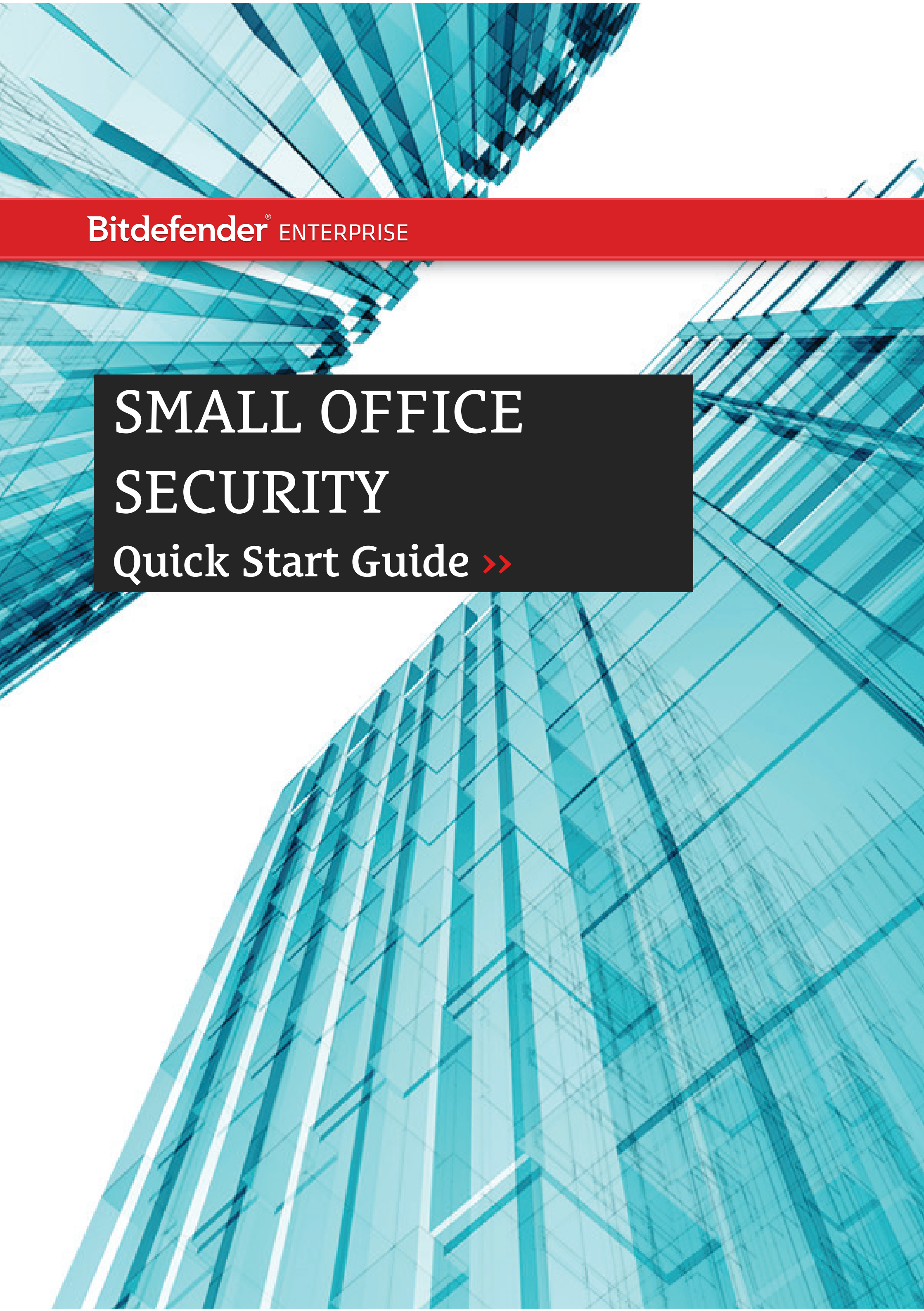


Bitdefender® ENTERPRISE

SMALL OFFICE SECURITY

Quick Start Guide ››

Small Office Security
Quick Start Guide

Publication date 2014.12.10

Legal Notice

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

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

Bitdefender®

Table of Contents

1. About Small Office Security 1

2. Getting Started 2
2.1. Connecting to Control Center 2
2.2. Control Center at a Glance 3
2.2.1. Control Center Overview 3
2.2.2. Table Data 4
2.2.3. Action Toolbars 5
2.2.4. Contextual Menu 6
2.3. Managing Your Account 6
2.4. Managing Your Company 7
2.5. Changing Login Password 9

3. License Management 10
3.1. Activating a License 10
3.2. Checking Current License Details 11

4. Installation and Setup 12
4.1. Preparing for Installation 12
4.2. Installing Service on Computers 12
4.2.1. Local Installation 14
4.2.2. Remote Installation 17
4.3. Organizing Computers (Optional) 22
4.4. Creating and Assigning a Security Policy 23

