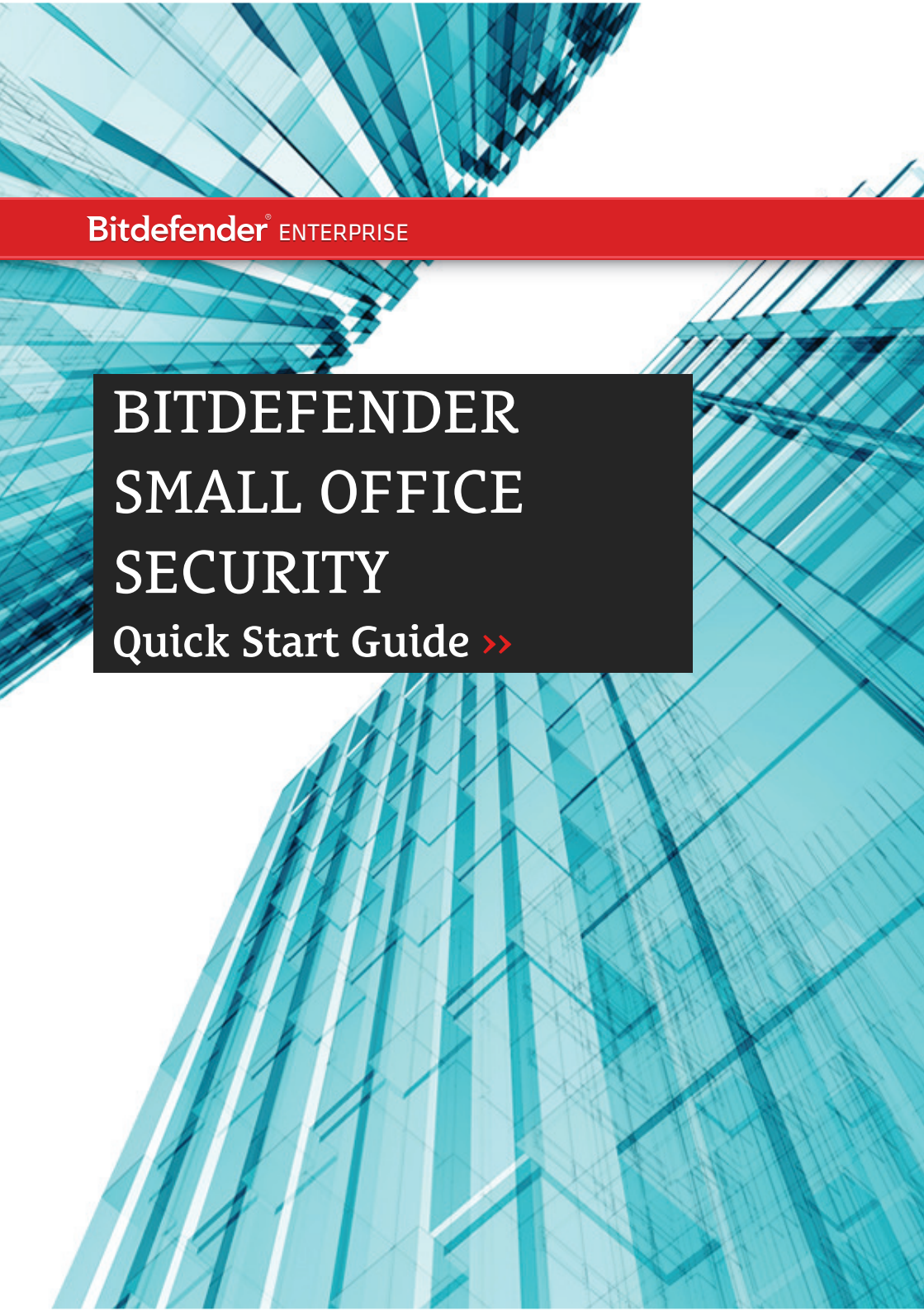

Bitdefender® ENTERPRISE
BITDEFENDER
SMALL OFFICE
SECURITY
Quick Start Guide ››

Bitdefender Small Office Security
Quick Start Guide

Publication date 2014.06.18


Bitdefender

Table of Contents

1. About Small Office Security 1

2. System Requirements 3
2.1. Small Office Security Appliance Requirements 3
2.1.1. Hardware Requirements 3
2.1.2. Internet Connection 3
2.1.3. Control Center Web Console Requirements 4
2.2. Security for Endpoints Requirements 4
2.2.1. Supported Operating Systems 4
2.2.2. Hardware Requirements 5
2.2.3. Supported Browsers 5
2.3. Security for Mobile Devices Requirements 6
2.3.1. Supported Platforms 6
2.3.2. Connectivity Requirements 6
2.3.3. Push Notifications 6
2.3.4. iOS Management Certificates 6
2.4. Small Office Security Communication Ports 6

3. Small Office Security Installation and Setup 8
3.1. Prepare for Installation 8
3.2. Deploy and Set Up Small Office Security Appliance 9
3.2.1. Configure Appliance Hostname (DNS) 9
3.2.2. Configure Network Settings 10
3.2.3. Configure Proxy Settings 10
3.3. Control Center Initial Setup 10
3.4. Enter License Keys 11
3.5. Configure Control Center Settings 11
3.6. Add Control Center Users 14

4. Install Security Services 17
4.1. Installing Security for Endpoints 17
4.1.1. Preparing for Installation 18
4.1.2. Local Installation 18
4.1.3. Remote Installation 22
4.1.4. How Network Discovery Works 27
4.2. Installing Security for Mobile Devices 30
4.2.1. Configure External Address for Communication Server 30
4.2.2. Create and Organize Custom Users 32
4.2.3. Add Devices to Users 33
4.2.4. Install GravityZone Mobile Client on Devices 34

5. Getting Started 35
5.1. Types of Users in Control Center 35

5.2. Connecting to Control Center 35
5.3. Control Center at a Glance 36
5.3.1. Control Center Overview 36
5.3.2. Table Data 38
5.3.3. Action Toolbars 39
5.3.4. Contextual Menu 39
5.3.5. Service Selector 39
5.4. Applying Security Policies 40
5.4.1. Creating and Configuring Policies 40
5.4.2. 41
5.5. Using Tasks 42
5.6. Monitoring and Reporting 43
5.6.1. Using the Dashboard 43
5.6.2. Working with Reports 45
6. Getting Help 47

1. About Small Office Security

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

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

Small Office Security includes the following components:

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

Control Center

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

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

Security for Endpoints

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

Security for Mobile Devices

Manages and controls iPhone, iPad and Android devices with a unified enterprise-grade management that keeps the device safe with real-time scanning and enforces organization's security policies on mobile devices to lock screen, require authentication, encrypt removable

media, locate lost devices and deny non-compliant or jailbroken devices accessing corporate services.

2. System Requirements

All of the Small Office Security solutions are installed and managed via Control Center.

