



Bitdefender® ENTERPRISE

**GRAVITYZONE
UNIFIED SECURITY
MANAGEMENT**
Quick Start Guide >>

GravityZone Unified Security Management

Quick Start Guide

Publication date 2013.02.22

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	4
2.2.3. Supported Browsers	5
2.3. Security for Virtualized Environments Requirements	5
2.3.1. Supported Virtualization Platforms	5
2.3.2. Supported Virtualization Management Tools	6
2.3.3. Security Server Requirements	6
2.3.4. Supported Guest Operating Systems	7
2.3.5. BDTools Requirements and Footprint	7
2.4. Security for Mobile Devices Requirements	8
2.5. GravityZone Communication Ports	8
3. Installation and Setup	10
3.1. Prepare for Installation	10
3.2. Deploy and Set Up GravityZone Appliance	11
3.2.1. Configure Appliance Hostname (DNS)	11
3.2.2. Configure Network Settings	12
3.2.3. Configure Proxy Settings	12
3.2.4. Install GravityZone Roles	12
3.3. Configure Control Center Root	13
3.4. Enter License Keys	14
3.5. Configure Control Center Settings	14
3.6. Add Control Center Users	16
3.7. Install Security Services	17
3.7.1. Installing Security for Endpoints	18
3.7.2. Installing Security for Virtualized Environments	22
3.7.3. Installing Security for Mobile Devices	29
4. Getting Started with Control Center	32
4.1. Types of Users in Control Center	32
4.2. Connecting to Control Center	32
4.3. Control Center at a Glance	33
4.3.1. User Consoles	33
4.3.2. Table Data	35
4.3.3. Action Toolbars	36

4.3.4. Service Selector	36
4.4. Applying Security Policies	37
4.4.1. Creating and Configuring Policies	37
4.4.2. Assigning and Applying Policies	37
4.5. Using Tasks	38
4.6. Monitoring and Reporting	39
4.6.1. Using the Dashboard	39
4.6.2. Working with Reports	41
5. Getting Help	43

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 an 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)

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

2.1.1. Hardware Requirements

For evaluation purposes, deploy the GravityZone appliance with the following 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: 1024x768 or higher
- The computer you connect from must have network connectivity to the Control Center appliance.

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
- 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
- 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:
 - 1 GHz for Windows XP, Windows Vista, Windows 7, Windows 8
 - Single processor with 1.5 GHz for Windows Server 2003 / 2003 R2, Windows SBS 2003
 - Single processor with 1.5 GHz (x64 processor) or 1.3 GHz (Dual Core) for Windows 2008 / 2008 R2, Windows Server 2012
 - Single processor with 2 GHz or 1.5 GHz (Dual Core) for Windows SBS 2008
 - Quad core 2 GHz (x64 processor) for Windows SBS 2011

- RAM memory:
 - 1 GB for Windows XP, Windows Vista, Windows 7, Windows 8 (32-bit), Windows 2008 / 2008 R2, Windows 2003 / 2003 R2
 - 1.5 GB for Windows SBS 2003
 - 2 GB for Windows 8 (64-bit), Windows Server 2012
 - 4 GB for Windows SBS 2008
 - 8 GB for Windows SBS 2011
- 1 GB of free hard-disk space

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 5.1, 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)



Note

Support for other virtualization platforms may be provided on request.

For integration with VMware vShield Endpoint, the following requirements must be met:

- 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.

2.3.5. BDTools Requirements and Footprint

BDTools 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, BDTools 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 BDTools 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 BDTools graphical user interface (GUI) is not loaded automatically at system startup, freeing up associated resources.

2.4. Security for Mobile Devices Requirements

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

- Apple iPhones and iPad tablets (iOS 5+)
- Google Android smartphones and tablets (2.2+)

*The Mobile Client application for iOS devices is not yet available on App Store, pending approval from Apple.

2.5. GravityZone Communication Ports

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

Port	Usage
80 (HTTP) / 443 (HTTPS)	Port used to access the Control Center web console.
8080 (HTTP) / 8443 (HTTPS)	Port used by client/agent software to connect to the Communication Server.
7074 (HTTP)	Update Server port

Port	Usage
27017	Default port used by the Communication Server and Control Center to access the Database.
7081 / 7083 (SSL)	Ports used by the BDTools agent to connect to Security Server.

