



Bitdefender® ENTERPRISE

**BITDEFENDER  
GRAVITYZONE**  
Quick Start Guide >>

# Bitdefender GravityZone

## Quick Start Guide

Publication date 2013.12.02

Copyright© 2013 Bitdefender

### Legal Notice

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

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

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

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



# Table of Contents

- 1. About GravityZone ..... 1**
- 2. System Requirements ..... 3**
  - 2.1. GravityZone Appliance Requirements ..... 3
    - 2.1.1. Hardware Requirements ..... 3
    - 2.1.2. Internet Connection ..... 3
    - 2.1.3. Control Center Web Console Requirements ..... 3
  - 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 Virtualized Environments Requirements ..... 5
    - 2.3.1. Supported Virtualization Platforms ..... 6
    - 2.3.2. Supported Virtualization Management Tools ..... 6
    - 2.3.3. Security Server Requirements ..... 7
    - 2.3.4. Supported Guest Operating Systems ..... 8
    - 2.3.5. Bitdefender Tools Requirements and Footprint ..... 8
  - 2.4. Security for Mobile Devices Requirements ..... 9
    - 2.4.1. Supported Platforms ..... 9
    - 2.4.2. Connectivity Requirements ..... 9
    - 2.4.3. Push Notifications ..... 9
    - 2.4.4. iOS Management Certificates ..... 10
  - 2.5. GravityZone Communication Ports ..... 10
- 3. GravityZone Installation and Setup ..... 11**
  - 3.1. Prepare for Installation ..... 11
  - 3.2. Deploy and Set Up GravityZone Appliance ..... 12
    - 3.2.1. Configure Appliance Hostname (DNS) ..... 12
    - 3.2.2. Configure Network Settings ..... 13
    - 3.2.3. Configure Proxy Settings ..... 13
    - 3.2.4. Install GravityZone Roles ..... 13
  - 3.3. Control Center Initial Setup ..... 14
  - 3.4. Enter License Keys ..... 15
  - 3.5. Configure Control Center Settings ..... 15
  - 3.6. Add Control Center Users ..... 19
- 4. Install Security Services ..... 22**
  - 4.1. Installing Security for Endpoints ..... 22
    - 4.1.1. Preparing for Installation ..... 22
    - 4.1.2. Using Installation Packages ..... 24
    - 4.1.3. Using Remote Installation Tasks ..... 26
  - 4.2. Installing Security for Virtualized Environments ..... 29
    - 4.2.1. Connect to vCenter Server ..... 30

4.2.2. Install Security Server on Hosts .....	30
4.2.3. Install Bitdefender Tools on Virtual Machines .....	33
4.3. Installing Security for Mobile Devices .....	37
4.3.1. Configure External Address for Communication Server .....	38
4.3.2. Create and Organize Custom Users .....	39
4.3.3. Add Devices to Users .....	40
4.3.4. Install GravityZone Mobile Client on Devices .....	40
<b>5. Getting Started .....</b>	<b>42</b>
5.1. Types of Users in Control Center .....	42
5.2. Connecting to GravityZone Control Center .....	42
5.3. Control Center at a Glance .....	43
5.3.1. GravityZone Console Overview .....	43
5.3.2. Table Data .....	44
5.3.3. Action Toolbars .....	45
5.3.4. Contextual Menu .....	45
5.3.5. Service Selector .....	46
5.4. Applying Security Policies .....	46
5.4.1. Creating and Configuring Policies .....	46
5.4.2. Assigning and Applying Policies .....	47
5.5. Using Tasks .....	48
5.6. Monitoring and Reporting .....	48
5.6.1. Using the Dashboard .....	48
5.6.2. Working with Reports .....	50
<b>6. Getting Help .....</b>	<b>52</b>

# 1. About GravityZone

Bitdefender has applied over a decade of security expertise and innovation for creating a highly scalable and integrated security management platform based on its new Gravity Architecture. The new Enterprise Security solutions form a “Gravity Zone” capable of protecting from hundreds to millions of endpoints on-demand with a private cloud hosted within the organization’s premises, or in public cloud hosted either by Bitdefender or a Service Provider.

The solution provides full visibility into organization’s overall security posture, global security threats, and control over its Security services that protect virtual or physical desktops, servers and mobile devices. All Bitdefender’s Enterprise Security solutions are managed within the Gravity Zone and a single console that provides control, reporting, and alerting services for various roles within the organization.

GravityZone includes the following components:

- [Control Center](#)
- [Security for Endpoints](#)
- [Security for Virtualized Environments](#)
- [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 virtual or physical desktops, servers and mobile devices. Powered by a Gravity Architecture, Control Center is capable of addressing the needs of even the largest organizations.

Control Center integrates with the existing system management and monitoring systems to make it simple to automatically apply protection to unmanaged desktops, servers or mobile devices that appear on the Microsoft Active Directory, VMware vCenter or Citrix XenServer.

## Security for Endpoints

Protects unobtrusively any number of Windows desktops, laptops and servers by using number-one-ranked antimalware technology combined with firewall, intrusion detection, web access control and filtering, sensitive data protection and application control. Employee productivity is ensured with low resource consumption, optimized system scanning and automated security that requires no end-user interaction.

