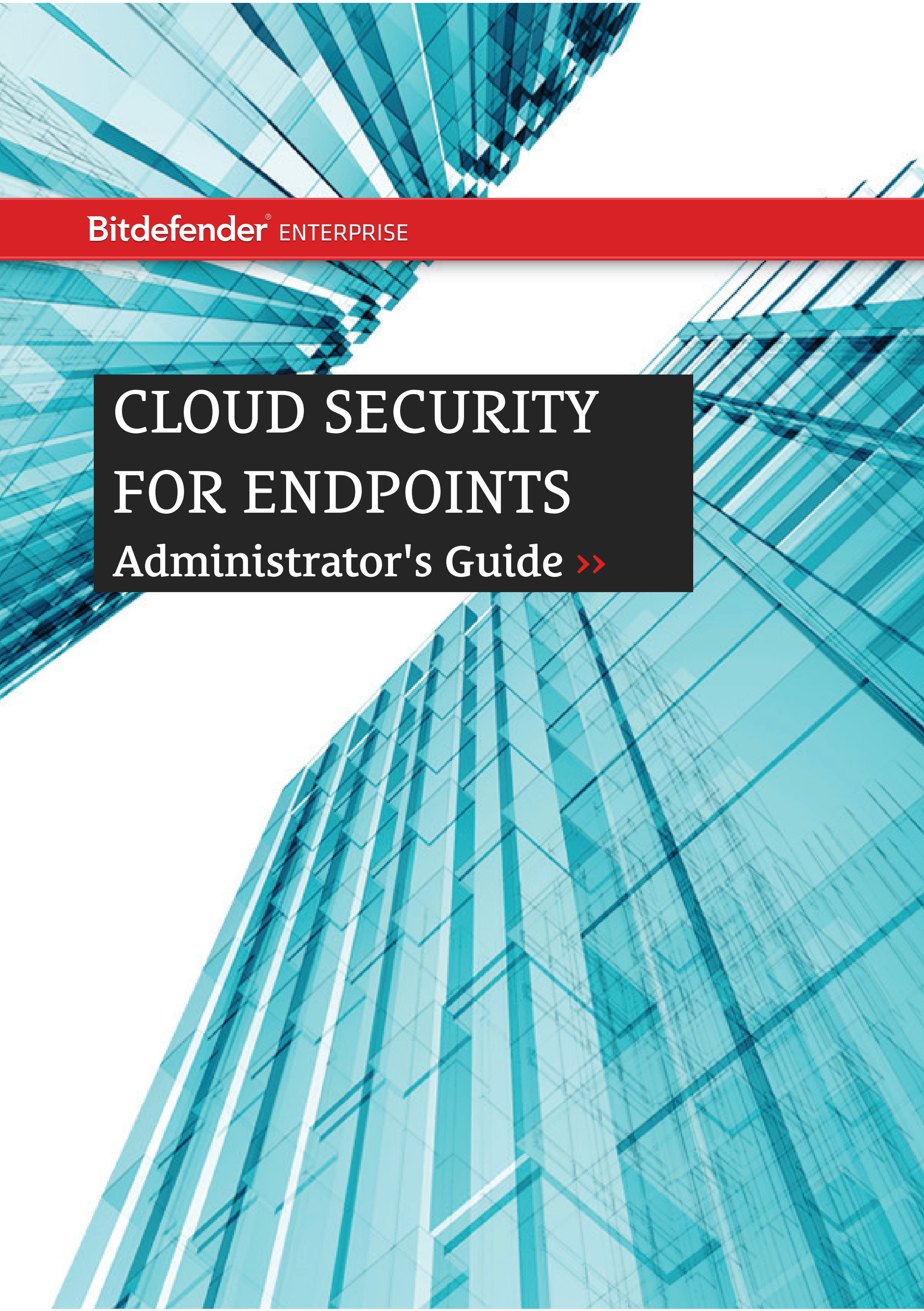


Bitdefender® ENTERPRISE

CLOUD SECURITY FOR ENDPOINTS

Administrator's Guide ››

Cloud Security for Endpoints by Bitdefender
Administrator's Guide

Publication date 2013.07.29

Legal Notice

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

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

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

Bitdefender®

Table of Contents

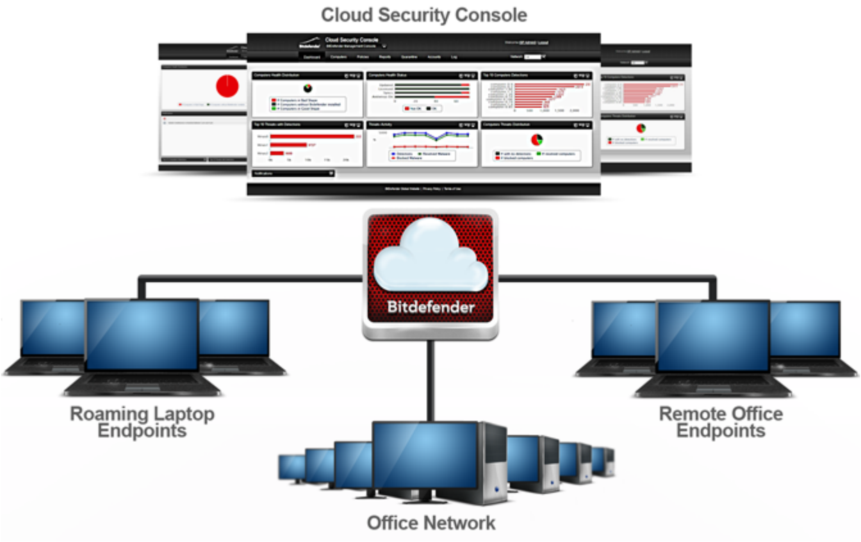
1. About Cloud Security for Endpoints

Cloud Security for Endpoints is a cloud-based malware protection service developed by Bitdefender for computers running Microsoft Windows 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.

This chapter provides an overview of Cloud Security for Endpoints:

- "Architecture" (p. 1)
- "User Accounts" (p. 2)
- "Threat Protection" (p. 3)
- "Workflow" (p. 6)

1.1. Architecture



Cloud Security for Endpoints Architecture

The security service is hosted on Bitdefender's public cloud. Subscribers have access to a Web-based management interface called **Cloud Security Console**. From this interface, administrators can remotely install and manage malware protection on all their Windows-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 Cloud Security Console; while scans, updates and configuration changes are commonly performed in the background.

An optional on-premise **Update Server** is also available. The Update Server centralizes endpoint clients' update and distribution within the local network, thus reducing Internet traffic for networks with a large number of endpoints. The Update Server also enables Endpoint Security update deployment on network computers without Internet access.

1.2. User Accounts

Cloud Security for Endpoints uses an integrated distribution and deployment ecosystem in which different types of accounts are connected in a hierarchical structure. Each account has visibility over its children accounts. For accountability reasons, user actions are documented in activity logs for both the current and children accounts.

There are four types of accounts:

1. **Partner** - Cloud Security for Endpoints distributors and resellers use partner accounts. Partner accounts can have two types of children: other partner accounts or customer accounts. When expanding their distribution chain, partners create subordinate partner accounts. When selling directly to end-users, they create company accounts. Since partners can act as security service providers, they have administrative privileges over security settings for their children company accounts.
2. **Company** - Company accounts are allocated to end-customers when they purchase a Cloud Security for Endpoints license from a partner. A customer will always have a single company account. A company account is a master account for a customer's entire Cloud Security for Endpoints deployment, allowing top-level control over all security settings (unless overridden by its parent partner account in a security service provider scenario). From a company account, operational responsibilities can be delegated to subordinate administrator and reporter children accounts.
3. **Administrator** - Administrator accounts are internal accounts with administrative privileges over the company's entire Cloud Security for Endpoints deployment or over a specific group of computers. Administrators are responsible for actively managing the Cloud Security for Endpoints security settings. For more information on typical administrator responsibilities, refer to "Workflow" (p. 6).
4. **Reporter** - Reporter accounts are internal read-only accounts. They only allow access to reports and logs. Such reports can be allocated to personnel with monitoring responsibilities or to other employees who must be kept up-to-date with security status.

The following table summarizes the relationships between the account types:

Account	Account Users	Allowed Children
Partner	Resellers, Distributors	Partner, Company
Company	End-customers/IT managers	Administrator, Reporter
Administrator	IT managers, network administrators	Administrator, Reporter
Reporter	Managers, various IT personnel, etc.	-

1.3. Threat Protection

Cloud Security for Endpoints provides protection against a wide range of threats using the following modules:

- Antimalware protection based on signature scanning, heuristic analysis (B-HAVE) and advanced behavior-based heuristic analysis (Active Virus Control) against: viruses, worms, trojans, spyware, adware, keyloggers, rootkits and other types of malicious software
- Antiphishing protection, browser toolbar and search advisor against website forgery/spoofing and Internet frauds
- Firewall and Intrusion Detection System against network attacks
- Data Protection against social engineering attempts and accidental data leaks
- User Control against company policy infringements related to Web access and application use

1.3.1. Antimalware

Bitdefender's antimalware scanning technology relies on 3 layers of protection:

1. First, a traditional scanning method is employed where scanned content is matched against the **signature database**. The signature database contains byte patterns specific to known threats and is regularly updated by Bitdefender. This scanning method is effective against confirmed threats that have been researched and documented. However, no matter how promptly the signature database is updated, there is always a vulnerability window between the time when a new threat is discovered and when a fix is released.
2. Against brand-new, undocumented threats, a second layer of protection is provided by **B-HAVE**, Bitdefender's heuristic engine. Heuristic algorithms detect malware based on behavioural characteristics. B-HAVE runs suspected malware in a virtual environment to test its impact on the system and ensure it poses no threat. If a threat is detected, the program is prevented from running.
3. For threats that elude even the heuristic engine, a third layer of protection is present in the form of **Active Virus Control (AVC)**. Active Virus Control continuously monitors

running processes and grades suspicious behaviours such as attempts to: disguise the type of process, execute code in another process's space (hijack process memory for privilege escalation), replicate, drop files, hide from process enumeration applications, etc. Each suspicious behaviour raises the process rating. When a threshold is reached, an alarm is triggered.

Cloud Security for Endpoints protects against several types of malware, including:

- **Viruses** - A computer virus is a computer program that self-replicates when executed, often while being concealed inside legitimate executable files, boot records, script files, document macros, etc. Besides self-replication, many viruses also carry a payload, meaning they also perform malicious actions on the host system like: destroying or corrupting data, displaying insulting or annoying messages, altering normal application behaviour, installing trojans or spyware, etc.
- **Worms** - Computer worms are also self-replicating computer programs that may carry malicious payloads. They differ from viruses in that they are standalone computer programs and have the ability to spread automatically, usually via computer networks.
- **Trojans** - Trojans are computer programs that expose the host system to attackers, hence the name. Typical payloads include: opening backdoors (methods of bypassing authentication), stealing data, hijacking the system for spamming or Denial of Service attacks, spying on the user, etc. Unlike viruses and worms, trojans don't self-replicate.
- **Spyware** - Spyware designates computer programs that covertly collect information about the user and transmit it to a third party. Spyware is often distributed as part of desirable software such as free utilities which perform spying activities on their users in addition to their advertised purpose.
- **Adware** - Adware programs are software packages that display unsolicited advertising in the form of pop-ups, or by corrupting the graphical user interface of various applications, notably web browsers. Like spyware, they are often bundled with other types of more or less useful software.
- **Keyloggers** - Keyloggers monitor the user's keyboard key presses. Although there are legitimate applications for keyloggers, they are often used by hackers to extract confidential information such as credentials, credit card numbers, addresses, etc. They are usually distributed through a trojan or virus.
- **Rootkits** - Rootkits are system drivers which modify the operating system's behaviour for various purposes. Just like keyloggers, they may have beneficial functionalities, but are also frequently used for harmful actions such as: concealing malicious software, preventing malware disinfection, enabling privilege escalation for unauthorised users, opening backdoors, etc. Because they corrupt the operating system's low level functions, once installed, rootkits are notoriously difficult to detect and remove.

