being scanned for malware while the traffic scan options are enabled.

To define a traffic scan exclusion:

1. Select the exclusion type from the menu.
2. Depending on the exclusion type, define the traffic entity to be excluded from scanning as follows:
   - **IP**. Enter the IP address for which you do not want to scan the incoming and outgoing traffic.

- **URL**. Excludes from scanning the specified web addresses. To define an URL scan exclusion:
  - Enter a specific URL, such as `www.example.com/example.html`
  - Use wildcards to define web address patterns:
    - Asterisk (*) substitutes for zero or more characters.
    - Question mark (?) substitutes for exactly one character. You can use several question marks to define any combination of a specific number of characters. For example, ??? substitutes for any combination of exactly three characters.

    In the following table, you can find several sample syntaxes for specifying web addresses.

Syntax	Exception Applicability
`www.example*`	Any website or web page starting with `www.example` (regardless of the domain extension). The exclusion will not apply to the subdomains of the specified website, such as `subdomain.example.com`.
`*example.com`	Any website ending in `example.com`, including pages and subdomains thereof.
`*string*`	Any website or web page whose address contains the specified string.
`*.com`	Any website having the `.com` domain extension, including pages and subdomains thereof. Use this syntax to exclude from scanning the entire top-level domains.
`www.example?.com`	Any web address starting with `www.example?.com`, where ? can be replaced with any single character. Such websites might include: `www.example1.com` or `www.exampleA.com`.

- **Application**. Excludes from scanning the specified process or application. To define an application scan exclusion:
  - Enter the full application path. For example, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Use environment variables to specify the application path. For example: `%programfiles%\Internet Explorer\iexplore.exe`
  - Use wildcards to specify any applications matching a certain name pattern. For example:
    - `c*.exe` matches all applications starting with "c" (chrome.exe).
    - `??????.exe` matches all applications with a name that contains six characters (chrome.exe, safari.exe, etc.).
    - `[^c]*.exe` matches all application except for those starting with "c".

- `[^ci]*.exe` matches all application except for those starting with "c" or "i".

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

To remove an entity from the list, click the corresponding **Delete** button.

Web

In this section you can configure the web browsing security preferences.

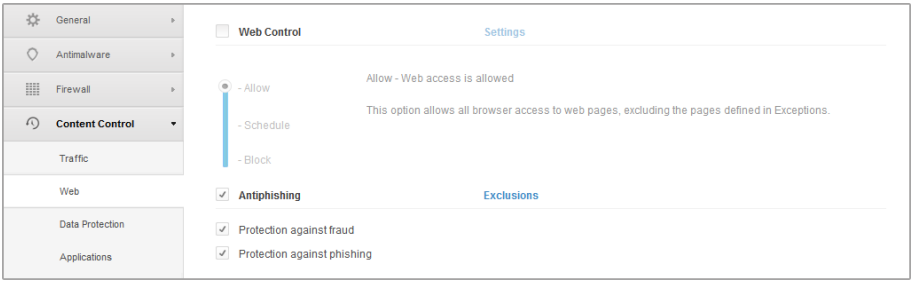
The settings are organized under the following sections:

- Web Control
- Antiphishing

Web Control

Web Control helps you allow or block web access for users or applications during specified time intervals.

The web pages blocked by Web Control are not displayed in the browser. Instead, a default web page is displayed informing the user that the requested web page has been blocked by Web Control.



Computer Policies - Content Control - Web

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

You have three configuration options:

- Select **Allow** to always grant web access.
- Select **Block** to always deny web access.
- Select **Schedule** to enable time restrictions on web access upon a detailed schedule.

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

Scheduler

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

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

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

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

2. Click **Save**.

Note

Endpoint Security will perform updates every hour no matter if web access is blocked.

Categories

Web Categories Filter dynamically filters access to websites based on their content. You can use the Web Categories Filter for defining exceptions to the selected Web Control action (Allow or Block) for entire web categories (such as Games, Mature Content or Online Networks).

To configure Web Categories Filter:

1. Select **Web Categories Filter**.
2. For a quick configuration, click one of the predefined profiles (**Aggressive**, **Normal** or **Permissive**). Use the description on the right side of the scale to guide your choice. You can view the predefined actions for available web categories by clicking the **Categories** button placed below.
3. If you are not satisfied with the default settings, you can define a custom filter:
   a. Select **Custom**.
   b. Click the **Categories** button to expand the corresponding section.
   c. Find the category that you want in the list and choose the desired action from the menu.
4. You can also choose to **Treat Web Categories as exceptions for Web Access** if you want to ignore the existing web access settings and apply only the Web Categories Filter.
5. Click **Save**.

Note

- **Allow** permission for specific web categories is also taken into account during time intervals when web access is blocked by Web Control.

- **Allow** permissions work only when web access is blocked by Web Control, while **Block** permissions work only when web access is allowed by Web Control.
- You can override the category permission for individual web addresses by adding them with opposite permission in **Web Control > Settings > Exclusions**. For example, if a web address is blocked by Web Categories Filter, add a web rule for that address with permission set to **Allow**.