## Security for Virtualized Environments

Security for Virtualized Environments is the first all-encompassing security solution for virtualized datacenters, protecting virtualized servers and desktops on Windows and Linux systems. Powered by cutting edge security technologies from Bitdefender, SVE has been specifically architected to meet the unique requirements of dynamic virtualized datacenters today.

## 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 any number of 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 GravityZone solutions are installed and managed via Control Center.

### 2.1. GravityZone Appliance Requirements

GravityZone is delivered as a virtual appliance. The GravityZone 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

Deploy the GravityZone appliance with the following minimum hardware configuration:

- CPU: 4 vCPU with 2 GHz each
- Minimum RAM memory: 6 GB
- 40 GB of free hard-disk space

The aforementioned hardware configuration is suitable for environments consisting of up to 50 computers, 50 virtual machines running on VMware infrastructure, 50 virtual machines running on Citrix XenServer infrastructure, 50 Active Directory users, 50 Android devices and 50 iOS devices.

#### 2.1.2. Internet Connection

The GravityZone 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

#### **Tablet and embedded operating systems\*:**

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

\*Specific operating system modules must be installed for 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:**
  - 512 MB minimum
  - 1 GB recommended
- **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 Virtualized Environments Requirements

Security for Virtualized Environments is delivered within a security virtual appliance called Security Server. Security Server is running on a hardened Linux Server distribution (2.6 kernel) and is managed by Control Center.

## 2.3.1. Supported Virtualization Platforms

Security for Virtualized Environments provides out-of-the-box support for the following virtualization platforms:

- VMware vSphere 5.5, 5.1, 5.0, 4.1 with VMware vCenter Server 5.1, 5.0, 4.1
- VMware View 5.1, 5.0
- Citrix XenServer 6.0, 5.6 or 5.5 (including Xen Hypervisor)
- Citrix XenDesktop 5.5 or 5.0 (including Xen Hypervisor)
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2 or Windows 2008 R2 (including Hyper-V Hypervisor)
- Microsoft Hyper-V Server 2012 or Windows 2012 Server (including Hyper-V Hypervisor)



### Note

Support for other virtualization platforms may be provided on request.

## Integration with VMware vShield Endpoint Requirements

- ESXi 5.1, 5.0 (build 474610 or higher), 4.1 (build 433742 or higher)
- vCenter Server 5.1, 5.0, 4.1
- vShield Manager 5.1, 5.0
- vShield Endpoint installed by vShield Manager on the host/hosts protected by Security for Virtualized Environments
- VMware Tools 8.6.0 build 446312 or higher installed on the protected virtual machines in the complete mode or with the vShield Endpoint driver selected under VMCI in custom mode.



### Important

It is recommended that you keep all VMware products updated with the latest patch.

If you are using ESXi 5.0, it is highly recommended to apply [VMware ESXi 5.0 Patch ESXi500-201204401-BG: Updates tools-light](#), which solves critical issues in the vShield Endpoint guest drivers. The patch updates VMware Tools to version 8.6.5 build 652272.

If you are using ESXi 4.1 P3, you must obtain the updated VMware Tools version and install it in the virtual machines. For more information, refer to [this KB article](#).

## 2.3.2. Supported Virtualization Management Tools

Control Center currently integrates with the following virtualization management tools:

- VMware vCenter Server
- Citrix XenServer

To set up integration, you must provide the username and password of an administrator.

### 2.3.3. Security Server Requirements

Security Server is a preconfigured virtual machine running on a hardened Linux Server distribution (2.6 kernel). Requirements depend on whether or not the appliance integrates with VMware vShield Endpoint.

#### In VMware Environments with vShield Endpoint

Security Server must be installed on each ESXi host to be protected.

You must provision the following resources on each host:

- Disk space: 80 GB.
- Memory and CPU resource allocation for the Security Server depends on the number and type of VMs running on the host. The following table lists the recommended resources to be allocated:

Number of protected VMs	RAM	CPUs
1-24 desktop VMs or 1-2 server VMs	2 GB	2 CPUs
25-49 desktop VMs or 3-7 server VMs	2 GB	4 CPUs
50+ desktop VMs or 8+ server VMs	4 GB	6 CPUs

#### In Other Environments

Although not mandatory, Bitdefender recommends installing Security Server on each physical host for improved performance.

You must provision the following resources on each Security Server host:

- Disk space: 8 GB.
- Memory and CPU resource allocation for the Security Server depends on the number and type of VMs running on the host. The following table lists the recommended resources to be allocated:

Number of protected VMs	RAM	CPUs
1-50 VMs	2 GB	2 CPUs
51-100 VMs	2 GB	4 CPUs
101-200 VMs	4 GB	6 CPUs

## 2.3.4. Supported Guest Operating Systems

Security for Virtualized Environments currently protects the following operating systems:

- Windows Server 2012
- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003 / Windows Server 2003 R2
- Windows 8
- Windows 7
- Windows Vista\*
- Windows XP with Service Pack 3 (32-bit) / Service Pack 2 (64-bit)\*
- Red Hat Enterprise Linux / CentOS 6.2, 6.1, 5.7, 5.6
- Ubuntu 11.04, 10.04
- SUSE Linux Enterprise Server 11
- OpenSUSE 12, 11
- Fedora 16, 15

\* VMware vShield Endpoint does not support the 64-bit versions of Windows XP and Vista.