5. Monitoring Security Status 27

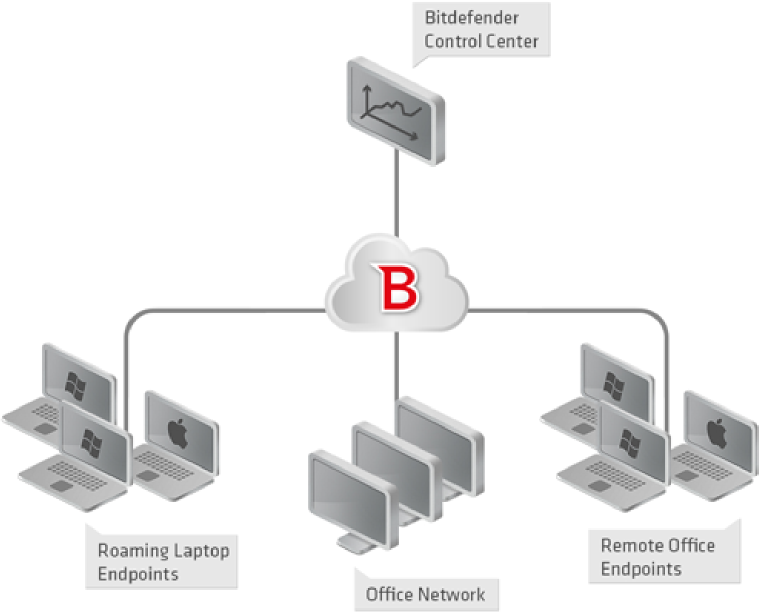
6. Scanning Managed Computers 29

7. Getting Help 31

A. Requirements 32
A.1. Security for Endpoints Requirements 32
A.1.1. Supported Operating Systems 32
A.1.2. Hardware Requirements 33
A.1.3. Supported Browsers 33
A.1.4. Small Office Security Communication Ports 33
A.2. How Network Discovery Works 34
A.2.1. More about the Microsoft Computer Browser Service 35
A.2.2. Network Discovery Requirements 36

1. About Small Office Security

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



Small Office Security Architecture

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

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

2. Getting Started

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

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 Control Center

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

Prerequisites:

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

To connect to Control Center:

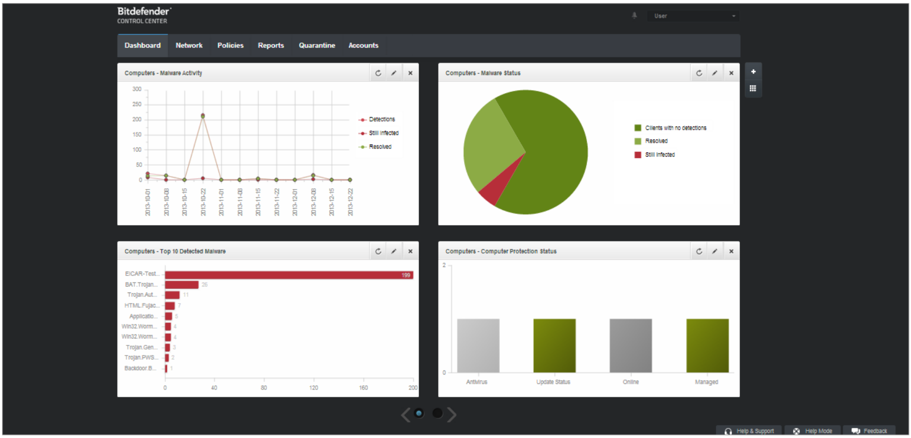
1. Open your web browser.
2. Go to the following address: https://gravityzone.bitdefender.com
3. Enter the email address and password of your account.
4. Click **Login**.

Note

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

2.2. Control Center at a Glance

Control Center is organized so as to allow easy access to all the features. Use the menu bar in the upper area to navigate through the console. Available features depend on the type of user accessing the console.



The Dashboard

2.2.1. Control Center Overview

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

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

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

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

Policies
Create and manage security policies.

Reports
Get security reports concerning the managed clients.

Quarantine
Remotely manage quarantined files.

Accounts

Manage the access to Control Center for other company employees.

Note

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

Additionally, in the upper-right corner of the console, the 🔔 **Notifications** icon provides easy access to notification messages and also to the **Notifications** page.

By pointing to the username in the upper-right corner of the console, the following options are available:

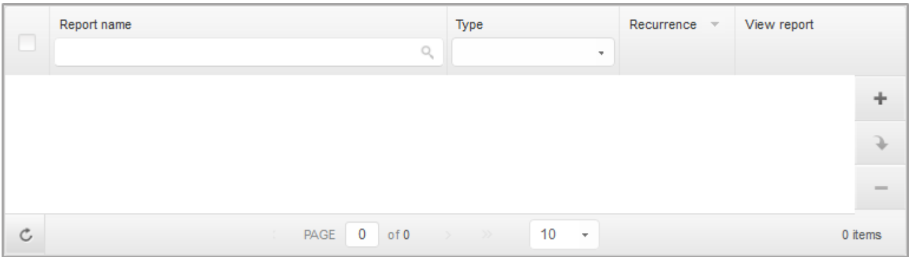
- **My Account**. Click this option to manage your user account details and preferences.
- **My Company**. Click this option to manage your company account details and preferences.
- **Credentials Manager**. Click this option to add and manage the authentication credentials required for remote installation tasks.
- **Logout**. Click this option to log out of your account.

On the lower-right corner of the console, the following links are available:

- **Help and Support**. Click this button to find help and support information.
- **Help Mode**. Click this button to enable a help feature providing expandable tooltips boxes placed on Control Center items. You will easily find out useful information regarding the Control Center features.
- **Feedback**. Click this button to display a form allowing you to edit and send your feedback messages regarding your experience with Small Office Security.

2.2.2. Table Data

Tables are frequently used throughout the console to organize data into an easy-to-use format.



The Reports page - Reports Table

Navigating through Pages

Tables with more than 10 entries span on several pages. By default, only 10 entries are displayed per page. To move through the pages, use the navigation buttons at the bottom of the table. You can change the number of entries displayed on a page by selecting a different option from the menu next to the navigation buttons.

