

**Bitdefender®**

**GravityZone**

**РУКОВОДСТВО ПО УСТАНОВКЕ**

## Bitdefender GravityZone

### Руководство по установке

Дата публикации 2021.09.30

Авторские права © 2021 Bitdefender

#### Правовое положение

**Все права защищены.** Никакая часть этой публикации не может быть воспроизведена или передана в любой форме или любыми средствами, электронными или механическими, включая фотокопирование, запись, использование средств хранения и поиска информации, без получения письменного разрешения уполномоченного представителя компании Bitdefender. Использование цитат в обзорах разрешается только со ссылкой на цитируемый источник. Запрещено вносить какие-либо изменения в данный материал.

**Предупреждение и ограничение ответственности.** Данный программный продукт и документация к нему защищены авторским правом. Данный программный продукт и документация к нему защищены авторским правом. Информация в этом документе предоставляется «как есть», без гарантии. Хотя в ходе подготовки этого документа были приняты все меры предосторожности, авторы не несут никакой ответственности перед любым лицом или организацией в отношении каких-либо потерь или ущерба, причиненных или предположительно вызванных прямо или косвенно информацией, содержащейся в документе.

Данная книга содержит ссылки на сторонние веб-сайты, не находящиеся под контролем Bitdefender, поэтому Bitdefender не несет ответственности за их содержание. Переходя на сторонние сайты, указанные в документе, вы делаете это на свой страх и риск. Bitdefender приводит эти ссылки только для удобства читателя, но наличие этих ссылок не означает, что Bitdefender берет на себя ответственность за содержание какого-либо стороннего веб-сайта.

**Торговые марки.** В этом документе могут упоминаться различные торговые марки. В этом документе могут упоминаться различные торговые марки. Все зарегистрированные и незарегистрированные торговые марки, упоминаемые в этом документе, принадлежат только их законным владельцам.

#### Правовое положение

**Все права защищены.** Никакая часть этой публикации не может быть воспроизведена или передана в любой форме или любыми средствами, электронными или механическими, включая фотокопирование, запись,

использование средств хранения и поиска информации, без получения письменного разрешения уполномоченного представителя компании Bitdefender Использование цитат в обзорах разрешается только со ссылкой на цитируемый источник. Запрещено вносить какие-либо изменения в данный материал.

**Предупреждение и ограничение ответственности.** Данный программный продукт и документация к нему защищены авторским правом. Данный программный продукт и документация к нему защищены авторским правом. Информация в этом документе предоставляется «как есть», без гарантии. Хотя в ходе подготовки этого документа были приняты все меры предосторожности, авторы не несут никакой ответственности перед любым лицом или организацией в отношении каких-либо потерь, или иного вреда, причиненного ими

вы делаете это на свой страх и риск. Bitdefender приводит эти ссылки только для удобства читателя, но наличие этих ссылок не означает, что Bitdefender берет на себя ответственность за содержание какого-либо стороннего веб-сайта.

**Торговые марки.** В этом документе могут упоминаться различные торговые марки. В этом документе могут упоминаться различные торговые марки. Все зарегистрированные и незарегистрированные торговые марки, упоминаемые в этом документе, принадлежат только их законным владельцам.

## Содержание

Предисловие .....	vii
1. Обозначения, используемые в данном руководстве .....	vii
1. О GravityZone .....	1
2. Уровни защиты GravityZone .....	2
2.1. Защита от вредоносного ПО .....	2
2.2. Расширенный контроль угроз (Advanced Threat Control) .....	4
2.3. Advanced Anti-Exploit .....	4
2.4. Брандмауэр .....	4
2.5. Контроль контента .....	4
2.6. Network Attack Defense .....	5
2.7. Управление исправлениями .....	5
2.8. Контроль устройств .....	5
2.9. Полное шифрование диска .....	6
2.10. Sandbox Analyzer .....	6
2.11. Network Traffic Security Analytics (NTSA) .....	6
2.12. Доступность уровней защиты GravityZone .....	7
3. Архитектура GravityZone .....	8
3.1. GravityZone VA .....	8
3.1.1. База данных GravityZone .....	9
3.1.2. Сервер обновлений GravityZone .....	9
3.1.3. Коммуникационный Сервер GravityZone .....	9
3.1.4. Веб-консоль (GravityZone Control Center) .....	9
3.2. Агенты безопасности .....	9
3.2.1. Bitdefender Endpoint Security Tools .....	10
3.2.2. Endpoint Security for Mac .....	12
3.3. Sandbox Analyzer Архитектура .....	12
4. Требования .....	14
4.1. Виртуальные устройства GravityZone .....	14
4.1.1. Поддерживаемые Форматы и Платформы Виртуализации .....	14
4.1.2. Оборудование .....	14
4.1.3. Подключение к сети Интернет .....	19
4.2. Control Center .....	20
4.3. Защита конечных точек .....	20
4.3.1. Оборудование .....	21
4.3.2. Поддерживаемые операционные системы .....	24
4.3.3. Поддерживаемые файловые системы .....	29
4.3.4. Поддерживаемые браузеры .....	30
4.3.5. Поддерживаемые виртуальные платформы .....	30
4.3.6. Использование трафика .....	32
4.4. Sandbox Analyzer On-Premises .....	34
4.4.1. ESXi Hypervisor .....	35
4.4.2. Sandbox Analyzer Виртуальное устройство .....	36
4.4.3. Виртуальное устройство безопасности сети .....	38

4.4.4. Требования к физическому хосту и аппаратное масштабирование . . . . .	38
4.4.5. Требования связи Sandbox Analyzer . . . . .	40
4.5. Полное шифрование диска . . . . .	41
4.6. Коммуникационные порты GravityZone . . . . .	42
<b>5. Установка защиты . . . . .</b>	<b>44</b>
5.1. Установка и настройка GravityZone . . . . .	44
5.1.1. Подготовка к установке . . . . .	44
5.1.2. Установка GravityZone . . . . .	45
5.1.3. Начальная настройка Control Center . . . . .	55
5.1.4. Настройка параметров Control Center . . . . .	57
5.1.5. Управление устройством GravityZone . . . . .	84
5.2. Управление лицензиями . . . . .	99
5.2.1. Поиск реселлера . . . . .	100
5.2.2. Ввод ваших лицензионных ключей . . . . .	100
5.2.3. Проверка текущих параметров лицензирования . . . . .	101
5.2.4. Сброс счетчика использования лицензии . . . . .	102
5.3. Установка агентов по безопасности . . . . .	102
5.3.1. Подготовка к установке . . . . .	103
5.3.2. Локальная установка . . . . .	103
5.3.3. Удаленная установка . . . . .	109
5.3.4. Подготовка систем Linux для сканирования при доступе . . . . .	115
5.3.5. Как работает сетевое обнаружение . . . . .	117
5.4. Установка Sandbox Analyzer On-Premises . . . . .	120
5.4.1. Подготовка к установке . . . . .	120
5.4.2. Разверните виртуальное устройство Sandbox Analyzer . . . . .	121
5.5. Установка полного шифрования диска . . . . .	127
5.6. Диспетчер учетных данных (Credentials Manager) . . . . .	127
5.6.1. Операционная система . . . . .	128
5.6.2. Виртуальная среда . . . . .	129
5.6.3. Удаление учетных данных из диспетчера учетных данных . . . . .	130
5.7. Bitdefender GravityZone и HIPAA . . . . .	130
5.7.1. GravityZone облачное решение . . . . .	130
5.7.2. GravityZone облачное решение . . . . .	131
<b>6. Обновление GravityZone . . . . .</b>	<b>134</b>
6.1. Обновление устройств GravityZone . . . . .	134
6.1.1. Обновление вручную . . . . .	135
6.1.2. Автоматическое обновление . . . . .	136
6.2. Настройка сервера обновлений . . . . .	137
6.3. Загрузка обновлений продуктов . . . . .	138
6.4. Обновление продукта в автономном режиме . . . . .	139
6.4.1. Требования к системе . . . . .	139
6.4.2. Настройка онлайн экземпляра GravityZone . . . . .	139
6.4.3. Настройка и загрузка начальных файлов обновлений . . . . .	140
6.4.4. Настройка автономного экземпляра GravityZone . . . . .	143
6.4.5. Использование автономных обновлений . . . . .	146
6.4.6. Использование веб-консоли . . . . .	146

7. Удаление защиты . . . . .	148
7.1. Удаление защиты конечных рабочих станций . . . . .	148
7.2. Удаление Sandbox Analyzer On-Premises . . . . .	150
7.3. Удаление ролей виртуального устройства GravityZone . . . . .	151
8. Получение справки . . . . .	154
8.1. Центр поддержки Bitdefender . . . . .	154
8.2. Обращение за помощью . . . . .	156
8.3. Использование инструментов поддержки . . . . .	156
8.3.1. Использование инструмента поддержки на операционных системах Windows . . . . .	156
8.3.2. Использование инструмента поддержки на операционных системах Linux . . . . .	158
8.3.3. Использование инструментов поддержки на операционных системах Mac . . . . .	160
8.4. Контактная информация . . . . .	161
8.4.1. Адреса веб-сайтов . . . . .	161
8.4.2. Местные дистрибуторы . . . . .	161
8.4.3. Офисы Bitdefender . . . . .	162
A. Приложения . . . . .	165
A.1. Поддерживаемые типы файлов . . . . .	165
A.2. Объекты Sandbox Analyzer . . . . .	166
A.2.1. Поддерживаемые Типы и Расширения Фалов для Отправки Вручную . . . . .	166
A.2.2. Типы Фалов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке . . . . .	166
A.2.3. Исключения По Умолчанию в Автоматической Отправке . . . . .	167
A.2.4. Рекомендуемые приложения для детонации виртуальных машин . . . . .	167

## Предисловие

Это руководство предназначено ИТ-администраторов, отвечающих за развертывание защиты GravityZone в своих организациях. ИТ-администраторы, которым необходима информация о GravityZone могут найти в этом руководстве требования GravityZone и доступные модули защиты.

Этот документ предназначен, чтобы разъяснить, как установить и настроить решение GravityZone и его агентов безопасности на всех видах конечных устройств в вашей компании.

## 1. Обозначения, используемые в данном руководстве

### Типографские обозначения

Это руководство использует несколько текстовых стилей для улучшения читаемости. Узнайте об их аспекте и значении из таблицы ниже.

Виды шрифтов и стилей	Описание
образец	Встроенные имена команд и синтаксис, пути и имена файлов, файлы конфигурации, вводимый текст печатается стандартными моноширинными шрифтами.
<a href="http://www.bitdefender.com">http://www.bitdefender.com</a>	Ссылки URL на внешние источники (http или ftp серверы).
<a href="mailto:gravityzone-docs@bitdefender.com">gravityzone-docs@bitdefender.com</a>	Адреса электронной почты в тексте приводятся в качестве контактной информации.
«Предисловие» (р. vii)	В кавычках приводятся внутренние ссылки на другие материалы в пределах этого документа.
<b>опция</b>	Все параметры продукта выделены <b>жирным</b> шрифтом.

Виды шрифтов и стилей	Описание
<b>ключевое слово</b>	Опции интерфейса, ключевые слова или сочетания клавиш выделены с помощью <b>bold</b> шрифта.

## Примечания

Примечания – это текстовая информация, выделенная в основном тексте различными средствами, целью которой является привлечение вашего внимания к дополнительной информации, имеющей отношение к содержанию текущего раздела руководства.



### Примечание

Примечание – это краткое замечание. Вы можете пропустить его, но в нем может содержаться ценная информация, например определенная особенность или ссылка на источник, имеющий отношение к данному материалу.



### Важно

Эта информация требует вашего внимания, и ее не рекомендуется пропускать. Обычно, здесь приводится важная информация о факторах, которые не имеют угрожающего характера для безопасности вашей системы.



### Предупреждение

Это критическая информация, к которой следует отнестись с максимальным вниманием. Ничего плохого не случится, если вы будете следовать указаниям. Внимательно прочтите и попытайтесь понять суть предупреждения, поскольку в нем описываются весьма опасные угрозы для безопасности вашей системы.

## 1. О GRAVITYZONE

Решение GravityZone было разработано специально для виртуализированных сред и облаков, с помощью которых можно предоставлять услуги по защите бизнеса для физических конечных устройств и виртуальных машин в частных и общедоступных облаках.

GravityZone это продукт с единой консолью управления доступной в облаке, предоставляемый Bitdefender, или организованный в качестве виртуального устройства установленного локально в компании, что обеспечивает единую точку для развертывания, соблюдения и управления политиками безопасности для любого количества конечных точек, любого типа, в любом месте.

GravityZone обеспечивает несколько уровней защиты для конечных точек: защита от вирусов с поведенческим мониторингом, защита от угроз нулевого дня, перемещение приложений в черный список и безопасную среду, файервол, управление устройствами и управление контентом.