On-access scanning is available for all supported Windows versions. A beta on-access scanning module is also available for specific Linux distributions and kernel versions, as shown in the following table:

Linux Distribution	Kernel Version
Ubuntu 10.04	2.6.32-44-generic-pae i686, 2.6.32-44-server x86_64, 2.6.32-45-generic-pae i686, 2.6.32-45-server x86_64
RHEL/CentOS 5.7, 5.6	2.6.18-308.24.1.el5 i686 & X86_64, 2.6.18-308.el5 i686 & x86_64, 2.6.18-348.el5 i686 & x86_64
RHEL/CentOS 6.2, 6.1	2.6.32-279.19.1.el6 i686 & x86_64, 2.6.32-279.el6 i686 & x86_64
Debian	2.6.32-5-amd64 x86_64

## 2.3.5. Bitdefender Tools Requirements and Footprint

Bitdefender Tools can be installed on virtual machines running any of the supported operating systems. No specific hardware or software requirements need to be met. As you can see in the following tables, Bitdefender Tools uses a minimum of system resources.

### In VMware Environments with vShield Endpoint

Platform	RAM	Disk Space
Windows	5/10* MB	15 MB
Linux	10 MB	70 MB

\*5 MB when the Silent Mode option is enabled and 10 MB when it is disabled. When Silent Mode is enabled, the Bitdefender Tools graphical user interface (GUI) is not loaded automatically at system startup, freeing up associated resources.

## In Other Environments

OS	RAM	Disk Space
Windows	20/25* MB	60 MB
Linux	50 MB	70 MB

\*20 MB when the Silent Mode option is enabled and 25 MB when it is disabled. When Silent Mode is enabled, the Bitdefender Tools graphical user interface (GUI) is not loaded automatically at system startup, freeing up associated resources.

## 2.4. Security for Mobile Devices Requirements

### 2.4.1. 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 (2.2+)

### 2.4.2. Connectivity Requirements

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

### 2.4.3. 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 GravityZone Mobile Device Management workflow, please refer to [this KB article](#).

## 2.4.4. 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 [“Configure Control Center Settings” \(p. 15\)](#).

## 2.5. GravityZone Communication Ports

The following table provides information on the ports used by the GravityZone components:

Port	Usage
<b>80 (HTTP) / 443 (HTTPS)</b>	Port used to access the Control Center web console.
<b>8080 (HTTP) / 8443 (HTTPS)</b>	Port used by client/agent software to connect to the Communication Server.
<b>7074 (HTTP)</b>	Update Server port
<b>27017</b>	Default port used by the Communication Server and Control Center to access the Database.
<b>7081 / 7083 (SSL)</b>	Ports used by the Bitdefender Tools agent to connect to Security Server.
<b>48651</b>	Communication port between the Bitdefender Tools agent for Linux and Security Server in VMware environments with vShield Endpoint.
<b>48652</b>	Communication port between the hypervisor (vmkernel) and Security Server in VMware environments with vShield Endpoint.
<b>5228, 5229, 5230</b>	Google Cloud Messaging (GCM) ports. The Communication Server uses GCM to send push notifications to managed Android devices.
<b>2195, 2196, 5223</b>	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 <a href="#">Apple KB article</a> .
<b>123 (UDP)</b>	User Datagram Protocol (UDP) port used by GravityZone appliances for time synchronization with the NTP server.

## 3. GravityZone Installation and Setup

To make sure installation goes smoothly, follow these steps:

1. [Prepare for installation.](#)
2. [Deploy and set up the GravityZone 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 GravityZone virtual appliance image. After you deploy and set up the GravityZone appliance, you can remotely install or download the necessary installation packages for all other security services components from the Control Center web interface.

The GravityZone 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 GravityZone appliances
- Username and password of a domain administrator
- vCenter Server, vShield Manager, XenServer details (hostname or IP address, communication port, administrator username and password)
- License key for each GravityZone security service (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 GravityZone Appliance

The GravityZone appliance can run one, several or all of the following roles:

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

A GravityZone deployment requires running one instance of each role. Consequently, depending on how you prefer to distribute the GravityZone roles, you will deploy one to four GravityZone appliances. The Database Server role is the first to be installed. In a scenario with multiple GravityZone appliances, you will install the Database Server role on the first appliance and configure all other appliances to connect to the existing database instance.

To deploy and set up the GravityZone appliance:

1. Import the GravityZone virtual appliance image in your virtualized environment.
2. Power on the appliance.
3. From your virtualization management tool, access the console interface of the GravityZone 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.](#)
  - d. [Install GravityZone roles.](#)

The GravityZone 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 GravityZone roles is performed using the IP address or DNS name of the appliance they are installed on. By default, the GravityZone components communicate using IP addresses. If you want to enable communication via DNS names, you must configure GravityZone 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.