Exclusions

You can also define web rules to explicitly block or allow certain web addresses, overriding the existing Web Control settings. Users will be able, for example, to access a specific webpage also when the web browsing is blocked by Web Control.

To create a web rule:

1. Select **Use Exceptions** to enable web exceptions.
2. Enter the address you want to allow or block in the **Web Address** field.
3. Select **Allow** or **Block** from the **Permission** menu.
4. Click the **Add** button at the right side of the table to add the address to the exceptions list.
5. Click **Save**.

To edit a web rule:

1. Click the web address you want to edit.
2. Modify the existing URL.
3. Click **Save**.

To remove a web rule:

1. Move the cursor over the web address you want to remove.
2. Click the **Delete** button.
3. Click **Save**.

Antiphishing

Antiphishing protection automatically blocks known phishing web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters. Instead of the phishing web page, a special warning page is displayed in the browser to inform the user that the requested web page is dangerous.

Select **Antiphishing** to activate antiphishing protection. You can further tune Antiphishing by configuring the following settings:

- **Protection against fraud**. Select this option if you want to extend protection to other types of scams besides phishing. For example, websites representing fake companies,

which do not directly request private information, but instead try to pose as legitimate businesses and make a profit by tricking people into doing business with them.

- **Protection against phishing**. Keep this option selected to protect users against phishing attempts.

If a legitimate web page is incorrectly detected as phishing and blocked, you can add it to the whitelist to allow users to access it. The list should contain only websites you fully trust.

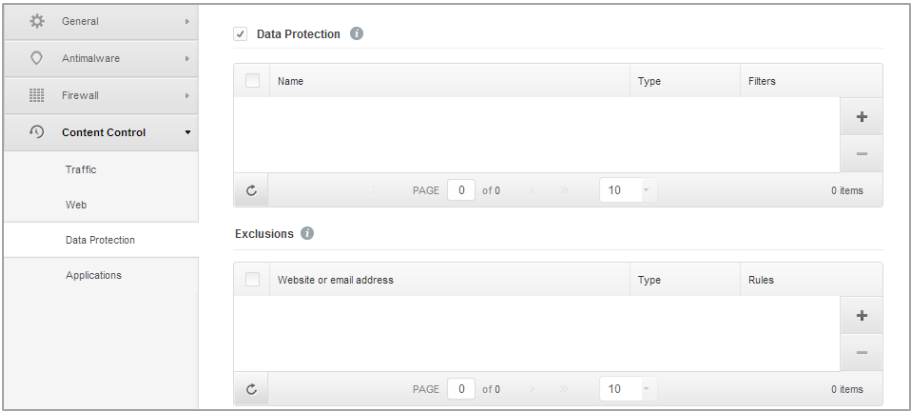
To manage antiphishing exceptions:

1. Click **Exclusions**.
2. Enter the web address and click the **Add** button.

   To remove an exception from the list, move the cursor over it and click the **Delete** button.
3. Click **Save**.

Data Protection

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



Computer Policies - Content Control - Data Protection

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

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

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

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

To configure Data Protection:

1. Use the checkbox to turn on Data Protection.
2. Create data protection rules for all of the sensitive data you want to protect. To create a rule:
   a. Click the + **Add** button at the right side of the table. A configuration window is displayed.
   b. Enter the name under which the rule will be listed in the rules table. Choose a suggestive name so that you or other administrator can easily identify what the rule is about.
   c. Enter the data you want to protect (for example, the phone number of a company executive or the internal name of a new product the company is working on). Any combination of words, numbers or strings consisting of alphanumerical and special characters (such as @, # or $) is accepted.

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

      Important

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

   d. Configure the traffic scan options as needed.
      - **Scan web (HTTP traffic)** - scans the HTTP (web) traffic and blocks the outgoing data that matches the rule data.
      - **Scan email (SMTP traffic)** - scans the SMTP (mail) traffic and blocks the outgoing email messages that contain the rule data.

      You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.
   e. Click **Save**. The new rule will be added to the list.

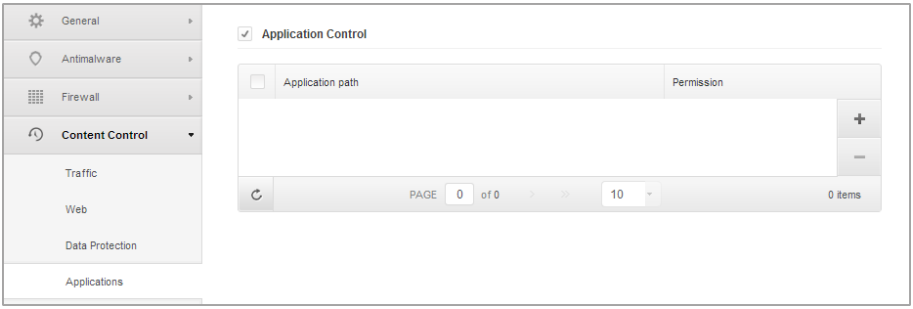
3. Configure exclusions to data protection rules so that users can still send protected data to authorized websites and recipients. Exclusions can be applied globally (to all rules) or to specific rules only. To add an exclusion:
   a. Click the + **Add** button at the right side of the table. A configuration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

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

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

Applications

In this section you can configure Application Control. Application Control helps you completely block or restrict users' access to applications on their computers. Games, media and messaging software, as well as other categories of software and malware can be blocked in this way.