## 2. УРОВНИ ЗАЩИТЫ GRAVITYZONE

GravityZone обеспечивает следующие уровни защиты:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Advanced Anti-Exploit
- Брандмауэр
- Контроль контента
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Network Traffic Security Analytics (NTSA)

### 2.1. Защита от вредоносного ПО

Уровень защиты от вредоносного ПО основан на сканировании сигнатур и эвристическом анализе (B-HAVE, ATC) против: вирусов, червей, троянов, программ-шпионов, рекламного ПО, кейлоггеров, рутkitов и других типов вредоносных программ.

Технология сканирования Bitdefender на наличие вредоносного ПО основана на следующих технологиях:

- Во-первых, используется традиционный метод сканирования, когда отсканированное содержимое сравнивается с базой данных сигнатур. В базе данных сигнатур содержатся записи байт-кодов, характерные для известных угроз, которые регулярно обновляются Bitdefender. Этот метод сканирования является эффективным против известных угроз, которые были исследованы и задокументированы. Тем не менее, независимо от того, насколько оперативно база данных обновляет записи, всегда есть окно уязвимости между временем, когда новая угроза обнаружена и когда исправление выпущено.
- Против новых, незарегистрированных угроз, защиту осуществляет второй слой Bitdefender, используя эвристический двигатель **B-HAVE**. Эвристические алгоритмы обнаруживают вредоносные программы на основе поведенческих характеристик. B-HAVE запускает подозрительные вредоносные программы в виртуальной среде, чтобы проверить их воздействие на систему и удостовериться, что они не представляют

никакой угрозы. Если угроза обнаружена, предотвращается запуск программы.

## Сканирующие движки

Bitdefender GravityZone может автоматически выбирать антивирусные движки при создании пакетов агентов безопасности в соответствии с конфигурацией конечной точки.

Также администратор может подстроить сканирующий движок, выбирая между несколькими технологиями сканирования:

1. **Локальное сканирование**, когда сканирование выполняется на конечном устройстве. Режим локального сканирования подходит для мощных машин, где все механизмы защиты хранятся локально.
2. **Гибридное сканирование со световыми двигателями (общее облако)**, для средних групп, использует сканирование в облаке и, частично, локальные механизмы защиты. Данный режим сканирования предоставляет лучшее задействование ресурсов, по сравнению с использованием удаленного сканирования.
3. **Централизованное сканирование в общем или частном облаке** с небольшим объемом памяти, требующим Security Server для сканирования. В этом случае механизмы защиты не хранятся локально и сканирование выгружается на Security Server.



### Примечание

Существует минимальный набор движков, хранящийся локально, необходимый для распаковки сжатых файлы.

4. **Централизованное сканирование (сканирование в частном или публичном облаке с помощью Security Server) с локальным резервом\*** (Local Scan - при наличии полных движков).
5. **Централизованное сканирование (сканирование в частном или публичном облаке с помощью Security Server) с резервом\* гибридного сканирования (Local Scan - публичное облако с облегченным движками).**

## 2.2. Расширенный контроль угроз (Advanced Threat Control)

Для угроз, которые ускользают даже от эвристического движка, присутствует еще один слой защиты в виде Advanced Threat Control (ATC).

АТС постоянно отслеживает запущенные процессы и оценивает подозрительное поведение, такое как: попытки замаскировать тип процесса, выполнение кода в пространстве памяти процесса (захват памяти для привилегированной эскалации), репликация, перемещение файлов, скрытность в списке технологических процессов и т.д. Каждое подозрительное поведение повышает рейтинг процесса. Когда достигается порог, включается сигнал тревоги.

## 2.3. Advanced Anti-Exploit

Основанная на машинном обучении, технология Advanced Anti-Exploit блокирует атаки нулевого дня, использующие трудно-обнаруживаемые эксплойты. Advanced anti-exploit в режиме реального времени отслеживает последние эксплойты и устраняет уязвимости повреждения памяти, которые могут использоваться для обхода существующих решений безопасности. Технология защищает большинство стандартных приложений, таких как браузеры, редакторы Microsoft Office и Adobe Reader и другие. Модуль следит за системными процессами и защищает от брешей в безопасности и перехватов существующих процессов.

## 2.4. Брандмауэр

Брандмауэр контролирует доступ приложений к сети и к Интернету. Доступ разрешается автоматически, основываясь на базе данных известных, легитимных приложений. Кроме того, брандмауэр может защитить систему от сканирования портов, ограничивать использование общего доступа к Интернет (ICS) и предупредить, когда новые узлы подключаются по Wi-Fi.

## 2.5. Контроль контента

Модуль Контентного Контроля помогает обеспечить соблюдение политики компании в отношении разрешенного трафика, веб-доступа, защиты данных и контроля приложений. Администраторы могут задавать параметры сканирования трафика и исключения, составлять график доступа к веб, блокировать или разрешать определенные веб-адреса или категории,

настраивать правила защиты данных и устанавливать разрешения для использования конкретных приложений.

## 2.6. Network Attack Defense

Модуль Network Attack Defense опирается на технологии Bitdefender, нацеленные на распознание сетевых атак, целью которых является получение доступа к конечным точкам при помощи таких средств как: атаки методом перебора, сетевые "эксплоиты", программы для кражи паролей, векторы заражения посредством скрытой загрузки, боты и трояны.

## 2.7. Управление исправлениями

Полностью интегрированный в GravityZone, модуль управления исправлениями поддерживает последнюю версию операционной системы и приложений, а также обеспечивает полное представление о состоянии исправления в управляемых точках Windows.

Модуль управления исправлениями GravityZone включает несколько особенностей, таких как сканирование патчей по требованию / запланированное, автоматическое / ручное сканирование исправлений или создание отчетов об отсутствующих патчах.

Вы можете узнать больше о продавцах и продуктах управления исправлениями GravityZone из этой [статьи базы знаний](#).



### Примечание

Модуль управления исправлениями - это дополнение, доступное при наличии отдельного лицензионного ключа для всех доступных пакетов GravityZone.

## 2.8. Контроль устройств

Модуль Контроля устройств позволяет предотвратить утечки конфиденциальных данных и проникновение вредоносного ПО через внешние устройства, подключаемые к конечным точкам, применяя блокирующие правила и исключения с помощью политик для широкого спектра устройств (таких, как USB флэш-накопители, устройства Bluetooth, CD/DVD-плееры, устройства хранения, и т.д.).

## 2.9. Полное шифрование диска

Данный уровень защиты позволяет Вам осуществлять шифрование всего диска на машине, управляя BitLocker для Windows, и FileVault и diskutil для macOS. Вы можете зашифровать и дешифровать загрузочные и обычные тома одним щелчком мыши, т.к. GravityZone обрабатывает весь процесс с минимальным вмешательством со стороны пользователей. Кроме того, GravityZone хранит ключи восстановления, необходимые для разблокировки томов, на тот случай, если пользователь забыл свой пароль.

### Примечание

Полное шифрование диска - это дополнение, доступное при наличии отдельного лицензионного ключа для всех доступных пакетов GravityZone.

## 2.10. Sandbox Analyzer

Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от продвинутых угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусным движком Bitdefender. Безопасная среда использует обширный набор технологий Bitdefender для размещения полезных данных в развернутой локально виртуальной среде, анализирует их поведение и сообщает о небольших системных изменениях, которые могут свидетельствовать о вредоносной природе.

Sandbox Analyzer использует ряд сенсоров для проверки данных от сетевых потоков трафика, централизованного карантина и ICAP серверов.

Кроме того, Sandbox Analyzer позволяет передать образцы вручную и через API.

### Примечание

Функциональность этого модуля обеспечивает Sandbox Analyzer On-Premises, который доступен по отдельному лицензионному ключу.

## 2.11. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) - сетевое решение безопасности, которое анализирует потоки трафика IPFIX на наличие подозрительного поведения и вредоносного ПО.

Bitdefender NTSA предназначен для того, чтобы действовать наряду с вашими существующими мерами безопасности как дополнительная гарантия, которая

способна покрыть слепые зоны, не отслеживаемые традиционными инструментами.

Традиционные инструменты безопасности сетей обычно пытаются предотвратить вредоносные заражения анализируя входящий трафик (с помощью песочницы, брандмауэра, антивируса и т.д.) Bitdefender NTSA фокусируется исключительно на анализе исходящего сетевого трафика на наличие подозрительного поведения.

## 2.12. Доступность уровней защиты GravityZone

Уровни защиты GravityZone отличаются в зависимости от операционной системы на конечной точке. Чтобы узнать больше, обратитесь к статье [Доступность слоев защиты GravityZone](#) в Базе Знаний.

### 3. АРХИТЕКТУРА GRAVITYZONE

Уникальная архитектура GravityZone позволяет с легкостью масштабировать решение и защитить любое количество систем. GravityZone может быть настроена на использование нескольких виртуальных устройств и множество экземпляров конкретных ролей (база данных, коммуникационный сервер, сервер обновлений и веб-консоль), чтобы обеспечить надежность и масштабируемость.

Каждый экземпляр роли может быть установлен на разных устройствах. Встроенные балансировщики ролей позволяют доказать, что развертывание GravityZone защитит даже самые крупные корпоративные сети, не вызывая замедления или узкие места. Уже существующие программные или аппаратные балансировщики также могут быть использованы вместо встроенной балансировки, если они присутствуют в сети.

Поставляясь в качестве виртуального контейнера, GravityZone может быть импортирована на любую платформу виртуализации, включая VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure.

Интеграция с VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element и Microsoft Azure упрощает развертывание защиты как для физических, так и для виртуальных машин.

Решение GravityZone включает в себя следующие компоненты:

- Виртуальные устройства GravityZone
- Агенты безопасности

#### 3.1. GravityZone VA

Локальное решение GravityZone поставляется как настроенное виртуальное устройство на базе Linux Ubuntu, встроенное в образ виртуальной машины, которое можно легко установить и настроить через CLI (Интерфейс командной строки). Виртуальное устройство доступно в нескольких вариантах, совместимых с основными платформами виртуализации (OVA, XVA, VHD, OVF, RAW).

### 3.1.1. База данных GravityZone

Центральная логика архитектуры GravityZone. Bitdefender использует не-реляционную базу данных MongoDB, которую легко масштабировать и реплицировать.

### 3.1.2. Сервер обновлений GravityZone

Сервер обновлений играет важную роль в обновлении решения GravityZone и конечных агентов путем репликации и публикации необходимых пакетов или установочных файлов.

### 3.1.3. Коммуникационный Сервер GravityZone

Коммуникационный Сервер является связующим звеном между агентами безопасности и базами данных, передавая политики и задачи для защиты конечных точек, а также генерируя отчеты от агентов безопасности.

### 3.1.4. Веб-консоль (GravityZone Control Center)

Решения безопасности Bitdefender управляются в GravityZone из единой точки управления - веб-консоли Control Center, которая обеспечивает более легкое управление и доступ к полным настройкам безопасности, глобальным угрозам безопасности, а также полный контроль над всеми модулями безопасности, защищающих виртуальные или физические настольные компьютеры и серверы. Работая на архитектуре Gravity, Control Center способна удовлетворить потребности даже самых крупных организаций.

Control Center интегрируется с существующими системами управления и мониторинга, чтобы упростить автоматическое применение защиты к неуправляемым рабочим станциям или серверам, находящимся в службе каталогов Microsoft Active Directory, или которые были просто обнаружены в сети.

## 3.2. Агенты безопасности

Чтобы Bitdefender защитил вашу сеть, необходимо установить соответствующих агентов безопасности GravityZone на сетевых конечных точках.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

### 3.2.1. Bitdefender Endpoint Security Tools

GravityZone обеспечивает защиту физических и виртуальных Windows и Linux машин с помощью Bitdefender Endpoint Security Tools - интеллектуального агента, который адаптируется к типу конечной точки. Bitdefender Endpoint Security Tools может быть развернут на любой машине, как физической так и виртуальной, обеспечивая гибкую систему сканирования и являясь идеальным выбором для смешанных сред (физических, виртуальных и облачных).

Bitdefender Endpoint Security Tools использует единый шаблон политики для физических и виртуальных устройств, а также один установочный комплект для любой среды (физической или виртуальной), работающей на Windows.

#### Слои защиты

Следующие уровни защиты доступны в Bitdefender Endpoint Security Tools:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Брандмауэр
- Контроль контента
- Network Attack Defense
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска

#### Роли конечных точек

- Привилегированный пользователь
- Ретранслятор
- Сервер кэширования патчей

#### Привилегированный пользователь

Администраторы Центра управления (Control Center) могут предоставлять права привилегированных пользователей обычным пользователям конечных устройств с помощью параметров политики безопасности. Модуль привилегированных пользователей разрешает предоставление администраторских прав уровню пользователей, которые разрешат конечным пользователям получать доступ и изменять настройки безопасности, используя локальную консоль. Control Center будет уведомлена, когда

конечная точка находится в режиме привилегированного пользователя и администратор Control Center всегда может переназначить локальные настройки безопасности.



### Важно

Этот модуль доступен только для поддерживаемых настольных и серверных операционных систем Windows. Для получения более подробной информации, обратитесь к «Поддерживаемые операционные системы» (р. 24).

## Ретранслятор

Агенты конечных точек с ролью Bitdefender Endpoint Security Tools Relay выступают как прокси-сервер и сервер обновлений для других конечных точек в сети. Агенты конечных устройств с ролью ретранслятора особенно необходимы в организациях с изолированными сетями, где весь трафик проходит через единую точку доступа.