### 3.2.4. Install GravityZone Roles

To install the GravityZone roles:

1. From the main menu, select **Install/Modify Roles**.
2. Select **Add or remove roles**.
3. Press Enter to continue.

4. Proceed according to the current situation:
  - If this is the initial GravityZone appliance deployment, press the space bar and then Enter to install the Database Server role. You must confirm your choice by pressing Enter again and then wait for the installation to complete.
  - If you have already deployed another appliance with the Database Server role, choose **Cancel** and return to the main menu. You must then choose **Configure Database Address** and enter the address of the database server.  
Use the following syntax: `http://<IP/Hostname>:<Port>`. The default database port is 27017.
5. Install the other roles by choosing **Add or remove roles** from the **Install/Modify Roles** menu and then the roles to install. Press the space bar to select a role and Enter to proceed. You must confirm your choice by pressing Enter again and then wait for the installation to complete.



#### Note

Each role is normally installed within a few minutes. During installation, required files are downloaded from the Internet. Consequently, the installation takes more time if the Internet connection is slow. If the installation hangs, redeploy the appliance.

## 3.3. Control Center Initial Setup

After deploying and setting up the GravityZone 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. 42).

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 GravityZone 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 keys required for validating the purchased GravityZone security services. Check the trial registration or purchase email to find your license keys. 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 security service and the expiry date for each license key in the corresponding columns.



### Note

During the initial setup, at least one valid license key must be provided to start using GravityZone. You can afterwards add more license keys or modify the existing ones.

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 GravityZone Control Center.

## 3.4. Enter License Keys

The GravityZone security services are licensed and sold separately. Each GravityZone security service requires a valid license key. At least one valid license key must be provided for using GravityZone.

Control Center is provided for free with any GravityZone security service.

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

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 **License** page.
3. You can view the existing license keys, status, expiry dates and usage count.

To change the license key for a service, 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 Settings** 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:
  - **When an unavailable Security Server image is needed.** The GravityZone appliance does not include by default the Security Server virtual machine images. If an administrator tries to download a Security Server image or to run a Security Server installation task, the action is going to fail. You can configure an automated action for this situation by choosing one of the following options:
    - **Download the image automatically**
    - **Notify the administrator and do not download**



#### Note

To avoid interference with administrator's work, you can manually download the necessary Security Server packages from the **Update > Product Update** page.

- **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 GravityZone appliances. A default NTP server address is provided, which you can change in the **NTP Server Address** field.



#### Note

For the GravityZone 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.

- Under the **Virtualization** tab, you can configure Control Center integration with virtualization management tools. Control Center can currently integrate with VMware vCenter Server and Citrix XenServer.
  - **Integrating with vCenter Server.**

You can integrate Control Center with one or multiple vCenter Server systems.



#### Note

vCenter Server systems in Linked Mode must be added separately to Control Center.

To set up integration with a vCenter Server:

- a. Click the **+** **Add** button at the right side of the table and choose **vCenter Server** from the menu. A configuration window will appear.
- b. Specify the vCenter Server details.
  - Name of the vCenter Server system in Control Center
  - Hostname or IP address of the vCenter Server system
  - vCenter Server port (default 443)

- c. Specify the details of the vShield Manager system integrated with the vCenter Server (if any).
  - Hostname or IP address of the vShield Manager system
  - vShield Manager port (default 443)

**Note**

If you do not use VMware vShield Endpoint in your environment, leave the corresponding fields blank.

- d. Specify the credentials to be used to authenticate with the vCenter Server. You can choose to use the credentials provided for integration with Active Directory or a different set of credentials. The user whose credentials you provide must have root level administrator permission on the vCenter Server.
  - e. Click **Save**.
- **Integrating with XenServer.**

You can integrate Control Center with one or multiple XenServer systems.

To set up integration with a XenServer:

- a. Click the **+ Add** button at the right side of the table and choose **XenServer** from the menu. A configuration window will appear.
  - b. Specify the XenServer details.
    - Name of the XenServer system in Control Center
    - Hostname or IP address of the XenServer system
    - XenServer port (default 443)
  - c. Specify the credentials to be used to authenticate with the XenServer. You can choose to use the credentials provided for integration with Active Directory or a different set of credentials.
  - d. Click **Save**.
- 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 GravityZone 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 GravityZone products and components and for both product and signature updates.
- Go to the **Infrastructure** tab for a quick overview of the installed GravityZone appliances and the roles they are running.

## 3.6. Add Control Center Users

You can create the first GravityZone user account during the initial Control Center setup, after deploying the GravityZone 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 create a custom user or add a user from Active Directory (provided Active Directory integration is configured). Choose the desired option from the **Type** menu.
  - When creating a custom user, you must specify a username and the user's full name and email address. You must also set the user password. Password must contain at least one upper case character, at least one lower case character and at least one digit or special character.
  - When adding a user from Active Directory, user details are imported from Active Directory and synchronized regularly according to the settings made in **Configuration > Active Directory** page. The user will log in to Control Center using the Active Directory user password.