2.1. Small Office Security Appliance Requirements

Small Office Security is delivered as a virtual appliance. The Small Office Security appliance is available in the following formats:

- OVA (compatible with VMware vSphere, View)
- XVA (compatible with Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (compatible with Microsoft Hyper-V)
- OVF (compatible with Red Hat Enterprise Virtualization)*
- OVF (compatible with Kernel-based Virtual Machine or KVM)*
- RAW (compatible with Oracle VM)*

*OVF and RAW packages are archived in tar.bz2 format.

Support for other formats and virtualization platforms may be provided on request.

2.1.1. Hardware Requirements

The following table describes the hardware requirements for the Small Office Security appliance, depending on the number of managed network objects.

Number of protected objects	RAM	HDD	CPUs
1-250 endpoints 1-250 mobile devices	4 GB	40 GB	2 virtual CPUs (2GHz each)
250-1000 endpoints 250-1000 mobile devices	8 GB	60 GB	4 virtual CPUs (2GHz each)

2.1.2. Internet Connection

The Small Office Security appliance requires Internet access.

2.1.3. Control Center Web Console Requirements

To access the Control Center web console, the following are required:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Recommended screen resolution: 1280x800 or higher
- The computer you connect from must have network connectivity to the Control Center appliance.

Warning
Control Center will not work / display properly in Internet Explorer 9+ with the Compatibility View feature enabled, which is equivalent with using an unsupported browser version.

2.2. Security for Endpoints Requirements

2.2.1. 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 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

2.2.2. 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.

2.2.3. 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+

2.3. Security for Mobile Devices Requirements

2.3.1. Supported Platforms

Security for Mobile Devices supports the following types of mobile devices and operating systems:

- Apple iPhones and iPad tablets (iOS 5.1+)
- Google Android smartphones and tablets (2.3+)

2.3.2. Connectivity Requirements

Mobile devices must have an active cellular data or Wi-Fi connection and connectivity with the Communication Server.

2.3.3. Push Notifications

Security for Mobile Devices uses push notifications to alert mobile clients when policy updates and tasks are available. Push notifications are sent by the Communication Server via the service provided by the operating system manufacturer:

- Google Cloud Messaging (GCM) service for Android devices. For GCM to work, the following are required:
  - Google Play Store must be installed.
  - Devices running a version lower than Android 4.0.4 must also have at least one logged in Google account.
  - To send push notifications, a number of ports must be open.
- Apple Push Notifications service (APNs) for iOS devices. For more information, refer to this Apple KB article.

To learn more about Small Office Security Mobile Device Management workflow, please refer to this KB article.

2.3.4. iOS Management Certificates

To set up the infrastructure for iOS mobile device management, you must provide a number of security certificates.

For more information, refer to Certificates.

2.4. 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.
8443 (HTTPS)	Port used by client/agent software to connect to the Communication Server.
7074 (HTTP)	Update Server port
7075	Handles communication between Small Office Security services and the outside world.
4369 / 6150	Ports used to allow communication between Control Center and Communication Server.
27017	Default port used by the Communication Server and Control Center to access the Database.
5228, 5229, 5230	Google Cloud Messaging (GCM) ports. The Communication Server uses GCM to send push notifications to managed Android devices.
2195, 2196, 5223	Apple Push Notification service (APNs) ports. Ports 2195 and 2196 are used by the Communication Server to communicate with the APNs servers. Port 5223 is used by managed iOS devices to communicate with the APNs servers over Wi-Fi in specific conditions. For more information, refer to this Apple KB article.
123 (UDP)	User Datagram Protocol (UDP) port used by Small Office Security appliances for time synchronization with the NTP server.

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

3. Small Office Security Installation and Setup

To make sure installation goes smoothly, follow these steps:

1. Prepare for installation.
2. Deploy and set up the Small Office Security virtual appliance.
3. Connect to Control Center and setup the first user account.
4. Enter your license keys.
5. Configure Control Center settings.
6. Add Control Center users.

3.1. Prepare for Installation

For installation, you need a Small Office Security virtual appliance image. After you deploy and set up the Small Office Security appliance, you can remotely install or download the necessary installation packages for all other security services components from the Control Center web interface.

The Small Office Security appliance image is available in several different formats, compatible with the main virtualization platforms. You can obtain the download links by registering for a trial on the Bitdefender Enterprise website.

For installation and initial setup, you must have the following at hand:

- DNS names or fixed IP addresses (either by static configuration or via a DHCP reservation) for the Small Office Security appliance
- Username and password of a domain administrator
- License key (check the trial registration or purchase email)
- Outgoing mail server settings
- If needed, proxy server settings
- Security certificates

Additional prerequisites must be met in order to install services.

3.2. Deploy and Set Up Small Office Security Appliance

Small Office Security appliance is delivered with the following preconfigured roles:

- **Database Server**
- **Update Server**
- **Web Console**
- **Communication Server**

To deploy and set up the Small Office Security appliance:

1. Import the Small Office Security virtual appliance image in your virtualized environment.
2. Power on the appliance.
3. From your virtualization management tool, access the console interface of the Small Office Security appliance.
4. Configure the password for the built-in `bdadmin` system administrator.
5. Press Enter to continue to the configuration interface.
6. Using the configuration interface, set up the appliance as follows:
   a. Assign the appliance a DNS name.
   b. Configure the network settings.
   c. If needed, configure the proxy settings.

   The Small Office Security appliance has a basic configuration interface. Use the arrow keys and the `Tab` key to navigate through menus and options. Press `Enter` to select a specific option.

3.2.1. Configure Appliance Hostname (DNS)

Communication with the Small Office Security roles is performed using the IP address or DNS name of the appliance they are installed on. By default, the Small Office Security components communicate using IP addresses. If you want to enable communication via DNS names, you must configure Small Office Security appliances with a DNS name and make sure it correctly resolves to the configured IP address of the appliance.

To assign the appliance a DNS name:

1. From the main menu, select **Configure Appliance Hostname (DNS)**.
2. Select **Configure appliance hostname (DNS)**.
3. Enter the DNS name.
4. Select **OK** to save the changes.

5. Select **Show appliance hostname (DNS)** to make sure the DNS name has been correctly configured.

3.2.2. Configure Network Settings

You can configure the appliance to automatically obtain network settings from the DHCP server or you can manually configure network settings. If you choose to use DHCP, you must configure the DHCP Server to reserve a specific IP address for the appliance.

To configure the network settings:

1. From the main menu, select **Configure Network Settings**.
2. Select the network interface.
3. Select the configuration method:
   - **Configure network settings manually.** You must specify the IP address, network mask, gateway address and DNS server addresses.
   - **Obtain network settings automatically via DHCP.** Use this option only if you have configured the DHCP Server to reserve a specific IP address for the appliance.
4. You can check current IP configuration details or link status by selecting the corresponding options.

3.2.3. Configure Proxy Settings

If the appliance connects to the Internet through a proxy server, you must configure the proxy settings.

To configure the proxy settings:

1. From the main menu, select **Configure Proxy Settings**.
2. Select **Configure proxy settings**.
3. Enter the proxy server address.
4. Select **OK** to save the changes.