В компаниях с распределенными сетями, агенты-ретрансляторы помогают снизить использование полосы пропускания, предотвращая непосредственное подключение защищаемой конечной точки к устройству GravityZone.

После того, как агент Bitdefender Endpoint Security Tools Relay установлен в сети, другие конечные точки могут быть сконфигурированы с помощью политик, чтобы общаться с Control Center через агента ретрансляции.

Агенты Bitdefender Endpoint Security Tools Relay служат для следующих целей:

- Обнаружение всех незащищенных конечных точек в сети.
- Разворачивание агентов конечных точек внутри локальной сети.
- Обновление защищаемых конечных точек в сети.
- Обеспечение связи между Control Center и подключенными конечными точками.
- Выступать в качестве прокси-сервера для защищаемых конечных точек.
- Оптимизации сетевого трафика во время обновления, развертывания, сканирования и других ресурсоемких задач.

## Сервер кэширования патчей

Конечные точки с ролью ретранслятора также могут выступать в качестве сервера кэширования исправлений. При включении этой роли ретрансляторы служат для хранения исправлений программного обеспечения, загружаемых с веб-сайтов поставщиков, и их распространения на конечные точки сети. Всякий раз, когда подключенная конечная точка имеет программное

обеспечение с отсутствующими исправлениями, она берет их с сервера, а не с веб-сайта поставщика, таким образом оптимизируя генерируемый трафик и нагрузку на пропускную способность сети.



### Важно

Эта дополнительная роль доступна с зарегистрированной надстройкой Patch Management.

## 3.2.2. Endpoint Security for Mac

Endpoint Security for Mac - это агент безопасности, предназначенный для защиты рабочих станций Macintosh и ноутбуков с процессорами Intel или Apple M1. В качестве технологии сканирования доступно **Локальное сканирование**, с локально расположенными механизмами защиты.

### Слои защиты

Следующие уровни защиты доступны в Endpoint Security for Mac:

- [Защита от вредоносного ПО](#)
- [Расширенный контроль угроз \(Advanced Threat Control\)](#)
- Контроль контента
- Контроль устройств
- Полное шифрование диска
- Обнаружение и отклик конечной точки (EDR)

## 3.3. Sandbox Analyzer Архитектура

Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от новейших угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусными ядрами Bitdefender.

Чтобы использовать данный модуль совместно с GravityZone, вам необходимо установить Sandbox Analyzer On-Premises.

### Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises представляет собой виртуальное устройство Linux Ubuntu, встроенное в образ виртуальной машины, его можно легко установить и сформировать при помощи интерфейса командной строки (CLI). Sandbox Analyzer On-Premises доступен в формате OVA, также может быть развернут в VMWare ESXi.

Экземпляр Sandbox Analyzer On-Premises содержит в себе следующие компоненты:

- **Менеджер песочницы.** Это компонент является оркестром песочницы. Sandbox Manager связывается с гипервизором ESXi посредством API и использует их технические оснащение для постройки и эксплуатации среды анализа вредоносных программ.
- **Виртуальная машины детонации.** Данный компонент состоит из машин, используемых Sandbox Analyzer, для создания файлов и анализа их режима работы. Виртуальные машины детонации могут управлять Windows 7, а также 64-разрядной версией системы Windows 10.

**GravityZone Control Center** работает как консоль управления и отчетности, где вы настраиваете политики безопасности и просматриваете аналитические отчеты и уведомления.

Sandbox Analyzer On-Premises управляет следующими датчики подачи:

- **Сетевой датчик.** Виртуальное устройство сетевой безопасности (NSVA) - это виртуальное устройство, которое можно развернуть в той же виртуализированной среде ESXi, что и экземпляр Sandbox Analyzer. Датчик сети извлекает контент из сетевых потоков и передает его в Sandbox Analyzer.
- **Датчик ICAP.** Развернутая на устройствах с сетевым хранилищем (NAS) по протоколу ICAP, Bitdefender Security Server поддерживает отправку содержимого в Sandbox Analyzer.

В дополнение к этим датчикам Sandbox Analyzer On-Premises поддерживает ручную отправку и через API. Подробнее см. Главу **Использование Sandbox Analyzer** в Руководстве администратора GravityZone.

## 4. ТРЕБОВАНИЯ

Все решения GravityZone устанавливаются и управляются посредством Control Center.

### 4.1. Виртуальные устройства GravityZone

#### 4.1.1. Поддерживаемые Форматы и Платформы Виртуализации

GravityZone представляет собой виртуальное устройство (VA). Оно доступно в следующих форматах, которые поддерживают большинство стандартных платформ виртуализации:

- OVA (совместимо с VMware vSphere, View, VMware Player)
- XVA (совместимо с Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (совместимо с Microsoft Hyper-V)
- VMDK (совместимо с Nutanix Prism)
- OVF (совместимо с Red Hat Enterprise Virtualization)\*
- OVF (совместимо с Oracle VM)\*
- RAW (совместимо с Kernel-based Virtual Machine или KVM)\*

\*OVF и RAW пакеты заархивированы в tar.bz2 формат.

Для проверки совместимости платформы Oracle VM VirtualBox смотрите [эту статью базы знаний](#).

Поддержка других форматов и платформ виртуализации могут быть предоставлены по запросу.

#### 4.1.2. Оборудование

Требования к оборудованию виртуального устройства GravityZone варьируются в зависимости от вашей сети и выбранной архитектуры установки. Для сетей до 3000 машин вы можете выбрать установку всех ролей GravityZone на одном устройстве, в то время как для больших сетей вам необходимо распределить роли между несколькими устройствами. Ресурсы, необходимые устройству, зависят от устанавливаемых на него ролей и от того, будете ли вы использовать Replica Set

**Примечание**

Replica Set - это функция базы данных MongoDB, которая поддерживает репликацию базы данных и обеспечивает высокую отказоустойчивость сохраненной информации. За подробной информацией, обратитесь к [документации MongoDB](#) и «Управление устройством GravityZone» (р. 84).

**Важно**

Данные измерения - результат внутренних тестов Bitdefender на базовой конфигурации GravityZone при регулярном использовании. Результаты могут варьироваться в зависимости от конфигурации сети, установленного ПО, количества событий и т.д. Для нестандартных показателей масштабирования, пожалуйста, обратитесь к Bitdefender.

**vCPU**

Следующая таблица показывает необходимое количество vCPU для каждой роли виртуального устройства.

Каждый vCPU должен иметь частоту минимум 2GHz.

Компонент	Количество машин							
	250	500	1000	3000	5000	10000	25000	50000
<b>Базовые функции GravityZone</b>								
Сервер обновлений*					4	4	6	8
Веб-консоль**					6	10	12	12
Коммуникационный Сервер	8	12	14	16		6	10	12
База данных ***					6	6	9	12
<b>Общее количество</b>	<b>8</b>	<b>12</b>	<b>14</b>	<b>16</b>	<b>22</b>	<b>30</b>	<b>39</b>	<b>50</b>
<b>GravityZone с Bitdefender HVI</b>								
Сервер обновлений*		4	4	4	4	4	6	8
Веб-консоль**		6	8	8	10	10	12	12
Коммуникационный Сервер	8	6	8	8	10	10	16	20
База данных ***		6	6	6	6	6	9	12
<b>Общее количество</b>	<b>8</b>	<b>22</b>	<b>26</b>	<b>26</b>	<b>30</b>	<b>30</b>	<b>43</b>	<b>52</b>

\* Рекомендовано, если не установлено ни одного Релея

\*\* Для каждой активной интеграции Добавьте один vCPU на виртуальное устройство с ролью Веб-консоли.

\*\*\* В случае распределенной установки ролей, вместе с Replica Set: для каждого дополнительного экземпляра Базы данных добавьте указанное число к общей сумме.

## ОЗУ (ГБ)

Компонент	Количество машин							
	250	500	1000	3000	5000	10000	25000	50000
<b>Базовые функции GravityZone</b>								
Сервер обновлений					2	2	3	3
Веб-консоль*					8	8	12	16
Коммуникационный Сервер	16	16	18	20	6	12	12	16
База данных **					8	10	12	12
<b>Общее количество</b>	<b>16</b>	<b>16</b>	<b>18</b>	<b>20</b>	<b>24</b>	<b>32</b>	<b>39</b>	<b>47</b>
<b>GravityZone с Bitdefender HVI</b>								
Сервер обновлений		2	2	2	2	2	3	3
Веб-консоль*		8	10	10	10	10	12	16
Коммуникационный Сервер	16	8	10	10	12	12	16	20
База данных **		8	8	8	8	12	12	12
<b>Общее количество</b>	<b>16</b>	<b>26</b>	<b>30</b>	<b>30</b>	<b>32</b>	<b>36</b>	<b>43</b>	<b>51</b>

\* Для каждой активной интеграции добавьте 1 GB RAM на виртуальное устройство с ролью Веб-консоли.

\*\* В случае распределенной установки ролей, вместе с Replica Set: для каждого дополнительного экземпляра Базы данных добавьте указанное число к общей сумме.

## Свободное пространство на диске (GB)

Компонент	Количество машин								
	250	250*	500	1000	3000	5000	10000	25000	50000
<b>Базовые функции GravityZone</b>									
Сервер обновлений							80	80	80
Веб-консоль							80	80	80
Коммуникационный Сервер	120	160	160	200	200		80	80	80
База данных **							80	120	200
<b>Общее количество</b>	<b>120</b>	<b>160</b>	<b>160</b>	<b>200</b>	<b>200</b>	<b>320</b>	<b>360</b>	<b>440</b>	<b>740</b>
<b>GravityZone с Bitdefender HVI</b>									
Сервер обновлений				80	80	80	80	80	80
Веб-консоль				80	80	80	80	80	80
Коммуникационный Сервер	120	160		80	80	80	80	80	80
База данных **				80	80	100	100	160	300
<b>Общее количество</b>	<b>120</b>	<b>160</b>	<b>320</b>	<b>320</b>	<b>340</b>	<b>340</b>	<b>400</b>	<b>540</b>	<b>940</b>



### Важно

Настоятельно рекомендуем использовать Solid-state drives (SSDs).

\* При выборе автоматической установки требуется дополнительное место на SSD, так как дополнительно проводится установка Security Server. После установки вы можете удалить Security Server, чтобы освободить место на жестком диске.

\*\* В случае распределенной установки ролей, вместе с Replica Set: для каждого дополнительного экземпляра Базы данных добавьте указанное число к общей сумме.

## Контроль приложений

В зависимости от количества конечных точек, использующих управление приложениями, GravityZone предъявляет особые требования к оборудованию и развертыванию:

Количество конечных точек	Минимальная рекомендуемая GravityZone конфигурация
< 500	Все роли установлены на одном устройстве
500 - 2999	Распространение среды, одна роль для каждого применения
3000 - 4999	Распространённая среда: <ul style="list-style-type: none"><li>● 3 x роль сервера базы данных</li><li>● 2 x роль сервера связи</li><li>● 1 x роль веб-консоли</li><li>● 1 x Роль сервера обновлений</li></ul>
5000 - 9999	Распространённая среда: <ul style="list-style-type: none"><li>● 3 x роль сервера базы данных</li><li>● 2 x роль сервера связи</li><li>● 1 x роль веб-консоли</li><li>● 1 x Роль сервера обновлений</li></ul>
10000 - 24999	Распространённая среда: <ul style="list-style-type: none"><li>● 3 x роль сервера базы данных</li><li>● 2 x роль сервера связи</li><li>● 2 x роль веб-консоли</li><li>● 1 x Роль сервера обновлений</li></ul>
25000 - 49999	Распространённая среда: <ul style="list-style-type: none"><li>● 3 x роль сервера базы данных</li><li>● 2 x роль сервера связи</li></ul>

Количество конечных точек	Минимальная рекомендуемая GravityZone конфигурация
	<ul style="list-style-type: none"><li>● 2 x роль веб-консоли</li><li>● 1 x Роль сервера обновлений</li></ul>
50000 <	Распространённая среда: <ul style="list-style-type: none"><li>● 3 x Сервер базы данных, настроенный в наборе реплик, по крайней мере, с 3 участниками</li><li>● 2 x роль сервера связи</li><li>● 2 x роль веб-консоли</li><li>● 1 x Роль сервера обновлений</li></ul>

Если у Вас есть конечные точки с большим количеством установленных приложений, что означает высокую нестабильность всей инфраструктуры, рассмотрите следующий уровень спецификаций, чтобы убедиться, что все работает должным образом.

Для распределенной среды: каждая роль имеет минимальную конфигурацию аппаратного обеспечения:

- 4 x vCPUs
- 8 ГБ ОЗУ
- Тонкое подготовленное хранилище SDD емкостью 120 ГБ

#### 4.1.3. Подключение к сети Интернет

Устройству GravityZone требуется доступ к Интернет.

## 4.2. Control Center

Для доступа к Web-консоли Control Center требуется следующее:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Рекомендуемое разрешение экрана 1280 x 800 или выше
- Для доступа к Control Center компьютер должен быть подключен к сети.