**Note**

Click the **Force Resync** button to manually synchronize with Active Directory and update Control Center with any new changes.

**Note**

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

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 rights:

**Company Administrator**

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

**Administrator**

Administrator accounts offer access to GravityZone security services management, monitoring and reporting features (install the security services, create user accounts, create reports, edit the dashboard). Administrators cannot view or change the Control Center configuration settings.

**Reporter**

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

## Custom

Reporter accounts offer access only to the monitoring and reporting features.

- **Rights.** Each predefined user role has a certain configuration of rights. However, for each user role, you can change the user rights according to your needs. In this case, the user role changes to **Custom**.
- Click **Next**.
- Select the network groups the user will have access to for each available security service. You can restrict the user access to a certain GravityZone security service or to specific areas of the network.

Click **Next** to configure the user access for each available security service.



### 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.

You must define at least one global administrator with privileges over the entire GravityZone deployment (all services and all groups). Once you have created the global administrator, log out and log in using this user to perform the network security management tasks.

## 4. Install Security Services

To protect your network with Bitdefender, you must install the GravityZone security services. To install the GravityZone 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 objects (computers, virtual machines, mobile devices).

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 Virtualized Environments	Virtual machines running on Microsoft Windows or Linux, under any virtualization platform
Security for Mobile Devices	iPhone, iPad and Android devices

### 4.1. Installing Security for Endpoints

Security for Endpoints is intended for workstations, laptops and servers running on Microsoft® Windows. 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 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.

#### 4.1.1. Preparing for Installation

Before you start:

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. The mechanism is the same as the one used in Cloud Security for Endpoints by Bitdefender. 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. Make sure you have the necessary credentials at hand for all computers.
4. Computers must have network connectivity to the Control Center appliance.

## Network Discovery Requirements

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.

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.

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.

## Remote 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.

### 4.1.2. Using Installation Packages

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.

You can download installation packages both as a downloader application and full installation kits for 32bit and 64bit operating systems.



### Note

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).

The full installation kits are bigger in size and they have to be run on the corresponding operating system type.

## Creating Endpoint Security Installation Packages

To create a Endpoint Security installation package:

1. Connect and log in to Control Center using your administrator account.
2. Go to the **Network > 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.
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 if you want the client to communicate directly with the GravityZone appliance.
  - **Endpoint Security Relay.** Endpoint Security Relay is a special role which installs an update server on the target machine along with Endpoint Security, that can be used to update all the other clients in the network, lowering the bandwidth usage between the client machines and the GravityZone appliance. If you install an Endpoint Security Relay in your network, all the managed computers will communicate with the GravityZone appliance through the endpoint with Endpoint Security Relay role.
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:
  - **GravityZone 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:

    - `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**, available for installation packages with Endpoint role. In this case, all endpoints with Endpoint Security Relay role detected in your network will be available in the table displayed below. Select the Endpoint Security Relay that you want to use for client updates.

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. Connect and log in to Control Center.
2. Go to the **Network > Packages** page.
3. Select the Endpoint Security installation package that 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 (downloader application or full installation kit).
5. Save the file to your computer.

## Running Installation Packages

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

1. Download or copy the installation file to the target computer or to a network share accessible from that computer.
2. Run the installation package.
3. 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. Using Remote Installation Tasks

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.

Security for Endpoints includes an automatic network discovery mechanism that allows detecting computers that are not in Active Directory. 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. 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.



### Note

For network discovery and remote installation to work, a number of requirements must be met. To learn more, refer to [“Preparing for Installation”](#) (p. 22).

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

To run a remote installation task:

1. Go to the **Network** page.
2. Choose **Computers** from the [service selector](#).
3. Select the desired 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.
6. Configure the installation options:
  - Select the role you want the client to have:
    - **Endpoint**. Select this option if you want the client to communicate directly with the GravityZone appliance.
    - **Endpoint Security Relay**. Endpoint Security Relay is a special role which installs an update server on the target machine along with Endpoint Security, that can be used to update all the other clients in the network, lowering the bandwidth usage between the client machines and the GravityZone appliance. If you install an Endpoint Security Relay in your network, all the managed computers will communicate with the GravityZone appliance through the endpoint with Endpoint Security Relay role.
  - 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 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**.
- Depending on the client role (Endpoint or Endpoint Security Relay), choose the entity through which the clients will communicate:
  - **GravityZone 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:

- `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**, available for clients with Endpoint role. In this case, all endpoints with Endpoint Security Relay role detected in your network will be available in the table displayed below. Select the Endpoint Security Relay that you want to use for client updates.

## 7. Click **Next**.

- 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:

- 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, `domain\user` or `user@domain.com`).



### Note

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

- Click the **+ Add** button. The account is added to the list of credentials.
  - Select the check box corresponding to the account you want to use.
- Click **Save**. A confirmation message will appear.