Computer Policies - Content Control - Applications

To configure Application Control:

1. Use the switch to turn on Application Control.
2. Specify the applications you want to restrict access to. To restrict access to an application:
   a. Click the + **Add** button at the right side of the table. A configuration window is displayed.

b. You must specify the path to the application executable file on the target computers. There are two ways to do this:
   - Choose from the menu a predefined location and complete the path as needed in the edit field. For example, for an application installed in the `Program Files` folder, select `%ProgramFiles` and complete the path by adding a backslash (\) and the name of the application folder.
   - Enter the full path in the edit field. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

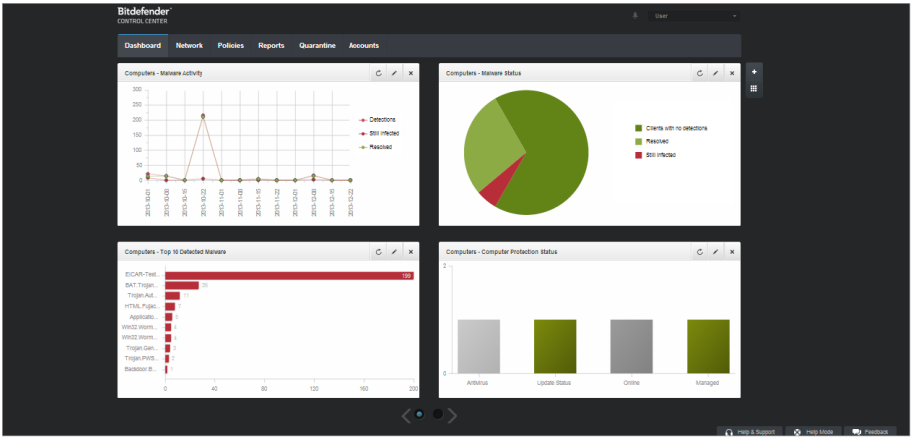
c. **Access Scheduler**. Schedule the applications access during certain times of day on a weekly basis:
   - Select from the grid the time intervals during which you want to block access to the application. You can click individual cells, or you can click and drag to cover longer periods. Click again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

To remove a rule from the list, click the corresponding **Delete** button at the right side of the table. To edit an existing rule, click the application name.

7. 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.
- 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. 118).
- 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.

7.1. Refreshing Portlet Data

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

7.2. 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.

7.3. 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:
   - Type of background report
   - Suggestive portlet name
   - Update interval

   For more information on available report types, refer to “Available Report Types” (p. 118).
4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

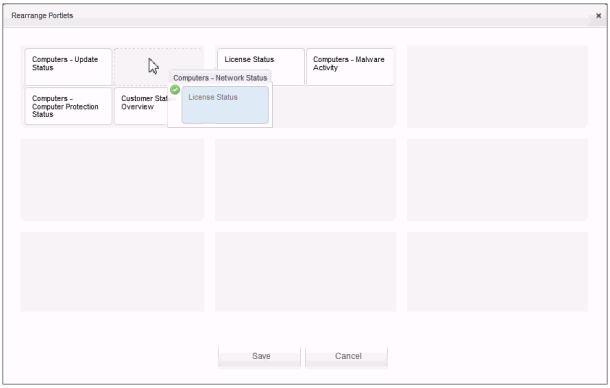
7.4. Removing a Portlet

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.

7.5. 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 dashboard portlets

8. 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).

8.1. Available Report Types

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 the last 24 hours.

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)

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

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)

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

Network Status

Provides you with detailed information on the overall security status of selected 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.

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 activity 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 activity 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 activity of the Application Control module of Endpoint Security. You can see the number of blocked applications on the selected computers.

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

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.

Data Protection
Informs you about the activity of the Data Protection module of Endpoint Security. You can see the number of blocked emails and 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).

Endpoint Modules Status

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

8.2. Creating Reports

You can create two categories of reports:

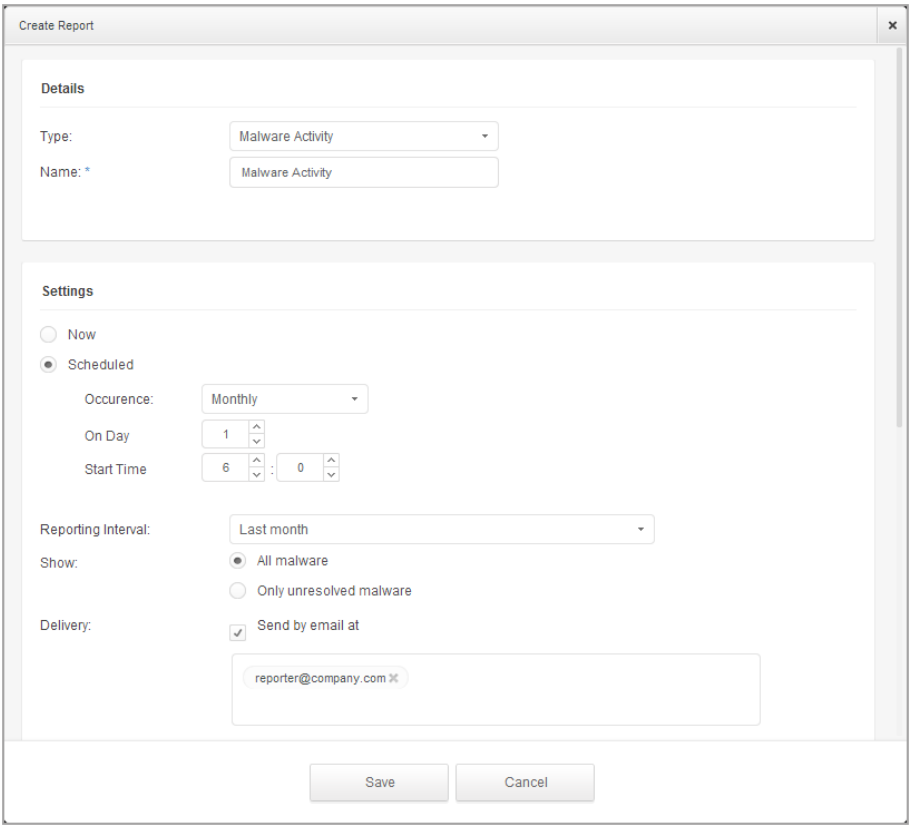
- **Instant reports.** Instant reports are automatically displayed after you generate them.
- **Scheduled reports.** Scheduled reports can be configured to run at a specified time and date and a list of all the scheduled reports is displayed in the **Reports** page.

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. Click the + **Add** button at the right side of the table. A configuration window is displayed.



Computer Reports Options

3. Select the desired report type from the menu. For more information, refer to “Available Report Types” (p. 118).
4. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
5. Configure the report recurrence:
   - Select **Now** to create an instant report.
   - Select **Scheduled** to configure the report to be automatically generated at the time interval that you want:
     – Hourly, at the specified interval between hours.
     – Daily. In this case, you can also set the start time (hour and minutes).

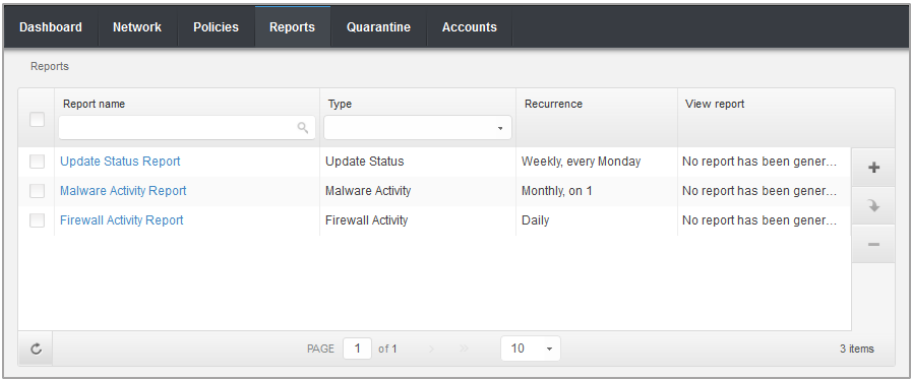
- Weekly, in the specified days of the week and at the selected start time (hour and minutes).
- Monthly, at each specified day on the month and at the selected start time (hour and minutes).

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

   For example, for an **Update Status** report you can choose to view only the list of computers that have updated in the selected time period, or the ones that need to be restarted to complete the update.
8. **Delivery**. To receive a scheduled report by email, select the corresponding option. Enter the email addresses that you want in the field below.
9. **Select Target**. Scroll down to configure the report target. Select the group you want to run the report on.
10. Click **Generate** to create an instant report or **Save** to create a scheduled 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.

8.3. Viewing and Managing Scheduled Reports

To view and manage scheduled reports, go to the **Reports** page.



The Reports page

All scheduled reports are displayed in a table. 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.

8.3.1. 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.

8.3.2. Editing Scheduled Reports

Note

When editing a scheduled report, any updates will be applied starting with the report's next recurrence. Previously generated reports will not be impacted by the editing.

To change the settings of a scheduled report:

1. Go to the **Reports** page.
2. Click the report name.
3. Change report settings as needed. You can change the following:
   - **Report name.** Choose a suggestive name for the report to help easily identify what it is about. When choosing a name, consider the report type and target, and possibly the report options. Reports generated by a scheduled report are named after it.
   - **Report recurrence (schedule).** You can schedule the report to be automatically generated hourly (by a certain hour interval), daily (at a certain start time), weekly (on a specific day of the week andf start time) or monthly (on a specific day of the month and start time). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.
   - **Settings.**
     – You can schedule the report to be automatically generated hourly (by a certain hour interval), daily (at a certain start time), weekly (on a specific day of the week andf start time) or monthly (on a specific day of the month and start time).