1.3.2. Antiphishing

The antiphishing module provides warnings and protection against website forgery/spoofing and against Internet frauds. The antiphishing module has three components:

- **Antiphishing** protection automatically blocks known phishing (website forgery/spoofing) web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters. In addition to website forgery, other types of Internet frauds may be suppressed such as: purchase frauds, get-rich-quick scams, Internet marketing frauds, click frauds, etc. Instead of the malicious web page, a special warning page is displayed in the browser to inform the user that the requested web page is dangerous.
- The **Bitdefender toolbar** informs users about the security rating of the web pages they are viewing. By clicking a small dragger at the top of the browser window, users can see if the currently displayed page is either: safe, suspect or unsafe.
- The **Search advisor** rates search engine results and Facebook/Twitter links, by placing an icon in front of every result. Icons indicate if the link leads to a safe, suspect or unsafe page.

There are two types of threats contained by Cloud Security for Endpoints antiphishing protection:

- **Spoofing** - Web site forgery (spoofing) consists of malicious web sites attempting to impersonate legitimate ones for fraudulent reasons such as collecting user credentials or credit card information.
- **Internet frauds** - Sites that do not assume false identities, but instead try to appear as honorable businesses and profit by tricking people into various scams such as:
  - **Purchase frauds** - Online vendors who don't actually deliver the advertised products
  - **Financial frauds** - Such as those originating from false financial institutions
  - **Get-rich-quick-scams** - Such as Ponzi schemes, work-at-home schemes or other "business-opportunity" schemes
  - **Internet marketing frauds** - Malicious sites that harvest credit card information under various pretexts such as age verification or by selling dubious health products
  - **Click frauds** - Sites that deceive visitors into clicking links that lead to different destinations than the ones advertised
  - **Unethical dissemination** - Domains that have been promoted using spam, blog comment spam, click frauds, social media scams or other dishonest methods

1.3.3. Firewall and Intrusion Detection

The firewall and the Intrusion Detection System (IDS) protect the system from network threats:

- The **Firewall** controls applications' access to network resources/services and to the Internet. A comprehensive database of known, legitimate applications can be automatically allowed access. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection.
- The **Intrusion Detection System** protects the system from specific actions with malicious potential such as: dll injections, installation of malware drivers, alteration of Bitdefender files by 3rd party applications, Internet Explorer exploits or keylogging attempts.

1.3.4. Data Protection

The Data Protection module prevents users from unwittingly revealing specific confidential information by scanning outgoing email (SMTP) and web (HTTP) traffic and blocking predefined text strings from being sent. These text strings may include sensitive data such as: account names, names for in-development products or technologies, contact information for company executives, etc. There are usually two scenarios for this type of exposure:

- **Social engineering** - This happens when another party actively attempts to deceive someone inside the company into revealing confidential information by techniques such as: impersonating co-workers or authorities, staging false situations or otherwise manipulating the victim to act in the social engineer's interest.
- **Accidental data leaks** - In these scenarios, the user is divulging confidential information out of negligence, without being enticed in any way by the recipient. Although this is not a deliberate data theft attempt, the consequences can be just as severe.

1.3.5. User Control

The User Control module restricts user's access to Internet and to applications either completely or based on a schedule. Online access restrictions can also be applied for: specific addresses, HTTP or SMTP traffic containing certain keywords, or for predefined Web site categories. There are over 30 types of websites that can be restricted including those providing: gambling, mature content, social networking, file sharing, online gaming, etc.

The User Control module helps enforce company policies related to Web access, thus preventing productivity losses caused by employee idling and reducing data traffic costs.

1.4. Workflow

Cloud Security for Endpoints administrators can perform a wide range of assignments, the most important of which being related to:

- Deployment
- Endpoint Management

- Security Policies
- Scan Tasks
- Reports

1.4.1. Deployment

The Endpoint Security can be installed either locally or remotely:

- **Local installation** - For a local installation, a generic or customized installation kit is run on the target computer either from a local or network storage device, or after being downloaded from the Bitdefender cloud. The administrator can set up customized installation kits with predefined settings for installed modules, passwords or upgrade locations. In a typical deployment, the administrator may set up a custom installation kit on the Bitdefender cloud and send the local user the corresponding download link via email. The user downloads the installation kit and runs it, without adjusting any installation parameters.
- **Remote installation** - When Endpoint Security is installed on a computer, it behaves as a network scanning agent and deployment assistant. Detected computers will show up in the Cloud Security Console allowing administrators to deploy Endpoint Security on the other computers within the local network remotely.

1.4.2. Endpoint Management

Endpoints can be managed individually or clustered into groups. Computer groups enable administrators to apply security policies and run reports and scan tasks collectively, on multiple computers sharing the same security requirements. In large networks, computer groups can be managed by different administrators for workload balancing.

1.4.3. Security Policies

In Cloud Security for Endpoints, security settings are always managed as a batch, via security policies. A security policy is a configuration which includes a specific set of values for:

- Endpoint interface settings such as: visibility, status alerts and technical support information
- General settings such as: logging, reporting, password protection and updates
- Security settings, namely: antimalware, firewall and content control modules

By enforcing the use of security policies, security settings are always applied as predefined all-inclusive profiles, adjusted to match the target computers' function. Applying individual security settings to a computer or group of computers is not permitted.

1.4.4. Scan Tasks

Administrators can run manual scans on managed endpoints from the Cloud Security Console at any time. Additionally, security policies allow configuring and scheduling periodical scan tasks to run automatically on target computers. Quick scans and full system scans can be run either manually or as a scheduled task. Scheduled tasks also support customized scans.

1.4.5. Reports

Reports provide graphical representations and listings for security data consolidated from multiple computers or computer groups. Data coverage may include: Endpoint Security update status, protection status, licence status, network activity, malware activity, top 10 detected malware, etc. Reports can be generated either manually, or scheduled to be run automatically, on a regular basis.

2. Getting Started

Cloud Security for Endpoints can be configured and managed using Cloud Security Console, a web-based interface hosted by Bitdefender.

By using Cloud Security Console, you can do the following:

- Install protection on endpoints (workstations, laptops, servers).
- Visualize the entire network (managed computers, unprotected computers detected in the network).
- Find out detailed information about a managed computer.
- Remotely run tasks on computers (install, uninstall, scan, configure protection modules).
- Assign policies to managed computers in order to configure and manage protection.
- Monitor protection.
- Obtain centralized easy-to-read reports regarding the managed computers.
- Check and manage quarantined files remotely.
- Create and manage user accounts for other company employees.
- Check user activity log.

2.1. Connecting to Cloud Security Console

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

To connect to Cloud Security Console:

1. Requirements:
   - Internet connection
   - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari or Opera
   - Recommended screen resolution: 1024x768 or higher
2. Open your web browser.
3. Go to the following website: https://cloud.bitdefender.net
4. Enter the email address and password of your account.
5. Click **Login**.

Note

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

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

2.2. Cloud Security Console Overview

Cloud Security Console is organized so as to allow easy access to all the features.

Use the menu bar in the upper area to navigate through the console.

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

Computers
Install protection, manage computers and run tasks remotely.

Policies
Create, apply and manage security policies.

Reports
Get security reports concerning the managed computers.

Quarantine
Remotely manage quarantined files.

Accounts
Manage your account details and preferences. Create and manage user accounts for other company employees.

Log
Check the user activity log.

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

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

2.3. First Steps

Note

When you first open the Cloud Security Console, a prompt might be displayed requesting you to change the password. Clicking it opens the account settings page where you can enter a new password for your account.

To get started:

1. Go to the **Computers > Installation Area** page and install Endpoint Security (the client software) on computers. Two installation methods are available:
   - Use the installation link to download and install protection manually on each computer.
   - Install protection manually on a computer, then use remote installation for unprotected endpoints detected in the network.
2. If you manage a larger number of computers (tens or more), organize them into groups to manage them more efficiently:
   a. Go to the **Computers > View Computers** page.

   b. Create groups in the left-side pane by right-clicking the root group (or a group you have created) and selecting **Create group**.

   c. Click the root group, then select computers and drag and drop your selection to the desired group.
3. The protection settings on computers are automatically configured according to the default security policy. To check the default protection settings, go to the **Policies > View Policies** page and click the default policy name. You can change protection settings as needed, and also configure additional protection features.

   If you have organized computers into groups, you can configure and apply different policies on each group according to their security requirements. To create additional policies:

   a. Go to the **Policies > New Policy** page and create a new policy.

   b. Configure the policy settings as needed.

Make sure to keep the Cloud Security for Endpoints protection up to date with network changes by following the previous steps for all new computers added to the network.

Later on, to manage and monitor protection, do the following:

- Check the **Dashboard** page regularly to see real-time information on the Cloud Security for Endpoints protection.
- Go to the **Reports > New Report** page to create the reports you need. It is recommended to create scheduled reports for the report types you need regularly. To view a generated report, go to the **Reports > View Reports** page and click the report name.
- Use the tasks on the **Computers > View Computers** page to scan managed computers, install protection remotely on unmanaged computers, reconfigure protection modules or completely remove protection.

2.4. Changing Default Login Password

It is recommended that you change the default login password received by email following your service subscription. It is also advisable to change your login password periodically.

To change the login password:

1. Go to the **Accounts > My Account** page.
2. Type a new password in the corresponding fields (under **Account Details**).
3. Click **Submit** to save the changes.

2.5. Managing Your Account

To check and change your account details and settings:

1. Go to the **Accounts > My Account** page.
2. Under **Account Details**, correct or update your account details.
   - **Full Name.**
   - **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
   - **Password.** To change your login password, type a new one in the corresponding fields.
   - **Company name.**
3. Under **License**, you can check your subscription details. Your subscription is managed by Bitdefender or by the Bitdefender partner who provides you the service. For more information, refer to "Service Subscription" (p. 15).
4. **Proxy settings**. If the company uses a proxy server to connect to the Internet, you must enable and configure the proxy settings. Otherwise, the clients installed on computers cannot communicate with Cloud Security Console.

   Note
   For companies using proxy authentication, Endpoint Security can be installed on computers using a Full Installation Kit only. For detailed information on Endpoint Security local installation, refer to "Local Installation" (p. 19).

   Warning
   If the company's proxy server is about to be changed, you must first replace the company's proxy settings with the new ones in the Cloud Security Console, before switching to the new proxy server.

5. Under **Settings**, configure the account settings according to your preferences.

- **Send email notification after login**. Enable this option to be notified for each successful login with your account credentials. The message sent to your email address will contain the source IP address of the request and the login date and time.
- **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.
- Define how managed computers from this company account are displayed in the Cloud Security Console, by choosing the appropriate option from the **Show** menu:
  - **Computer Name**, to display computers by their local names (for example, `ComputerName`)
  - **FQDN** (Fully Qualified Domain Name), to display computers by their full system name, including their local name and domain name (for example, `ComputerName.domain.com`). Use this option to differentiate between several computers with the same name and IP address.