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

## 4.2. Installing Security for Virtualized Environments

Security for Virtualized Environments helps you protect Windows and Linux virtual machines, running under any virtualization platform, using technologies designed specifically for virtualized environments. For comprehensive information on supported infrastructures and requirements, refer to [“Security for Virtualized Environments Requirements”](#) (p. 5).

Before you start, you must provide the credentials to [connect to the existing vCenter Server infrastructure](#).

To install Security for Virtualized Environments:

- [Install Security Server on hosts.](#)
- [Install Bitdefender Tools on virtual machines.](#)

## 4.2.1. Connect to vCenter Server

In order to have access to the virtualized infrastructure integrated with Control Center, you must provide your user credentials for each vCenter Server system available. Control Center uses your credentials to connect to the virtualized infrastructure, displaying only resources you have access to (as defined in vCenter Server).

To specify the credentials to connect to the vCenter Server systems:

1. Point to your username in the upper-right corner of the page and choose **Credentials Manager**.
2. Go to the **Virtual Environment** tab.
3. Specify the necessary authentication credentials.
  - a. Select a server from the corresponding menu.



### Note

If the menu is unavailable, either no integration has been configured yet or all necessary credentials have already been configured.

- b. Enter your username and password and a suggestive description.
- c. Click the **+ Add** button. The new set of credentials is displayed in the table.



### Note

If you have not specified your authentication credentials, you will be required to enter them when you try to browse the inventory of any vCenter Server system. Once you enter your credentials, they are saved to your Credentials Manager so that you do not need to enter them the next time.

## 4.2.2. Install Security Server on Hosts

Security Server is a dedicated virtual machine that deduplicates and centralizes most of the antimalware functionality of antimalware clients, acting as a scan server.

You must install Security Server on hosts as follows:

- In VMware environments with vShield Endpoint, you must install the purpose-built appliance on each host to be protected. All virtual machines on a host are automatically connected via vShield Endpoint to the Security Server instance installed on that host.
- In all other environments, you must install Security Server on one or more hosts so as to accommodate the number of virtual machines to be protected. You must consider the number of protected virtual machines, resources available for Security Server on hosts, as well as network connectivity between Security Server and protected virtual machines. The Bitdefender Tools installed on virtual machines connects to Security Server over TCP/IP, using details configured at installation or via a policy.

If Control Center is integrated with vCenter Server and XenServer, you can automatically deploy Security Server on hosts from Control Center. You can also download Security Server packages for standalone installation from Control Center.



### Note

For VMware environments with vShield Endpoint, you can deploy Security Server on hosts exclusively via installation tasks.

## Using Remote Installation Tasks

Control Center allows you to remotely install Security Server on visible hosts by using installation tasks.


To install Security Server remotely on one or several hosts:

1. Go to the **Network** page.
2. From the menu in the upper-right corner of the page, select **Virtual Machines**.
3. Browse the VMware or Citrix inventory and select the check boxes corresponding to the desired hosts or containers (vCenter Server, XenServer or datacenter). For a fast selection, you can directly select the root container (VMware Inventory or Citrix Inventory). You will be able to select hosts individually from the installation wizard.



### Note

You cannot select hosts from different folders.

4. Click the  **Tasks** button at the right side of the table and choose **Install Security Server** from the menu. The **Security Server Installation** window is displayed.
5. Select the hosts on which you want to install the Security Server instances.
6. Choose the configuration settings you want to use.



### Important

Using common settings while deploying multiple Security Server instances simultaneously requires the hosts to share the same storage, have their IP addresses assigned by a DHCP server and be part of the same network.

7. Click **Next**.
8. Enter a suggestive name for the Security Server.
9. Select the container in which you want to include the Security Server from the **Deploy Container** menu.
10. Select the destination storage.
11. Choose the disk provisioning type. It is recommended to deploy the appliance using thick disk provisioning.



### Important

If you use thin disk provisioning and the disk space in the datastore runs out, the Security Server will freeze and, consequently, the host will remain unprotected.

12. Configure the memory and CPU resource allocation based on the VM consolidation ratio on the host. Choose **Low**, **Medium** or **High** to load the recommended resource allocation settings or **Manual** to configure resource allocation manually.
13. Optionally, you can choose to set an administrative password for the Security Server console. Setting an administrative password overrides the default root password ("sve").
14. Set the timezone of the appliance.
15. Select the network configuration type for the Bitdefender network. The IP address of the Security Server must not change in time, as it is used by Linux agents for communication.  
If you choose DHCP, make sure to configure the DHCP server to reserve an IP address for the appliance.  
If you choose static, you must enter the IP address, subnet mask, gateway and DNS information.
16. Select the vShield network and enter the vShield credentials. Default label for the vShield network is `vmervice-vshield-pg`.
17. Click **Save**.


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

## Using Installation Packages

In all virtualized environments that are not integrated with Control Center, you must install Security Server on hosts manually, using an installation package. The Security Server package is available for download from Control Center in several different formats, compatible with the main virtualization platforms.

### Downloading Installation Packages

To download Security Server installation packages:

1. Go to the **Network > Packages** page.
2. Select the Security Server package.
3. Click the  **Download** button at the right side of the table and choose the package type from the menu.
4. Save the selected package to the desired location.