3.3. Control Center Initial Setup

After deploying and setting up the Small Office Security appliance, you must access the Control Center web interface and configure your company administrator account.

Note
For more information on Control Center users, refer to "Types of Users in Control Center" (p. 35).

1. In the address bar of your web browser, enter the IP address or the DNS hostname of the Control Center appliance (using the `https://` prefix). A configuration wizard will appear.
2. You must first register your Small Office Security deployment to a Bitdefender account. Provide the username and password of your Bitdefender account. If you do not have a Bitdefender account yet, click the corresponding link to create one.

   Click **Next** to continue.
3. Provide the license key required for validating Small Office Security. Check the trial registration or purchase email to find your license key. Enter the license key in the **Key** field and click the + **Add** button. Wait until the license key is validated. You can also view the expiry date for your license key in the corresponding column.

   Click **Next** to continue.
4. Specify the required details for your company administrator account: username, email address and a password. Password must contain at least one upper case character, at least one lower case character and at least one digit or special character.
5. Click **Create Account**.

The company administrator account will be created and you will automatically log on with the new account to Bitdefender Control Center.

3.4. Enter License Keys

Small Office Security is licensed with a single key for all security services.

Control Center is provided for free with any Small Office Security security service.

Check the trial registration or purchase email to find your license key.

To view existing license information and enter your license keys:

1. Connect and log in to the Control Center web interface using an account with manage company right.
2. Go to the **Configuration > License** page.
3. You can view the existing license keys, status, expiry dates and usage count.

   To change the license key, enter it in the **Key** field and click the + **Add** button. The provided license key is added to the list, invalidating at the same time the existing key.

3.5. Configure Control Center Settings

To configure the necessary Control Center settings:

1. Connect and log in to the Control Center web interface using a company administrator account.

2. Go to the **Configuration** page.
   - Select the **Mail Server** tab.

     To enable Control Center to send emails, select the **Mail Server Settings** check box and configure the required settings:

     – **Mail server (SMTP).** Enter the IP address or hostname of the mail server that is going to send the emails.

     – **Port.** Enter the port used to connect to the mail server.

     – **Encryption type.** If the mail server requires an encrypted connection, choose the appropriate type from the menu (SSL/TLS or STARTTLS).

     – **From email.** Enter the email address that you want to appear in the From field of the email (sender's email address).

     – **Use authentication.** Select this check box if the mail server requires authentication. You must specify a valid username / email address and password.

     Click **Save** to save the changes.
   - Select the **Proxy** tab.

     If your company connects to the Internet through a proxy server, select **Use Proxy Settings** and configure the required settings:

     – **Address** - type in the IP address of the proxy server.

     – **Port** - type in the port used to connect to the proxy server.

     – **Username** - type in a user name recognized by the proxy.

     – **Password** - type in the valid password of the previously specified user.

     Click **Save** to save the changes.
   - Select the **Miscellaneous** tab to configure the following general preferences:

     – **Concurrent deployments.** Administrators can remotely deploy security components by running installation tasks. Use this option to specify the maximum number of simultaneous deployments that can be performed at a time.

       For example, if the maximum number of concurrent deployments is set to 10 and a remote client installation task is assigned to 100 computers, Control Center will initially send 10 installation packages through the network. In this case, the client installation is performed simultaneously on a maximum number of 10 computers, all the other sub-tasks being in pending state. As soon as a sub-task is done, another installation package is sent, and so on.

     – **NTP Server Settings**. The NTP server is used to synchronize time between all Small Office Security appliances. A default NTP server address is provided, which you can change in the **NTP Server Address** field.

Note
For the Small Office Security appliances to communicate with the NTP Server, 123 (UDP) port must be open.

Click **Save** to save the changes.

- Under the **Active Directory** tab, select **Synchronize with Active Directory** to integrate and synchronize Control Center with an Active Directory domain. You must specify the following:
  - Synchronization interval (in hours)
  - Active Directory domain name (including the domain extension)
  - Username and password of a domain administrator

  Click **Save** to save the changes.

  Wait a few seconds until Control Center synchronizes with the Active Directory from the specified domain. When done, check the **Synchronization Status** field for more details.
- Select the **Certificates** tab.

  Obtain and upload all necessary security certificates. Except for the Control Center certificate, all other security certificates are exclusively required for iOS mobile device management.

  - **Control Center Security.** To avoid browser security warnings, add an SSL certificate signed by your company or by an external Certificate Authority (CA).
  - **Communication Server.** The Communication Server certificate is used to secure communication between the Communication Server and iOS mobile devices. This SSL certificate can be signed either by your company or by an external Certificate Authority. The certificate common name must match exactly the domain name or IP address used by mobile clients to connect to the Communication Server. This is configured as the external MDM address in the configuration interface of the Small Office Security appliance console.
  - **Apple MDM Push.** The Apple MDM Push certificate is required by Apple to ensure secure communication between the Communication Server and the Apple Push Notifications service (APNs) servers when sending push notifications. Follow the steps from the **Add Apple MDM Push Certificate** page to easily obtain and import your Apple MDM Push certificate.
  - **iOS MDM Identity and Profile Signing.** The iOS MDM Identity and Profile Signing certificate is used by the Communication Server to sign identity certificates and configuration profiles sent to mobile devices. It must be an Intermediate or End-Entity certificate, signed either by your company or by an external Certificate Authority.

– **iOS MDM Trust Chain.** The iOS MDM Trust Chain must include all intermediate certificates up to the root certificate of your company or to the intermediate certificate issued by the external Certificate Authority.

3. Point to **Configuration** menu and select **Update**.
   - Under the **Product Update** tab, download or update all necessary installation packages.
   - Under the **Update Server** tab, you can configure the Bitdefender update settings. Update settings apply to all Small Office Security products and components and for both product and signature updates.
   - Go to the **Infrastructure** tab for a quick overview of the installed Small Office Security appliances and the roles they are running.

3.6. Add Control Center Users

You can create the first Small Office Security user account during the initial Control Center setup, after deploying the Small Office Security appliance. The initial Control Center user account has company administrator role, with full rights over Control Center configuration and network management. From this account you can create all the other user accounts required for the management of your company's network.

User accounts are managed from the **Accounts** page in Control Center.

Note
All users with Manage Users right have access to the **Accounts** page.

To add a Control Center user:

1. Connect and log in to the Control Center web interface using the company administrator account.
2. Go to the **Accounts** page.
3. Click the + **Add** button at the right side of the table. A configuration page is displayed.
4. Under the **Details** section, specify the user details. You can either add a user from Active Directory (provided Active Directory integration is configured), or create a custom user.
   - To add a user from Active Directory, select **Import from Active Directory** option. You can then specify the user account in the **Username** field.

     When adding a user from Active Directory, user details are imported from Active Directory. The user will log in to Control Center using the Active Directory user password.

Note

By default, Control Center is automatically synchronized with Active Directory by a specified interval. To make sure the latest Active Directory changes are imported in Control Center, click the **Synchronize** button.