Searching for Specific Entries

To easily find specific entries, use the search boxes available below the column headers.

Enter the search term in the corresponding field. Matching items are displayed in the table as you type. To reset the table contents, clear the search fields.

Sorting Data

To sort data by a specific column, click the column header. Click the column header again to revert the sorting order.

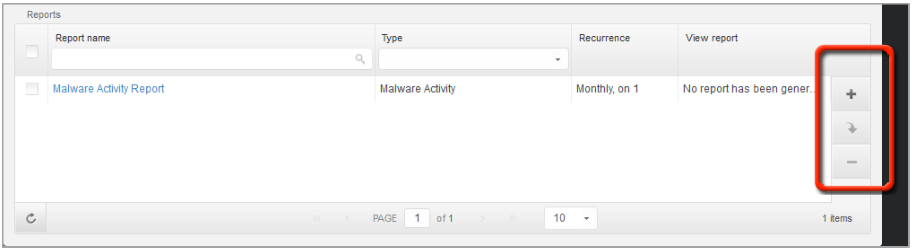
Refreshing Table Data

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

2.2.3. Action Toolbars

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

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



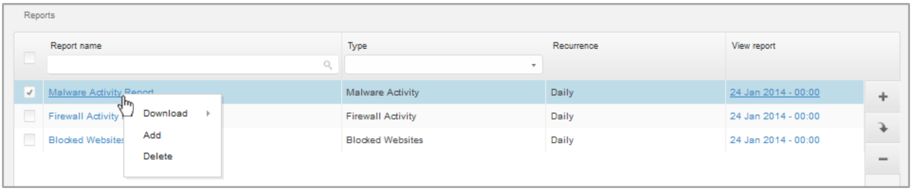
Reports

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

The Reports page - Action Toolbars

2.2.4. Contextual Menu

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



Reports

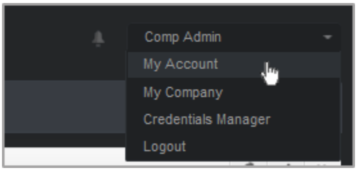
	Report name	Type	Recurrence	View report
☑	Malware Activity Report	Malware Activity	Daily	24 Jan 2014 - 00:00
□	Firewall Activity	Firewall Activity	Daily	24 Jan 2014 - 00:00
□	Blocked Websites	Blocked Websites	Daily	24 Jan 2014 - 00:00

The Reports page - Contextual menu

2.3. Managing Your Account

To check or change your account details and settings:

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



The User Account menu

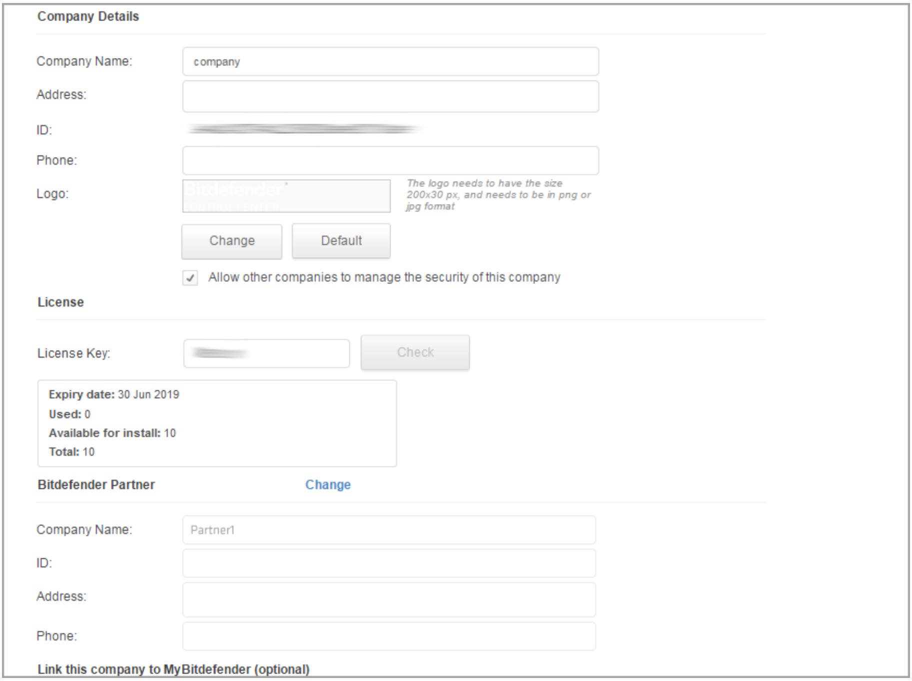
2. Under **Account Details**, correct or update your account details.
   - **Full name.** Enter your full name.
   - **Email.** This is your login and contact email address. Reports and important security notifications are sent to this address. Email notifications are sent automatically whenever important risk conditions are detected in the network.
   - **Password.** A **Change password** link allows you to change your login password.
3. Under **Settings**, configure the account settings according to your preferences.
   - **Timezone.** Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
   - **Language.** Choose from the menu the console display language.
   - **Session Timeout.** Select the inactivity time interval before your user session will expire.
4. Click **Save** to apply the changes.

Note
You cannot delete your own account.

2.4. Managing Your Company

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

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



Company Details

Company Name: company

Address:

ID: [redacted]

Phone:

Logo:

The logo needs to have the size 200x30 px, and needs to be in png or jpg format
Change
Default

☑ Allow other companies to manage the security of this company

License

License Key: [redacted]

Expiry date: 30 Jun 2019
Used: 0
Available for install: 10
Total: 10

Bitdefender Partner

Company Name: Partner1

ID:

Address:

Phone:

Link this company to MyBitdefender (optional)

My Company Page

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

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

   To change your managed service provider:

   a. Click the **Change** button.
   b. Enter the partner's company ID code in the **Partner ID** field.