    Note
    This setting will apply at the next synchronization with the network for online computers (after maximum 30 minutes, or less). You can apply the setting immediately by sending a task or a policy to online computers.
- **Logo.** You can change the default cloud-shaped Cloud Security Console logo with your company logo. This will allow you to customize PDF report layout. To change the logo, click **Custom** and load the logo image file from your computer. The following restrictions apply:
  - Logo dimensions: 81x41 pixels.
  - Supported file formats: PNG and JPG.

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

Important
You cannot delete your own account. If you no longer want to use the Cloud Security for Endpoints service and you want your account to be deleted, please contact your service provider.

2.6. Working with Table Data

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

- Tables can span several pages (only 10 entries are displayed per page by default). To move through the pages, use the navigation buttons at the bottom of the table. To change the number of entries displayed on a page, select an option from the menu next to the navigation buttons.

- To easily find what you are looking for, use the search boxes or the filtering options below the column headers.
- You can also click column headers to sort data by a specific column. Click the column header again to reverse the sorting order.

To make sure the displayed information is up to date, click the ⟳ **Refresh** button in the bottom-left corner of the table.

3. Service Subscription

You can try Cloud Security for Endpoints for free for a period of 30 days. During the trial period all features are fully available and you can use the service on any number of computers. Before the trial period ends, if you want to continue using the service, you must opt for a paid subscription plan and make the purchase.

There are two ways to subscribe to the service:

- Subscribe through a Bitdefender reseller. Our resellers will assist you with all the information you need and help you choose the best subscription plan for you. Some resellers offer value-added services, such as premium support, and others can provide you with a fully-managed service.

  To find a Bitdefender reseller in your country:

  1. Go to http://www.bitdefender.com/partners.
  2. Go to **Partner Locator**.
  3. The contact information of the Bitdefender partners should be displayed automatically. If this does not happen, select the country you reside in to view the information.
  4. If you do not find a Bitdefender reseller in your country, feel free to contact us by email at sales@bitdefender.com. Please write your email in English in order for us to be able to assist you promptly.
- Subscribe on the Bitdefender website.

Your subscription is managed by Bitdefender or by the Bitdefender partner who sells you the service. Some Bitdefender partners are security service providers. Depending on your subscription arrangements, Cloud Security for Endpoints' day-to-day operation may be handled either internally by your company or externally by the security service provider.

3.1. Activating a License

When you purchase a paid subscription plan for the first time, a license key is issued for you. The Cloud Security for Endpoints subscription is enabled by activating this license key. New license keys may also be issued when a subscription is renewed or when the number of licensed endpoints is extended.

✖ **Warning**
Activating a license does NOT append its features to the currently active license. Instead, the new license overrides the old one. For example, activating a 10 endpoints license on

top of a 100 endpoints license will NOT result in a subscription for 110 endpoints. On the contrary, it will reduce the number of covered endpoints from 100 to 10.

The license key is sent to you via email when you purchase it. Depending on your service agreement, once your license key is issued, your service provider may activate it for you. Alternately, you can activate your license manually, by following these steps:

1. Log in to Cloud Security Console using your customer account.
2. Go to the **Accounts > My Account** page.
3. In the **License** section, click the link next to the **License no.** or **License expires** field. This opens the **License Information** page, which displays information about the current license (if one is presently active).
4. In the **License key** field, enter your license key.
5. Click **Change key** and wait for the authorization process to complete.

3.2. Renewing a License

To prolong a license or to reactivate an expired license, contact your service provider.

3.3. Extending the Number of Licensed Endpoints

To increase the number of endpoints covered by the current license, contact Bitdefender customer support.

3.4. Checking Your Subscription Status

To check your subscription status:

1. Log in to Cloud Security Console using your customer account.
2. Go to **Accounts > My Account**.
3. In the **License** section, click the link next to the **License no.** or **License expires** field. This opens the **License Information** page, which displays information about your subscription status.

4. Installing Protection on Endpoints

Cloud Security for Endpoints is intended for workstations, laptops and servers running on Microsoft® Windows. To protect your computers with Cloud 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 Cloud Security Console to receive the administrator's commands and to send the results of its actions.

There are two installation methods:

- **Local installation.** Download an installation kit or web installer and use it to install the Endpoint Security locally, on each computer you want to protect. Installation kits and web installers are customized based on service subscription to automatically link the Endpoint Security to the corresponding customer account.
- **Remote installation.** Once installed on a computer, Endpoint Security automatically detects unprotected computers in the local network. The Cloud Security for Endpoints protection can then be installed on those computers remotely from the console. Remote installation is performed in the background, without the user knowing about it.

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

4.1. System Requirements

All of the Bitdefender cloud security services are managed by Cloud Security Console. Since Cloud Security Console is hosted, there are no hardware or software requirements for managing Cloud Security for Endpoints. All that is needed is an Internet connection.

Minimum Endpoint Requirements

Workstation operating systems:

- Windows 8
- Windows 7
- Windows Vista with Service Pack 1
- Windows XP with Service Pack 3

Server operating systems:

- 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

Embedded and tablet operating systems*:

- 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 Cloud Security for Endpoints to work.

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
- RAM memory:
  - Minimum: 512 MB
  - Recommended: 1 GB
- HDD space: 1.5 GB of free hard-disk space

Internet connection: Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari or Opera for endpoint browser security or accessing Cloud Security Console

4.2. Preparing for Installation

Prepare for installation as follows:

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 Cloud Security for Endpoints simultaneously with other security software on a computer may affect their operation and cause major problems with the system.

   Many of the security programs Cloud Security for Endpoints is incompatible with are automatically detected and can be removed at Endpoint Security 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. Web installer based installations also require Internet access. Make sure these conditions are fulfilled.

4.3. Local Installation

Local installation can be performed by yourself, by logging on to each computer, or you can ask computer users for help. It requires locally running an installation file, which you can download from Cloud Security Console. Two types of installation files are available:

- **Web Installer.** The web installer 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 Installation Kit.** This is the full installation package, which is to be used to install protection on computers with slow or no Internet connection. Download this file on an Internet-connected computer and then distribute it to other computers using external storage media or a network share. Note that two versions are available: one for 32-bit systems, the other for 64-bit systems. Make sure to use the correct version for the computer you install on.

To obtain or distribute the download link for local installation:

1. Connect to Cloud Security Console using your account.
2. Go to the **Computers > Installation Area** page.
3. If you want to, you can configure the installation options by clicking **Customize Package**. For more information, refer to "Customizing the Installation Package" (p. 22).

4. To view the link, click the **Installation Link** button and choose **View**. Use the appropriate link to download the preferred installation file (Web Installer or Full Installation Kit), which then you can run on the local computer to install protection. You can also copy the file on external storage media and run it on other computers.
5. Another option is to send users within the organization's network email invites with the installation link, asking them to download and install protection on their computer. You must have a default mail client configured on your computer. To email the link, click the **Installation Link** button and choose **Send by Email**. Note that users are sent the web installer link.

Once you have the installation file stored locally, to manually install protection on a computer:

1. Locate the downloaded installation file and double-click it.

   Note

   When using the web installer, the full installation package is downloaded from the Internet. The download may take a while, depending on your Internet connection. Once the download is complete, installation will start automatically.

2. The installer first checks the system for other security software.

   If an incompatible antivirus program is detected, you will be prompted to remove it from your system. Please follow the directions to remove the software from your system, thus avoiding problems occurring later on.

   Note

   You must restart the computer to complete the removal of detected antivirus programs. Installation will automatically resume after computer restart.

3. Wait for the installation to complete. Critical areas on your system are scanned for viruses, the latest versions of the application files are downloaded and installed, and the Bitdefender services are started. This step can take a couple of minutes.
4. Click **Finish**.

4.4. Remote Installation

To make deployment easier, Cloud Security for Endpoints includes an automatic network discovery mechanism based on which the client software (Endpoint Security) can be installed on endpoints remotely from Cloud Security Console. Detected computers are displayed as **unmanaged computers** on the **Computers** page. For detailed information on network discovery, refer to “How Network Discovery Works” (p. 23).

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

Note

Once Endpoint Security is installed on a computer, it may take a few minutes for the rest of the network computers to become visible in the Cloud Security Console.

Note

Each target computer must have the admin$ administrative share enabled for the installation to work.

To remotely install protection:

1. Connect to Cloud Security Console using your account.
2. Go to the **Computers > View Computers** page.
3. Click the **Show** menu located above the table (to the left) and choose **Unmanaged Computers**.
4. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
5. Select the check boxes corresponding to the computers on which you want to install protection.
6. Click **Quick Tasks** and choose **Install Client** from the menu. The Installation Options window will appear.
7. Configure the installation options:
    a. Select the protection modules you want to install. Please note that only antimalware protection is available for server operating systems.

    b. 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.

    c. 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.

    d. If a local Bitdefender update server is set up in the network, you can configure Endpoint Security to update from this server instead of updating from the Internet. Change the Internet update address in the **Update location** field with the address of the local update server. Use one of these syntaxes:

    - `update_server_ip:port`
    - `update_server_name:port`

    The default port is 7074.

    To learn more, refer to "Using Update Server" (p. 92).

Note

The update address configured here is used temporarily after installation. As soon as a policy is applied to the client, the update location is changed according to policy settings. To make sure the client continues to update from the local update server, configure the update location options in the policy settings.

e. Remote installation is performed from a computer on which Cloud Security for Endpoints is already installed (deployer computer). If you want to use a specific computer for remote installation, clear the **Detect deployer automatically** check box, start typing the name or IP address of the computer in the corresponding field and choose the computer from the list.

f. Provide the administrative credentials required for remote authentication on selected computers.

   Enter the user name and password of an administrator account for each of the selected computers. 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, `domain\user` or `user@domain.com`).

8. Click **Install**. A confirmation window will appear.
9. You can view and manage the task on the **Computers > View Tasks** page.

4.5. Customizing the Installation Package

You can customize the installation package by choosing which protection modules to be installed and by setting the default installation options. The default configuration is suitable for most installation scenarios.

To customize the installation package:

1. Go to the **Computers > Installation Area** page.
2. Click the **Customize Package** button in the upper-right corner of the page.
3. Select 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.

4. 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.
5. 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.
6. If a local Bitdefender update server is set up in the network, you can configure Endpoint Security to update from this server instead of updating from the Internet. Change the Internet update address in the **Update location** field with the address of the local update server. Use one of these syntaxes:
   - `update_server_ip:port`
   - `update_server_name:port`

   The default port is 7074.

   To learn more, refer to "Using Update Server" (p. 92).

   Note
   The update address configured here is used temporarily after installation. As soon as a policy is applied to the client, the update location is changed according to policy settings. To make sure the client continues to update from the local update server, configure the update location options in the policy settings.
7. Click **Save** to save changes. All future installations from your account will use by default the configuration you have made.

4.6. How Network Discovery Works

Cloud 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.

Important
Cloud Security for Endpoints 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.

Cloud Security for Endpoints 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 Cloud Security Console. Cloud Security Console 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 Cloud Security Console.
- If Endpoint Security is installed on a domain computer, only computers from that domain will be visible in Cloud Security Console. 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, Cloud Security Console 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, Cloud Security Console 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.

4.6.1. 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.