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

- The report will only include data from the selected time interval. You can change the interval starting with the next recurrence.
- Most reports provide filtering options to help you easily find the information you are interested in. When you view the report in the console, all information will be available, regardless of the selected options. If you download or email the report however, only the report summary and the selected information will be included in the PDF file. Report details will only be available in CSV format.
- You can choose to receive the report by email.

- **Select target.** The selected option indicates the type of the current report target (either groups or individual network objects). Click the corresponding link to view the current report target. To change it, select the groups or network objects to be included in the report.

4. Click **Save** to apply changes.

8.3.3. 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.

8.4. 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.

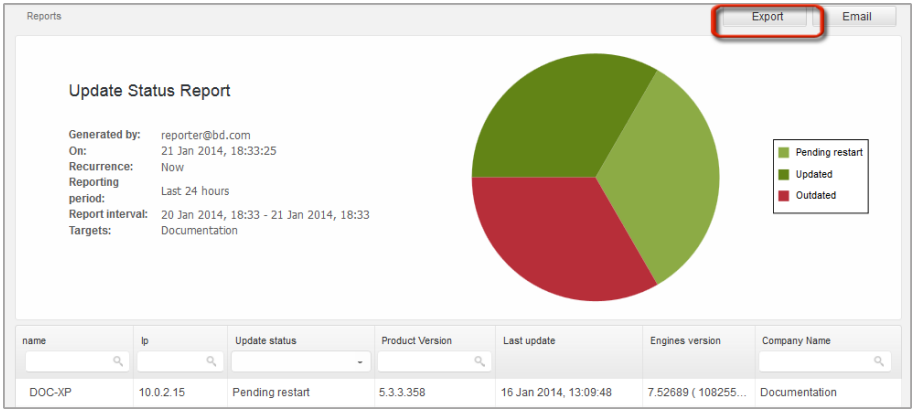
You have two ways of saving reports:

- Export
- Download

8.4.1. Exporting Reports

To export the report to your computer:

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



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.

8.4.2. 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.

8.5. 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.

8.6. Printing Reports

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

9. Quarantine

By default, Endpoint Security isolates suspicious files and the malware-infected files that cannot be disinfected in a secure area named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

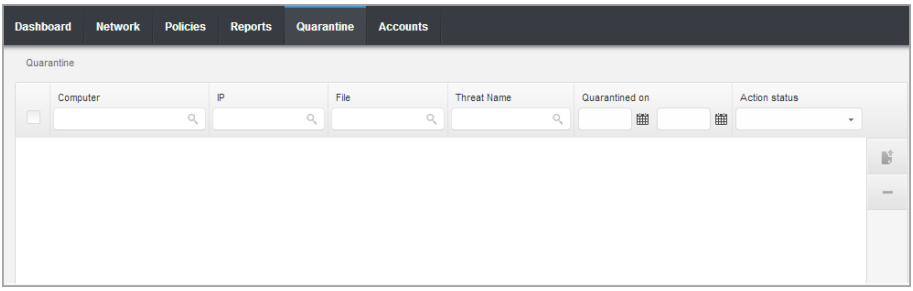
Security for Endpoints stores the quarantined files on each managed computer. Using Control Center you have the option to either delete or restore specific quarantined files.

By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

In addition, quarantined files are scanned after each malware signature update. Cleaned files are automatically moved back to their original location.

Control Center provides detailed information on all files moved to quarantine on the network objects managed from your account.

To check and manage quarantined files, go to the **Quarantine** page.



The Quarantine page

Information about quarantined files is displayed in a table. You are provided with the following information:

- The name of network object the threat was detected on.
- The IP of network object the threat was detected on.
- Path to the infected or suspicious file on the network object it was detected on.
- Name given to the malware threat by the Bitdefender security researchers.
- Time when the file was quarantined.
- Pending action requested by administrator to be taken on the quarantined file.

To make sure the latest information is being displayed, click the **Refresh** button in the bottom-left corner of the table. This may be needed when you spend more time on the page.

9.1. Navigation and Search

Depending on the number of managed network objects and the nature of infections, the number of quarantined files can be sometimes large. The 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 to filter displayed data. For example, you can search for a specific threat detected in the network or for a specific network object. You can also click column headers to sort data by a specific column.

9.2. Restoring Quarantined Files

On particular occasions, you may need to restore quarantined files, either to their original location or to an alternate location. One such situation is when you want to recover important files stored in an infected archive that has been quarantined.

To restore one or more quarantined files:

1. Go to the **Quarantine** page.
2. Select the check boxes corresponding to the quarantined files you want to restore.
3. Click the **Restore** button at the right side of the table.
4. Choose the location where you want the selected files to be restored (either the original or a custom location on the target computer).

   If you choose to restore to a custom location, you must enter the path in the corresponding field. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers. For more information, refer to “Using System Variables” (p. 145).
5. Select **Automatically add exclusion in policy** to exclude the files to be restored from future scans. The exclusion applies to all policies affecting the selected files, except for the default policy, which cannot be modified.
6. Click **Save** to request the file restore action. You can notice the pending action in the **Action** column.