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

   c. Click **Save**.

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

2.5. Changing Login Password

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

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

To change the login password:

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

3. License Management

The security service provided by Small Office Security requires a valid license key.

You can try Small Office Security 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.

- 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, Small Office Security' 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 Small Office Security subscription is enabled by activating this license key.

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 Control Center using your customer account.
2. Point to your user account in the upper-right corner of the console and choose **My Company**.

   Note
   This privilege is specific to company administrator accounts.

3. Check details about the current license in the **License** section.
4. From the **Type menu**, choose a **License** subscription type.
5. Enter the key in the **License key** field.
6. Click the **Check** button and wait until Control Center retrieves information about the entered license key.
7. Click **Save**.

3.2. Checking Current License Details

To check your subscription status:

1. Log in to Control Center using your email and password received by email.
2. Point to your user account in the upper-right corner of the console and choose **My Company**.

   Note
   This privilege is specific to company administrator accounts.

3. Check details about the current license in the **License** section:
   - **Expiry date**: the date until the license key can be used.
   - **Used**: the number of used seats from the total amount of seats on the license key. A license seat is used when the Bitdefender client has been installed on an endpoint from the network under your management.
   - **Available for install**: the number of free seats from the total number of seats on a monthly license pool (excluding used seats).
   - **Total**: the total number of license seats available for your subscription.
4. Click **Save**.

4. Installation and Setup

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

1. Step 1 - Preparing for installation.
2. Step 2 - Installing service on computers.
3. Step 3 - Organizing computers into groups (optional).
4. Step 4 - Creating and configuring a security policy.

For the first two steps, computer login information are required. The other two steps are performed from Control Center.

4.1. Preparing for Installation

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

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

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

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

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

4.2. Installing Service on Computers

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

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

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

Warning

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

There are two installation methods:

- **Local installation**. Download the installation packages from Control Center on individual computers, then run locally the Endpoint Security installation. Another option is to download the package, save it on a network share and send users within the company email invites with the package link, asking them to download and install protection on their computer. Local installation is wizard-guided.
- **Remote installation**. Once you have locally installed the first client with Endpoint Security Relay role, it may take a few minutes for the rest of the network computers to become visible in Control Center. The Security for Endpoints protection can then be remotely installed from the console on other computers in the network. 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.

By default, the display language of the user interface on protected computers is set at installation time based on the language of your account. To install the user interface in another language on certain computers, you can create an installation package and set the preferred language in the package configuration options. For more information on creating installation packages, refer to “Creating Endpoint Security Installation Packages” (p. 14).

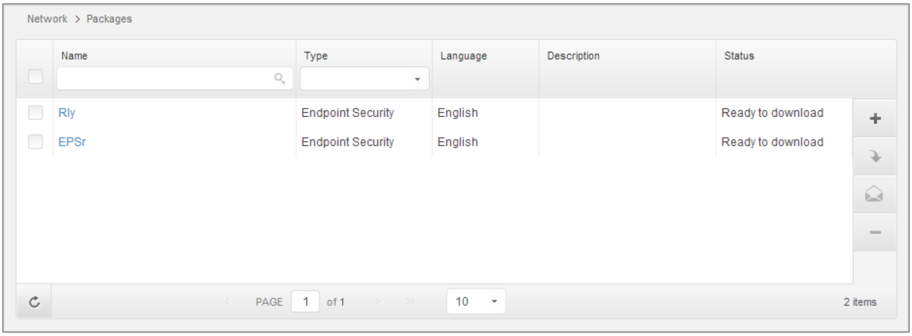
4.2.1. Local Installation

Local installation requires downloading from Control Center and running the installation package on each target computer. You can create different installation packages according to specific requirements of each computer (for example, the installation path or the user interface language).

Creating Endpoint Security Installation Packages

To create an Endpoint Security installation package:

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

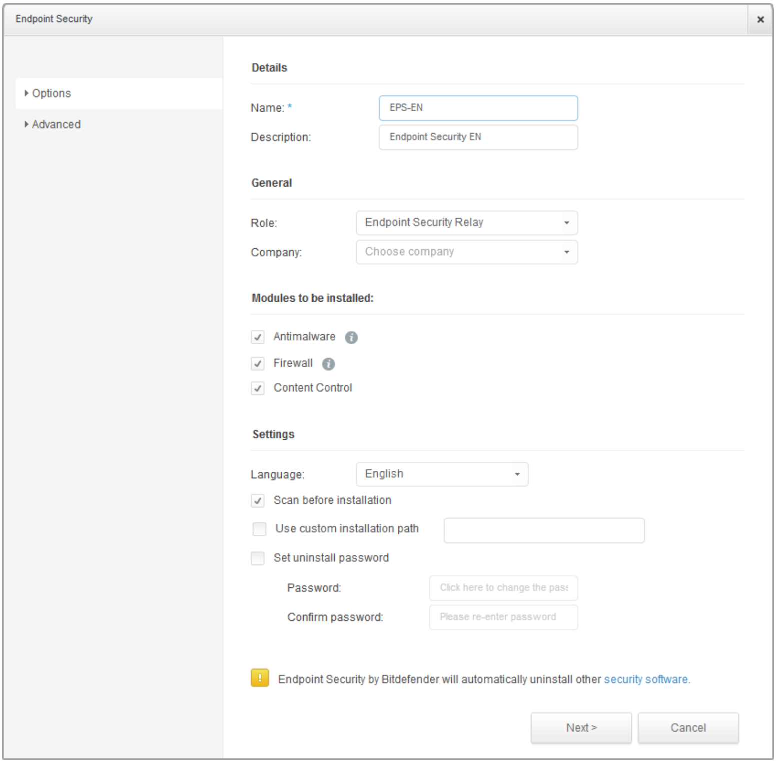


Network > Packages

Name	Type	Language	Description	Status
Rly	Endpoint Security	English		Ready to download
EPSr	Endpoint Security	English		Ready to download