4.6.2. Network Discovery Requirements

In order to successfully discover all the computers (servers and workstations) that will be managed from Cloud Security Console, 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

To view the computers under your account, go to the **Computers > View Computers** page. From the **View Computers** page, you can do the following:

- Organize computers into groups to manage their security more efficiently. This is recommended if you manage a larger number of computers (tens or more).
- Check computer and protection details.
- View and change security policy settings.
- Remotely run tasks on computers to scan them, install the Cloud Security for Endpoints protection or modify the current installation. To find out more, refer to "Running and Managing Tasks" (p. 34).
- Create quick reports in order to obtain various security information about specific computers.

Besides the computers protected by Cloud Security for Endpoints, you can also view other computers detected in the network. To find out more, refer to "How Network Discovery Works" (p. 23).

The page consists of two panes:

- Left-side pane helps you organize computers into groups.
- Right-side pane contains a table displaying information about the computers under your account. The table columns provide you with useful information about the listed computers:
  - Computer name and IP address.
  - Operating system installed on the computer.
  - Update status of the Cloud Security for Endpoints protection.
  - When the computer has last been seen.

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

The icon next to the name of each computer informs you about that computer:

🖥 Computer on which the Cloud Security for Endpoints protection is installed.
🖵 Computer on which the Cloud Security for Endpoints protection has not been installed yet.

Computer you have excluded from management.

5.1. About Managed, Unmanaged and Excluded Computers

Computers are organized into three main categories:

- **Managed Computers** - computers on which the Cloud Security for Endpoints protection is installed.
- **Unmanaged Computers** - detected computers on which the Cloud Security for Endpoints protection has not been installed yet.

> **Note**
>
> Once installed on the first computer, Endpoint Security automatically detects unprotected computers in the local network. Subsequently, network discovery is performed regularly every hour. Unmanaged computers will be available on the **View Computers** page as they are detected.

- **Excluded Computers** - computers that you have excluded from management.

Use the **Show** menu located above the table (to the left) to choose the computer categories to be displayed.

5.2. About Offline Computers

Offline computers normally have Cloud Security for Endpoints protection installed, but there is no recent activity from Endpoint Security. Computers are considered to be offline if Endpoint Security is inactive for more than 1 minute.

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 has been manually uninstalled from the computer. In such cases, you must manually delete the computer from the **Computers > View Computers** page.
- Computer has no Internet access or communication with Cloud Security Console is blocked by a firewall. The second situation is highly unlikely as communication is done via HTTPS. The problem might occur if you protect computers using another firewall instead of the Endpoint Security firewall. It might also be caused by a network firewall or router.

- Endpoint Security might not be working properly.

To find out for how long computers have been inactive:

1. Go to the **Computers > View Computers** page.
2. Check the **Last Seen** field. To easily find the information you need, choose **Offline** from the corresponding menu and then sort computers by inactivity period by clicking the column header.

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.

5.3. Using Computer Groups

If you manage a larger number of computers (tens or more), you will probably need to organize them into groups. Organizing your computers into groups helps you manage them more efficiently. A major benefit is that you can use group policies to meet different security requirements.

Computer groups are displayed in the left-side pane of the **View Computers** page. Initially, there is only the root group named after your company. All computers on which you have installed the Cloud Security for Endpoints protection, as well as those detected in the network, are automatically placed in this group. You can organize your computers by creating groups under the root group and moving computers to the appropriate group.

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, right-click the group and choose **View all computers**.

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.).

Creating Groups

To divide your network into groups:

1. Right-click the root group in the left-side pane and choose **Create group**. A new group (named **New Group**) will appear under the parent group in the tree menu.
2. Rename the newly created group.
3. Follow the previous steps to create additional groups.
4. Move computers from the root group to the appropriate group.

To create sub-groups:

1. Right-click the group into which the new sub-group is to be included and select **Create group**. A new group (named **New Group**) will appear under the parent group in the tree menu.
2. Rename the newly created group.

Renaming Groups

To rename a group, right-click it, select **Rename group** and enter the new name.

Moving Groups

Groups can be moved anywhere inside the group hierarchy. To move a group, drag and drop it from the current location to the new one.

Moving Computers to Another Group

To move computers from the current group to another group:

1. Select the check boxes corresponding to the computers you want to move.
2. Drag and drop your selection to the desired group in the left-side pane.

Deleting Groups

You can only delete empty groups (which contain no computers).

To delete a group:

1. Move all the computers in the group to other groups. If the group includes sub-groups, you can choose to move entire sub-groups rather than individual computers.
2. Right-click the group and select **Delete group**. You will have to confirm your action by clicking **Yes**.

5.4. Searching and Sorting 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 or the menus under the column headers to filter displayed data. For example, you can search for a specific computer or choose to view only the offline computers.

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

When using groups, select a group in the left-side pane to view the computers it contains. Please note that computers placed in sub-groups are not displayed by default. To view all computers included in the group and in its sub-groups, right-click the group and choose **View all computers**.

5.5. Checking Computer and Protection Details

From the **View Computers** page, you can find various information on any computer:

- General computer details, such as its name, IP address or operating system.
- Security policy settings.
- License and update status of the Cloud Security for Endpoints protection.
- Status of the Cloud Security for Endpoints protection modules on the computer (installed or not, enabled or disabled).
- Status of Endpoint Client upgrade.
- Information concerning malware detected on the computer.
- Latest scan log.

To get computer and protection details:

1. Go to the **Computers > View Computers** page.
2. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
3. Click the name of the computer you are interested in. The computer details page is displayed. Click available links for more details.

5.6. Checking and Changing Security Settings

Security settings on computers are managed using policies. For more information, refer to "Security Policies" (p. 41).

To view the security settings applied on a particular computer:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
4. Click the name of the computer you are interested in.
5. Check the **Active policy** field. Click the policy name to view its settings.
6. You can change security settings as needed. Please note that any change you make will also apply to all other computers on which the policy is active.

5.7. Creating Quick Reports

To create quick reports from the **View Computers** page:

1. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
2. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
3. Select the check boxes corresponding to the computers to be included in the report.
4. Click **Reports** and choose the report type from the menu. Activity reports will only include data from the last week.

5.8. Excluding Computers from Management

Endpoint Security automatically detects unprotected computers in the network. Detected computers are displayed in Cloud Security Console as unmanaged so that you can remotely install protection on them.

If you do not plan to manage some of the detected computers, you can move them to the **Excluded Computers** list. In this way, you will not be bothered about them.

To exclude detected computers from management:

1. Go to the **Computers > View Computers** page.

2. Click the **Show** menu located above the table (to the left) and choose **Unmanaged Computers**.
3. Select the check boxes corresponding to the computers you want to exclude.
4. Click the **Quick Tasks** button in the upper-right corner of the page and choose **Exclude**.

If protection is manually installed on an excluded computer, it will be moved automatically to the **Managed Computers** list.

To view excluded computers:

1. Go to the **Computers > View Computers** page.
2. From the menu above the table, choose **Excluded Computers**.

5.9. Restoring/Deleting Excluded Computers

Excluded computers cannot be directly restored to the **Unmanaged Computers** list. If you want to restore an excluded computer, you must delete it from the console. If the deleted computer is still connected to the network, it will eventually be detected and displayed as unmanaged in the console.

To delete excluded computers:

1. Go to the **Computers > View Computers** page.
2. From the menu above the table, choose **Excluded Computers**.
3. Select the check boxes corresponding to the computers you want to delete.
4. Click the **Quick Tasks** button in the upper-right corner of the page and choose **Delete**.

Note

It will take up to an hour for deleted computers to be detected again. Some computers might be detected only after several hours.

5.10. Deleting Managed Computers

Delete managed computers from the console:

- To remove protection from a managed computer.
- To clean up the Managed Computers list of duplicate entries or inactive computers. When reinstalling the operating system or removing protection from certain computers, you must manually delete the corresponding entries from the list.

If the deleted computer is still connected to the network, it will eventually be detected and displayed as unmanaged in the console.

To delete managed computers:

1. Go to the **Computers > View Computers** page.

2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the computers you want to delete.

> **Note**
>
> - Check the **Last Seen** field to identify computers inactive for a long time.
> - Search or sort computers by name to identify duplicate entries or computers that have been permanently disconnected from the network.

5. Click the **Quick Tasks** button in the upper-right corner of the page and choose **Uninstall Endpoint**. Protection will be uninstalled from selected computers and they will be deleted from the console.

5.11. Deleting Unmanaged Computers

The Unmanaged Computers list is updated regularly with the new computers detected in the network. Computers that are no longer detected continue to remain in the list until you remove them manually.

You must first exclude an unmanaged computer in order to delete it from the console. If the deleted computer is still connected to the network, it will eventually be detected and displayed as unmanaged in the console.

To delete unmanaged computers:

1. Go to the **Computers > View Computers** page.
2. Exclude the computers you want to delete:
   a. From the menu above the table, choose **Unmanaged Computers**.
   b. Select the check boxes corresponding to the computers you want to delete.
   c. Click the **Quick Tasks** button in the upper-right corner of the page and choose **Exclude**.
3. Delete excluded computers:
   a. From the menu above the table, choose **Excluded Computers**.
   b. Select the check boxes corresponding to the computers you want to delete.
   c. Click the **Quick Tasks** button in the upper-right corner of the page and choose **Delete**.

6. Running and Managing Tasks

From the **View Computers** page, you can remotely run a number of administrative tasks on computers. This is what you can do:

- Install protection on detected computers.
- Scan managed computers for malware.
- Remove protection from computers.
- Modify installation to reconfigure protection modules.
- Upgrade the Endpoint Client.

6.1. Installing Protection on Unmanaged Computers

Once you have installed a Cloud Security for Endpoints client in a network, it will automatically detect unprotected computers in that network. The Cloud Security for Endpoints protection can then be installed on those computers remotely from the console. 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 Cloud 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 Cloud Security for Endpoints protection on one or several detected computers:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Unmanaged Computers**.
3. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the computers on which you want to install protection.
5. Click **Quick Tasks** and choose **Install** from the menu. The Installation Options window will appear.
6. Configure the installation options:

a. Select the protection modules you want to install. Please note that only antimalware protection is available for server operating systems.

b. 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.

c. 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.

d. If a local Bitdefender update server is set up in the network, you can configure Endpoint Security to update from this server instead of updating from the Internet. Change the Internet update address in the **Update location** field with the address of the local update server. Use one of these syntaxes:

   - `update_server_ip:port`
   - `update_server_name:port`

   To learn more, refer to "Using Update Server" (p. 92).

   Note

   The update address configured here is used temporarily after installation. As soon as a policy is applied to the client, the update location is changed according to policy settings. To make sure the client continues to update from the local update server, configure the update location options in the policy settings.

e. Remote installation is performed from a computer on which Cloud Security for Endpoints is already installed (deployer computer). If you want to use a specific computer for remote installation, clear the **Detect deployer automatically** check box, start typing the name or IP address of the computer in the corresponding field and choose the computer from the list.

f. Provide the administrative credentials required for remote authentication on selected computers.

   Enter the user name and password of an administrator account for each of the selected computers. 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, `domain\user` or `user@domain.com`).

7. Click **Install Client**. A confirmation window will appear.
8. You can view and manage the task on the **Computers > View Tasks** page.

6.2. Scanning Managed Computers

There are three ways to scan computers protected by Cloud Security for Endpoints:

- The user logged on to the computer can start a scan from the Endpoint Security user interface.
- You can create scheduled scan tasks using the policy.
- Run an immediate scan task from the console.