3. 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. [Configure the Control Center root account.](#)
4. [Enter your license keys.](#)
5. [Configure Control Center settings.](#)
6. [Add Control Center users.](#)
7. [Install security services on network objects.](#)

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 components of the GravityZone security services 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

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 (Control Center)**
- **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. Deploy or 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. Configure Control Center Root

After deploying and setting up the GravityZone appliance, you must access the Control Center web interface and configure the root account.



Note

For more information on Control Center users, refer to [“Types of Users in Control Center”](#) (p. 32).

To configure the Control Center root account:

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. 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. Specify the required details for your root 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.

Click **Create Account**.

4. Log in using the configured username and password to access the Control Center root console. The first time you log in, you must read and agree with the License Agreement.

3.4. Enter License Keys

The GravityZone security services are licensed separately. 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 the root account.
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 the root account.
2. Go to the **Integration** page.
 - 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.

 - 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” \(p. 15\)](#)
 - [“Integrating with XenServer” \(p. 16\)](#)
3. Go to the **Settings** page. 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.
- **From email.** Enter the email address that you want to appear in the From field of the email (sender's email address).
- **Encryption type.** If the mail server requires an encrypted connection, choose the appropriate type from the menu (SSL, TLS or STARTTLS).
- **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.

4. Go to the **Update** page.

- 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.
- Under the **Product Update** tab, download or update all necessary installation packages.

5. Go to the **Certificates** page. 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.

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:

1. Click the **+** **Add** button at the right side of the table and choose **vCenter Server** from the menu. A configuration window will appear.
2. 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)
3. 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.

4. 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.
5. Click **Save**.

Integrating with XenServer

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

To set up integration with a XenServer:

1. Click the **+** **Add** button at the right side of the table and choose **XenServer** from the menu. A configuration window will appear.
2. Specify the XenServer details.
 - Name of the XenServer system in Control Center
 - Hostname or IP address of the XenServer system
 - XenServer port (default 443)
3. 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.
4. Click **Save**.

3.6. Add Control Center Users

The built-in root account is to be used exclusively for Control Center setup. From the root account, you must add to Control Center the users designated to perform the network and security management tasks.

To add a Control Center user:

1. Connect and log in to the Control Center web interface using the root 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 configuration on the **Integration > Active Directory** page. The user logs in to Control Center using the Active Directory user password.



Note

If the [mail server settings](#) are configured, Control Center automatically sends the user an email with the login details.

5. Under the **Settings and Privileges** section, configure the Control Center settings and privileges for the specified user. You must specify the following:

- **Role.** A user can have one of the following roles:

Administrator

Administrator accounts offer full access to all management features of the GravityZone security services.

Reporter

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

- **Timezone and language.** Select the preferred timezone and language.
- **Target.** In the table, select the services and groups the user will have access to. You can restrict access to a specific GravityZone security service or to specific areas of the network.



Important

Whenever you set 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.

3.7. 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

3.7.1. 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.

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 Windows XP workstation that is part of a workgroup, or of a different domain than the Control Center appliance, NOT to use simple 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.

Using Installation Packages

One way to install Endpoint Security on a computer is to locally run an installation package. A default installation package is available for download from Control Center (as a downloader application). You can also create additional custom packages as needed.



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).

Creating Custom Installation Packages

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


To create a custom 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. The **Endpoint Security Package Configuration** window will appear.
4. Enter a suggestive name and description for the installation package you want to create.
5. Select the protection modules you want to install.
6. Configure settings as needed.
7. Click **Save**.

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

Downloading Installation Packages

To download Endpoint Security 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 to a custom Endpoint Security installation package.
4. Click the  **Download** button at the right side of the table.
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.

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 it to detect 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** on 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” \(p. 18\)](#). 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. From the menu in the upper-right corner of the page, select **Computers**.
3. Apply filters to display unmanaged computers only. Click the filters button and select the following options in each category: **Unmanaged**, **Show all** and **Show all computers (including subfolders)**.
4. Select the check boxes corresponding to the computers on which you want to install protection.

**Note**

You cannot simultaneously select computers from Active Directory folders and from Custom Groups.

5. Click the  **Tasks** button at the right side of the table and choose **Install client** from the menu. The **Install Endpoint Security** window is displayed.
6. You can change default installation options as needed.
7. Go to the **Credentials** tab and provide the administrative credentials required for remote authentication on selected computers. Enter the user name and password of an administrator account for each of the selected computers. If computers are in a domain, it suffices to enter the credentials of the domain administrator. Use Windows conventions when entering the name of a domain user account (for example, `domain\user` or `user@domain.com`).