The Packages page

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



Endpoint Security

- Options
- Advanced

Details

Name: * EPS-EN

Description: Endpoint Security EN

General

Role: Endpoint Security Relay

Company: Choose company

Modules to be installed:

☑ Antimalware

☑ Firewall

☑ Content Control

Settings

Language: English

☑ Scan before installation

□ Use custom installation path

□ Set uninstall password

Password: Click here to change the pass

Confirm password: Please re-enter password

Endpoint Security by Bitdefender will automatically uninstall other security software.

Create Endpoint Security Packages - Options

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

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

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

14. Click **Save**.

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

Downloading and Installing Endpoint Security

1. Connect to https://gravityzone.bitdefender.com/ using your account from the computer on which you want to install protection.
2. Go to the **Network > Packages** page.
3. Select the appropriate company from the list available under **Company** column header. Only the packages available for the selected company will be displayed.
4. Select the Endpoint Security installation package you want to download.
5. Click the **Download** button at the right side of the table and select the type of installer you want to use. Two types of installation files are available:
    - **Downloader**. The downloader first downloads the full installation kit from the Bitdefender cloud servers and then starts the installation. It is small in size and it can

be run both on 32-bit and 64-bit systems (which makes it easy to distribute). On the downside, it requires an active Internet connection.

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

6. Save the file to the computer.
7. Run the installation package.

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

8. Follow the on-screen instructions.

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

4.2.2. Remote Installation

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

To make deployment easier, Security for Endpoints includes an automatic network discovery mechanism that allows detecting computers in the same network. Detected computers are displayed as **unmanaged computers** in the **Network** 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. It may take a few minutes for the rest of the network computers to become visible in Control Center.

Remote Installation Requirements

For network discovery to work, a number of requirements must be met. To learn more, refer to “How Network Discovery Works” (p. 34).

For remote installation to work:

- Each target computer must have the admin$ administrative share enabled. Configure each target workstation to use advanced file sharing.

- Temporarily turn off User Account Control on all computers running Windows operating systems that include this security feature (Windows Vista, Windows 7, Windows Server 2008 etc.). If the computers are in a domain, you can use a group policy to turn off User Account Control remotely.
- Disable or shutdown firewall protection on computers. If the computers are in a domain, you can use a group policy to turn off Windows Firewall remotely.

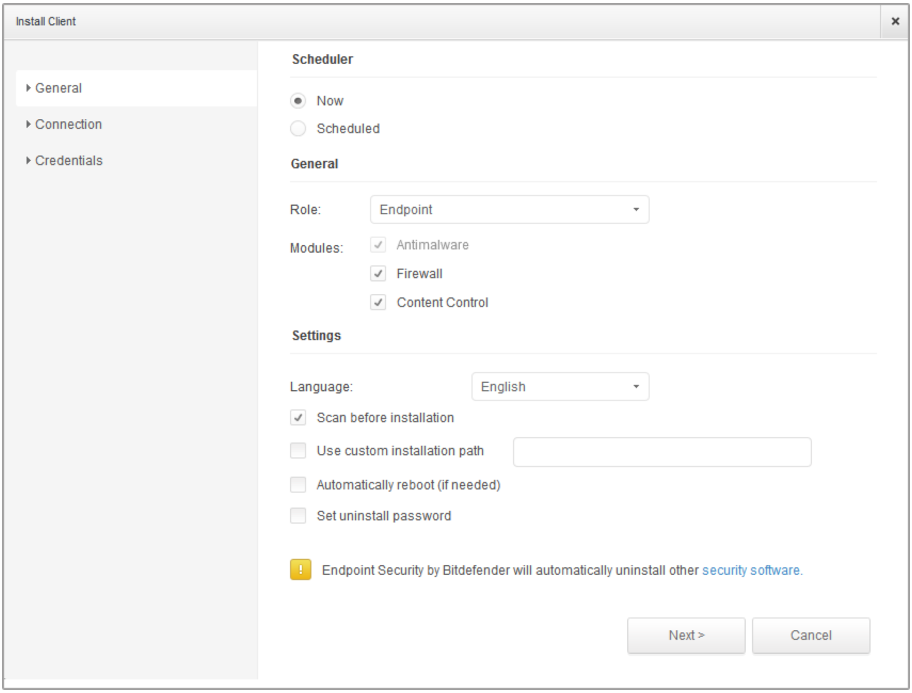
Running Remote Endpoint Security Installation Tasks

To run a remote installation task:

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

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

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



Install Client

Scheduler

● Now

○ Scheduled

General

Role: Endpoint

Modules: ☑ Antimalware ☑ Firewall ☑ Content Control

Settings

Language: English

☑ Scan before installation

□ Use custom installation path

□ Automatically reboot (if needed)

□ Set uninstall password

! Endpoint Security by Bitdefender will automatically uninstall other security software.