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

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the computers you want to scan.
5. Click **Quick Tasks** and choose **Scan** from the menu.
6. Select the type of scan to be performed:
   - **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 System Scan** checks the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.
7. Click **Request Scan**. A confirmation window will appear.
8. You can view and manage the task on the **Computers > View Tasks** page.

6.3. Uninstalling Protection from Computers

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

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the computers you want to uninstall protection from.
5. Click **Quick Tasks** and choose **Uninstall Endpoint** from the menu.
6. If you do not plan to reinstall the service, clear the **Keep quarantined files** option.

7. Click **Uninstall** to create and send the uninstall task to selected computers. A confirmation window immediately informs you if the task has been created successfully.

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

6.4. Configuring Installed Modules

To change which protection modules are installed on one or several computers:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
4. Select the check boxes corresponding to the computers on which you want to reconfigure protection.
5. Click **Quick Tasks** and choose **Configure modules** from the menu.
6. Select 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.

7. Click **Configure** to apply changes on computers.

6.5. Upgrading the Endpoint Client

Starting with July 2013, the Endpoint Client included in Cloud Security for Endpoints has been replaced with Endpoint Security. It is recommended to upgrade to the new client as soon as possible. For this purpose, a new task has been added in the **Quick Tasks** list, allowing you to run the client upgrade on every computer having the Not upgraded status.

To remotely upgrade the client on managed computers:

1. Go to the **Computers > View Computers** page.
2. Click the **Show** menu located above the table (to the left) and choose **Managed Computers**.
3. If you have organized computers into groups, select the desired group from the left-side pane. To view all of your computers, right-click the root group and choose **View all computers**.
4. From the **Updated** column header, choose **Not upgraded** to display the old client endpoints only.
5. Select the check boxes of computers where you want to run a client upgrade.
6. Click **Quick Tasks** and choose **Upgrade Endpoint** from the menu.

   The Upgrade Endpoint window will appear.
7. Configure the upgrade options:
   - Select only the Endpoint Security 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.

   - Define the time when you want the endpoints to upgrade:

- Use **Disable Upgrade** option to cancel an already created upgrade task. This option is useful as upgrade tasks are not managed in the **Computers > View Tasks** page.
- Select **Upgrade now** to run the Endpoint upgrade immediately.
- Select **Schedule Upgrade** to define a certain time interval for running the Endpoint Client upgrade on selected computers. This option is useful for endpoints that cannot complete the upgrade task (such as powered off or offline computers), and you want to re-run it periodically, to make sure the task is eventually completed.

  You can define an upgrade schedule using the following options:

  - To re-run the task periodically, enter the frequency for the selected period of time (for example, run the task every 3 hours).
  - To re-run the task at a certain moment, check **Start running the task at** and define the date and time in the corresponding fields.
  - You can also choose to stop the upgrade task from running at a certain moment by using the **Stop running the task at** option. In this case, all running upgrades will be canceled at the specified time.
  - You can also opt to **Run the task as soon as possible after a scheduled start is missed**, by checking the corresponding option.

  > **Note**
  > The scheduled upgrade options work in conjunction with each other. You can define a scheduled upgrade, for example, to run every two weeks starting with Sunday from 1 AM to 3 AM.

8. Click **Save** to create the upgrade client task. A confirmation message will appear. You can check the upgrade status in the details of the corresponding computers.

6.6. Viewing and Managing Tasks

The tasks you have created can be viewed and managed on the **Computers > View Tasks** page. You can see the existing tasks and details about them:

- Task name.
- Execution progress on the target computers.
- When the task was created.

6.6.1. Checking Execution Status and Results

Tasks will start running immediately on online computers, but they will take some time to complete (more or less, depending on the task).

To check if a task has run on the target computers:

1. Go to the **Computers > View Tasks** page.
2. Find the task in the list and check the **Progress** field. You can see on how many of the target computers the task has run.
3. To access the task report, which provides details on the task execution, click the task name.

The task report consists of a Summary page and a Details page.

6.6.2. Deleting Tasks

Once a task has run and you no longer need the task report, it is best to delete it.

To delete one or several tasks:

1. Go to the **Computers > View Tasks** page.
2. Select the check boxes corresponding to the tasks you want to delete.
3. Click the **Delete** button located above the table. A confirmation window will appear.

7. Security Policies

Once installed, the Cloud Security for Endpoints protection can be configured and managed from Cloud Security Console using security policies. A policy specifies the security settings to be applied on target computers.

Immediately after installation, computers are assigned the default policy, which is preconfigured with the recommended protection settings. You can change protection settings as needed, and also configure additional protection features.

If you manage a larger number of computers (tens or more), you may want to create several policies to apply different settings based on security requirements. For example, you can configure different policies for office workstations, laptops and servers.

This is what you need to know about policies:

- There is a single default policy template, which allows configuring all protection settings. When you create a new policy, you must choose the policy template you want to use. You can choose either the default policy template or an existing policy.
- Policies are pushed to target computers immediately after creating or modifying them. Settings should be applied on computers in less than a minute (provided they are online). If a computer 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.
- Policies can be assigned either to individual computers or to groups of computers. The policy target cannot be a mix of computers and groups.
- Several policies can be assigned at a given time to a computer or group. However, there will always be only one active policy: the one that was last created or modified.

To view and manage security settings and policies, go to the **Policies > View Policies** page. Existing policies are displayed in the table. For each policy, you can see:

- Policy name.
- Policy target (computers or groups the policy applies to).
- How many of the target computers comply with the policy.
- User who created the policy.
- Time when the policy was last modified.

7.1. Creating New Policies

To create a new policy:

1. Go to the **Policies > New Policy** page.
2. Enter a suggestive name for the policy. When choosing a name, consider the purpose and target of the policy.
3. Choose a policy template from the menu. The new policy will be initialized with the settings of the template policy. You can choose either the default policy template or an existing policy.
4. Configure the policy target (computers to which the policy will apply). You can choose one of the following options:
   - **Groups.** Select this option to apply the policy to groups of managed computers. Click the corresponding link and choose the desired computer groups.

     Note
     The policy will apply automatically to any computer that is later added to a selected group.

   - **Computers.** Select this option to apply the policy to individual computers. Click the corresponding link and choose the desired computers.
5. Click **Submit** to create the policy and to go to the policy page.
6. Next, configure the policy settings. For detailed information, refer to "Configuring Policy Settings" (p. 42).
7. Click **Save** to save changes and apply protection settings to the target computers. The new policy will be displayed on the **View Policies** page.

7.2. Configuring Policy Settings

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

To change the settings of a policy:

1. Go to the **Policies > View Policies** page.
2. Click the policy name. This will open the policy page.
3. Configure the policy settings as needed. Settings are organized around the protection modules into the following categories:
   - Summary
   - 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**.

7.2.1. Summary

The Summary page contains general policy details:

- **Policy name.** You can rename the policy by entering the new name in this field.
- **Specified target.** If you want to change the policy target, click the link and select the new target.
- **Complying.** This field indicates how many of the target computers are compliant with the policy.

7.2.2. General

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

The settings are organized under the following tabs:

- Display
- Advanced
- Update

Display Tab

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

- **Silent Mode.** Use the switch 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.
  - The firewall protection level is set to **Ruleset, known files and allow**.
- **Show icon in notification area.** Select this option to show the Bitdefender icon B in the notification area (also known as the system tray). The icon informs users on their protection status and allows them to open the main program window or to quickly start a scan or update.

- **Display notification pop-ups.** Select this option if you want users to be informed about important security events through small notification pop-ups (for example, a pop-up will inform users whenever a virus has been detected and blocked on their computer).
- **Display alert pop-ups.** Different from notification pop-ups, alert pop-ups prompt users for action. Alert pop-ups are generated in the following situations:
  - If the firewall is set to prompt the user for action when unknown applications request network or Internet access. You can configure this setting in the **Firewall > Advanced** section.
  - 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 are informed about their protection status in two ways:
  - The security status area of the main window displays an appropriate status message and changes its color depending on detected issues.
  - The Bitdefender icon B in the notification area changes its appearance when issues are detected.

  The protection status is determined based on the selected status alerts and it refers to security configuration issues or other security risks. For example, if the **Antimalware status** option is selected, users will be informed whenever there is a problem relating to their antimalware protection (for example, if on-access scanning is disabled or a system scan is overdue).

  Select the security aspects that you want to be monitored. If you do not want users to be informed about existing issues, clear all check boxes.
- **Technical Support Information.** Fill in the fields to customize the technical support and contact information available in Endpoint Security. Users can access this information from the Endpoint Security window by clicking the i icon in the lower-right corner (or, alternatively, by right-clicking the B Endpoint Security icon in the system tray and selecting **About**).

Advanced Tab

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

- **Remove events older than {30} days.** Endpoint Security keeps a detailed log of events concerning its activity on the computer (also including computer activities monitored by User 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 Tab

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

- **Update interval (hours).** Endpoint Security automatically checks for, downloads and installs updates every hour (default setting). Automatic updates are performed silently in the background.

  To change the automatic update interval, choose a different option from the menu. Please note that automatic update cannot be turned off.

- **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).

- **Enable proxy.** Select this option if computers connect to the Internet (or to the local update server) through a proxy server. There are two 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.

  – **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.
    - **User name** - type in a user name recognized by the proxy.
    - **Password** - type in the valid password of the previously specified user.

  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.** If a local Bitdefender update server is set up in the network, you can configure Endpoint Security to update from this server instead of updating from the Internet.

  Note
  To learn more, refer to "Using Update Server" (p. 92).

  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.
  4. Use the Up/Down arrows in the **Action** column to set the local update address the first one in the list. If the first update location is unavailable, clients will try the second one and so on.

  To remove a location from the list, click the corresponding ✖ **Remove** button. Although you can remove the default Internet update location, this is not recommended.

7.2.3. 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 into 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 contain 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 under the following tabs:

- On-access
- On-demand

- Exclusions
- Quarantine

On-access Tab

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

- On-access Scanning
- Active Virus Control

On-access Scanning Settings

On-access scanning prevents new malware threats from entering the system - it scans files when they are accessed (opened, moved, copied or executed), email messages sent and received, and web traffic.

To configure on-access scanning:

1. Use the switch to turn on-access scanning on or off. If you turn off on-access scanning, computers will be vulnerable to malware.
2. Choose the protection level that best suits your security needs. For a quick configuration, drag the slider along the scale to a predefined protection level. Use the description on the right side of the scale to guide your choice.
3. Advanced users can configure the scan settings in detail by clicking the **Custom** button. A configuration window will appear. Custom scan settings are organized under two tabs, as follows:

   General

   - **File Types.** 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. 105).

     If you want only specific extensions to be scanned, choose **User defined extensions** from the corresponding menu and enter the extensions (separated by semicolons ";") in the corresponding field.

- **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:

  – **Limit archive size to {10} 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).

  – **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.

Advanced

- **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.

  – **Deferred scanning.** Select this option to prioritize the scanning of files accessed for read operations over those accessed for write operations. This is intended to optimize the scan process.

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

  – **Action to take 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.

- **Action to take 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.

  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:

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.

Deny access
Deny access to detected files.

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 block the detected process.

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 switch to turn Active Virus Control on or off. If you turn off Active Virus Control, computers will be vulnerable to unknown malware.
2. Choose the protection level that best suits your security needs. Drag the slider along the scale to set the desired protection level. 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).

3. 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.