- To create a custom user, disable the **Import from Active Directory** option and fill in the user's username, email address, full name and password.

Note

– The password must contain at least one upper case character, at least one lower case character and at least one digit or special character.

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

5. Under the **Settings and Privileges** section, configure the following:
   - **Timezone.** Choose from the menu the timezone of the account. The console will display time information according to the selected timezone.
   - **Language.** Choose from the menu the console display language.
   - **Role.** Select one role defining the user's privileges:

     Company Administrator
     Company Administrator accounts offer full access to Control Center configuration and management features of the Small Office Security security services.

     Administrator
     Administrator accounts offer access to Small Office Security security services management, monitoring and reporting features (install the security services, create user accounts, create reports, edit the dashboard). The administrators privileges can be restricted to certain parts of the network or to certain Small Office Security security services. Administrators cannot view or change the Control Center configuration settings.

     Reporter
     Reporter accounts offer access only to the monitoring and reporting features. The reporters privileges can be restricted to certain parts of the network or to certain Small Office Security security services. Reporters cannot view or change the network or security configuration.

     Custom
     Predefined user roles include a certain combination of user rights. If a predefined user role does not fit your needs, you can create a custom account by selecting only the rights that you are interested in.

   - **Rights.** You can assign the following user rights to Small Office Security user accounts:

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

- **Select Targets**. Scroll down the configuration window to display the targets section. You can restrict the user access to a certain Small Office Security security service or to specific areas of the network. Select the network groups the user will have access to for each available security service.

Note
The target selection options will not be displayed for users with Manage Solution right, which, by default, have privileges over the entire network and security services.

Important
Whenever you make changes to your network structure, or when setting up a new integration with another vCenter Server or XenServer system, remember to also review and update access privileges for existing users.

6. Click **Save** to add the user. The new account will appear in the user accounts list.

   Control Center automatically sends the user an email with the login details, provided the mail server settings have been properly configured.

4. Install Security Services

To protect your network with Bitdefender, you must install the Small Office Security security services. To install the Small Office Security security services, you need a Control Center user with administrator privileges over all services and over the entire network. You also need administrator access to the network computers.

The following table shows the type of network objects each service is designed to protect:

Service	Network Objects
Security for Endpoints	Computers (workstations, laptops and servers) running on Microsoft Windows
Security for Mobile Devices	iPhone, iPad and Android devices

4.1. Installing Security for Endpoints

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

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

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

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

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

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

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

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

4.1.1. 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 Endpoint Security is incompatible with 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.

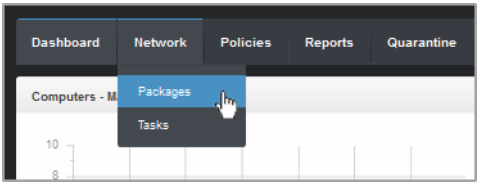
   Important
   No need to worry about Windows security features (Windows Defender, Windows Firewall), as they will be turned off automatically before installation is initiated.

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 network connectivity to the Control Center appliance.

4.1.2. Local Installation

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

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



The Network > Packages menu

Once the first client has been installed, it will be used to detect other computers in the same network, based on the Network Discovery mechanism. For detailed information on network discovery, refer to "How Network Discovery Works" (p. 27).

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

1. Create an installation package according to your needs.

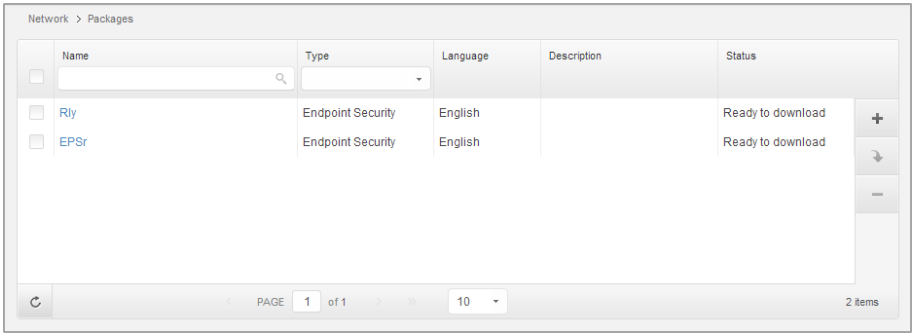
> **Note**
> This step is not mandatory if an installation package has already been created for the network under your account.

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

Creating Endpoint Security Installation Packages

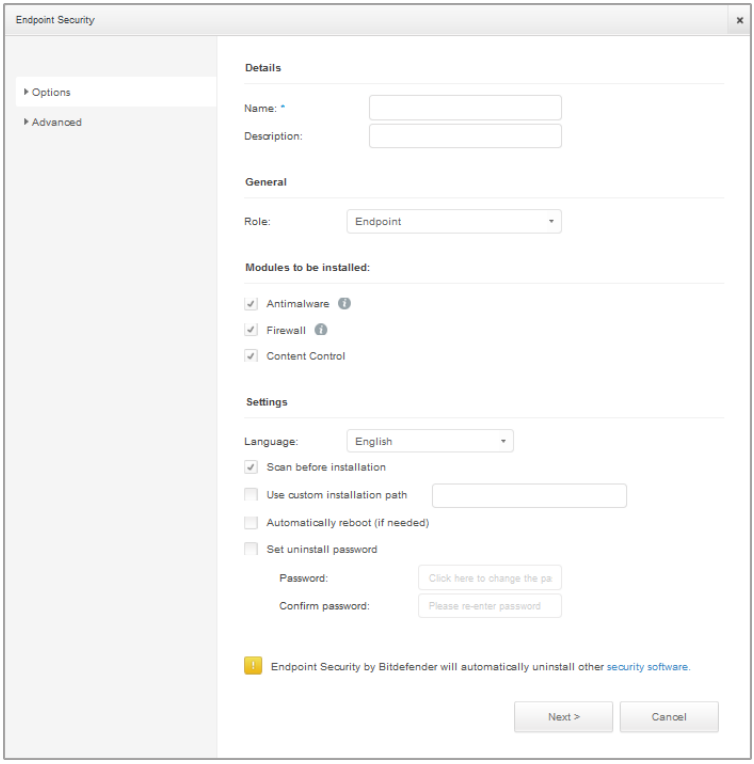
To create an Endpoint Security installation package:

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



The Packages page

3. Click the + **Add** button at the right side of the table and choose **Endpoint Security** from the menu. A configuration window will appear.



Create Endpoint Security Packages - Options

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

9. 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.
10. 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.
11. Click **Next**.
12. 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:
    - **Small Office Security Appliance**, available for both roles. You can also configure the Communication Server and local update addresses in the following fields, if required.

      To change the local update address, use one of these syntaxes:

      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 same update address, configure it accordingly in the policy settings.

      - `update_server_ip:port`
      - `update_server_name:port`
    - **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.
13. Click **Save**.

You can find the new installation package in the list of packages.