7. The requested action is sent to the target computers immediately or as soon as they get back online. Once a file is restored, the corresponding entry will disappear from the Quarantine table.

9.3. Automatic Deletion of Quarantined Files

By default, quarantined files older than 30 days are automatically deleted. This setting can be changed by editing the policy assigned to the managed network objects.

To change the automatic deletion interval for quarantined files:

1. Go to the **Policies** page.
2. Find the policy assigned to the network objects on which you want to change the setting and click its name.
3. Go to the **Antimalware > Quarantine** section.
4. Select the desired automatic deletion period from the menu.
5. Click **Save** to apply changes.

9.4. Deleting Quarantined Files

If you want to delete quarantined files manually, you should first make sure the files you choose to delete are not needed. Use these tips when deleting quarantined files:

- A file may actually be the malware itself. If your research leads you to such a situation, you can search the quarantine for the specific threat and delete it from quarantine.
- You can safely delete:
  - Unimportant archive files.
  - Infected setup files.

To delete one or more quarantined files:

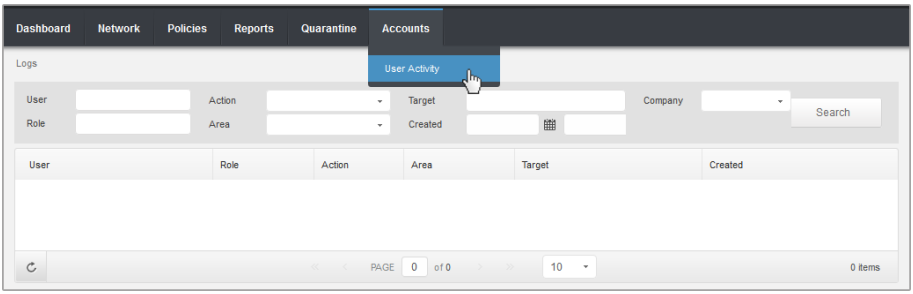
1. Go to the **Quarantine** page.
2. Check the list of quarantined files and select the check boxes corresponding to the ones you want to delete.
3. Click the **– Delete** button at the right side of the table. You can notice the pending status in the **Action** column.
4. The requested action is sent to the target network objects immediately or as soon as they get back online. Once a file is deleted, the corresponding entry will disappear from the Quarantine table.

10. User Activity Log

Control Center logs all the operations and actions performed by users. The user activity list includes the following events, according to your administrative permission level:

- Logging in and logging out
- Creating, editing, renaming and deleting reports
- Adding and removing dashboard portlets
- Creating, editing, and deleting credentials
- Creating, modifying, downloading and deleting network packages
- Creating network tasks
- Creating, editing, renaming and deleting user accounts
- Deleting or moving computers between groups
- Creating, moving, renaming and deleting groups
- Deleting and restoring quarantined files
- Creating, editing and deleting user accounts
- Creating, editing, renaming, assigning and deleting policies

To examine the user activity records, go to the **Accounts > User Activity** page.



The User Activity Page

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

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

- The username of who performed the action.
- User role.
- Action that caused the event.

- Type of console object affected by the action.
- Specific console object affected by the action.
- Time when the event occurred.

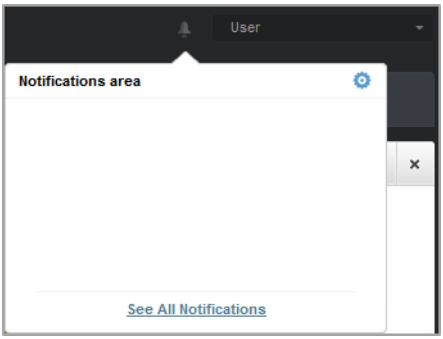
To sort events by a specific column, simply click the header of that column. Click the column header again to reverse the sorting order.

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

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

11. 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 red icon indicating the number of newly detected events. Clicking the icon displays the list of detected events.

11.1. Notification Types

This is the list of available notifications types:

Malware Outbreak

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

You can configure the malware outbreak threshold in the **Notifications Settings** window. For more information, refer to “Configuring Notification Settings” (p. 137).

License Expires

This notification is sent 30, seven days and also one day before the license expires.

License Usage Limit Has Been Reached

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

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

Update Available
This notification informs you about the availability of a new Small Office Security update.

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

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

AVC/IDS event
This notification is sent each time a potentially dangerous application is detected and blocked on an endpoint in your network. You will also find details about the dangerous application type, name and path.

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

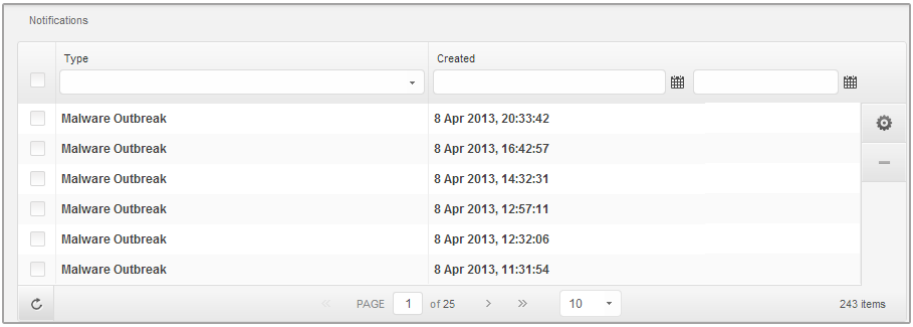
Data Protection event
This notification is sent each time data traffic is blocked on an endpoint according to data protection rules.