On-demand Tab

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

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.
- Time when the task was first run.
- Schedule based on which the task runs regularly (recurrence).
- Actions you can take on the scan task.

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 System 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 task, click **Add Task** and choose the type of task you want to create. To change the settings of an existing 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, click the corresponding ✖ **Remove** button.

Configuring Scan Tasks

The scan task settings are organized under three tabs: General - set task name, execution schedule and scan target; Options - choose a scan profile for quick configuration of the scan settings; Advanced - configure scan settings in detail. The Advanced tab can be accessed only after selecting the **Custom** check box on the Options tab.

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

- **Task 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.
- **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 from the menu either a predefined location or the **Specific paths** option.
  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 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 ➕ **Add** button.

   To edit an existing location, click it. To remove a location from the list, click the corresponding ✖ **Remove** button.

- **Scan Options.** For a quick configuration of the scan options, choose one of the predefined scan profiles. Drag the slider along the scale to the profile that best suits your security needs. Use the description on the right side of the scale to guide your choice.

  Based on the selected profile, the scan options on the **Advanced** tab 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 **Advanced** tab.

- **Scan Operations.**
  - **Run the task with low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
  - **Shut down computer when the task is finished.** This option may be useful when you run scans during off-working hours.

- **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. 105).

  If you want only specific extensions to be scanned, choose **User defined extensions** from the corresponding menu and enter the extensions (separated by semicolons ";") in the corresponding field.

- **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 {10} 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 check email archives for malware.
- **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 memory.** Select this option to scan programs running in the system's memory.
    - **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 cookies.** Select this option to scan the cookies stored by browsers on the computer.
    - **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.
    - **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.
    - **Ignore commercial keyloggers.** Select this option if commercial keylogger software is installed on the target computers. Commercial keyloggers are legitimate computer monitoring software whose most basic function is to record everything that is typed on the keyboard.
- **Actions.** Depending on the type of detected file, the following actions are taken automatically:
    - **Action to take 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.

– **Action to take when a suspect file 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.

– **Action to take 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.

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

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

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 B 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.

To configure device scanning, use the following options:

- **Scan detected devices.** Select this option to enable the automatic detection and scanning of storage devices. You can configure device scanning individually for each type of devices using the following options:
  - **Automatically scan CD/DVD media**
  - **Automatically scan USB storage devices**
  - **Automatically scan mapped network drives**
- **Do not scan devices with more than {0} 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 Tab

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:

- **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 switch 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.** Enter the file extension you want to exclude, without the preceding dot. For example, enter `txt` to exclude text files. Note that you can specify only one extension per exclusion rule.

     ### 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 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 ✖ **Remove** button.

Quarantine Tab

In this section you can configure the quarantine settings. You can set Endpoint Security to automatically perform the following actions:

- **Delete files older than {30} 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 {1} hours.** Keep this option selected to automatically send quarantined files to Bitdefender Labs. 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 update.** Keep this option selected to automatically scan quarantined files after each malware signatures update. Cleaned files are automatically moved back to their original location.

7.2.4. Firewall

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

The settings are organized under the following tabs:

- Settings
- Profiles
- Advanced

Settings Tab

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

- **Firewall.** Use the switch 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 your computer. They might then break into your 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 switch to turn Intrusion Detection System on or off.
  2. Choose the protection level that best suits your security needs. Drag the slider along the scale to set the desired protection level. 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.

Profiles Tab

In this section you can configure how firewall profiles and the Stealth Mode option are applied to network connections.

Firewall Profiles

A firewall profile is applied automatically to each detected network connection to define the basic traffic filtering options. There are four firewall profiles:

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.

You can choose between two ways to apply firewall profiles to network connections:

- **Apply firewall profiles by network type (default option).** For each network connection, the firewall will automatically detect the network type from Windows and use the corresponding firewall profile. Please note that the **Untrusted network** profile will never be applied with this option.

  If you want to apply a firewall profile by default to all new network connections, select the corresponding option under the profile name.
- **Apply firewall profile by adapter type.** Choose a specific firewall profile to be applied for each type of network adapters (wired, wireless and virtual).

Stealth Mode

Stealth Mode hides the computer from malicious software and hackers in the network or the Internet. Configure Stealth Mode as needed for each network type (or 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.

Advanced Tab

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.

Application Network Access

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.
- **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 process** to automatically allow changed signed applications to connect to the Internet.

Data Traffic 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.

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.

DNS over UDP / TCP
Allow or deny DNS over UDP and TCP. By default, this type of connection is allowed.

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 connection is denied.

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

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

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

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

Windows Explorer traffic on HTTP / FTP
Allow or deny HTTP and FTP traffic from Windows Explorer. By default, this type of connection 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. Refer to the following topic for more information.

To remove a rule from the list, click the corresponding ✖ **Remove** button.

Note
You can neither delete/modify the default firewall rules.

Configuring Custom Rules

To create and configure a new rule, click the ✚ **Add** button. 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.** 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.** 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.** 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.

- **Events.** Depending on the selected protocol, choose the network events the rule applies to. The following events may be taken into account:

Event	Description
Connect	Preliminary exchange of standard messages used by connection-oriented protocols (such as TCP) to establish a connection. With connection-oriented protocols, data traffic between two computers occurs only after a connection is established.
Traffic	Flow of data between two computers.
Listen	State in which an application monitors the network awaiting to establish a connection or to receive information from a peer application.

- **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 **Other**. An edit field will appear. Type the number assigned to the protocol you want to filter in the edit field.

    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 Type.** Select the type of network the rule applies to.
- **Set Permission.** Select one of the available permissions:

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

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

Click **Save** to add the rule.

7.2.5. 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.

The content control settings are organized under the following tabs:

- Traffic
- Web
- Data Protection
- Applications

Traffic Tab

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

- Options
- Traffic Scan
- Traffic Scan Exclusions

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.

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

Web Tab

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

The settings are organized under the following sections:

- Web Access Control
- Web Categories Filter
- Antiphishing

Web Access Control

Web Access Control works in conjunction with Web Categories Filter to enable you to filter web access. Web Access Control helps you allow or block web access for users or applications during specified time intervals. The web pages blocked by Web Access Control are not displayed in the browser. Instead, a default web page is displayed informing the user that the requested web page has been blocked by Web Access Control. Use the switch to turn **Web Access Control** on or off.

You have three configuration options:

- Select **Allow** to allow all web traffic and then explicitly **block** access to specific web content categories and web addresses using Web Categories Filter and Web Access Control settings respectively.
- Select **Block** to block all web traffic and then explicitly **allow** access to specific web content categories and web addresses using Web Categories Filter and Web Access Control respectively.
- Set time restrictions on web access and then explicitly **allow or block** access to specific web content categories and web addresses using Web Categories Filter and Web Access Control respectively. To restrict Internet access to certain times of day on a weekly basis:
  1. Select **Schedule**.
  2. Click **Edit Settings**.
  3. Go to **Scheduler** tab.
  4. 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. To start a new selection, click **Clear All**.
  5. Click **Save**.

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

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

To create a web rule:

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

Web Access Control can also be used to override Web Categories Filter in certain situations. You can create a Web Access Control rule to explicitly allow users to access a website that keeps getting blocked by Web Categories Filter. Web Access Control rules with **Allow** permission for specific web addresses are also taken into account during time intervals when web access is blocked by Web Access Control.

Web Categories Filter

Web Categories Filter dynamically filters access to websites based on their content. Using Web Categories Filter, you can allow or block access to entire categories of websites, such as social networking or video sharing websites. **Allow** permissions work only when web access is blocked by Web Access Control, while **Block** permissions work only when web access is allowed by Web Access Control.

> **Note**
> You can override the category permission for individual web addresses by adding them with opposite permission in Web Access Control > Edit Settings > Web Rules. For example, if a web address is blocked by Web Categories Filter, add a Web Access Control rule for that address with permission set to **Allow**.

To configure Web Categories Filter:

1. Use the switch to turn on Web Categories Filter.
2. For a quick configuration, click one of the predefined profiles (Aggressive, Normal, Permissive). Use the description on the right side of the scale to guide your choice.
3. If you are not satisfied with the default settings, you can define a custom filter:
   a. Select **Custom**.
   b. Click **Edit Settings**.

c. Find the category that you want in the list and choose the desired action from the menu.

d. 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.

Use the switch to turn Antiphishing on or off. 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 **Whitelist**.
2. Enter the web address and click the + **Add** button.

   To remove an exception from the list, click the corresponding **Delete** button.
3. Click **Save**.

Data Protection Tab

Data Protection prevents unauthorized disclosure of sensitive data based on administrator-defined rules. 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 switch 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 Rule** button. 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 Cloud Security Console 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, use the last row of the **Exclusions** table:
   a. Select the type of exclusion (web or email address).
   b. Enter the web or email address that users are authorized to disclose protected data to.

c. Click the ✚ **Add** button. 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 ✖ **Remove** button.

Applications Tab

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.

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 Rule** button. 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. Set the desired permission:
      - **Block** - to block access to the application completely.
      - **Restrict** - to restrict access to the application to certain time intervals.

        If you choose to restrict access rather than block the application completely, you must also select from the grid the days of the week and the time intervals during which access is blocked. You can click individual cells, or you can click and drag to cover longer periods. To start a new selection, click **Clear All**.
      - **Allow** - to temporarily allow access, but keep the restriction schedule.
   d. Click **Save**. The new rule will be added to the list.

To remove a rule from the list, click the corresponding ✖ **Remove** button. To edit an existing rule, click the application name.

7.3. Monitoring Policy Execution

To check if a policy has been applied on the target computers:

1. Go to the **Policies > View Policies** page.
2. Check the status in the **Complying** column. You can see how many of the target computers are compliant.
3. Click the link to open a window with more details. All computers that have been assigned the policy are displayed in a table. You can check the compliance status for each target computer.

   Note

   If there are too many entries, you can use the search boxes or the menus under the column headers to filter displayed data. You can also click column headers to sort data by a specific column. To move through the pages, use the navigation buttons at the bottom of the table.

7.4. Checking and Changing Policy Assignments

Policies can be assigned either to individual computers or to groups of computers.

To check and change policy assignments:

1. Go to the **Policies > View Policies** page.
2. Click the policy name. This will open the policy page.
3. Assigned computers or groups are listed in the **Specified targets** field. Click the link to see more details and change current assignments. Please note that you cannot change the target type (computers or groups).
4. To change the current assignments, follow these steps:
   a. Depending on the target type, proceed as follows:
      - If the policy has originally been assigned to groups, select the new groups you want the policy to apply to.
      - If the policy has originally been assigned to computers, you must select the new computers you want the policy to apply to. First of all, clear the **Display only the selected computers** check box in the upper-left corner of the window. Next, select the check boxes corresponding to the desired computers.

      Note

      If there are too many entries, you can use the search boxes or the menus under the column headers to filter displayed data. You can also click column headers to sort data by a specific column. To move through the pages, use the navigation buttons at the bottom of the table.

b. Click **Change** to save the new target.

c. Click **Save** to apply policy changes.

7.5. 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 > View Policies** page.
2. Click the policy name. This will open the policy page.
3. Enter a new name for the policy.
4. Click **Save** to apply policy changes.

7.6. Deleting Policies

If you no longer need a policy, delete it. Once the policy is deleted, the computers 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.

To delete a policy:

1. Go to the **Policies > View Policies** page.
2. Select the corresponding check box.
3. Click the **Delete** button in the upper-right corner of the page. You will have to confirm your action by clicking **Yes**.