## Deploying Installation Packages

Once you have the installation package, deploy it to the host using your preferred virtual machine deployment tool.

After deployment, set up the Security Server as follows:

1. Access the appliance console from your virtualization management tool (for example, vSphere Client). Alternatively, you can connect to the appliance via SSH.
2. Log in using the default credentials.
  - User name: `root`
  - Password: `svs`
3. Run the `sva-setup` command.
4. Configure the appliance with DHCP/static network settings.

If you have created an IP reservation for the appliance on the DHCP server, skip this configuration by pressing Enter. If you configure with static network settings follow these steps:

  - a. Type `Y` and press Enter to continue.
  - b. Enter the network settings: IP address, network mask, gateway, DNS servers.
  - c. Type `Y` and press Enter to save the changes.
5. Configure the Security Console IP: enter the GravityZone Control Center IP address.
6. Configure the Communication Server IP address. Since the communication server role runs on Control Center virtual machine, you must enter the following:
  - The IP address or hostname Control Center virtual machine.
  - Port number 8443, using the following format: `https://GravityZone-IP:8443`.
7. Configure Update Server address. Since the local update server runs on the Control Center machine, you must enter the IP address or hostname of that machine.
8. Configure the Update Server port: 7074.



### Note

If you are connected to the appliance via a SSH client, changing the network settings will immediately terminate your session.

## 4.2.3. Install Bitdefender Tools on Virtual Machines

Bitdefender Tools is the component to be installed on the virtual machines you want to protect.

In VMware vSphere environments, Security for Virtualized Environments can integrate with VMware vShield Endpoint to provide agentless protection for Windows virtual machines. All virtual machines on a host are automatically connected via vShield Endpoint to the Security

Server instance installed on that host. Optionally, you can deploy the Bitdefender Tools on Windows virtual machines to take advantage of the additional functionality it provides.

- Allows you to run Memory and Process Scan tasks on the machine.
- Informs the user about the detected infections and actions taken on them.

## Preparing for Installation

Before you start:

1. Make sure the virtual machines run a [supported guest operating system](#). For some virtual machines, you may need to install the latest operating system service pack available.
2. Uninstall (not just disable) any existing antimalware software from the virtual machines. Running other security software simultaneously with Security for Virtualized Environments may affect their operation and cause major problems with the system.
3. The installation requires administrative privileges. Make sure you have the necessary credentials at hand for all virtual machines.
4. Virtual machines must have network connectivity to the Control Center appliance.

## Using Remote Installation Tasks

In environments integrated with Control Center, you can remotely install Bitdefender Tools on virtual machines by using installation tasks. Remote installation relies on VMware Tools in VMware environments and, respectively, on Windows administrative shares and SSH in Citrix XenServer environments.



### Note

For remote installation to work, a number of requirements must be met. To learn more, refer to [“Preparing for Installation”](#) (p. 34).

To run a remote installation task:



1. Go to the **Network** page.
2. Choose **Virtual Machines** from the [service selector](#).
3. Select the desired group from the left-side pane. All virtual machines contained in the selected group are displayed in the right-side pane table.



### Note

Optionally, you can apply filters to display unmanaged virtual machines 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 virtual machines on which you want to install protection.

5. Click the  **Tasks** button at the right-side of the table and choose **Install client**. The **Bitdefender Tools Installation** wizard is displayed.
6. Configure the appropriate settings for your environment.
7. Under **Security Server Assignment**, select the Security Server that will manage the selected virtual machines. Choose the Security Server from the **Security Server** list, then click the  **Add** button at the right side of the table.

When several Security Server machines are available, you can set their priority using the arrow buttons available at the right side of the table.

8. Click **Next**.
9. Under the **Credentials Manager** section, specify the administrative credentials required for remote authentication on selected virtual machines.



#### Note

A warning message is displayed as long as you have not selected an administrator account yet. This step is mandatory to remotely install the Bitdefender Tools on virtual machines.


If you have not already defined the credentials in the **Credentials manager**, add the required administrator accounts as follows:

- a. Enter the user name and password of an administrator account for each of the selected virtual machines in the corresponding fields. Optionally, you can add a description that will help you identify each account more easily.
  - If virtual machines are in a domain, it suffices to enter the credentials of the domain administrator. Use Windows conventions when entering the name of a domain user account (for example, `domain\user` or `user@domain.com`).
  - For Linux virtual machines, you must provide the credentials of the root account.



#### 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 new account credentials are added.
  - c. Select the check box corresponding to the accounts you want to use.
10. Click **Save**. A confirmation message will appear.

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



## Using Installation Packages

In all virtualized environments that are not integrated with Control Center, you must install Bitdefender Tools on virtual machines manually, using an installation package. A default installation package is available for download from Control Center (as a downloader application for Windows and as an installation script for Linux). You can also create additional custom packages as needed.

### Creating Bitdefender Tools Installation Packages

You can create custom installation packages if you want to configure the installation settings (for example, uninstall password or modules to install).