**Note**

Specified credentials are automatically saved to your Credentials Manager so that you do not have to enter them the next time. To access your Credentials Manager, click your username in the upper-right corner of the page and select **Credentials Manager**.

8. Click **Save**.

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

3.7.2. 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:

1. [Install Security Server on hosts](#).

2. Install BDTools on virtual machines.

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.

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 BDTools 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 a host:

1. Go to the **Network** page.
2. From the menu in the upper-right corner of the page, select **Virtual Machines**.
3. Browse the corresponding inventory (VMware or Citrix) and select the check box corresponding to the host.



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. Configure the installation settings:
 - a. Enter a suggestive name for the virtual appliance.
 - b. Select the destination storage.
 - c. For VMware environments, you can 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.

- d. 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.
- e. Select the Bitdefender network. The Security Server uses this network to communicate with the other Security for Virtualized Environments components.

- f. 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.
 - g. If you are deploying the appliance in a VMware environment integrated with vShield Endpoint, you must additionally specify the following:
 - Specify the credentials to be used to register the Security Server with vShield Endpoint. Your vCenter Server credentials are used by default. You can select **Specify custom credentials** in order to enter other credentials.
 - Select the vShield network. Default label is `vmervice-vshield-pg`.
6. Click **Save**.


You can view and manage the task on 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 appliance:

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: `administrator`

- Password: `admin`
3. Obtain root privileges by running the `sudo su` command and then entering the `admin` password.
 4. Run the `sva-setup` command.
 5. Enter the IP address or hostname of the local update server. Since the local update server runs on the Control Center machine, you must enter the IP address or hostname of that machine.
 6. Optionally, you can configure the appliance with static network settings. If you have created an IP reservation for the appliance on the DHCP server, skip this configuration by pressing Enter.
 - 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.



Note

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

Install BDTools on Virtual Machines

BDTools 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 BDTools 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 BDTools 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. 26).


To run a remote installation task:

1. Go to the **Network** page.
2. From the menu in the upper-right corner of the page, select **Computers**.
3. Apply filters to display unmanaged virtual machines only. Click the filters button and select the following options in each category: **Unmanaged**, **Show all VMs recursively** and **Show all VMs**.
4. Select the check boxes corresponding to the virtual machines on which you want to install protection.



Note

You cannot simultaneously select virtual machines from different virtualization infrastructures.

5. Click the  **Download** button at the right side of the table and choose **Install client** from the menu. The **BDTools Installation** window is displayed.
6. Configure installation settings as needed.
7. Go to the **Credentials** tab and provide the administrative credentials required for remote authentication on selected virtual machines. Enter the user name and password of an administrator account for each of the selected virtual machines. 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`).



Note

Specified credentials are automatically saved to your Credentials Manager so that you do not have to enter them the next time. To access your Credentials Manager, click your username in the upper-right corner of the page and select **Credentials Manager**.

8. Click **Save**.

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

Using Installation Packages

In all virtualized environments that are not integrated with Control Center, you must install BDTools 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 Custom Installation Packages

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

To create a custom BDTools 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 **BDTools** from the menu. The **BDTools Package 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. Click **Save**.

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

Downloading Installation Packages

To download BDTools 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 to a custom BDTools 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 BDTools 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 BDTools 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 `downloader`.
 2. Grant execute permission to current user on the `downloader` file.

```
$ chmod u+x downloader
```

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

```
$ sudo ./downloader
```

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

3.7.3. 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 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.

To install Security for Mobile Devices:

1. If you do not use Active Directory, you must [create users for mobile device owners](#).
2. [Add devices to users](#).
3. [Install Mobile Client on devices and activate it](#).

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.

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.



Note

The configuration window displays the unique activation token assigned to the device and the communication server address, as well as the corresponding QR code. If you are going to install the client app on the user's device, proceed to that without closing this window. After installation, when prompted to activate the device, enter the activation token and the communication server address or scan the QR code displayed on your computer screen.

6. 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).



Important

The email and the QR code include the internal address of the communication server. Devices configured with this address can only be managed when they are directly connected to the company network.

To be able to manage mobile devices when not connected to the company network:

1. Configure port forwarding for the Bitdefender communication server.
2. Set the external communication server address in the GravityZone appliance CLI interface.
3. Activate devices using the external address of the communication server.