8. Monitoring Dashboard

Each time you connect to Cloud Security Console, the **Dashboard** page is displayed automatically. The dashboard is a status page consisting of 7 portlets, which provide you with a quick security overview of all protected endpoints (workstations, laptops, servers).

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

Some portlets offer status information, while other report on security events in the last period.

You can check and configure the reporting period of a portlet by clicking the ▼☰ button on its title bar.

8.1. Dashboard Portlets

The dashboard consists of the following portlets:

Network Status

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

- Unmanaged computers do not have Cloud Security for Endpoints protection installed and their security status cannot be assessed.
- Offline computers normally have Cloud Security for Endpoints protection installed, but there is no recent activity from Endpoint Security. The security status of offline computers cannot be accurately assessed because status information is not current. For more information, refer to “About Offline Computers” (p. 27).
- Protected computers have Cloud Security for Endpoints protection installed and no security risks have been detected.
- Vulnerable computers have Cloud Security for Endpoints protection installed, but specific conditions prevent proper protection of the computer. The report details show you which security aspects need to be addressed.

Computer Status

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

- Protection update status
- Antimalware protection status

- License status
- Network activity status (online/offline)

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

Top 10 Most Infected Computers

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

Top 10 Detected Malware

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

Malware Activity

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

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

Computer Malware Status

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

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

Notifications

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

8.2. Managing Portlets

The dashboard is easy to configure based on individual preferences.

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

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

↻ The refresh option will re-load data for each portlet.

▾☰ Click this button to configure portlet options. Some portlets include data from a specific time period.

▬ Minimize the portlet to the bottom of the page.

❐ Restore a minimized portlet.

9. Using Reports

Cloud Security for Endpoints allows you to create and view centralized reports on the security status of the managed computers. 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 pie charts, tables and graphics, allowing you to quickly check the network security status and identify security issues.

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

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

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

9.1. Available Report Types

This is the list of available report types:

Update Status

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

Computer Status

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

- Protection update status
- License status

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

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

Malware Activity

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

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

Protection Module Status

Informs you of the status of the Cloud Security for Endpoints protection modules (Antimalware, Firewall, Content Control) on selected computers. The protection status can be Enabled, Disabled or Not installed. The report details also provide information on the update status.

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

Top 10 Most Infected Computers

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

Top 10 Detected Malware

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

Network Status

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

- Unmanaged computers do not have Cloud Security for Endpoints protection installed and their security status cannot be assessed.
- Offline computers normally have Cloud Security for Endpoints protection installed, but there is no recent activity from Endpoint Security. The security status of offline computers cannot be accurately assessed because status information is not current. For more information, refer to "About Offline Computers" (p. 27).
- Protected computers have Cloud Security for Endpoints protection installed and no security risks have been detected.

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

Computer Malware Status

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

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

Executive

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

9.2. Creating Reports

To create a report:

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

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

2. Select the desired report type from the menu. For more information, refer to "Available Report Types" (p. 77).
3. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
4. Configure the report target. Select one of the available options and click the corresponding link to choose the computer groups or the individual computers to be included in the report.
5. Configure report recurrence (schedule). You can choose to create the report immediately, daily, weekly (on a specific day of the week) or monthly (on a specific day of the month).
6. Configure the report options.
   a. For most report types, when you create an immediate report, you must specify the reporting period. The report will only include data from the selected time period.
   b. Several report types provide filtering options to help you easily find the information you are interested in. Use the filtering options to obtain only the desired information.

For example, for an **Update Status** report you can choose to view only the list of computers that have updated (or, on the contrary, that have not updated) in the selected time period.

Note

When you view the report in the console, all information will be available, regardless of the selected options. If you download or email the report however, only the report summary and selected information will be included in the PDF file. Full report details will only be available in CSV format.

c. To receive the report by email, select the corresponding option.

7. Click **Generate** to create the report.
   - If you have chosen to create an immediate report, it will be displayed on the View Reports page. The time required for reports to be created may vary depending on the number of managed computers. Please wait for the requested report to be created. Once the report has been created, you can view the report by clicking its name.
   - If you have chosen to create a scheduled report, it will be displayed on the Scheduled Reports page.

9.3. Viewing and Managing Generated Reports

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

Note

Scheduled reports can be managed on the Reports > Scheduled Reports page.

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

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

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

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

Indicates a one-time only report.

Indicates a scheduled report.

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

9.3.1. Viewing Reports

To view a report:

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

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

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

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

9.3.2. Searching Report Details

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

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

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

9.3.3. Saving Reports

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

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

To save the report you are viewing to your computer:

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

9.3.4. Printing Reports

Cloud Security for Endpoints doesn't currently support print button functionality. To print a report, you must first save it to your computer.

9.3.5. Emailing Reports

To email the report you are viewing:

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

9.3.6. Automatic Deletion of Reports

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

To change the automatic deletion period for generated reports:

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

9.3.7. Deleting Reports

To delete a report:

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

9.4. Managing Scheduled Reports

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

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

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

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

9.4.1. Viewing Last Report Generated

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

9.4.2. Renaming Scheduled Reports

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

To rename a scheduled report:

1. Go to the **Reports > Scheduled Reports** page.
2. Click the report name.
3. Change the report name in the corresponding field. Choose a suggestive name for the report to help easily identify what it is about. When choosing a name, consider the report type and target, and possibly the report options.
4. Click **Generate** to save changes.

9.4.3. Editing Scheduled Reports

> **Note**
> You can only edit scheduled reports that have been generated at least once. If the report has not been generated yet, delete it and define a new one with updated parameters.
> 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 > Scheduled Reports** page.
2. Click the report name.
3. Change report settings as needed. You can change the following:
   - **Report name.** Choose a suggestive name for the report to help easily identify what it is about. When choosing a name, consider the report type and target, and possibly the report options. Reports generated by a scheduled report are named after it.

- **Report target.** The selected option indicates the type of the current report target (either groups or individual computers). Click the corresponding link to view the current report target. To change it, click any of the two links and select the groups or computers to be included in the report.
- **Report recurrence (schedule).** You can set the report to be automatically generated daily, weekly (on a specific day of the week) or monthly (on a specific day of the month). Depending on the selected schedule, the report will only include data from the last day, week or month, respectively.
- **Report options.** You can choose to receive the report by email. Most reports provide filtering options to help you easily find the information you are interested in. When you view the report in the console, all information will be available, regardless of the selected options. If you download or email the report however, only the report summary and selected information will be included in the PDF file. Full report details will only be available in CSV format.

4. Click **Generate** to save changes.

9.4.4. Deleting Scheduled Reports

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

To delete a scheduled report:

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

10. Quarantine

The Cloud Security for Endpoints client software isolates suspicious files and the malware-infected files it cannot disinfect in a secure area named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

Each client has its own quarantine folder. To make your life easier, quarantine content is managed automatically.

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.

Cloud Security Console provides detailed information on all files moved to quarantine on the computers managed from your account. To check and manage quarantined files, go to the **Quarantine** page.

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

- Name given to the malware threat by the Bitdefender security researchers.
- Path to the infected or suspicious file on the computer it was detected on.
- Computer the threat was detected on.
- 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.

10.1. Navigation and Search

Depending on the number of managed computers 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 computer. You can also click column headers to sort data by a specific column.

10.2. 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. Check the list of quarantined files and select the check boxes corresponding to the ones you want to restore.
3. Click the **Restore** button in the upper-right corner of the page.
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. 105).
5. Click **Restore** to request the file restore action. You can notice the pending action in the **Action** column.
6. 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.

10.3. 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 computers.

To change the automatic deletion interval for quarantined files:

1. Go to the **Policies > View Policies** page.
2. Find the policy assigned to the computers 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 save changes.

10.4. 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 in the upper-right corner of the page. You can notice the pending action in the **Action** column.
4. The requested action is sent to the target computers immediately or as soon as they get back online. Once a file is deleted, the corresponding entry will disappear from the Quarantine table.

11. User Accounts

The Cloud Security for Endpoints service can be set up and managed from the Cloud Security Console account received after subscribing to the service. This is your company administrator account.

To allow other company employees access to Cloud Security Console, you can create internal user accounts. User accounts can be used to limit access to the Cloud Security Console features or to specific parts of the company network.

You can create two types of accounts:

Administrator

Administrator accounts offer full access to all areas of the console, allowing users full control over Cloud Security for Endpoints. You can allow access to the entire network or to a specific computer group only.

Reporter

Reporter accounts offer limited access to the console features. Users can only view the dashboard, reports and activity log sections, without being able to view or change the network or security configuration. You can allow access to the entire network or to a specific computer group only.

To create and manage user accounts, go to the **Accounts > Users** page.

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

- Name of the account owner.
- Email address of the account (used to log in to Cloud Security Console and also 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.
- Computer group that the user is in charge of.
- User role (administrator / reporter).

11.1. Creating User Accounts

Create user accounts to delegate administrative or reporting responsibility to other people.

To create a user account:

1. Go to the **Accounts > Users** page.
2. Click the **New** button in the upper-right corner of the page.

3. Under **Account Details**, fill in the account details.
   - **Full name.** Enter the full name of the account owner.
   - **Email.** Enter the user's email address (which will be used by the user to log in to Cloud Security Console). Login information will be sent to this address immediately after creating the account.
   - **Roles.** Select the user role:
     - **Administrator** - has administrative rights over the assigned computers.
     - **Reporter** - has limited access to the console, being able only to monitor and create reports on the security of the assigned computers.
   - **Group.** Choose the computer group that the user will be in charge of. The rest of the company network will be invisible to the user. By default, the user can see the entire network.
4. Under **Settings**, you can configure the account settings.
   - **Send email notification after login**. Enable this option to notify the user for each successful login with the user's account credentials. The message sent to the user's email address will contain the source IP address of the request and the login date and time.
   - **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.
5. Click **Submit**. The new account will appear in the user accounts list.

11.2. Editing Accounts

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

To edit a user account:

1. Go to the **Accounts > Users** page.
2. Click the user's name.
3. Change account details and settings as needed.
4. Click **Submit** to save the changes.

11.3. 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. Go to the **Accounts > Users** page.
2. Select the account from the list.
3. Click the **Delete** button in the upper-right corner of the page.

11.4. 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. Go to the **Accounts > Users** page.
2. Click the user's name.
3. Type a new password in the corresponding fields (under **Account Details**).
4. Click **Submit** to save the changes. Be sure to inform the account owner of the new password.

12. User Activity Log

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

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

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

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

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

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

13. Using Update Server

Update Server allows you to set up a Bitdefender update location within the local network. Having a local update server, you can configure and assign policies to Bitdefender clients so that they update from the local mirror instead of updating from the Internet.

By using a local Bitdefender update location, you can reduce Internet traffic (only one computer connects to the Internet to download updates) and achieve faster updates.

Update Server is completely automated. In order to update the Bitdefender clients from the local network, you only have to install Update Server and assign them policies with the address of the local update server. The update location can be configured in the **General** policy settings category, **Update** tab.

The local update address that must be configured on the Bitdefender client products must follow one of these syntaxes:

- `update_server_ip:update_server_port`
- `update_server_name:update_server_port`

The default port is `7074`.

Note
Update Server can be used to update not only the Cloud Security for Endpoints clients, but also other Bitdefender products. Refer to their documentation to learn how to configure them to update from a local update server.

13.1. Installation

This is where you can find all the information you need to successfully install Update Server in the local network.