### Предупреждение

Control Center не будет работать должным образом / отображаться в Internet Explorer 9 и выше с включенным режимом совместимости, что эквивалентно использованию неподдерживаемой версии браузера.

## 4.3. Защита конечных точек

Чтобы защитить вашу сеть с помощью Bitdefender, вы должны установить агентов безопасности GravityZone на конечных рабочих станциях сети. Для этого вам нужен пользователь Control Center с правами администратора на услуги, которые вы должны установить, и на конечные точки сети, находящиеся под вашим управлением.

Требования к агенту безопасности отличаются в зависимости от наличия дополнительных ролей, таких как Ретранслятор, Защита при обмене или Сервер кеширования патчей. Для получения более подробной информации о роли агента обратитесь к [«Агенты безопасности»](#) (р. 9).

### 4.3.1. Оборудование

#### Агент безопасности без ролей

##### Использование ЦП

Целевые системы	Тип ЦП	Поддерживаемые ОС
Рабочие станции	Совместимые процессоры Intel® Pentium 2 GHz или быстрее	Настольная ОС Microsoft Windows
	Intel® Core 2 Duo, 2 GHz или быстрее Apple M1	ОС MAK
Умные устройства	Совместимые процессоры Intel® Pentium 800 MHz или быстрее	Встроенные ОС Microsoft Windows
Серверы	Минимум: совместимые процессоры Intel® Pentium, 2.4 GHz	Сервер ОС Microsoft Windows и ОС Linux
	Рекомендуется: Intel® Xeon multi-core CPU, 1.86 GHz или быстрее	

#### Свободная оперативная память

##### Во время установки (МБ)

ОС	Один движок					
	Локальное сканирование		Гибридное сканирование		Централизованное сканирование	
	Только AV	Полные опции	Только AV	Полные опции	Только AV	Полные опции
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
ОС MAK	1024	1024	н/д	н/д	н/д	н/д

##### Для ежедневного использования (МБ) \*

ОС	Антивирус (Одиночный процессор)			Поведенческая проверка	Брандмаузер	Мониторинг
	Локальный	Гибридный	Централизованный			
Windows	75	55	30	+13	+17	
Linux	200	180	90	-	-	
ОС MAK	650	-	-	+100	-	

\* Измерения охватывают ежедневную активность клиентов конечных устройств, без учета дополнительных задач, таких как сканирование по запросу или обновление продукта.

### Свободное пространство на диске

#### Во время установки (МБ)

ОС	Один движок						Двойной движок	
	Локальное сканирование		Гибридное сканирование		Централизованное сканирование		Централизованное + локальное сканирование	
	Только AV	Полные опции	Только AV	Полные опции	Только AV	Полные опции	Только AV	Полные опции
Windows	1024	1200	500	700	350	570	1024	1200
Linux	1600	1600	1100	1100	600	600	1600	1600
ОС MAK	1024	1024	н/д	н/д	н/д	н/д	н/д	н/д

#### Для ежедневного использования (МБ) \*

ОС	Антивирус (Одиночный процессор)			Поведенческая проверка	Брандмаузер	Мониторинг
	Локальный	Гибридный	Централизованный			
Windows	410	190	140	+12	+5	
Linux	500	200	110	-	-	
ОС MAK	1700	-	-	+20	-	

\* Измерения охватывают ежедневную активность клиентов конечных устройств, без учета дополнительных задач, таких как сканирование по запросу или обновление продукта.

## Агент безопасности с ролью ретранслятора

Роль ретранслятора требует аппаратных ресурсов помимо базовых конфигураций агента безопасности. Эти требования необходимы, чтобы поддерживать Сервер обновлений и установочные пакеты, размещенные в конечной точке:

Количество связанных конечных точек	Центральный процессор (CPU) для поддержки Сервера обновлений	ОЗУ	Свободное пространство на диске для Сервера обновлений
1-300	Минимум Intel® Core™ i3 или эквивалент, 2 vCPU на ядро	1,0 ГБ	10 ГБ
300-1000	Минимум Intel® Core™ i5 или эквивалент, 4 vCPU на ядро	1,0 ГБ	10 ГБ



### Предупреждение

- Для агентов-ретрансляторов необходимы SSD диски для реализации большого количества операций чтения\записи.



### Важно

- Если вы хотите сохранить установочные пакеты и обновления в другом разделе, чем тот, в котором установлен агент, убедитесь, что на обоих разделах достаточно свободного пространства (10 ГБ), в противном случае агент прерывает установку. Это требование только при установке.
- Для конечных точек Windows, local to local символические ссылки должны быть включены.

## Агент безопасности с функцией сервера кеширования патчей

Агент с функцией сервера кеширования патчей должен иметь следующие совокупные требования:

- Все требования к устройству для обычного агента безопасности (без дополнительных функций)
- Все требования к устройству для функции ретранслятора
- Дополнительно 100 ГБ свободного дискового пространства для хранения загруженных патчей

**Важно**

Если вы хотите сохранить патчи в другом разделе, чем тот, в котором установлен агент, убедитесь, что на обоих разделах достаточно свободного пространства (100 ГБ), в противном случае агент прерывает установку. Это требование только при установке.

### 4.3.2. Поддерживаемые операционные системы

#### Рабочий стол Windows

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

**Предупреждение**

Bitdefender не поддерживает сборки Windows Insider Program.

## Планшет Windows и встроенная ОС

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

## Сервер Windows

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

## Linux



### Важно

Конечные точки Linux используют места лицензий из лицензий для серверных ОС.

- Ubuntu 14.04 LTS или выше
- Red Hat Enterprise Linux / CentOS 6. 0 или выше <sup>(2)</sup>
- SUSE Linux Enterprise Server 11 SP4 или выше
- OpenSUSE Leap 42.x
- Fedora 25 или выше<sup>(1)</sup>
- Debian 8.0 или более поздняя версия
- Oracle Linux 6. 3 или более поздняя версия

- Amazon Linux AMI 2016.09 или выше
- Amazon Linux 2



### Предупреждение

(1) В Fedora 28 и выше Bitdefender Endpoint Security Tools требует ручной установки пакета libnsl, выполнив следующую команду:

```
sudo dnf install libnsl -y
```

(2) Для минимальной установки CentOS Bitdefender Endpoint Security Tools требуется ручная установка пакета libnsl, выполнив следующую команду:

```
sudo yum install libnsl
```