Syntax: <GatewayAddress> : <Port>

Install Mobile Client on Devices

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

To install Mobile Client on a device:

1. Search for the application on the official app store.
 - [Google Play link](#)
2. Download and install the application on the device.
3. Start the application and make the required configuration:
 - a. Enter the activation token and the communication server address or, alternatively, scan the QR code received by email.
 - b. Click **Activate**.

4. Getting Started with Control Center

Bitdefender GravityZone security services 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.

4.1. Types of Users in Control Center

Control Center allows access for the following types of users:

Root

The built-in `root` user is to be used to perform the Control Center setup, including:

- Integration with Active Directory
- Integration with virtualization management tools (vCenter Server, XenServer)
- Configuring mail server settings
- Update configuration for installed components and installation packages
- Security certificates management
- License key management
- Configuring user access to Control Center

The root user does not provide access to the features that allow managing the GravityZone security services.

Administrator

Administrator users offer full access to all management features of the GravityZone security services. User access can be restricted to a specific GravityZone security service or to specific areas of the network.

Reporter

Reporter users offer access only to the monitoring and reporting features. Reporters cannot view or change the network or security configuration. User access can be restricted to a specific GravityZone security service or to specific areas of the network.

The root login details are configured during initial Control Center setup. Administrator and reporter users can be created either by the root or an administrator user.

4.2. Connecting to 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 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.



Note

To add users and set up Control Center, log in as root. For more information, refer to [“Configure Control Center Settings”](#) (p. 14).

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.

The first time you log in to the console, you will be prompted to read and confirm that you agree with the End User License Agreement.

4.3. 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.

4.3.1. User Consoles

Root Console

Root can access the following sections from the menu bar:

Integration

Set up integration with Active Directory and with existing virtualization management tools (VMware vCenter Server and Citrix XenServer).

Settings

Configure general installation preferences and the mail server settings.

Update

Update deployed GravityZone appliances, configure the update settings and download the latest installation packages for the GravityZone security services.

Infrastructure

View information on the installed GravityZone appliances and the roles they are running.

Certificates

Manage the Control Center security certificate and the security certificates required for iOS mobile device management.

License

Enter your license keys for the GravityZone security services.

Accounts

Set up access to Control Center for administrator and reporter users.

Logs

Check the user activity log.

Additionally, at the right side of the menu bar, 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 account details and preferences.
- **Logout.** Click this option to log out of your account.

Administrator Console

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

Set up access to Control Center for other company employees.

Logs

Check the user activity log.

Additionally, at the right side of the menu bar, 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 account details and preferences.
- **Credentials Manager.** Click this option to add and manage the authentication credentials required for remote installation tasks and for authentication with the available vCenter Server systems.
- **Logout.** Click this option to log out of your account.

Reporter Console

Reporters can access the following sections from the menu bar:

Dashboard


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

Reports

Get security reports concerning the managed clients.

Logs

Check the user activity log.

Additionally, at the right side of the menu bar, 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 account details and preferences.
- **Logout.** Click this option to log out of your account.

4.3.2. 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.

4.3.3. 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.

4.3.4. 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.

4.4. Applying Security Policies

Once installed, the GravityZone security services can be configured and managed exclusively from Control Center using security policies. A policy specifies the security settings to be applied on target clients (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.

4.4.1. 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.

4.4.2. 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  **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.



Note

The **Policy** button is unavailable if you have directly selected an unmanaged network object (not applicable to groups).

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.


4.5. 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 on 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.

4.6. Monitoring and Reporting

Control Center includes powerful monitoring and reporting features. The main GravityZone monitoring tool is the Control Center dashboard.

- [Dashboard](#)
- [Reports](#)

4.6.1. 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).

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

Control Center comes with 12 predefined dashboard portlets, four for each GravityZone security service. Dashboard portlets are displayed in groups of four, a slider at the bottom of the page allowing navigation between groups.

The dashboard is easy to configure based on individual preferences. You can [edit](#) portlet settings, [add](#) additional portlets, [remove](#) or [rearrange](#) existing portlets.


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.


Creating Custom Portlets

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

To create a custom 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:
 - Type of network objects
 - Type of background report
 - Suggestive portlet name
 - Background report options, if any
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**.

4.6.2. 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 sent 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.

5. 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.