Downloading Installation Packages

To download Endpoint Security installation packages:

1. Log in to Control Center from the computer on which you want to install protection.
2. Go to the **Network > Packages** page.

3. Select the Endpoint Security installation package you want to download.
4. Click the **Download** button at the right side of the table and select the type of installer you want to use. Two types of installation files are available:
   - **Downloader**. The downloader first downloads the full installation kit from the Control Center appliance 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).
   - **Full Kit**. The full installation kits are bigger in size and they have to be run on the corresponding operating system type.

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

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

Running Installation Packages

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

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

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

4.1.3. Remote Installation

Control Center allows you to remotely install Endpoint Security on Active Directory computers and on other computers detected in the network by using installation tasks.

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 Control Center.

Endpoint Security includes an automatic network discovery mechanism that allows detecting computers that are not in Active Directory. Detected computers are displayed as **unmanaged computers** in the **Network** page, **Computers** section, under **Custom Groups**. Control Center automatically removes Active Directory computers from the detected computers list.

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 and install Endpoint Security on unprotected computers.

For detailed information on network discovery, refer to "How Network Discovery Works" (p. 27).

Remote Endpoint Security Installation Requirements

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

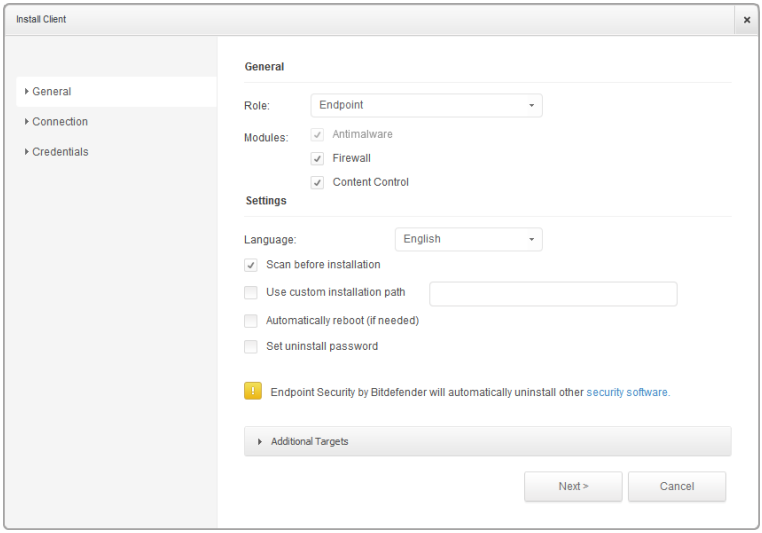
To run a remote installation task:

1. Connect and log in to Control Center.
2. Go to the **Network** page.
3. Choose **Computers** from the service selector.
4. 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.

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



Installing Endpoint Security from the Tasks menu

7. Configure the installation options:
   - Select the role you want the client to have:
     - **Endpoint**. Select this option if you want to install the client on a regular endpoint.
     - **Endpoint Security Relay**. Select this option to install the client with Endpoint Security Relay role on the target computer. Endpoint Security Relay is a special role which installs an update server on the target machine along with Endpoint Security, which can be used to update all the other clients in the network, lowering the bandwidth usage between the client machines and the Small Office Security appliance.
   - 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.

- Select **Additional targets** if you want to deploy the client to specific machines from your network that are not shown in the network inventory. Enter the IP addresses or the hostnames of those machines in the dedicated field, separated by a comma. You can add as many IPs as you need.

- Click **Next**.

- In the **Connection** tab, choose the entity through which the clients will communicate:

  – **Small Office Security Appliance**. You can also configure the Communication Server and local update addresses in the following fields, if required.

    To change the local update address, use one of these syntaxes:
    - `update_server_ip:port`
    - `update_server_name:port`

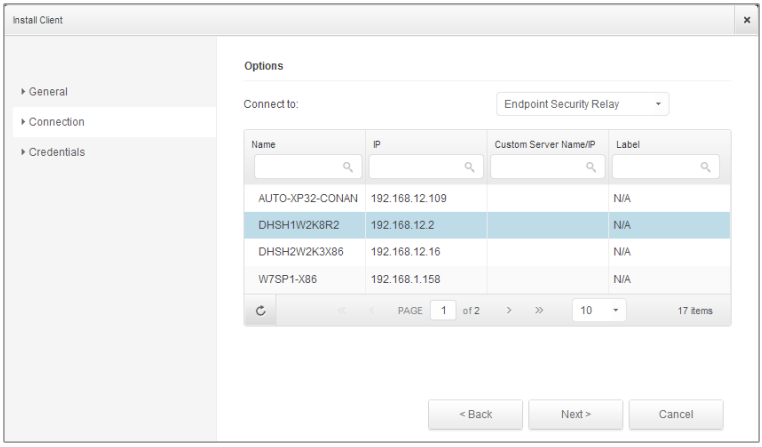
    

    Note
    The update address configured here is used temporarily after installation. As soon as a policy is applied to the client, the update location is changed according to policy settings. To make sure the client continues to update from the same update address, configure it accordingly in the policy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

  – **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.

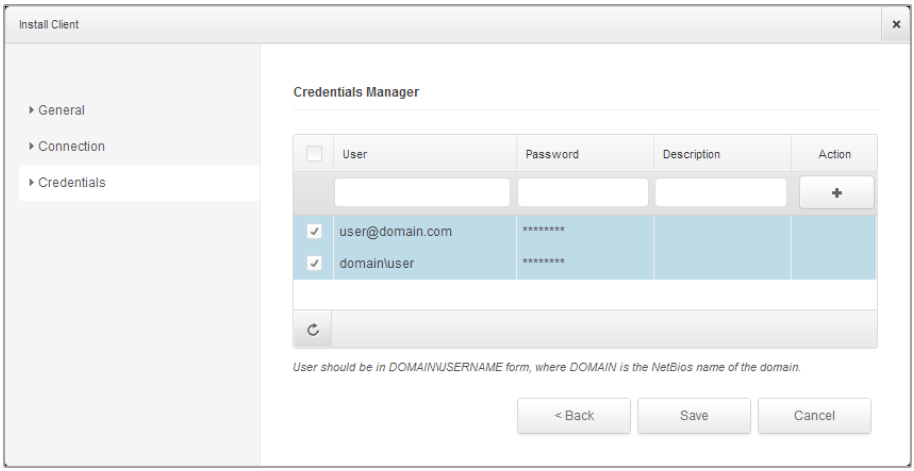
    Important
    Port 7074 must be open for the deployment through Endpoint Security Relay to work.



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

Note

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



To add the required OS credentials:

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

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

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

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

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

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

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

4.1.4. How Network Discovery Works

Besides integration with Active Directory, Security for Endpoints also includes an automatic network discovery mechanism intended to detect workgroup computers.

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

The Net view command

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

Important

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

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

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

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

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

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

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

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.

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.

4.2. Installing Security for Mobile Devices

Security for Mobile Devices is a mobile device management solution designed for iPhone, iPad and Android devices. For a complete list of supported operating system versions, check the system requirements.