- "System Requirements" (p. 92)
- "Obtaining the Installation File" (p. 93)
- "Installing Update Server" (p. 93)

13.1.1. System Requirements

You can install Update Server on any computer running Windows XP or a newer Windows operating system.

Supported browsers (for configuration and management):

- Internet Explorer 8 (+)
- Firefox 8 (+)

- Chrome 10 (+)
- Safari 4 (+)

13.1.2. Obtaining the Installation File

To obtain the Update Server installation file:

1. Connect to Cloud Security Console using your account.
2. Go to the **Computers > Installation Area** page.
3. Click the **Installation Link** button and choose **View**.
4. Depending on the computer platform on which you install Update Server, choose the 32-bit or the 64-bit version of the setup file.

13.1.3. Installing Update Server

The computer on which you install Update Server must be permanently connected to the Internet and accessible from the computers protected by Bitdefender.

To install Update Server:

1. Copy or download the installation file to the designated computer.
2. Double-click the installation file to start the installation wizard.
3. Click **Next**.
4. Please read the License Agreement, select **I accept the terms in the License Agreement** and click **Next**.

   Note
   If you do not agree to these terms click **Cancel**. The installation process will be abandoned and you will exit setup.

5. Choose one of the available installation types to continue:
   - **Default** - to install using the default options.
   - **Custom** - to configure the installation options.

   If you opt for default installation, skip directly to step 8.
6. **Custom Installation!** Update Server will be installed in `?:\Program Files\Bitdefender\Update Server`. To change the installation folder, click **Browse** and choose another folder.

   Click **Next**.
7. **Custom Installation!** The default port is `7074`. If you want to change the default port, type another value in the edit field.

Important

Please take the following into account:

- Provide port values between 1 and 65535.
- Configure the firewall on the computer where Update Server is installed to allow this port to be used.
- The Update Server port must not be used by other applications installed on the system.

Click **Next**. If the port is in use, you will be prompted to set a new port. Otherwise, a new window will appear.

8. Click **Install** to start installation.
9. Wait until installation is completed and then click **Finish**.

13.2. Configuration and Management

Refer to the following topics to find out how to configure and manage a Bitdefender update location in the local network using Update Server.

- "Accessing Management Panel" (p. 94)
- "What You Have to Do After Installation" (p. 94)
- "Managing Client Products and Downloaded Updates" (p. 95)
- "Configuring Settings" (p. 96)
- "Changing Login Password" (p. 97)

13.2.1. Accessing Management Panel

Update Server has a web-based interface, which facilitates easy configuration and monitoring from any computer connected to the network.

To access the Update Server management panel, do any of the following:

- Open a web browser and type the server address using one of these syntaxes:
  - `http://update_server_ip:port`
  - `http://update_server_name:port`
- On the computer on which Update Server is installed, go to the Windows Start menu and follow the path: **Start** → **Programs** → **Update Server** → **Update Server**.

Type the login password in the corresponding field and click **Login**. The default password is `admin`.

13.2.2. What You Have to Do After Installation

This is what you have to do after installation:

1. Change the default `admin` password to prevent unauthorized access. For more information, refer to "Changing Login Password" (p. 97).
2. If the computer on which Update Server is installed connects to the Internet through a proxy server, you must configure the proxy settings.
   a. Access the **Settings** page.
   b. Select the **Use proxy settings** check box.
   c. Specify the proxy settings to be used. For more information, refer to "Configuring Settings" (p. 96).
3. Configure the client products installed in the network to download updates from the local update server. Use the policy to configure Endpoint Security with the local update address (**General** settings category, **Update** tab).

   The local update address that must be configured on the Bitdefender client products must follow one of these syntaxes:
   - `update_server_ip:port`
   - `update_server_name:port`

   The default port is `7074`.

13.2.3. Managing Client Products and Downloaded Updates

To manage the client products for which updates are downloaded and to see update information, access the **Products** page (displayed by default after logging in to the management panel).

You can see Update Server statistics and the list of client products for which updates are downloaded. The status and time of each client product's latest update are displayed.

Downloading Latest Updates

To download the updates available for all the products in the list, click the ⟳ **Update now** button.

Adding New Products

To select additional products to be updated by Update Server, click the + **Add Products** button. A new page is displayed.

You can see the list of additional Bitdefender client products that can be updated using Update Server. To browse easily through the list, you can filter products by type, platform and language.

Select the check box corresponding to the desired products and click the ✓ **Save** button.

Removing Products

To remove a product from the list of updated products, click the corresponding **Remove** link in the **Actions** column. When you remove a client product from the list:

1. Update Server will no longer download updates for that client product. However, if the client product later connects to Update Server to check for updates, it will be automatically added to the list.
2. The updates downloaded for that client product are removed if they are not used by another product in the list. For example, malware signatures are common to all language versions of a specific product and platform (32-bit or 64-bit).

13.2.4. Configuring Settings

To configure the Update Server settings, access the **Settings** page. The following settings can be configured:

- **Update server.** By default, Update Server will download updates on the local computer from `upgrade.bitdefender.com:80`. This is a generic address that is automatically resolved to the closest server that stores Bitdefender malware signatures in your region.

  To check for and download updates from a local update server (cascading configuration), replace the Internet update address with the address of the local update server. Use one of these syntaxes:
  - `update_server_ip:port`
  - `update_server_name:port`

  The default port is `7074`.
- **Local directory.** If you want to change the folder the updates are downloaded to, type the path to the new folder in this field.
- **Update server port.** In this field you can change the Update Server port configured during installation. The default port is `7074`. The Update Server port must not be used by other applications installed on the system.

  Note

  If you change the port at a time when Update Server is already in use, the update location of all Bitdefender products configured to download updates from the local update server must be changed accordingly.
- **Update period.** By default, Update Server downloads updates from the Internet update location every hour. If you want to change the update period, type a new value in this field.
- **Session period.** By default, you are automatically logged out of the management panel after 5 minutes of inactivity. If you want to change the maximum allowed period of inactivity, type a new value in this field. You can set this period between 1 and 30 minutes.

- **View advanced settings.** Select this check box to view and configure advanced settings.
  - **Gateway roles.** Update Server can act as gateway for data sent by the Bitdefender client products installed in the network to the Bitdefender servers. This data may include anonymous reports regarding virus and spam activity, product crash reports and data used for online registration. Enabling the gateway roles is useful for traffic control and in networks with no Internet access.

    Note

    You can disable the product modules that send statistical or crash data to Bitdefender Labs anytime you want. You can use policies to remotely control these options on the computers managed by Cloud Security Console.

  - **Download not-selected locations.** Update Server automatically downloads updates for any Bitdefender client product that requests them (even if you have not selected that product in the Products page). If you want only updates for the authorized products to be downloaded, clear this check box.
  - **Allow update for unused products.** Update Server checks for and downloads updates regularly for all Bitdefender products that request updates. If you want to stop downloading updates that have not been requested for some time, clear this check box and specify the inactivity period.
- **Use proxy settings.** Select this check box if your company connects to the Internet through a proxy. You must fill in the following fields:
  - **Proxy Address** - type in the IP address of the proxy server.
  - **Proxy Port** - type in the port used to connect to the proxy server.
  - **Proxy Username** - type in a user name recognized by the proxy.
  - **Proxy Password** - type in the valid password of the previously specified user.

  If you select **Use proxy cache**, Update Server will first check the proxy server's cache for recently downloaded updates and will use such updates, if available. This option is not recommended, but it may be useful if you pay your Internet connection for traffic.

Click the ✓ **Save** button to save the changes.

13.2.5. Changing Login Password

To change the login password:

1. Choose **Change Password** from the **Administrator** menu in the upper-right corner of the management panel. A new page is displayed.
2. You must fill in the following fields:
   - **Old password** - type in the old password.
   - **New password** - type in the new password.
   - **Confirm password** - type in the new password again.

3. Click **Change Password** to save the new password.

13.3. Cascading Configuration

You can set up Bitdefender local update servers to download Bitdefender updates from another local update server instead of the Internet. This particular configuration is known as cascading configuration.

Cascading configuration is generally used in geographically distributed computer networks, when one of the following conditions apply:

- Only the central network has direct Internet access (the other networks may connect through the central network or they may not have Internet access at all).
- The connection to the central network is faster (or more convenient in some other way) than the direct Internet connection.

To set up a cascading configuration:

1. Install and set up the local update server that will download Bitdefender updates from the Internet. No special configuration is required for this update server to allow distribution of Bitdefender updates to other local update servers (updates are automatically available to both Bitdefender clients and other local update servers, provided they are properly configured).
2. Configure the update servers in the isolated networks to download updates from the main update server. This is what you have to do:
    a. Access the **Settings** page.
    b. In the **Update Server** field, replace the Internet update address with the address of the local update server that downloads updates from the Internet. Use one of these syntaxes:
        - `main_update_server_ip:main_update_server_port`
        - `main_update_server_name:main_update_server_port`

       The default port is `7074`.
    c. Make sure the update servers can communicate. The easiest way to test this is to go to the Products page, add a new product to the list and start an update. If the update cannot be performed, check your network and firewall configurations.
3. There are no changes in how you configure the Bitdefender client products to update from their local update server.

14. Getting Help

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

Note
You can find out information about the support services we provide and our support policy at the Support Center.

14.1. Bitdefender Support Center

Bitdefender Support Center, available at http://www.bitdefender.com/businesshelp, 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/businesshelp.

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.

14.2. 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.

14.3. Using Support Tool

The Cloud Security for Endpoints 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 Cloud Security Console using your account.
   b. Click the **Help and Support** link in the upper-right corner of the console.

   c. The download links are available in the **Support Tool** 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 from the corresponding menu the type of issue you have encountered.
      iv. Choose your country from the corresponding menu.
      v. Enter a description of the issue you encountered.
   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.

      You can send the zip archive together with your request for support in order to reduce the time needed to resolve the query.

14.4. 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.

14.4.1. Web Addresses

Sales Department: sales@bitdefender.com
Support Center: http://www.bitdefender.com/businesshelp
Documentation: documentation@bitdefender.com
Local Distributors: http://www.bitdefender.com/partners
Partner Program: partners@bitdefender.com
Media Relations: pr@bitdefender.com
Job Opportunities: jobs@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

14.4.2. Local Distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to http://www.bitdefender.com/partners.
2. Go to **Partner Locator**.
3. The contact information of the Bitdefender local distributors should be displayed automatically. If this does not happen, select the country you reside in to view the information.
4. If you do not find a Bitdefender distributor in your country, feel free to contact us by email at sales@bitdefender.com. Please write your email in English in order for us to be able to assist you promptly.

14.4.3. Bitdefender Offices

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

United States

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

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/businesshelp

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/businesshelp

Spain

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1° 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/businesshelp

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/businesshelp

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/businesshelp

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

ActiveX

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

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

Adware

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

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

Archive

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

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

Backdoor

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

Boot sector

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

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory.

Every time you boot your system from that point on, you will have the virus active in memory.

Browser

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

Command line

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

Cookie

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

Disk drive

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

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

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

Download

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

Email

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

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive

Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension

The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

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.

Java applet

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

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

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.

Mail client

An email client is an application that enables you to send and receive email.

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.

Memory

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

Non-heuristic

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

Packed programs

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

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

Path

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

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

Phishing

The act of sending an 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.

Startup items

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

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has its own update module that allows you to manually check for updates, or let it automatically update the product.

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.