Product Modules event
This notification is sent each time a security module of an installed agent gets disabled.

Product Registration event
This notification informs you when the registration status of an agent installed in your network has changed.

11.2. Viewing Notifications

To view the notifications, click the **Notification Area** button and then click **See All Notifications**. A table containing all the notifications is displayed.



The Notifications page

Depending on the number of notifications, the table can span several pages (only 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.

- 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.

11.3. 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.

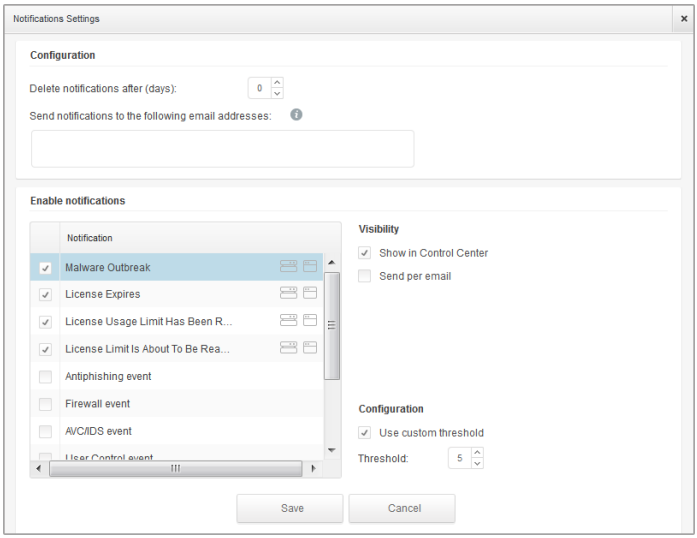
You can also configure notifications to be automatically deleted after a specified number of days. For more information, refer to “Configuring Notification Settings” (p. 137).

11.4. 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.



Notifications Settings

Note

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

3. Under **Configuration** section you can define the following settings:
   - You can configure notifications to be automatically deleted after a certain number of days. Enter the number of days that you want in the **Delete notifications after (days)** field.

- Optionally, you can choose to send the notifications by email to specific email addresses. Type the email addresses in the dedicated field, pressing `Enter` after each address.

4. Under **Enable Notification** section you can choose the type of notifications you want to receive from Small Office Security. You can also configure the visibility and sending options individually for each notification type.

   Select the notification type that you want from the list. For more information, refer to "Notification Types" (p. 134). While a notification type is selected, you can configure its specific options in the right-side area:

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

   Note
   By default, the Malware Outbreak notification is sent to the users that have at least 5% of all their managed network objects infected by the same malware. To change the malware outbreak threshold value, select the option **Use Custom Threshold**, then enter the value that you want in the **Malware Outbreak Threshold** field.

5. Click **Save**.

12. Getting Help

Bitdefender strives to provide its customers with an unparalleled level of fast and accurate support. If you experience any issue with or if you have any question about your Bitdefender product, go to our online Support Center. It provides several resources that you can use to quickly find a solution or an answer. Or, if you prefer, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and they will provide you with the assistance you need.

12.1. Bitdefender Support Center

Bitdefender Support Center, available at http://www.bitdefender.com/support/business.html, is the place where you will find all the assistance you need with your Bitdefender product.

You can use several resources to quickly find a solution or an answer:

- Knowledge Base Articles
- Bitdefender Support Forum
- Product Documentation

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

Knowledge Base Articles

The Bitdefender Knowledge Base is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about virus prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Knowledge Base is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Knowledge Base, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Knowledge Base for business products is available any time at http://www.bitdefender.com/support/business.html.

Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others. You can post any problem or question related to your Bitdefender product.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at http://forum.bitdefender.com, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Business Protection** link to access the section dedicated to business products.

Product Documentation

Product documentation is the most complete source of information about your product.

You can check and download the latest version of documentation for Bitdefender business products at Support Center > Documentation.

12.2. Asking for Assistance

You can contact us for assistance through our online Support Center:

1. Go to http://www.bitdefender.com/support/contact-us.html.
2. Use the contact form to open an email support ticket or access other available contact options.

12.3. Using Support Tool

The Small Office Security Support Tool is designed to help users and support technicians easily obtain the information needed for troubleshooting. Run the Support Tool on affected computers and send the resulting archive with the troubleshooting information to the Bitdefender support representative.

To use the Support Tool:

1. Download the Support Tool and distribute it to the affected computers. To download the Support Tool:
   a. Connect to Control Center using your account.
   b. Click the **Help and Support** link in the lower-right corner of the console.
   c. The download links are available in the **Support** section. Two versions are available: one for 32-bit systems and the other for 64-bit systems. Make sure to use the correct version when running the Support Tool on a computer.