Security for Mobile Devices is managed in Control Center by adding mobile devices to specific users and then installing the GravityZone Mobile Client application on devices. You can add mobile devices to existing Active Directory users or you can create custom users to add the devices to.

Before you start, make sure to configure a public (external) address for the Communication Server.

To install Security for Mobile Devices:

1. If you do not have integration with Active Directory, you must create users for mobile device owners.
2. Add devices to users.
3. Install GravityZone Mobile Client on devices and activate it.

4.2.1. Configure External Address for Communication Server

In the default Small Office Security setup, mobile devices can be managed only when they are directly connected to the corporate network (via Wi-Fi or VPN). This happens because when enrolling mobile devices they are configured to connect to the local address of the Communication Server appliance.

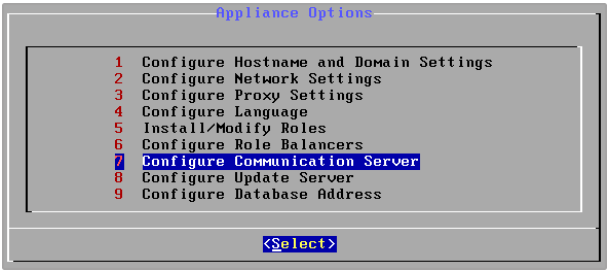
To be able to manage mobile devices over the Internet, no matter where they are located, you must configure the Communication Server with a publicly reachable address.

To be able to manage mobile devices when they are not connected to the company network, the following options are available:

- Configure port forwarding on the corporate gateway for the appliance running the Communication Server role.
- Add an additional network adapter to the appliance running the Communication Server role and assign it a public IP address.

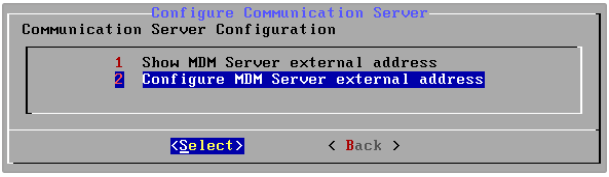
In both cases, you must configure the Communication Server with the external address to be used for mobile device management:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client).
2. From the main menu, select **Configure Communication Server**.



Application Options window

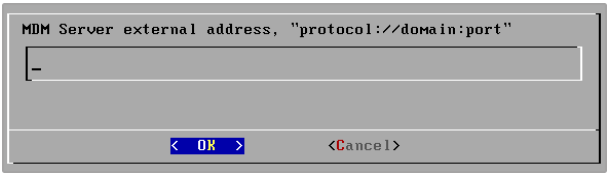
3. Select **Configure MDM Server external address**.



Configure Communication Server window

4. Enter the external address.

   Use the following syntax: `https://<IP/Domain>:<Port>`.



MDM Server external address input window

   - If you use port forwarding, you must enter the public IP address or domain name and the port open on the gateway.
   - If you use a public address for the Communication Server, you must enter the public IP address or domain name and the Communication Server port. The default port is `8443`.

5. Select **OK** to save the changes.

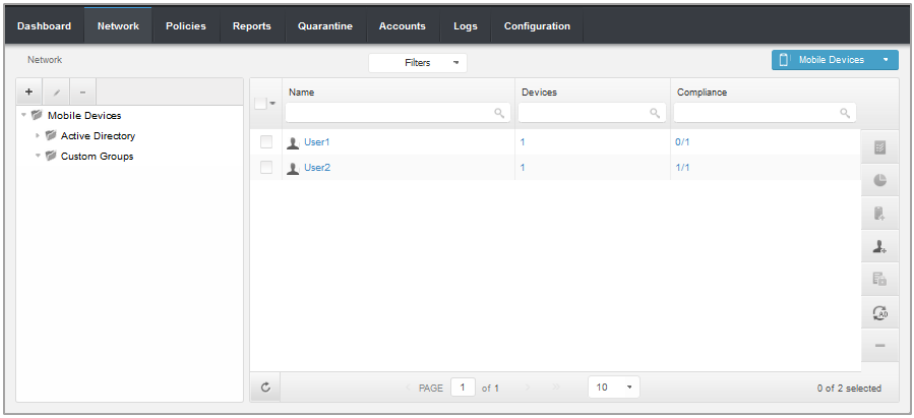
4.2.2. Create and Organize Custom Users

In non-Active Directory situations, you must first create custom users in order to have a mean to identify the owners of mobile devices. Specified mobile device users are not linked in any way with Active Directory or with other users defined in Control Center.

Creating Custom Users

To create a custom user:

1. Go to the **Network** page.
2. From the menu in the upper-right corner of the page, choose **Mobile Devices**.
3. In the left-side pane, select **Custom Groups**.



Network - Mobile devices page - Users view

4. Click the **Add User** icon on the action toolbar. A configuration window will appear.
5. Specify the required user details:
   - A suggestive username (for example, the user's full name)
   - User's email address

> **Important**
> Make sure to provide a valid email address. The user will be sent the installation instructions by email when you add a device.

6. Click **OK**.

Organizing Custom Users

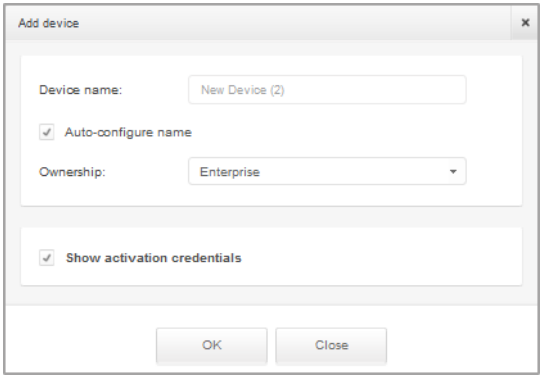
To organize custom users:

1. Create custom groups.
   a. Select **Custom Groups** in the left-side pane and click the **Add Group** icon on the action toolbar (above the pane).
   b. Enter a suggestive name for the group and click **OK**. The new group is displayed under **Custom Groups**.
2. Move custom users into appropriate custom groups.
   a. Select users in the right-side pane.
   b. Drag and drop the selection over the desired group in the left-side pane.

4.2.3. Add Devices to Users

To add a device to a user:

1. Go to the **Network** page.
2. From the menu in the upper-right corner of the page, choose **Mobile Devices**.
3. Search the user in the Active Directory folders or in Custom Groups.
4. Click the **Add Device** icon on the action toolbar. A configuration window will appear.



Add mobile device to a user

5. Enter a suggestive name for the device.
6. Use the **Auto-configure name** option if you want the device name to be automatically generated. Once this option is enabled, the device name cannot be edited, instead a default name is automatically assigned.

7. Select the device ownership type (Enterprise or Personal).
8. Select the **Show activation credentials** option after clicking the **OK** button if you are going to install the GravityZone Mobile Client on the user's device.
9. Click **OK**. The user is immediately sent an email with the installation instructions and the activation details to be configured on the device. The activation details include the activation token and the communication server address (and corresponding QR code).