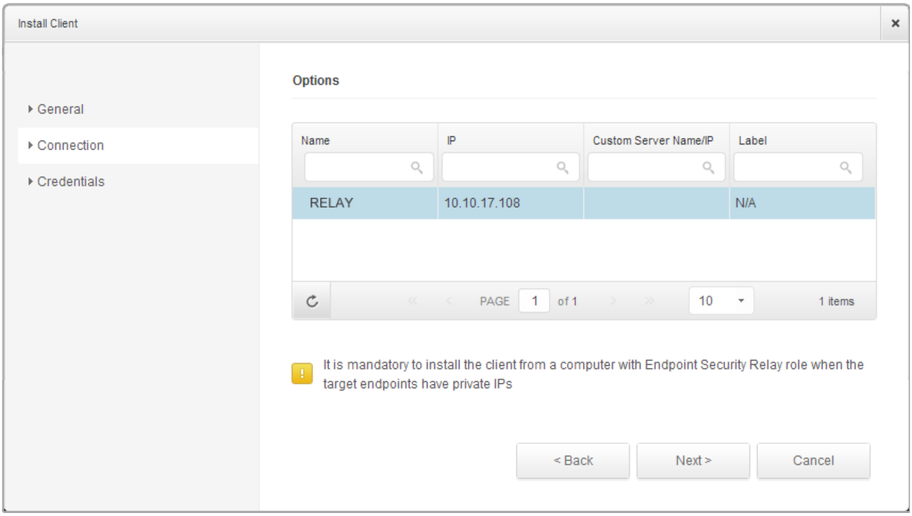
Installing Endpoint Security from the Tasks menu

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

       Note
       For example, when certain operations are required on the target machine before installing the client (such as uninstalling other software and restarting the OS), you can schedule the deployment task to run every 2 hours. The task will start on each target machine every 2 hours until the deployment is successful.
   - Select the protection modules you want to install. Please note that only antimalware protection is available for server operating systems.
   - From the **Language** field, select the desired language for the client's interface.

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

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



Name	IP	Custom Server Name/IP	Label
RELAY	10.10.17.108		N/A

It is mandatory to install the client from a computer with Endpoint Security Relay role when the target endpoints have private IPs

7. Click **Next**.

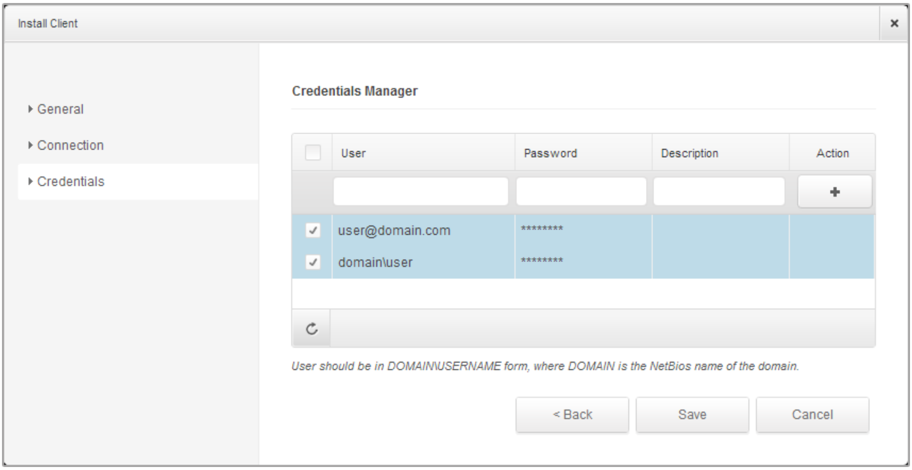
8. Under the **Credentials Manager** section, specify the administrative credentials required for remote authentication on selected endpoints. You can add the required credentials by entering the user and password of each target operating system.

Important

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

Note

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



☐	User	Password	Description	Action
☑	user@domain.com	********		
☑	domain\user	********		

User should be in DOMAIN\USERNAME form, where DOMAIN is the NetBios name of the domain.

To add the required OS credentials:

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

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

   ### Note

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

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

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

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

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

4.3. Organizing Computers (Optional)

Company networks are displayed in the left-side pane of the **Network** page. There is a default root group for each of your companies. All of its protected or detected computers are automatically placed in this group.

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

You can organize computers by creating groups under the default company 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.).

Note

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

To organize a customer's network into groups:

1. Go to the **Network** page.
2. In the left-side pane, under **Companies**, select the customer company you want to manage.

   Note
   For partner companies under your account having the right to manage networks, select the **Networks** group.

3. Click the + **Add group** button at the top of the left-side pane.

4. Enter a suggestive name for the group and click **OK**. The new group is displayed under the corresponding company.
5. Follow the previous steps to create additional groups.
6. 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. Creating and Assigning a Security Policy

Once installed, the Security for Endpoints protection can be configured and managed from Control Center 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** page and click the default policy name. You can change protection settings as needed, and also configure additional protection features, by creating and assigning customized policies.

Note

You cannot modify or delete the default policy. You can only use it as a template for creating new policies.

You can create as many policies as you need based on security requirements. For example, you can configure different policies for office workstations, laptops and servers. A different approach is to create separate policies for each of your customer networks.

This is what you need to know about policies:

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

- Computers under a company account can be managed through policies both by the company administrator and by the partner who created the account. Policies created from the partner account cannot be edited from the company account.

To create a new policy:

1. Go to the **Policies** page.
2. Click the + **Add** button at the right side of the table. This command creates a new policy starting from the default policy template.
3. Enter a suggestive name for the policy. When choosing a name, consider the purpose and target of the policy.
4. Next, configure the policy settings. Default security settings are recommended for most situations.
5. Click **Save**. The new policy is listed in the **Policies** table.