### Необходимые компоненты Active Directory

При интеграции конечных точек Linux с доменом Active Directory с помощью демона службы безопасности системы (SSSD) убедитесь, что инструменты ldbsearch, krb5-user, и krb5-config установлены, и Kerberos настроен правильно.

```
/etc/krb5.conf

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    default_realm = DOMAIN.NAME
    dns_lookup_realm = true
    dns_lookup_kdc = true
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    fcc-mit-ticketflags = true
    default_keytab_name = FILE:/etc/krb5.keytab
```

```
[realms]
DOMAIN.NAME = {
    kdc = dc1.domain.name
    kdc = dc2.domain.name
    admin_server = dc.domain.com
    default_domain = domain.com
}

[domain_realm]
domain.name = DOMAIN.NAME
.domain.name = DOMAIN.NAME

[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```



### Примечание

Все записи чувствительны к регистру.

## Поддержка сканирования при доступе

Сканирование при доступе доступно для всех поддерживаемых гостевых операционных систем. В системах Linux, сканирование при доступе обеспечивается в следующих ситуациях:

Версии ядра	Дистрибутивы Linux	Требования к доступу
2.6.38 или более поздняя версия	Red Hat Enterprise Linux / <b>Fanotify</b> (опция ядра) должна CentOS 6.0 или более поздней быть включена. версии	

Версии ядра	Дистрибутивы Linux	Требования к доступу
	OpenSUSE Leap 42.x Fedora 25 или выше Debian 9.0 или более поздняя версия Oracle Linux 6. 3 или более поздняя версия Amazon Linux AMI 2016.09 или выше	
2.6.38 или выше	Debian 8	<b>Fanotify</b> должен быть включен и установлен в режим принудительного применения, затем необходимо перестроить пакет ядра. Для получения подробной информации смотрите <a href="#">эту статью базы знаний</a> .
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender обеспечивает поддержку через <b>DazukoFS</b> помошью встроенных модулей ядра.
Все остальные ядра	Все другие поддерживаемые системы	Модуль <b>DazukoFS</b> должен быть скомпилирован вручную. Дополнительные сведения см. в разделе <a href="#">«Компиляция вручную модуля DazukoFS»</a> (п. 115).

\* С некоторыми ограничениями, описанными ниже.

## Ограничения сканирования при доступе

Версии ядра	Дистрибутивы Linux	Подробная информация
2.6.38 или выше	Все поддерживаемые системы	<p>Сканирование при доступе контролирует подключенные сетевые ресурсы только в следующих условиях:</p> <ul style="list-style-type: none"> <li>● <b>Fanotify</b> включается как на удаленных, так и на локальных системах.</li> <li>● Общий ресурс основан на файловых системах CIFS и NFS.</li> </ul> <p> <b>Примечание</b> Сканирование при доступе не сканирует сетевые ресурсы, установленные с помощью SSH или FTP.</p>
Все ядра	Все поддерживаемые системы	Сканирование при доступе не поддерживается в системах с <b>DazukoFS</b> для сетевых ресурсов, установленных на путях, уже защищенных модулем доступа.

## ОС MAK

- macOS Big Sur (11.x)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

### 4.3.3. Поддерживаемые файловые системы

Bitdefender устанавливает и защищает следующие файловые системы:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

**Примечание**

Для NFS и CIFS / SMB поддержка сканирования по доступу не предусмотрена.

#### 4.3.4. Поддерживаемые браузеры

Безопасность браузера конечной точки проверяется, чтобы обеспечить работу со следующими браузерами:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

#### 4.3.5. Поддерживаемые виртуальные платформы

Security for Virtualized Environments обеспечивает поддержку "из коробки" следующих платформ виртуализации:

- VMware vSphere & vCenter Server 7.0 обновление 1 7.0, 6.7 обновление 3, обновление 2a, 6.7 обновление 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

**Примечание**

Функция управления рабочей нагрузкой в vSphere 7.0 не поддерживается.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix Hypervisor 8.2 LTSR, XenServer 7.1 LTSR
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 или Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (включая Hypervisor Hyper-V)

- Red Hat Enterprise Virtualization 3.0 (включая KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism при AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism при AOS 5.6, 5.11 5.18 STS
- Призма Nutanix с AHV 20170830.115, 20170830.301, 20170830.395 и 20190916.294 Выпуск сообщества



### Примечание

Поддержка других форматов и платформ виртуализации может быть предоставлена по запросу.

## Поддерживаемые Облачные Платформы

Наряду с локальными средами виртуализации, GravityZone может также интегрировать со следующими облачными платформами:

- **Amazon EC2**

Как клиент Amazon EC2 вы можете интегрировать инвентарь экземпляров EC2, сгруппированных по регионам и зонам доступности, с сетевым инвентарем GravityZone.

- **Microsoft Azure**

Как клиент Microsoft Azure вы можете интегрировать виртуальные машины Microsoft Azure, сгруппированные по регионам и зонам доступности, с сетевым инвентарем GravityZone.

## Совместимость с рабочим столом и технологиями виртуализации приложений

GravityZone совместим со следующими технологиями виртуализации, начиная с Bitdefender Endpoint Security Tools версии 6.6.16.226:

- **VMware:**

VMware V-App (та же версия при vCenter Server)

VMware ThinApp 5.2.6

VMware AppVolumes 2.180

**Важно**

Рекомендуется не устанавливать в стек приложений или записываемые Тома.

- **Microsoft:**

Microsoft Приложение-V 5.0, 5.1

Microsoft FSLogix 2.9.7237

- **Citrix:**

Наслоение приложений Citrix 19.10

Citrix Appdisks 7.12

**Важно**

Назначьте политики на основе пользовательских правил, чтобы управление устройствами не препятствовало созданию уровней ОС и платформы.

Возможно, Вам потребуется настроить правила Firewall GravityZone, чтобы разрешить работу сетевого трафика для каждого из этих приложений. Для получения более подробной информации обращайтесь к [Документация продукта о наслоении приложений Citrix](#).

## Поддерживаемые инструменты управления виртуализацией

Control Center в настоящее время интегрируется со следующими инструментами управления виртуализацией:

- VMware vCenter Server
- Citrix XenServer
- Nutanix Prism Element

Чтобы настроить интеграцию, необходимо указать имя пользователя и пароль администратора.

### 4.3.6. Использование трафика

- **Трафик обновления продукта между клиентом конечного устройства и сервером обновлений**

Каждое периодическое обновление продукта Bitdefender Endpoint Security Tools генерирует следующий исходящий трафик на каждом клиенте конечной точки:

- На Windows ОС: ~20 МБ
- На Linux ОС: ~26 МБ
- На ОС Mac: ~25 МБ
- **Загружаемый трафик обновлений механизмов защиты между клиентом конечной точки и Сервером обновлений (МВ / день)**

Тип сервера обновлений	Тип движка сканирования		
	Локальный	Гибридный	Централизованное
Ретранслятор	65	58	55
Bitdefender Публичный Сервер Обновлений	3	3.5	3

- **Трафик централизованного сканирования между клиентом конечной точки и Security Server**

Проверенные объекты	Тип трафика		Загрузка (МБ)	Выгрузка (МБ)
Файлы*	Первое сканирование		27	841
	Кэширующее сканирование		13	382
Веб-сайты**	Первое сканирование	Веб-трафик	621	Данные отсутствуют
		Security Server	54	1050
	Кэширующее сканирование	Веб-трафик	654	Данные отсутствуют
		Security Server	0.2	0.5

\* Представленные данные были измерены при размере файлов 3.49 ГБ (6 658 файлов), 1.16 ГБ из которых исполняемые портируемые файлы(Portable Executable - PE).

\*\* Представленные данные были измерены для топ-рейтинга 500 веб-сайтов.

- **Трафик гибридного сканирования между клиентом конечной точки и облачным сервисом Bitdefender**

Проверенные объекты	Тип трафика	Загрузка (МБ)	Выгрузка (МБ)
Файлы*	Первое сканирование	1.7	0.6
	Кэширующее сканирование	0.6	0.3
Веб-трафик**	Веб-трафик	650	Данные отсутствуют
	Облачные услуги Bitdefender	2.6	2.7

\* Представленные данные были измерены при размере файлов 3.49 ГБ (6 658 файлов), 1.16 ГБ из которых исполняемые портируемые файлы(Portable Executable - PE).

\*\* Представленные данные были измерены для топ-рейтинга 500 веб-сайтов.

- **Трафик загрузки механизмов защиты между клиентами Bitdefender Endpoint Security Tools Relay и Сервером обновлений**

Клиенты с ролью Bitdefender Endpoint Security Tools Relay скачивают ~16 МБ / день\* с сервера обновлений.

\* Доступно для клиентов Bitdefender Endpoint Security Tools, начиная с версии 6.2.3.569.

- **Трафик между клиентами конечных устройств и web-консолью Control Center**

Средний трафик, генерируемый между клиентами конечных устройств и web-консолью Control Center, составляет 618 КБ / день.

#### 4.4. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises имеет конкретные требования:

- **ESXi Гипервизор** (платформа виртуализации, запускающая среду).

- **Sandbox Analyzer** Виртуальное устройство (устройство, которое будет управлять виртуальными машинами детонации).
- **Виртуальное устройство сетевой безопасности** (VM, инкапсулирующая сетевой датчик, способный извлекать полезную нагрузку из сетевого трафика).
- Подключение к существующей GravityZone Control Center, используемой для высокоуровневого управления средой песочницы.
- Интернет-соединение для загрузки виртуального устройства Sandbox Analyzer с минимальной пропускной способностью 5 Мбит/с.



### Важно

Убедитесь, что нет других приложений или процессов, которые могут блокировать подключение к Интернету при загрузке и установке Sandbox Analyzer.

#### 4.4.1. ESXi Hypervisor

Виртуальное устройство Sandbox Analyzer доступно в формате OVA и может быть развернуто на одном физическом хосте под управлением гипервизора VMware ESXi (версия 6.5 или 6.7).

#### Требования к оборудованию для физического хоста

- CPU: общее количество ядер процессора (с учетом гиперпотока) можно экстраполировать посредством расчета, представленного в разделе «Требования к физическому хосту и аппаратное масштабирование» (р. 38).
- Оперативная память: общий объем оперативной памяти, необходимый для физического хоста, может быть экстраполирован с помощью расчета, представленного в разделе «Требования к физическому хосту и аппаратное масштабирование» (р. 38).
- Пространство на диске: не менее 1 ТБ SSD-накопителя (достаточно для детонационной среды 8-VM, масштабируемой не менее чем на 50 ГБ для каждой дополнительной детонационной VM).
- Сеть: одна выделенная физическая сетевая карта (NIC)

Эта сетевая карта может быть разделена на две виртуальных сетевых карты со следующим маппингом:

- Одна сетевая карта для интерфейса управления
- Одна сетевая карта для детонационной сети



#### Примечание

Рекомендуется использовать указанные физические NICs с теми же отображениями, что и вышеупомянутые vNICs, если это позволяет аппаратная конфигурация.

### Требования к программному обеспечению

Поддерживаемые версии ESXi сервера: 6.5 или выше, VMFS версия 5.

Дополнительная конфигурации для хоста ESXi:

- SSH включается при запуске.
- Служба NTP настроена и активна.
- Включена функция **запустить/остановить при хосте**.



#### Примечание

Sandbox Analyzer совместим с пробной версией VMWare ESXi. Однако для производственных развертываний рекомендуется использовать лицензионную версию ESXi.

### 4.4.2. Sandbox Analyzer Виртуальное устройство

Sandbox Analyzer Виртуальное устройство обеспечивает практически неограниченную масштабируемость, пока доступны базовые аппаратные ресурсы.

Из общего объема доступных ресурсов ESXi Sandbox Analyzer разделяет ЦП и ОЗУ между Sandbox Manager и виртуальными машинами детонации.

### Минимальные требования к системе для менеджера песочницы

- 6 vCPUs
- 20 ГБ ОЗУ
- 600 ГБ дискового пространства

Sandbox Manager имеет три внутренние виртуальные сетевые карты, выделенные следующим образом:

- Одна сетевая карта для связи с консолью управления (GravityZone Control Center).
- Одна сетевая карта для подключения к интернету.
- Одна сетевая карта для связи с детонационными виртуальными машинами.



### Примечание

Чтобы разрешить обмен данными, vNIC управления ESXi и vNIC управления менеджером песочницы должны находиться в одной сети.

## Виртуальные машины детонации

### Системные требования

- 4 vCPUs (перепрофилировано в соотношение 4:1, ссылайтесь на «Требования к физическому хосту и аппаратное масштабирование» (р. 38))
- 3 ГБ ОЗУ
- 50 ГБ дискового пространства

Sandbox Analyzer On-Premises обеспечивает пользовательские образы виртуальных машин. Это допускает детонацию образца в среде выполнения, которая имитирует реалистичную производственную среду.

Создание образа виртуальной машины требует следующих условий:

- Образ виртуальной машины представлен в формате VMDK, версия 5.0.
- Поддерживаемые операционные системы для построения детонационных виртуальных машин:
  - 64-битная Windows 7 (любой уровень патча)
  - 64-битная Windows 10 (любой уровень патча)



### Важно

- Операционная система должна быть установлена во втором разделе таблицы разделов и смонтирована на диске C: (конфигурация установки Windows по умолчанию).

- Локальная учетная запись «Администратор» должна быть включена и иметь пустую строку пароля (пароль отключен).
- Перед экспортом образа виртуальной машины необходимо правильно лицензировать операционную систему и все установленное программное обеспечение в образе виртуальной машины.

## Программное обеспечение образа виртуальной машины

Sandbox Analyzer поддерживает детонацию широкого спектра форматов и типов файлов. Дополнительные сведения см. в разделе [«Объекты Sandbox Analyzer» \(р. 166\)](#).

Для исчерпывающих отчетов убедитесь, что вы установили в пользовательский образ программное обеспечение, которое может открыть файл определенного типа, который вы хотите детонировать. Дополнительные сведения см. в разделе [«Рекомендуемые приложения для детонации виртуальных машин» \(р. 167\)](#).

### 4.4.3. Виртуальное устройство безопасности сети

Виртуальное устройство безопасности сети управляет сетевым датчиком, который извлекает полезную нагрузку из сетевых потоков и передает его в Sandbox Analyzer. Минимальные требования к оборудованию:

- 4 vCPUs
- 4 ГБ ОЗУ
- 1 ТБ дискового пространства
- 2 vNICs

### 4.4.4. Требования к физическому хосту и аппаратное масштабирование

Алгоритм масштабирования среды Sandbox Analyzer учитывает следующую формулу, где "K" равно числу детонационных слотов (или детонационных VMs):

- Sandbox Analyzer VA vCPU = 6 vCPUs + K x 1vCPU
- Sandbox Analyzer VA RAM = 20 GB RAM + K x 2GB

Аналогично, алгоритм масштабирования для хоста является следующим:

- ESXi Host vCPU = 6 vCPUs + K x 2 vCPU
- ESXi Host RAM = 20 GB RAM + K x 5 GB

Главное отличие между Sandbox Analyzer VA и ESXi ресурсами задается ресурсами, которые выделены для каждой детонационной VM.

Таким образом, типичная детонационная среда (8 VMs) будет требовать следующего:

- Sandbox Analyzer VA vCPU = 6 vCPUs + 8 x 1vCPU = 14 vCPUs
- Sandbox Analyzer VA RAM = 20 GB RAM + 8 x 2GB = 36GB RAM
- ESXi Host vCPU = 6 vCPUs + 8 x 2 vCPUs = 22 vCPUs

#### **Примечание**

Каждая детонационная VM требует 1 vCPU из Sandbox Analyzer VA и 1 vCPU для детонационной VM. Виртуальная машина детонации будет обеспечена 4 vCPUs, но они будут перегружены в соотношении 4:1, в результате чего для хоста ESXi потребуется только 1 vCPU.

- ESXi Host RAM = 20 GB RAM + 8 x 5 GB = 60 GB RAM

#### **Примечание**

RAM используется в соотношении 1:1 между Sandbox Analyzer VA, детонационными VMs и хостом ESXi. Таким образом, каждая VM детонации потребует 5 ГБ оперативной памяти от хоста ESXi, из которых 2 ГБ будет выделено в Sandbox Analyzer и 3 ГБ будет выделено для самой VM детонации.

Полученный физический хост требует в вышеупомянутом сценарии минимум 22 ядра процессора (включая гиперпоточность) и 60 ГБ оперативной памяти, причем дополнительные 10-20% оперативной памяти зарезервированы для самого гипервизора.

Как правило, детонация образца занимает девять минут для выполнения и создания отчета о ней, который использует все подготовленные ресурсы. Рекомендуется спроектировать среду песочницы, начиная с детонационной емкости (файлы/час), а затем преобразовать эту метрику в необходимые ресурсы на уровне для Хоста и VM.

#### 4.4.5. Требования связи Sandbox Analyzer

Локальные компоненты Sandbox Analyzer используют определенные коммуникационные порты, привязанные к конкретным сетевым интерфейсам, для связи между собой и/или с публичными серверами Bitdefender.

Для среды песочницы необходимо три сетевых интерфейса:

- **eth0 – сетевой интерфейс управления.** Он подключен к GravityZone и к хосту ESXi.

Рекомендуется подключить eth0 к той же сети, что и интерфейс управления ESXi. Также рекомендуется сопоставить его с указанным сетевым адаптером.

В следующей таблице описывается ряд требований к сетевой коммуникации для eth0:

Направление	Коммуникационные порты (на TCP)	Источник/назначение
Исходящий (Outbound)	8443	Коммуникационный Сервер GravityZone
	443	Виртуальные устройства GravityZone
	80	Виртуальные устройства GravityZone
	22	ESXi хост
	443	ESXi хост API
Входящий (Inbound)	8443	Любой

- **eth1 – Детонационная сеть.** Это не требует какой-либо конфигурации. Данный процесс установки создает необходимые виртуальные ресурсы.
- **eth2 – сетевой Интернет-доступ.** Рекомендуется иметь неограниченное и нефильтрованное подключение к интернету.

Рекомендуется, чтобы сеть управления и сеть доступа в интернет были назначены для разных подсетей.

Виртуальное устройство GravityZone требует доступа к виртуальному устройству Sandbox Analyzer на порту 443 (по TCP) для просмотра и загрузки отчетов Sandbox Analyzer.



Виртуальное устройство GravityZone требует подключения к виртуальному устройству Sandbox Analyzer на порту 443 (по TCP) для запроса состояния детонированных образцов.

## 4.5. Полное шифрование диска

GravityZone Полное шифрование диска позволяет использовать BitLocker на конечных точках Windows, а также FileVault и утилиту командной строки diskutil на конечных точках macOS через Control Center.

Чтобы обеспечить защиту данных, данный модуль проводит полное шифрование диска для загрузочных и не загружаемых томов на фиксированных дисках и хранит ключи восстановления, на случай если пользователь забудет пароль доступа.

Модуль Шифрования использует существующие аппаратные ресурсы в среде GravityZone.

С точки зрения программного обеспечения, требования почти такие же, как для BitLocker, FileVault и утилиты командной строки diskutil, а также большинство ограничений, относящихся к этим утилитам.

### Для Windows

GravityZone Шифрование поддерживает BitLocker, начиная с версии 1.2, на компьютерах с и без чипа Trusted Platform Module (TPM).

GravityZone поддерживает BitLocker на конечных точках со следующими операционными системами:

- Windows 10 Образовательная
- Windows 10 Корпоративная
- Windows 10 Про
- Windows 8.1 Корпоративная
- Windows 8.1 Про
- Windows 8 Корпоративная
- Windows 8 Про
- Windows 7 Ultimate (с TPM)
- Windows 7 Корпоративная (с TPM)

- Windows Server 2019\*
- Windows Server 2016\*
- Windows Server 2012 R2\*
- Windows Server 2012\*
- Windows Server 2008 R2\* (с TPM)

\* BitLocker не входит в эти операционные системы и должен устанавливаться отдельно. Дополнительные сведения о развертывании BitLocker на Windows Serverсмотрите эти статьи базы знаний, предоставленных Microsoft:

- <https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server>
- [https://technet.microsoft.com/en-us/library/cc732725\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx)



### Важно

GravityZone не поддерживает шифрование в Windows 7 и Windows 2008 R2 без TPM.

Подробные требования к BitLocker см. в статье базы знаний, предоставленной Microsoft: [https://technet.microsoft.com/en-us/library/cc766200\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx)

## На ОС Mac

GravityZone поддерживает FileVault и diskutil на конечных точках macOS со следующими операционными системами:

- macOS Big Sur (11.x)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

## 4.6. Коммуникационные порты GravityZone

GravityZone - это распределенное решение, означающее, что его компоненты взаимодействуют друг с другом через локальную сеть или Интернет. Каждый компонент использует серию портов для связи с другими. Вы должны убедиться, что эти порты открыты для GravityZone.

Для получения более подробной информации о портах GravityZone, обратитесь к [этой статье](#).

## 5. УСТАНОВКА ЗАЩИТЫ

GravityZone является клиент-серверным решением. Для защиты вашей сети с помощью Bitdefender, вам необходимо установить серверные роли GravityZone, зарегистрировать вашу лицензию, настроить установочные пакеты и развернуть их с помощью агентов безопасности на конечные точки.

### 5.1. Установка и настройка GravityZone

Чтобы убедиться, что установка идет без проблем, выполните следующие действия:

1. Подготовка к установке
2. Установка и настройка GravityZone
3. Подключитесь к Control Center и настройте первую учетную запись
4. Настройка параметров Control Center

#### 5.1.1. Подготовка к установке

Для инсталляции вам необходим образ виртуального устройства GravityZone. После развертывания и настройки устройства GravityZone, вы можете удаленно установить клиент или скачать необходимые пакеты установки через веб-интерфейс Control Center.

Образ устройства GravityZone доступно в нескольких различных форматах, совместимых с основными платформами виртуализации. Вы можете получить ссылки для загрузки триала, пройдя регистрацию на [сайте Bitdefender](#).

Для установки и первоначальной настройки, вы должны иметь следующее:

- DNS-имена или фиксированные IP-адреса (статическая настройка или резервирование DHCP) для устройств GravityZone
- Имя пользователя и пароль администратора домена
- VCenter Server, данные XenServer (имя хоста или IP-адрес, порт связи, имя пользователя и пароль администратора)
- Лицензионные ключи (проверьте триальную регистрацию или почту, с которой происходила покупка)
- Настройки сервера исходящей почты

- Если необходимо, параметры прокси-сервера
- Сертификаты безопасности

## 5.1.2. Установка GravityZone

GravityZone состоит из одного или нескольких устройств, выполняющих серверные роли. Количество устройств зависит от различных критериев, таких как размер и топология вашей сети или функции GravityZone, которые вы будете использовать. Серверные роли делятся на три типа: базовые, вспомогательные и необязательные.



### Важно

Вспомогательные и необязательные роли доступны только для определенных решений GravityZone.

Роль GravityZone	Тип роли	Установить
Сервер базы данных Update Server	Базовые (необходимые)	Хотя бы один экземпляр каждой роли.
Веб-консоль		Устройство GravityZone может выполнять одну, несколько или все данные роли.
Коммуникационный Сервер		

В зависимости от предпочтений по распределению ролей GravityZone, вам потребуется развернуть от одного до четырех устройств GravityZone. Первой должна быть установлена База данных.

В сценарии с несколькими устройствами GravityZone, вы будете устанавливать роль сервера базы данных на первом устройстве и настраивать все другие устройства на подключение к существующему экземпляру базы данных.

Вы можете установить несколько экземпляров ролей Базы данных, Веб-консоли и коммуникационного сервера. В данном случае, вам понадобится Набор Реплик (Replica Set) для Базы данных и Балансировщик нагрузки для Веб-консоли и коммуникационного сервера на устройствах GravityZone.

Для установки и настройки GravityZone:

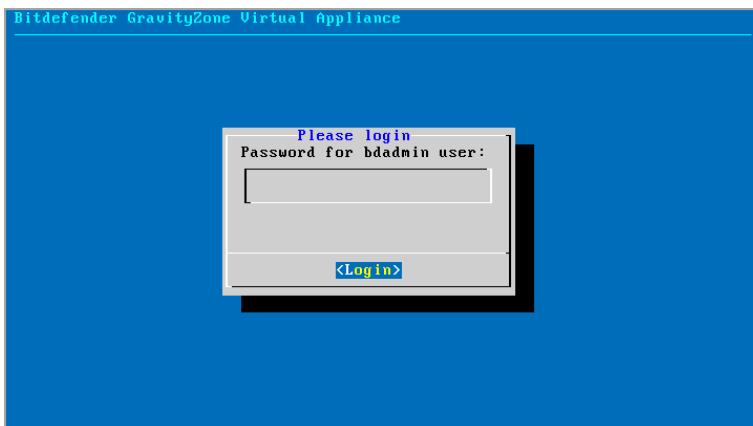
1. Загрузите образ виртуального устройства GravityZone с веб-сайта Bitdefender (ссылки приведены при регистрации триала или в письме о покупке).

2. Импортируйте образ виртуального устройства GravityZone в вашу виртуальную среду.
3. Включите устройство.
4. Из вашего инструментария управления виртуализацией, получите доступ к интерфейсу консоли устройства GravityZone.
5. Задайте пароль для встроенной учетной записи администратора `bdadmin`.