Note
You can view the activation details of a device at any time by clicking its name in Control Center.

Note
You can also add mobile devices to a selection of users and groups. In this case, the configuration window will allow defining the devices ownership only. Mobile devices created by multiple selection will be given by default a generic name. As soon as a device is enrolled, its name will automatically change, including the corresponding manufacturer and model labels.

4.2.4. Install GravityZone Mobile Client on Devices

The GravityZone Mobile Client application is exclusively distributed via Apple App Store and Google Play.

To install GravityZone Mobile Client on a device:

1. Search for the application on the official app store.
   - Google Play link
   - Apple App Store link
2. Download and install the application on the device.
3. Start the application and make the required configuration:
   a. On Android devices, tap **Activate** to enable GravityZone Mobile Client as device administrator. Read carefully the provided information.
   b. Enter the activation token and the communication server address or, alternatively, scan the QR code received by email.
   c. Tap **Activate**.
   d. On iOS devices, you are prompted to install the MDM profile. If your device is password protected, you will be asked to provide it. Follow the on-screen instructions to complete profile installation.

5. Getting Started

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

5.1. Types of Users in Control Center

Control Center includes several predefined user account roles. Each predefined role grants the user with specific rights over Control Center.

The privileges of each user account can be restricted to a certain Small Office Security security service or to specific areas of the network.

Company Administrator

Users with company administrator role have full privileges over the Control Center settings and network security settings, including:

- Integration with Active Directory
- Mail server settings
- Update settings for Small Office Security components and installation packages
- Security certificates management
- License key management
- User management
- Network Security Management (client installation, policies, tasks, quarantine)
- Reports management

Administrator

Administrator accounts offer full access to all Small Office Security security services management features, including user management. Administrators cannot view or change the Control Center settings.

Reporter

Reporter users offer access only to the monitoring and reporting features. Reporters cannot view or change the network or security configuration.

5.2. 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

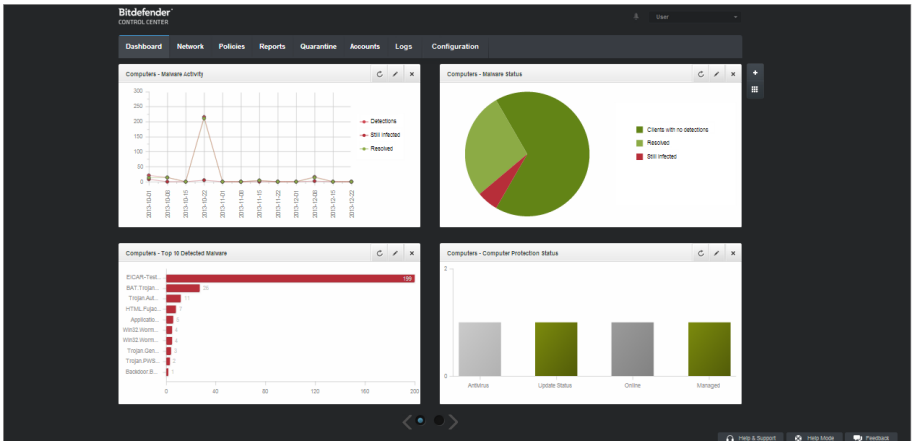
To connect to Control Center:

1. In the address bar of your web browser, enter the IP address or the DNS hostname of the Control Center appliance (using the `https://` prefix).
2. Enter your user name and password.
3. 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.

5.3. 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

5.3.1. 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.

Logs
Check the user activity log.

Configuration
Configure Control Center settings, such as mail server, proxy settings and security certificates.

Note
This menu is available only to users with Manage Solution 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.
- **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.

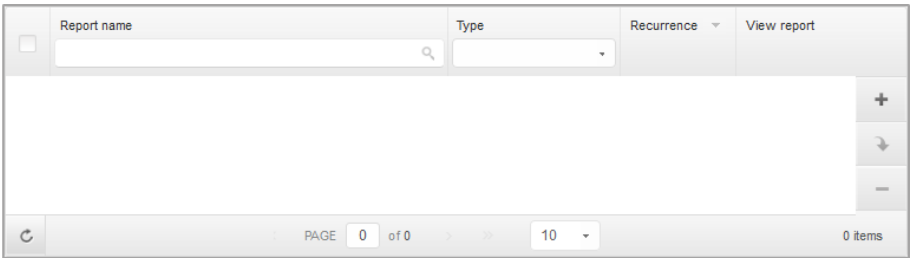
On the lower-right corner of the console, the following links are available:

- **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.

5.3.2. 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.

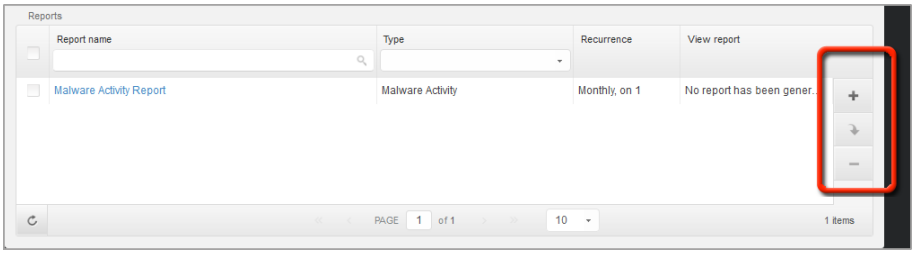
Refreshing Table Data

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

5.3.3. Action Toolbars

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

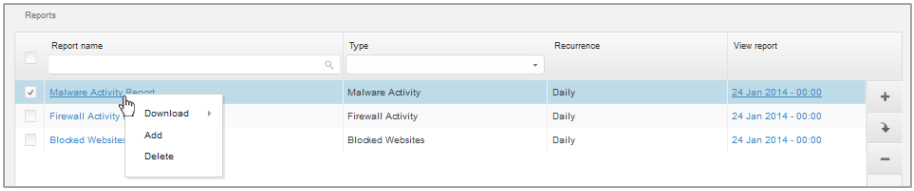
- Create a new report.
- Download reports generated by a scheduled report.
- Delete a scheduled report.



The Reports page - Action Toolbars

5.3.4. Contextual Menu

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



The Reports page - Contextual menu

5.3.5. Service Selector

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

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

The services menu contains the following options:

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

Note
You will see only the services you have permissions to view, permissions granted to you by the administrator who added your user to Control Center.

5.4. Applying Security Policies

Once installed, the Bitdefender protection can be configured and managed from Control Center using security policies. A policy specifies the security settings to be applied on target network inventory objects (computers or mobile devices).

Immediately after installation, clients are assigned a default policy, which is preconfigured with the recommended protection settings. You can change protection settings as needed, and also configure additional protection features, by creating and assigning customized policies.

5.4.1. Creating and Configuring Policies

Each Small Office Security security service has a unique policy template containing the security settings for the specific type of protected network objects. You must create at least one customized policy for each type of network objects.