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

All network objects are initially assigned with the default policy.

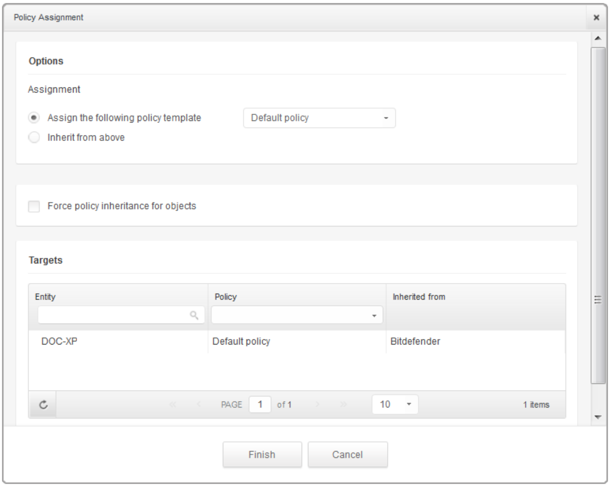
Note
You can assign only policies created by you. To assign a policy created by another user, you have to clone it first in the **Policies** page.

To assign a policy:

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

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

   The **Policy assignment** window is displayed:


Policy Assignment

Options

Assignment

● Assign the following policy template: Default policy

○ Inherit from above

□ Force policy inheritance for objects

Targets

Entity	Policy	Inherited from
DOC-XP	Default policy	Bitdefender

Policy Assignment Settings

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

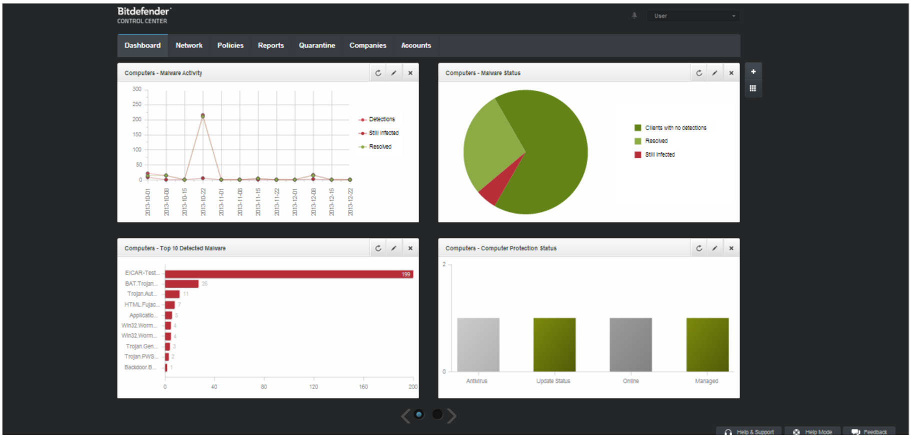
     Select **Force policy inheritance for objects** option to apply the chosen policy to a group, including to the group's children assigned with a different policy. In this case, the table placed below will display the selected group's children that do not inherit the group policy.
5. Click **Finish** to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

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

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

5. Monitoring Security Status

The main Security for Endpoints monitoring tool is the Control Center dashboard, a customizable visual display providing a quick security overview of your network.



The Dashboard

Check the **Dashboard** page regularly to see real-time information on the network security status.

Dashboard portlets display various security information using easy-to-read charts, thus allowing you to quickly identify any issues that might require your attention.

This is what you need to know about managing your dashboard:

- Control Center comes with several predefined dashboard portlets. You can also add more portlets using the + **Add Portlet** button at the right side of the dashboard.
- Each dashboard portlet includes a detailed report in the background, accessible with just one click on the chart.
- The information displayed by portlets refers only to the network objects under your account. You can customize the information displayed by a portlet (type, reporting interval, targets) by clicking the ✎ **Edit Portlet** icon on its title bar.

  For example, you can configure portlets to display information on a certain company of your network.

- You can easily remove any portlet by clicking the × **Remove** icon on its title bar. Once you remove a portlet, you can no longer recover it. However, you can create another portlet with the exact same settings.
- Click the chart legend entries, when available, to hide or display the corresponding variable on the graph.
- You can rearrange dashboard portlets to better suit your needs, by clicking the ▦ **Rearrange Portlets** button at the right side of the dashboard. You can then drag and drop portlets to the desired position.
- The portlets are displayed in groups of four. Use the slider at the bottom of the page to navigate between portlet groups.

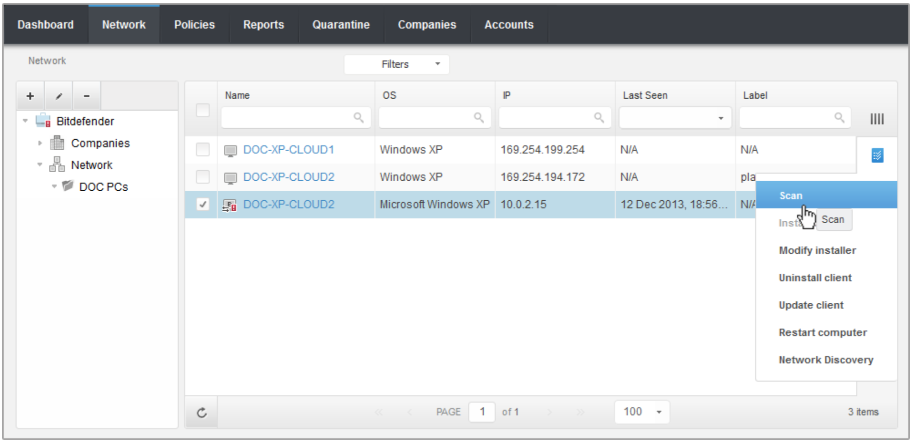
6. Scanning Managed Computers

There are three ways to scan computers protected by Endpoint Security:

- 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 **Network** page.
2. Select the desired network group from the left-side pane. All computers from the selected group are displayed in the right-side pane table.
3. Select the entities you want to be scanned. You can select certain managed computers or an entire group.
4. Click the **Task** button at the right-side of the table and choose **Scan**. A configuration window will appear.



