



Bitdefender® ENTERPRISE

**CLOUD SECURITY  
FOR ENDPOINTS**  
Quick Start Guide >>

# Cloud Security for Endpoints by Bitdefender

## Quick Start Guide

Publication date 2013.07.30

Copyright© 2013 Bitdefender

### Legal Notice

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

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

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

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



# Table of Contents

<b>Using This Guide</b> .....	<b>v</b>
<b>1. About Cloud Security for Endpoints</b> .....	<b>1</b>
1.1. Architecture .....	1
1.2. User Accounts .....	2
1.3. Threat Protection .....	3
1.3.1. Antimalware .....	3
1.3.2. Antiphishing .....	5
1.3.3. Firewall and Intrusion Detection .....	5
1.3.4. Data Protection .....	6
1.3.5. Content Control .....	6
1.4. Workflow .....	6
1.4.1. Deployment .....	7
1.4.2. Endpoint Management .....	7
1.4.3. Security Policies .....	7
1.4.4. Scan Tasks .....	8
1.4.5. Reports .....	8
<b>2. Getting Started</b> .....	<b>9</b>
2.1. Connecting to Cloud Security Console .....	9
2.2. Cloud Security Console Overview .....	9
2.3. Managing Your Account .....	10
2.4. Changing Default Login Password .....	12
<b>3. Service Subscription</b> .....	<b>13</b>
3.1. Activating a License .....	13
3.2. Renewing a License .....	14
3.3. Extending the Number of Licensed Endpoints .....	14
3.4. Checking Your Subscription Status .....	14
<b>4. Installation and Setup</b> .....	<b>15</b>
4.1. Step 1 - Prepare for Installation .....	15
4.2. Step 2 - Install Service on Computers .....	15
4.3. Step 3 - Organize Computers (Optional) .....	18
4.4. Step 4 - Create and Configure a Security Policy .....	19
<b>5. Monitoring Security Status</b> .....	<b>21</b>
<b>6. Scanning Managed Computers</b> .....	<b>23</b>
<b>7. Getting Help</b> .....	<b>24</b>
<b>A. Requirements</b> .....	<b>25</b>
A.1. System Requirements .....	25
A.2. Network Discovery Requirements .....	26

# Using This Guide

This Quick Start Guide is intended for IT administrators who want to use the Cloud Security for Endpoints service to protect and control company computers (workstations, laptops and servers). It provides them with the basics of getting familiar with, setting up and managing the service.

The guide is designed to help new users quickly get Cloud Security for Endpoints up and running on company computers.

The information presented herein should be easy to understand by anyone who is able to work under Windows.

We wish you a pleasant and useful lecture.

## How to Use This Guide

This guide is organized so as to make it easy to find the information you need.

[“About Cloud Security for Endpoints” \(p. 1\)](#)

Learn about Cloud Security for Endpoints.

[“Getting Started” \(p. 9\)](#)

Get started with Cloud Security Console (the service management console).

[“Service Subscription” \(p. 13\)](#)

What you need to know about service subscription.

[“Installation and Setup” \(p. 15\)](#)

Steps to follow to get the service up and running on computers.

[“Monitoring Security Status” \(p. 21\)](#)

Find out how to monitor the network security status.

[“Scanning Managed Computers” \(p. 23\)](#)

Learn how to scan managed computers for viruses and other malware.

[“Getting Help” \(p. 24\)](#)

Where to look and where to ask for help if something unexpected appears.

[“Requirements” \(p. 25\)](#)

Requirements for using the service.

## Additional Documentation

The following is a list of additional documentation for Cloud Security for Endpoints:

## Help

Comprehensive documentation available in Cloud Security Console (click the **Help and Support** link in the upper-right corner).

## Administrator's Guide

Comprehensive documentation in PDF format for service administrators.

## Reporter's Guide

Comprehensive documentation in PDF format for Cloud Security Console users with Reporter role.

## Endpoint Security User's Guide

Comprehensive documentation in PDF format for the end users on protected computers.

All PDF documentation is available at the [online Bitdefender Support Center](#). The Support Center also provides you with useful Knowledge Base articles.

## Conventions Used in This Guide

Several text styles are used in the guide for an improved readability. Their aspect and meaning are presented in the table below.

Appearance	Description
<a href="https://cloud.bitdefender.net">https://cloud.bitdefender.net</a>	The URL link is pointing to some external location, on http or ftp servers.
"Using This Guide" (p. v)	This is an internal link, towards some location inside the document.
<b>option</b>	All user interface options are printed using <b>bold</b> characters.
<b>keyword</b>	Important keywords or phrases are highlighted using <b>bold</b> characters.
<code>sample syntax</code>	Syntax samples are printed with <code>monospaced</code> characters.

The admonitions are in-text notes, graphically marked, bringing to your attention additional information related to the current paragraph.



### Note

The note is just a short observation. Although you can omit it, the notes can provide valuable information, such as specific feature or a link to some related topic.



### Important

This requires your attention and is not recommended to skip over it. Usually, it provides non-critical but significant information.



## Warning

This is critical information you should treat with increased caution. Nothing bad will happen if you follow the indications. You should read and understand it, because it describes something extremely risky.