```
You need to change the initial password for bdadmin user. Choose an option:  
[c]ontinue  
[e]xit  
  
NOTE: On this terminal, the exit option restarts this verification,  
unless initial password is changed. Otherwise the installer will run.  
  
New password:
```

Интерфейс консоли устройства: введите новый пароль

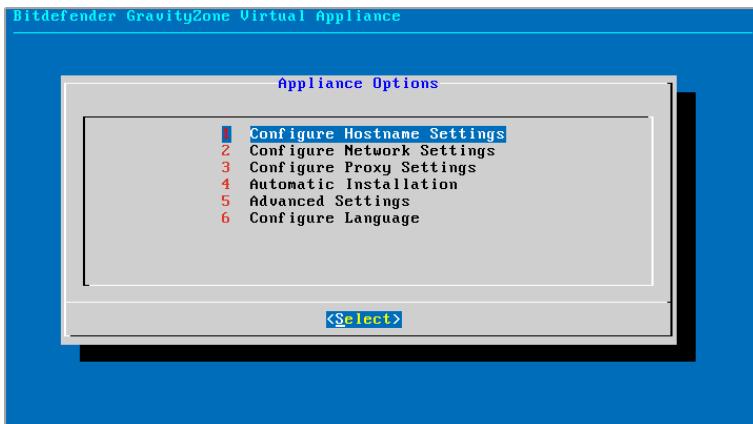
6. Войдите с помощью заданного пароля.



Интерфейс консоли устройства: вход

Вы получите доступ к интерфейсу конфигурации устройства.

Используйте клавиши со стрелками и клавишу Tab для навигации по меню и опциям. Нажмите Enter для выбора определенных опций.



Интерфейс консоли устройства: главное меню

7. Если Вам необходимо изменить язык интерфейса, выберите меню **Настройка языка**. За подробной информацией о настройке, перейдите к «**Настройка языка**» (р. 54).
8. **Настройте параметры имени хоста.**
9. **Настройка сетевых параметров.**
10. **Настройте параметры прокси-сервера.** (если это необходимо)
11. Установите роли GravityZone. Доступны две опции:
  - **Автоматическая установка.** Выберите данный вариант, если вам необходимо установить одно устройство GravityZone в вашей сети.
  - **Дополнительные настройки.** Выберите данный вариант, если вам необходимо установить GravityZone вручную или создать распределенную архитектуру.

После развертывания и настроек GravityZone, вы можете в любое время редактировать настройки устройства с помощью конфигурационного интерфейса. Для получения более подробной информации, касающейся

конфигурации устройства GravityZone, обратитесь к «[Управление устройством GravityZone](#)» (п. 84).

## Настройка параметров имени хоста

Связь с ролями GravityZone осуществляется по IP-адресу или DNS-имени устройства, на которых они установлены. По умолчанию компоненты GravityZone связываются по IP-адресам. Если вы хотите обеспечить связь через имена DNS, необходимо настроить DNS-имена устройств GravityZone и убедиться, что они корректно разрешаются в IP-адреса, назначенные устройствам.

Требования к системе:

- Настройка DNS-записи на сервере DNS.
- DNS-имя должно корректно разрешаться в IP-адрес, назначенный устройству. Таким образом, вы должны убедиться, что устройство настроено на корректный IP-адрес.

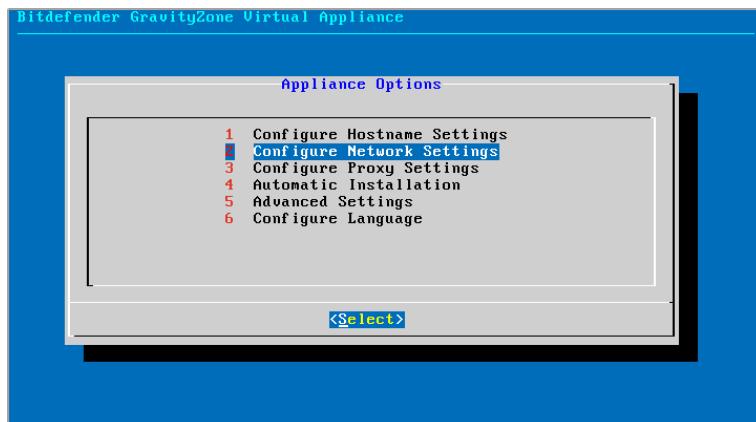
Чтобы задать настройки имени хоста:

1. Выберите из главного меню **Configure Hostname Settings**.
2. Введите имя хоста устройства и имя домена службы каталогов (Active Directory, в случае необходимости).
3. Нажмите **OK**, чтобы сохранить изменения.

## Настройка сетевых параметров

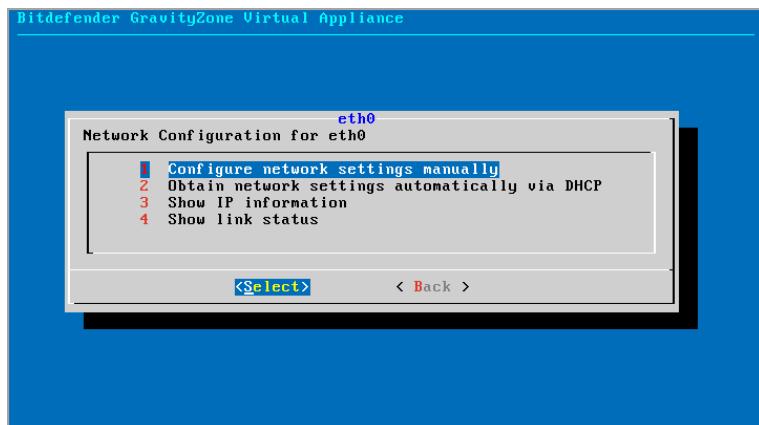
Вы можете настроить устройство на автоматическое получение сетевых параметров от сервера DHCP или выбрать настройки параметров сети вручную. Если вы выберите использование DHCP, вы должны настроить DHCP-сервер, чтобы зарезервировать для устройства определенный IP-адрес.

1. Выберите из главного меню **Configure Network Settings**.



Интерфейс консоли устройства: настройка сетевых параметров

2. Выберите сетевой интерфейс.
3. Выберите способ настройки:
  - **Настройка параметров сети вручную.** Вы должны указать IP-адрес, маску сети, адрес шлюза и DNS-сервера.
  - **Автоматическое получение сетевых настроек от сервера DHCP.** Используйте эту опцию только если вы настроили DHCP-сервер на резервирование определенного IP-адреса для устройства.



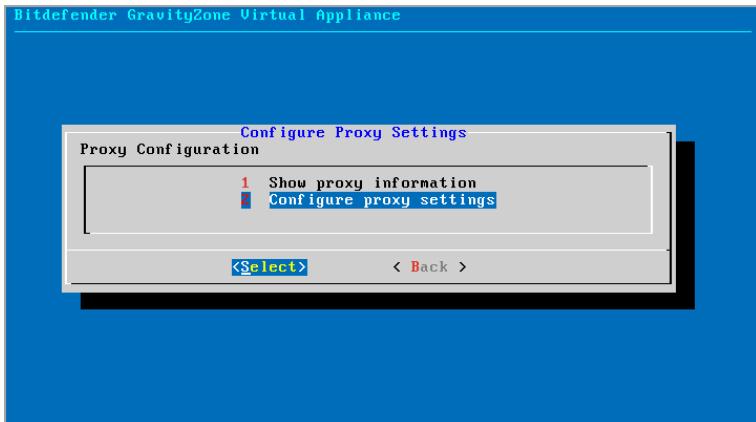
Интерфейс консоли устройства: настройка сети

4. Вы можете проверить детали текущей IP-конфигурации или состояния соединения, выбрав соответствующие опции.

## Настройка параметров прокси-сервера

Если устройство должно быть подключено к сети Интернет через прокси-сервер, вы должны настроить параметры прокси сервера.

1. Выберите из главного меню **Configure Proxy Settings**.
2. Выберите **Показать информацию о прокси** чтобы проверить, включено ли прокси-соединение.
3. Выберите **OK** для возврата на предыдущий экран.
4. Снова выберите **Настроить параметры прокси-сервера**.



Интерфейс консоли устройства: настройка параметров прокси-сервера

5. Введите адрес прокси-сервера. Используйте следующий синтаксис:
  - Если прокси-сервер не требует авторизации:  
`http(s)://<IP/hostname>:<port>`
  - Если прокси-сервер требует авторизацию:  
`http(s)://<username>:<password>@<IP/hostname>:<port>`
6. Нажмите **OK**, чтобы сохранить изменения.

## Автоматическая установка

Во время автоматической установки все базовые роли устанавливаются на одно и тоже устройство. Для распределенной установки GravityZone, перейдите к «[Дополнительные настройки](#)» (р. 52).

### Важно

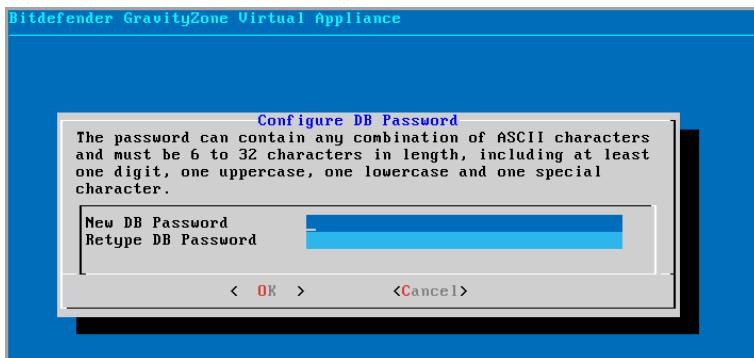
Автоматическая установка также развернет Security Server, встроенный в устройство GravityZone. Вы можете удалить эту роль впоследствии, потому что тип вашей лицензии ограничивает ее использование.

Опция автоматической установки доступна только при первоначальной настройке GravityZone.

Чтобы автоматически установить роли:

1. Из главного меню выберите **Automatic Installation**.
2. Прочтайте и примите Лицензионное соглашение с конечным пользователем (EULA), чтобы продолжить.
3. Подтвердите устанавливаемые роли.
4. Установите пароль от Базы данных.

Пароль может содержать любую комбинацию ASCII-символов и должен состоять от 6 до 32 символов в длину, включать по меньшей мере одну цифру, одну заглавную букву, одну букву нижнего регистра и один специальный символ.



Интерфейс консоли устройства: настройка пароля базы данных

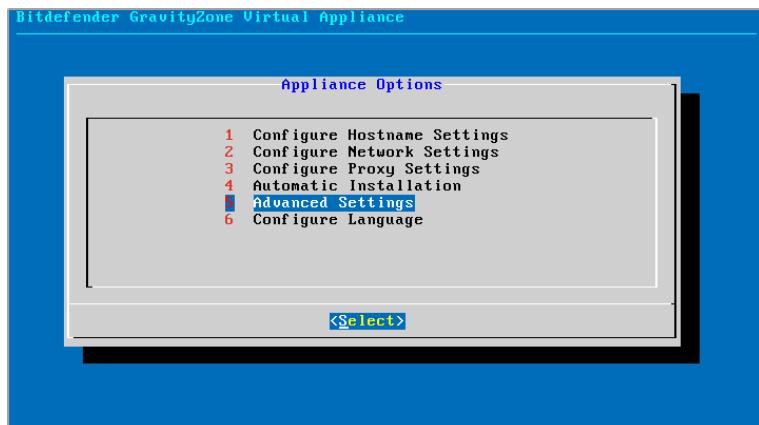
5. Дождитесь завершения процесса установки.

## Дополнительные настройки

Используйте эту опцию для установки только части или всех ролей GravityZone по отдельности для расширения инфраструктуры GravityZone. Вы можете установить роли на одно или несколько устройств. Данный метод установки требуется для возможности промежуточных обновлений, для расширения GravityZone в больших сетях с распределенным вариантом установки GravityZone и для обеспечения высокой отказоустойчивости служб GravityZone.

Чтобы установить роли по отдельности:

1. Из главного меню выберите **Advanced Settings**.



Интерфейс консоли устройства: установка ролей

2. Выберите **Install/Uninstall Roles**, чтобы установить устройство в среде GravityZone с одним сервером баз данных.



#### Примечание

Другие варианты предназначены для расширения развертывания GravityZone до распределенной архитектуры. Для получения более подробной информации, обратитесь к «[Подключитесь к существующей базе данных](#)» (р. 96) или «[Подключитесь к существующей базе данных \(Безопасный VPN-клuster\)](#)» (р. 97)

3. Выберите **Add or remove roles**. Появится окно подтверждения.
4. Нажмите **Enter** для продолжения.
5. Нажмите клавиш **Пробел** и затем клавишу **Enter**, чтобы установить роль **Базы данных**. Вы должны подтвердить свой выбор, нажав **Enter** снова.
6. Задайте пароль **Базы данных**.  
Пароль может содержать любую комбинацию ASCII-символов и должен состоять от 6 до 32 символов в длину, включать по меньшей мере одну цифру, одну заглавную букву, одну букву нижнего регистра и один специальный символ.
7. Нажмите **Enter** и дождитесь завершения установки.

8. Установите остальные роли, выбрав пункт **Добавить или удалить роли** из меню **Установка/Удаление Ролей** и затем выбрав устанавливаемые роли.
  - a. Выберите **Добавить или удалить роли** из меню **Установка/Удаление Ролей**.
  - b. Прочтите Лицензионное Соглашение с Конечным Пользователем. Нажмите **Enter**, чтобы принять и продолжить.



### Примечание

Это потребуется только один раз после установки Базы данных.

- c. Выберите устанавливаемые роли. Нажмите клавишу **Space**, чтобы выбрать роль и **Enter**, чтобы продолжить.
- d. Нажмите **Enter** для подтверждения и дождитесь окончания установки.



### Примечание

Каждая роль обычно устанавливается в течение нескольких минут. Во время установки, необходимые файлы загружаются из Интернет. Следовательно, установка занимает больше времени, если Интернет-соединение медленное. Если установка зависла, разверните устройство заново.

## Настройка языка

Первоначально интерфейс настройки устройства представлен на английском языке.

Чтобы изменить язык интерфейса:

1. Выберите **Configure Language** из главного меню.
2. Выберите язык из доступных вариантов. Появится окно подтверждения.



### Примечание

Вы должны прокрутить вниз, чтобы найти свой язык.

3. Нажмите **OK**, чтобы сохранить изменения.

### 5.1.3. Начальная настройка Control Center

После развертывания и настройки GravityZone, необходимо получить доступ к веб-интерфейсу Control Center и настроить учетную запись администратора компании.

1. В адресной строке веб-браузера введите IP-адрес или DNS-имя хоста Control Center (используя префикс `https://`). Появится мастер настройки.
2. Укажите лицензионный ключ, необходимый для проверки решения GravityZone. Вы также можете предоставить любой имеющийся у вас ключ дополнения GravityZone.

Проверьте пробную регистрацию или электронную почту покупки, чтобы найти ключи лицензии.

- a. Нажмите кнопку **+ Добавить** в верхней части таблицы. Появится окно настроек.
- b. Выберите способ регистрации лицензии (он-лайн или офф-лайн).
- c. Введите лицензионный ключ в поле **License key**. Для регистрации в офф-лайн режиме, вы должны также предоставить регистрационный код.
- d. Подождите пока лицензионный ключ проверяется. Нажмите **Add** для завершения.

Лицензионный ключ и истечение его срока действия будет отображаться в таблице лицензий.

#### Примечание

- Во время начальной установки необходимо предоставить действительный базовый лицензионный ключ для начала использования GravityZone. Вы можете впоследствии добавить дополнительные ключи лицензии или изменить существующие.