2. Run the Support Tool locally on each of the affected computers.
   a. Select the agreement check box and click **Next**.
   b. Complete the submission form with the necessary data:
      i. Enter your email address.
      ii. Enter your name.
      iii. Choose your country from the corresponding menu.
      iv. Enter a description of the issue you encountered.
      v. Optionally, you can try to reproduce the issue before starting to collect data. In this case, proceed as follows:
         A. Enable the option **Try to reproduce the issue before submitting**.
         B. Click **Next**.
         C. Select the type of issue you have experienced.
         D. Click **Next**.
         E. Reproduce the issue on your computer. When done, return to Support Tool and select the option **I have reproduced the issue**.
   c. Click **Next**. The Support Tool gathers product information, information related to other applications installed on the machine and the software and hardware configuration.
   d. Wait for the process to complete.
   e. Click **Finish** to close the window. A zip archive has been created on your desktop.

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

12.4. Contact Information

Efficient communication is the key to a successful business. During the past 10 years Bitdefender has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

12.4.1. Web Addresses

Sales Department: enterprisesales@bitdefender.com
Support Center: http://www.bitdefender.com/support/business.html
Documentation: documentation@bitdefender.com
Local Distributors: http://www.bitdefender.com/partners
Partner Program: partners@bitdefender.com

Media Relations: pr@bitdefender.com
Virus Submissions: virus_submission@bitdefender.com
Spam Submissions: spam_submission@bitdefender.com
Report Abuse: abuse@bitdefender.com
Web site: http://www.bitdefender.com

12.4.2. Bitdefender Offices

The Bitdefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

United States

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Phone (sales&technical support): 1-954-776-6262
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com
Support Center: http://www.bitdefender.com/support/business.html

France

PROFIL TECHNOLOGY
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Phone: +33 (0)1 47 35 72 73
Email: supportpro@profiltechnology.com
Website: http://www.bitdefender.fr
Support Center: http://www.bitdefender.fr/support/professionnel.html

Spain

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Phone (office&sales): (+34) 93 218 96 15
Phone (technical support): (+34) 93 502 69 10
Sales: comercial@bitdefender.es

Website: http://www.bitdefender.es
Support Center: http://www.bitdefender.es/support/business.html

Germany

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Phone (office&sales): +49 (0)2301 91 84 222
Phone (technical support): +49 (0)2301 91 84 444
Sales: vertrieb@bitdefender.de
Website: http://www.bitdefender.de
Support Center: http://www.bitdefender.de/support/business.html

UK and Ireland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Phone (sales&technical support): +44 (0) 8451-305096
Email: info@bitdefender.co.uk
Sales: sales@bitdefender.co.uk
Website: http://www.bitdefender.co.uk
Support Center: http://www.bitdefender.co.uk/support/business.html

Romania

BITDEFENDER SRL
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Fax: +40 21 2641799
Phone (sales&technical support): +40 21 2063470
Sales: sales@bitdefender.ro
Website: http://www.bitdefender.ro
Support Center: http://www.bitdefender.ro/support/business.html

United Arab Emirates

Bitdefender FZ-LLC
Dubai Internet City, Building 17

Office # 160
Dubai, UAE
Phone (sales&technical support): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Sales: sales@bitdefender.com
Web: http://www.bitdefender.com/world
Support Center: http://www.bitdefender.com/support/business.html

A. Appendices

A.1. List of Application File Types

The antimalware scanning engines included in the Bitdefender security solutions can be configured to limit scanning to application (or program) files only. Application files are far more vulnerable to malware attacks than other types of files.

This category includes files with the following extensions:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu;
acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat;
bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek;
dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe;
ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd;
ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam;
maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt;
mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one;
onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx;
ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub;
puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr;
script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx;
tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm;
wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls;
xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
```

A.2. Using System Variables

Some of the settings available in the console require specifying the path on the target computers. It is advisable to use system variables (where appropriate) to make sure the path is valid on all target computers.

Here is the list of the predefined system variables:

`%ALLUSERSPROFILE%`

The All Users profile folder. Typical path:

```
C:\Documents and Settings\All Users
```

`%APPDATA%`

The Application Data folder of the logged-in user. Typical path:

- Windows XP:

`C:\Documents and Settings\{username}\Application Data`

- Windows Vista/7:

  `C:\Users\{username}\AppData\Roaming`

`%HOMEPATH%`
The user folders. Typical path:

- Windows XP:

  `\Documents and Settings\{username}`

- Windows Vista/7:

  `\Users\{username}`

`%LOCALAPPDATA%`
The temporary files of Applications. Typical path:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`
The Program Files folder. A typical path is `C:\Program Files`.

`%PROGRAMFILES(X86)%`
The Program Files folder for 32-bit applications (on 64-bit systems). Typical path:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`
The Common Files folder. Typical path:

`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`
The Common Files folder for 32-bit applications (on 64-bit systems). Typical path:

`C:\Program Files (x86)\Common Files`

`%WINDIR%`
The Windows directory or SYSROOT. A typical path is `C:\Windows`.

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.

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.