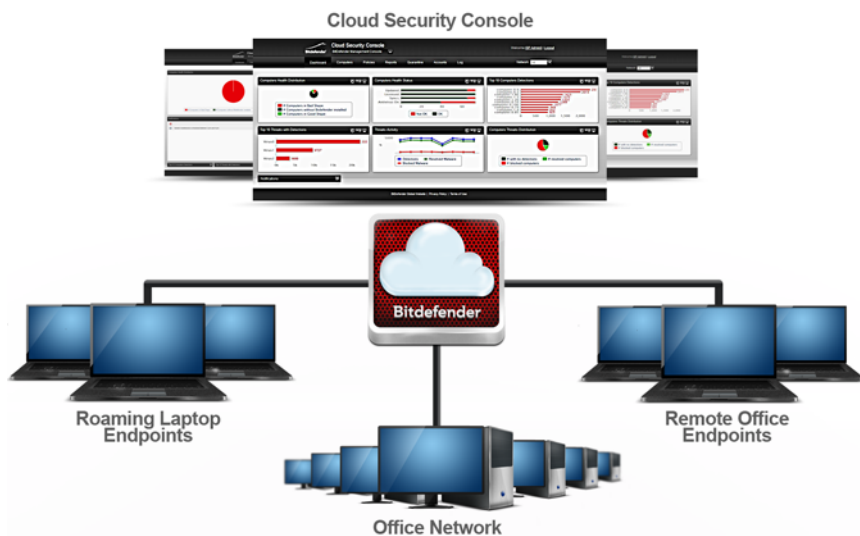
# 1. About Cloud Security for Endpoints

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
- [Content 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 3<sup>rd</sup> 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. Content Control

The Content 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 Content 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. Access to Cloud Security Console is done via user accounts.

Following your registration for a trial version or your purchase of the service, you will receive an email from the Bitdefender Registration Service. The email contains your login information.

### 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. 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” \(p. 13\)](#).
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.

**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.

## 2.4. 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.

## 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](mailto: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. Installation and Setup

Once you have received your login credentials, you can log in to Cloud Security Console and start installing the service on computers.

Installation and setup is fairly easy. These are the main steps:

1. [Prepare for installation.](#)
2. [Install service on computers.](#)
3. [Organize computers into groups \(optional\).](#)
4. [Create and configure a security policy.](#)

### 4.1. Step 1 - Prepare for Installation

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

1. Make sure the computers meet the [minimum system requirements](#). For some computers, you may need to install the latest operating system service pack available or free up disk space.
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 and Internet access. Make sure these conditions are fulfilled.

### 4.2. Step 2 - Install Service on Computers

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.** Use the installation link from your Cloud Security Console account to download and install Endpoint Security locally on individual computers. 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. Local installation is wizard-guided.
- **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.

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

The display language of the user interface on protected computers is set at installation time based on the language of your account. To install the user interface in another language on certain computers, you must temporarily [change your account language](#) and only then proceed to installation (using either the new installation link or remote installation).

## Local Installation

Local installation requires running an installation file, which you can download from Cloud Security Console, on each computer to be protected. 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.

For local installation:

1. Connect to Cloud Security Console using your account.
2. Go to the **Computers > Installation Area** page.
3. You can configure default installation options by clicking **Customize Package**.

- 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 **Uninstall password protection** 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`



### 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.

4. 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. To view the link, click the **Installation Link** button and choose **View**.
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. To email the link, click the **Installation Link** button and choose **Send by Email**. Note that users are sent the web installer link.

## 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.

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. For network



discovery to work, a number of requirements must be met. To learn more, refer to “[Network Discovery Requirements](#)” (p. 26).

**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.

For remote installation:

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 on which you want to install protection.
4. Click **Tasks** and choose **Install** from the menu. The Installation Options window will appear.
5. You can change default installation options as needed.
6. 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.
7. 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.

## 4.3. Step 3 - Organize Computers (Optional)

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.

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, Management etc.).
- Security needs (Desktops, Laptops, Servers etc.).
- Location (Headquarter, Local Offices, Remote Workers, Home Offices etc.).

To organize your network into groups:

1. Go to the **Computers > View Computers** page.
2. 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.
3. Rename the newly created group.
4. Follow the previous steps to create additional groups.
5. Move computers from the root group to the appropriate group.
  - a. Select the check boxes corresponding to the computers you want to move.
  - b. Drag and drop your selection to the desired group in the left-side pane.

## 4.4. Step 4 - Create and Configure a Security Policy

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. 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 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.

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.

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. 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. Default security settings are recommended for most situations. There are some features you may want to configure:
  - **Password protection.** To prevent users with administrative rights from uninstalling protection, you must set a password. Go to **General > Advanced** and set the desired password.
  - **Update preferences.** Endpoint Security automatically checks for, downloads and installs updates every hour (default setting). To change the update frequency and other settings, go to **General > Update**. If your company connects to the Internet through a proxy server, you must specify the proxy settings. 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.
  - **Scheduled scan tasks.** You can create and configure scheduled scan tasks to run regularly on computers. To create and configure a new scan task, go to **Antimalware > On-Demand** and click **Add Task**.
  - **Firewall permissions and rules.** You can go to **Firewall > Advanced** to check and configure firewall permissions and create firewall rules for applications that need access to network and Internet services.
  - **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. This is what you can do:
    - Configure traffic scan
    - Allow or block web access for users or applications during specified time intervals
    - Use Web Categories Filter to allow or block access to entire categories of websites
    - Create Data Protection rules to protect any piece of personal or confidential information
    - Configure Application Control to completely block or restrict users' access to applications on their computers
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.

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.

## 5. Monitoring Security Status

The main Cloud Security for Endpoints monitoring tool is the Cloud Security Console dashboard. Check the **Dashboard** page regularly to see real-time information on the network security status.

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.

### 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.
- 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.

### 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.

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.

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.

## 6. 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. If you have not done this already, you will be prompted to select the customer company you want to manage.
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.

## 7. Getting Help

To find additional help resources or to get help from Bitdefender:

- Click the **Help and Support** link in the upper-right corner of Cloud Security Console.
- Go to our [online Support Center](#).

To open an email support ticket, use [this web form](#).

# A. Requirements

## A.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

## A.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.