To create a custom Bitdefender Tools installation package:

1. Connect and log in to Control Center using your administrator account.
2. Go to the **Network > Packages** page.
3. Click the **+** **Add** button at the right side of the table and choose **Bitdefender Tools** from the menu. A configuration window will appear.
4. Enter a suggestive name and description for the installation package you want to create.
5. Configure settings as needed.
6. Select the Security Server that will be used for scanning the virtual machines:
  - a. Click the **Security Server** field. The list of detected Security Servers is displayed.
  - b. Select an entity.
  - c. Click the **+** **Add** button at the right side of the table.


The Security Server is added to the list. All target virtual machines will be scanned by the specified Security Server.
  - d. Follow the same steps to add several Security Servers, if available. In this case, you can configure their priority using the up and down arrows available at the right side of each entity.
  - e. To delete one entity from the list, click the corresponding **-** **Delete** button at the right side of the table.
7. Click **Save**.

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

### Downloading Installation Packages

To download Bitdefender Tools installation packages:

1. Connect and log in to Control Center using your administrator account.

2. Go to the **Network > Packages** page.
3. Select the check box corresponding to the default or a custom Bitdefender Tools installation package.
4. Click the  **Download** button at the right side of the table and choose the type of installation package.
5. Save the file to your computer.

### Running Installation Packages

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

- To manually install Bitdefender Tools on a Windows virtual machine:
  1. Download or copy the installation file to the target virtual machine or to a network share accessible from that machine.
  2. Run the installation package.
  3. Follow the on-screen instructions.
- To manually install Bitdefender Tools on a Linux virtual machine:
  1. Download or copy the installation file to the target virtual machine or to a network share accessible from that machine. The downloaded file is named `installer`.
  2. Grant execute permission to current user on the `installer` file.

```
$ chmod u+x installer
```

3. Run `installer` as root. The script downloads the full installation package from the Control Center appliance and then starts the installation.

```
$ sudo ./installer
```

Installation will normally complete in less than a minute. Once Bitdefender Tools has been installed, the virtual machine will show up as managed in Control Center (**Network** page) within a few minutes.

## 4.3. 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](#).

### 4.3.1. Configure External Address for Communication Server

In the default GravityZone 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**.
3. Select **Configure MDM Server external address**.
4. Enter the external address.

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

- 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.

## 4.3.2. 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**.
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.

### 4.3.3. Add Devices to Users

You can only add one device to one specific user at a time.

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.
5. Enter a suggestive name for the device.
6. Select the device ownership type (Enterprise or Personal).
7. 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.

### 4.3.4. 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 GravityZone 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 GravityZone 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
- Integration with virtualization management tools (vCenter Server, XenServer)
- Mail server settings
- Update settings for GravityZone 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 GravityZone 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 GravityZone Control Center

Prerequisites:

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

- The computer you connect from must have network connectivity to the Control Center appliance.

To connect to GravityZone 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.

### 5.3.1. GravityZone Console 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, GravityZone 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, integration with Active Directory or virtualization environments 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 GravityZone.

## 5.3.2. Table Data

Tables are frequently used throughout the console to organize data into an easy-to-use format. There are several ways of working with table data:

- [Navigate through table pages](#)
- [Search for specific entries](#)
- [Sort data](#)
- [Refresh table data](#)

## 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.

### 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.

## 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)
- **Virtual Machines** (Security for Virtualized Environments)
- **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, virtual machines 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 GravityZone 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, virtual machines 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.

## 5.4.2. Assigning and Applying Policies

By default, all managed clients inherit the policy from their parent. You can change the default policy at the top-level group or configure different policies for specific groups by changing the inheritance options.

To assign and apply a policy:

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, virtual machines or mobile devices).
3. Browse for and select the specific network objects or groups you want to assign the policy to. You can only select objects from the same parent group.
4. Click the  **Assign Policy** button at the right side of the table. The **Policy Assignment** window is displayed. Under the **Status** tab, you can check the current policy assignments for selected items.
5. Go to the **Options** tab to change the current policy assignments.
6. Select the desired **Inheritance** option to configure policy assignment:
  - **Use current policy.** Select this option if you want selected items to continue using their current policy.
  - **Inherit from above.** Select this option if you want to apply to each selected item the current policy of its parent.
  - **Don't inherit and assign the following policy template.** Select this option if you want to apply a specific policy to selected items. In this case, you can select to force inheritance of the selected policy on the subgroups of the selected items.
7. Click **Ok** to save changes and apply new protection settings on the target clients.


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

## 5.5. Using Tasks

Control Center offers a number of administrative tasks that you can run remotely on network objects (computers, virtual machines or mobile devices). Tasks are related to the GravityZone 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, virtual machines 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.

## 5.6. Monitoring and Reporting

Control Center includes powerful monitoring and reporting features. The main GravityZone 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, virtual machines 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:

- 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**, **Virtual Machines** 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 GravityZone 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, virtual machines 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 GravityZone 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 upper-right corner of Control Center.
- Go to our [online Support Center](#).

To open a support ticket, go [here](#) and fill in the form.