	Name	OS	IP	Last Seen	Label
☐	DOC-XP-CLOUD1	Windows XP	169.254.199.254	N/A	N/A
☐	DOC-XP-CLOUD2	Windows XP	169.254.194.172	N/A	pla
☑	DOC-XP-CLOUD2	Microsoft Windows XP	10.0.2.15	12 Dec 2013, 18:56...	N/A

Computers Scan Task

5. In the **General** tab, select the type of scan from the **Type** menu:
   - **Quick Scan** checks for malware running in the system, without taking any action. If malware is found during a Quick Scan, you must run a Full System Scan task to remove detected malware.

- **Full Scan** checks the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.
- **Custom Scan** allows you to choose the locations to be scanned and to configure the scan options.

6. Click **Save** to create the scan task. A confirmation message will appear.

> **Note**
> Once created, the scan task will start running immediately on online computers. If a computer is offline, it will be scanned as soon as it gets back online.

7. You can view and manage tasks on the **Network > Tasks** page.

7. Getting Help

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

- Click the **Help and Support** link in the lower-right corner of Control Center.
- Go to our online Support Center.

To open an email support ticket, use this web form.

A. Requirements

A.1. Security for Endpoints Requirements

A.1.1. Supported Operating Systems

Security for Endpoints currently protects the following operating systems:

Workstation operating systems:

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

Tablet and embedded operating systems:

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

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

Server operating systems:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003

  - Windows Server 2003 R2
  - Windows Server 2003 with Service Pack 1
  - Windows Home Server

A.1.2. Hardware Requirements

- Intel® Pentium compatible processor:

  Workstation Operating Systems

  – 1 GHz or faster for Microsoft Windows XP SP3, Windows XP SP2 64 bit and Windows 7 Enterprise (32 and 64 bit)

  – 2 GHz or faster for Microsoft Windows Vista SP1 or higher (32 and 64 bit), Microsoft Windows 7 (32 and 64 bit), Microsoft Windows 7 SP1 (32 and 64bit), Windows 8

  – 800 MHZ or faster for Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded with Service Pack 2, Microsoft Windows XP Tablet PC Edition

  Server Operating Systems

  – Minimum: 2.4 GHz single-core CPU

  – Recommended: 1.86 GHz or faster Intel Xeon multi-core CPU
- **Free RAM memory**:

  – For Windows: 512 MB minimum, 1 GB recommended

  – For Mac: 1 GB minimum
- **HDD space**:

  – 1.5 GB of free hard-disk space

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

A.1.3. Supported Browsers

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

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

A.1.4. Small Office Security Communication Ports

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

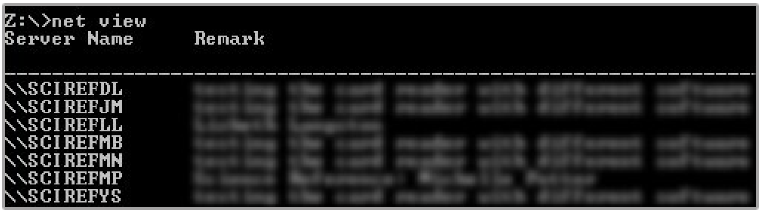
Port	Usage
80 (HTTP) / 443 (HTTPS)	Port used to access the Control Center web console.
80	Update Server port.
8443 (HTTPS)	Port used by client/agent software to connect to the Communication Server.
7074 (HTTP)	Communication with Endpoint Security Relay (if available)

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

A.2. How Network Discovery Works

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

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



```
Z:\>net view
Server Name       Remark

-------------------------------------------------------------------------------
\\SCIREFDL
\\SCIREFJM
\\SCIREFLL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

The Net view command

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

Important

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

Control Center is not actively involved in the Computer Browser service operation. Endpoint Security only queries the Computer Browser service for the list of workstations and servers currently visible in the network (known as the browse list) and then sends it to Control Center. Control Center processes the browse list, appending newly detected computers to its

Unmanaged Computers list. Previously detected computers are not deleted after a new network discovery query, so you must manually exclude & delete computers that are no longer on the network.

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

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

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

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

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

A.2.1. 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.

A.2.2. Network Discovery Requirements

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

- Computers must be joined in a workgroup or domain and connected via an IPv4 local network. Computer Browser service does not work over IPv6 networks.
- Several computers in each LAN group (workgroup or domain) must be running the Computer Browser service. Primary Domain Controllers must also run the service.
- NetBIOS over TCP/IP (NetBT) must be enabled on computers. Local firewall must allow NetBT traffic.
- File sharing must be enabled on computers. Local firewall must allow file sharing.
- A Windows Internet Name Service (WINS) infrastructure must be set up and working properly.
- For Windows Vista and later, network discovery must be turned on (**Control Panel > Network and Sharing Center > Change Advanced Sharing Settings**).

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

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

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