To create and configure a new policy:

1. Go to the **Policies** page.
2. From the menu in the upper-right corner of the page, choose the type of network objects (computers or mobile devices).
3. Click the + **Add** button at the right side of the table.
4. Enter a suggestive name for the policy. When choosing a name, consider the purpose and target of the policy.
5. Next, configure the policy settings. Default security settings are recommended for most situations.
6. Click **Save**. The new policy is listed in the **Policies** table.

Once you have created all the necessary policies, you can start assigning them to network objects.

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

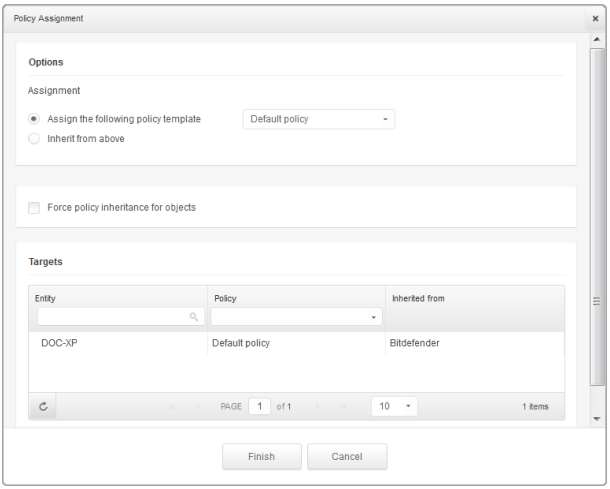
All network objects are initially assigned with the default policy.

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

To assign a policy:

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

   The **Policy assignment** window is displayed:



Policy Assignment Settings

5. 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.

6. 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.

5.5. Using Tasks

Control Center offers a number of administrative tasks that you can run remotely on network objects (computers or mobile devices). Tasks are related to the Small Office Security security services and differ based on the type of network object.

For example, you can run a remote scan on managed clients. The scan task is available for all types of network objects.

To create and run a remote scan task:

1. Go to the **Network** page.
2. From the menu in the upper-right corner of the page, choose the type of network objects (computers or mobile devices).
3. Browse for and select the specific network objects or groups on which to run the task. You can only select objects from the same parent group.
4. Click the **Tasks** button at the right side of the table and choose **Scan** from the menu. The **Scan Task** window is displayed.
5. Configure scan settings as needed.
6. Click **Save**. The task will start running immediately on online clients. If a client is offline, the task will run as soon as it gets back online.

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

- To check execution progress on target clients, click the link in the **Progress** column.
- Once the task is done, you can click the icon in the **Report** column to view a detailed task report.
- You can choose to re-run failed installation, uninstallation or update tasks, instead of creating new ones, by selecting them and using the **Run again** button at the right side of the table.

5.6. Monitoring and Reporting

Control Center includes powerful monitoring and reporting features. The main Small Office Security monitoring tool is the Control Center dashboard.

- Dashboard
- Reports

5.6.1. Using the Dashboard

The Control Center dashboard is a customizable visual display providing a quick security overview of all protected network objects (computers or mobile devices).

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

This is what you need to know about dashboard portlets:

- Control Center comes with several predefined dashboard portlets for each Small Office Security security service.
- Each dashboard portlet includes a detailed report in the background, accessible with just one click on the chart.
- There are several types of portlets that include various information about your network objects protection, such as update status, malware status, firewall activity etc. Portlet types correspond to available report types.
- The information displayed by portlets refer only to the network objects under your account.
- Click the chart legend entries, when available, to hide or display the corresponding variable on the graph.
- The dashboard is easy to configure, based on individual preferences. You can edit portlet settings, add additional portlets, remove or rearrange existing portlets.
- The portlets are displayed in groups of four. Use the slider at the bottom of the page to navigate between portlet groups.

Editing Portlet Settings

Some portlets offer status information, while other report on security events in the last period. You can check and configure the reporting period of a portlet by clicking the **Edit Portlet** icon on its title bar.

Adding a New Portlet

You can create additional portlets to obtain the information you need. The maximum number of portlets is 36.

To add a new portlet:

1. Go to the **Dashboard** page.
2. Click the **Add Portlet** button at the right side of the dashboard. The portlet configuration window is displayed.
3. Under the **Details** tab, configure the portlet details:
   - Security service (**Computers** or **Mobile Devices**)
   - Type of background report
   - Suggestive portlet name
   - Update interval
4. Under the **Targets** tab, select the network objects and groups to include.
5. Click **Save**.

Removing a Portlet

You can easily remove any portlet by clicking the **Remove** icon on its title bar. Once you remove a portlet, you can no longer recover it. However, you can create another portlet with the exact same settings.

Rearranging Dashboard Portlets

You can rearrange dashboard portlets to better suit your needs.

To rearrange portlets:

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

5.6.2. Working with Reports

Control Center allows you to create and view centralized reports on the security status of the managed clients. The reports can be used for multiple purposes, such as:

- Monitoring and ensuring compliance with the organization's security policies.
- Checking and assessing the network security status.
- Identifying network security issues, threats and vulnerabilities.
- Monitoring security incidents and malware activity.
- Providing upper management with easy-to-interpret data on network security.

Several different report types are available for each Small Office Security security service so that you can easily get the information you need. The information is presented as easy-to-read pie charts, tables and graphics, allowing you to quickly check the network security status and identify security issues.

Creating a Report

To create a scheduled report or to view an instant report:

1. Go to the **Reports** page.
2. From the menu in the upper-right corner of the page, choose the type of network objects (computers or mobile devices).
3. Click the + **Add** button at the right side of the table. The report configuration page is displayed.
4. Select the desired report type from the menu.
5. Enter a suggestive name for the report. When choosing a name, consider the report type and target, and possibly the report options.
6. Configure the report target. Click **Change target** and choose the network objects or groups to be included in the report.
7. Configure report recurrence (schedule). You can choose to create the report immediately, daily, weekly (on a specific day of the week) or monthly (on a specific day of the month).

   Note
   Scheduled reports are generated on the due date immediately after 00.00 UTC (default timezone of the Small Office Security appliance).

8. Configure the report options.
   a. For most report types, when you create an immediate report, you must specify the reporting period. The report will only include data from the selected time period.

b. Several report types provide filtering options to help you easily find the information you are interested in. Use the filtering options to obtain only the desired information. For example, for an **Update Status** report you can choose to view only the list of clients that have updated (or, on the contrary, that have not updated) in the selected time period.
c. To send the report by email, select the corresponding option. You must specify the email addresses of the intended recipients.

9. Click **Generate/Save** to create an instant/scheduled report.
   - If you have chosen to create an instant report, it will be displayed on a separate page. The time required for reports to be created may vary depending on the number of managed clients. Please wait for the requested report to be created. You can download or email the report if you want to keep a copy.
   - If you have chosen to create a scheduled report, it will be displayed on the **Reports** page. You can edit or delete the scheduled report at any time.

6. 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 a support ticket, go here and fill in the form.