- Надстройки можно использовать до тех пор, пока предоставляется действительная базовая лицензия. В противном случае вы будете видеть функции, но не сможете их использовать.

Product Registration

MyBitdefender Account      Enter License Keys      English ▾

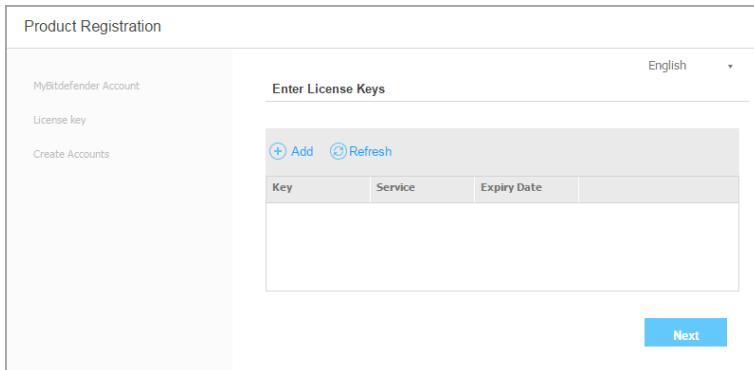
License key

Create Accounts

[+ Add](#) [⟳ Refresh](#)

Key	Service	Expiry Date

[Next](#)



Первоначальная настройка - предоставление лицензионного ключа

3. Для продолжения нажмите **Next**.
4. Заполните информацию о вашей компании, такую как название компании, адрес и телефон.
5. Вы можете изменить логотип, отображаемый в Control Center, а также в отчетах вашей компании и уведомлениях по электронной почте следующим образом:
  - Нажмите **Change**, чтобы найти изображение логотипа на вашем компьютере. Формат файла изображения должен быть .png или .jpg, а размер изображения должен быть 200x30 пикселей.
  - Нажмите **Default**, чтобы удалить изображение и сбросить его на изображение, предоставленное Bitdefender.
6. Укажите необходимые данные для учетной записи администратора вашей компании: имя пользователя, адрес электронной почты и пароль. Пароль должен содержать, по крайней мере, один символ верхнего регистра, по крайней мере, одну строчную букву и, по крайней мере, одну цифру или специальный символ.

Product Registration

MyBitdefender Account      English ▾

License key

Create Accounts

**Enter Company Details**

Company Name:

Address:

Phone:

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

**Change** **Default**

**Enter Company Administrator Account Details**

Username:

Email:

Full Name:

Password:

Confirm password:

**Create account**

Первоначальная настройка - Параметры вашей учетной записи

## 7. Нажмите **Create account**.

Учетная запись администратора компании будет создана и вы автоматически войдете с новой учетной записью в Control Center Bitdefender.

### 5.1.4. Настройка параметров Control Center

После первоначальной настройки, вам необходимо настроить параметры Control Center. Как администратор компании, вы можете сделать следующее:

- Настроить почту, прокси-сервер и другие общие настройки.
- Запустить или запланировать создание резервной копии базы данных Control Center.
- Настроить интеграцию службы каталогов (Active Directory) с инструментами управления виртуализацией (vCenter Server, XenServer).
- Установить сертификаты безопасности.

The screenshot shows the Bitdefender GravityZone Control Center interface. On the left is a sidebar with links like Dashboard, Network, Packages, Tasks, Policies, Assignment Rules, Reports, Quarantine, Accounts, User Activity, Configuration (which is selected), Update, and License. The main area has tabs for Mail Server, Proxy, Miscellaneous, Backup, Active Directory, Virtualization, and Certificates. Under Mail Server, the 'Mail Server Settings' section is active, containing fields for Mail server (SMTP) address (mail.comp.com), Port (25), Encryption type (None), and From email (noreply@comp.com). There is also a checkbox for 'Use authentication' which is unchecked, with a field for Username below it.

Настройки почтового сервера

## Почтовый сервер

Control Center требует внешнего почтового сервера для отправки сообщений электронной почты.



### Примечание

Рекомендуется создать отдельную учетную запись электронной почты, которая будет использоваться Control Center.

Чтобы разрешить Control Center отправлять электронную почту:

- Перейдите к странице **Configuration**.
- Выберите вкладку **Mail Server**.
- Выберите **Mail Server Settings** и настройте необходимые параметры:
  - Почтовый сервер (SMTP)**. Введите IP-адрес или имя почтового сервера, который будет отправлять электронные письма.
  - Порт**. Введите порт, используемый для связи с почтовым сервером.
  - Тип шифрования**. Если почтовый сервер требует шифрованного соединения, выберите соответствующий тип из меню (SSL, TLS или STARTTLS).

- **Адрес электронной почты отправителя (поле "От"/"From").** Введите адрес электронной почты, который вы хотите, чтобы появлялся в поле "От" (From - адрес электронной почты отправителя).
- **Использование проверки подлинности.** Выберите эту опцию, если почтовый сервер требует проверки подлинности. Вы должны указать действительное имя пользователя/адрес электронной почты и пароль.

#### 4. Нажмите Сохранить.

Control Center автоматически проверяет настройки электронной почты, когда вы их сохраняете. Если представленные параметры не могут быть подтверждены, сообщение об ошибке информирует вас о неправильной настройке. Измените настройки и попробуйте снова.

### Прокси-сервер

Если ваша компания подключена к Интернет через прокси-сервер, необходимо настроить параметры прокси-сервера:

1. Перейдите к странице **Configuration**.
2. Выберите вкладку **Proxy**.
3. Выберите **Use Proxy Settings** и настройте необходимые параметры:
  - **Address** - введите IP-адрес прокси-сервера.
  - **Port** - введите порт, для подключения к прокси-серверу.
  - **Пользователь** — введите имя пользователя, распознаваемого прокси-сервером.
  - **Пароль** — введите действующий пароль указанного ранее пользователя.

#### 4. Нажмите Сохранить.

### Разное

На странице **Configuration**, на вкладке > **Miscellaneous** вы можете настроить следующие общие параметры:

- **Если необходим недоступный комплект .** Вы можете настроить автоматическое действие для такой ситуации, выбрав один из следующих вариантов:
  - **Автоматическая загрузка пакетов**

– **Предупредите администратора и не выполняйте загрузку**

- **Параллельное развертывание.** Администраторы могут удаленно развертывать компоненты безопасности, запустив задачи по установке. Используйте эту опцию, чтобы указать максимальное количество одновременных процессов развертывания, которые могут быть выполнены одновременно.

Например, если максимальное количество одновременных процессов развертывания установлено на 10, а задача удаленной установки клиентов присваивается 100 компьютерам, Control Center первоначально запустит 10 установок пакетов через сеть. В этом случае, установка клиентов выполняется одновременно максимум на 10 компьютерах, все остальные подзадачи находятся в состоянии ожидания. Как только подзадача завершится, другой установочный пакет будет отправлен, и так далее.

- **Принудительная двухфакторная проверка подлинности для всех учетных записей.** Двухфакторная аутентификация (2FA) добавляет дополнительный слой защиты учетным записям GravityZone, запрашивая код аутентификации помимо ваших учетных данных в Control Center. Эта функция требует загрузки и установки приложения Google Authenticator, Microsoft Authenticator или любого двухфакторного аутентификатора TOTP (Time-Based One-Time Password Algorithm), совместимого со стандартом RFC6238. - на мобильном устройстве пользователя, а затем привязать приложение к учетной записи GravityZone и использовать его при каждом входе в Control Center. Приложение аутентификации генерирует шестизначный код каждые 30 секунд. Для завершения входа в Control Center после ввода пароля пользователь должен будет также ввести шестизначный код аутентификации.

Двухфакторная аутентификация включена по умолчанию при создании компании. После этого, при входе в систему, окно конфигурации предложит пользователям включить эту функцию. Пользователи смогут пропустить включение двухфакторной аутентификации только 3 раза. На четвертой попытке входа пропуск настройки 2FA будет невозможен, и пользователю будет не разрешен вход.

Если вы хотите отключить принудительную двухфакторную аутентификацию для всех учетных записей GravityZone в вашей компании, просто снимите флажок с этой опции. У вас будет запрошено подтверждение перед тем как изменения вступят в силу. С этого момента у пользователей будет активна двухфакторная аутентификация, но они

будут иметь возможность отключить ее в настройках своей учетной записи.

### Примечание

- Вы можете просмотреть статус двухфакторной аутентификации для учетной записи на странице **Учетные записи**.
  - Если пользователь, у которого включена двухфакторная аутентификация не может войти в систему GravityZone (из-за нового устройства или потерянного секретного ключа), вы можете отключить активацию этой функции со страницы учетной записи пользователя в разделе **Двухфакторная аутентификация**. За подробностями обратитесь к главе **Учетные записи пользователей > Управление двухфакторной аутентификацией** из Руководства Администратора.
- **NTP Server Settings.** Сервер NTP используется для синхронизации времени между всеми устройствами GravityZone. По умолчанию адрес сервера NTP настроен, но вы можете изменить его в поле **NTP Server Address**.

### Примечание

Для устройств GravityZone для связи с сервером NTP необходимо, чтобы порт 123 (UDP) был открыт.

- **Enable Syslog.** Включение этой функции позволяет GravityZone отправлять события на лог-сервер, работающий по протоколу Syslog. Таким образом, у вас есть возможность лучше контролировать события GravityZone.

Чтобы просмотреть или настроить список событий, отправляемых на сервер Syslog, обратитесь к главе **Уведомления** из руководства администратора GravityZone.

Чтобы включить ведение журнала на удаленном Syslog-сервере:

1. Отметьте флагок **Включить Syslog**.
2. Введите имя сервера или IP-адрес, предпочтительный протокол и порт Syslog-сервера.
3. Выберите формат для отправки данных на Syslog-сервер:
  - **Формат JSON.** JSON - это легкий формат обмена данными, который полностью независим от любого языка программирования. JSON представляет данные в удобочитаемом текстовом формате. В

формате JSON детали каждого события структурированы в объекты, каждый объект состоит из пары имя / значение.

Например:

```
{  
    "name": "Login from new device",  
    "created": "YYYY-MM-DDThh:mm:ss+hh:ss",  
    "company_name": "companynname",  
    "user_name": "username",  
    "os": "osname",  
    "browser_version": "browserversion",  
    "browser_name": "browsename",  
    "request_time": "DD MMM YYYY, hh:mm:ss +hh:ss",  
    "device_ip": "computerip"  
}
```

Для дополнительной информации, см. [www.json.org](http://www.json.org).

Это формат по умолчанию в GravityZone.

- **Common Event Format (CEF).** CEF - это открытый стандарт, разработанный ArcSight, который упрощает управление журналами.

Например:

```
CEF:0|Bitdefender|GZ|<GZ version>|NNNNN|Login from new  
device|3|start=MMM DD YYYY hh:mm:ss+hh:mm  
BitdefenderGZCompanyName=companynname suser=username  
BitdefenderGZLoginOS=osname  
BitdefenderGZAuthenticationBrowserName=browsename  
BitdefenderGZAuthenticationBrowserVersion=browserversion  
dvhost=computerip
```

Для получения дополнительной информации см. [ArcSight Common Event Format \(CEF\) Implementation Standard](#).

- В главе **Уведомления** Руководства администратора вы можете просмотреть доступные типы уведомлений для каждого формата.

#### 4. Нажмите кнопку Add из столбца Action.

Нажмите Сохранить, чтобы сохранить изменения.

## Резервное копирование

Чтобы быть уверенным, что все ваши данные Control Center находятся в безопасности, вы можете сделать резервную копию базы данных GravityZone. Вы можете запускать столько задач резервного копирования баз данных, сколько хотите или можете запланировать периодические резервные копии автоматически через определенные промежутки времени.

Каждая команда резервного копирования базы данных создает файл `.tgz` (GZIP файл сжатого Tar-архива) в месте, указанном в настройках резервного копирования.

Когда несколько администраторов имеют права управления, заданные настройками Control Center, вы также можете настроить **Notification Settings**, чтобы предупреждать вас каждый раз, когда задача резервного копирования базы данных завершена. Для получения более подробной информации, обратитесь к главе **Notifications** из руководства администратора GravityZone.

### Создание резервных копий баз данных

Чтобы запустить резервное копирование базы данных:

- Перейдите на страницу **Configuration** в Control Center и нажмите вкладку **Backup**.
- Нажмите кнопку  **Backup Now** в верхней части таблицы. Появится окно настроек.
- Выберите место, где архив резервной копии будет сохранен:

- Local** для сохранения архива на устройстве GravityZone. В этом случае вы должны указать путь к определенной директории устройства GravityZone, где архив будет сохранен.

Устройство GravityZone имеет структуру каталогов Linux. Например, вы можете выбрать создание резервной копии в каталоге `tmp`. В этом случае введите `/tmp` в поле **Path**.

- FTP** для сохранения архива на FTP-сервере. В этом случае, введите данные FTP-сервера в соответствующих полях.
- Network** для сохранения архива на общем сетевом ресурсе. В этом случае введите путь к нужной сетевой папке (например, `\computer\folder`), имя домена и учетные данные пользователя домена.

4. Нажмите кнопку **Test Settings**. Текст уведомления проинформирует вас, если указанные параметры корректны или некорректны.  
Для создания резервной копии все настройки должны быть корректными.
5. Нажмите **Создать**. Отобразится страница **Backup**. Новая запись резервной копии будет добавлен в список. Проверьте **Status** новой резервной копии. Когда резервное копирование будет завершено, вы найдете `tgz` архив в выбранном месте.



### Примечание

Список, доступный на странице **Backup**, содержит журналы создания всех архивов. Журналы не предоставляют доступа к резервным архивам; они содержат только детальную информацию по созданию архивов.

Чтобы запланировать резервное копирование базы данных:

1. Перейдите на страницу **Configuration** в Control Center и нажмите вкладку **Backup**.
2. Нажмите кнопку **Backup Settings** в верхней части таблицы. Появится окно настроек.
3. Выберите **Scheduled Backup**.
4. Настройте интервал резервного копирования (ежедневно, еженедельно или ежемесячно) и время начала.

Например, вы можете запланировать резервное копирование еженедельно, каждую пятницу, начиная в 22:00.

5. Настройка размещения резервного копирования по расписанию.
6. Выберите место, где архив резервной копии будет сохранен:
  - **Local** для сохранения архива на устройстве GravityZone. В этом случае вы должны указать путь к определенной директории устройства GravityZone, где архив будет сохранен.  
Устройство GravityZone имеет структуру каталогов Linux. Например, вы можете выбрать создание резервной копии в каталоге `tmp`. В этом случае введите `/tmp` в поле **Path**.
  - **FTP** для сохранения архива на FTP-сервере. В этом случае, введите данные FTP-сервера в соответствующих полях.

- **Network** для сохранения архива на общем сетевом ресурсе. В этом случае введите путь к нужной сетевой папке (например, \\ computer \ folder ), имя домена и учетные данные пользователя домена.
7. Нажмите кнопку **Test Settings**. Текст уведомления проинформирует вас, если указанные параметры корректны или некорректны.
- Для создания резервной копии все настройки должны быть корректными.
8. Нажмите **Save**, чтобы создать планируемое резервное копирование.

## Восстановление резервных копий баз данных

Если по разным причинам ваш экземпляр GravityZone работает неправильно (сбой обновления, дисфункциональный интерфейс, поврежденные файлы, ошибки и т. д.), Вы можете восстановить базу данных GravityZone из Резервной копии с использованием:

- этого же устройства
- Свежего образа GravityZone
- Функции репликации

Выберите вариант, который наилучшим образом соответствует вашей ситуации и продолжайте процедуру восстановления только после внимательного изучения рекомендаций, описанных далее.

## Восстановление базы данных на само виртуальное устройство GravityZone.

### Требования к системе

- SSH-подключение к машине GravityZone с полномочиями **root**.  
Вы можете использовать **putty** и учетные данные **bdadmin** для подключения к устройству через SSH, выполнив затем команду **sudo su**, чтобы переключиться на учетную запись **root**.
- Инфраструктура GravityZone не меняется во время резервного копирования.
- Резервная копия более поздняя, чем 30 апреля 2017 года, а версия GravityZone выше 6. 2. 1- 30. В противном случае обратитесь в службу технической поддержки.
- В распределенной архитектуре GravityZone не должен использовать репликацию баз данных (Replica Set).

Для подтверждения конфигурации, выполните следующие действия:

1. Откройте файл /etc/mongodb.conf.
2. Убедитесь, что replSet не настроен, как показано в примере ниже:

```
# replSet = setname
```



### Примечание

Для восстановления базы данных с включенной функцией репликации перейдите к «Восстановление базы данных в среде с репликацией» (р. 70).

- Не должно быть запущено CLI-процессов.

Чтобы убедиться, что все процессы CLI остановлены, выполните следующую команду:

```
# killall -9 perl
```

- Пакет **mongoconsole** установлен на машине.

Чтобы проверить выполняется ли условие, запустите комманду:

```
# /opt/bitdefender/bin/mongoshellrestore --version
```

Команда не должна возвращать какие-либо ошибки, в противном случае запустите:

```
# apt-get update  
# apt-get install --upgrade mongoconsole
```

## Восстановление базы данных

1. Перейдите в место, где содержится архив базы данных:

```
# cd /directory-with-backup
```



, где Каталог с резервной копией - это путь к месту, где вы сохранили файлы резервной копии.

Например:

```
# cd /tmp/backup
```

## 2. Восстановление базы данных.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password'
--authenticationDatabase admin --gzip --drop --archive < \
gz-backup-$YYYYMMDDtimestamp
```

### Важно

Убедитесь, что вы заменили строку `GZ_db_password` настоящим паролем от Базы данных GravityZone и заменили переменную отметку времени в имени архива на актуальную дату.

Например, актуальная дата должна выглядеть следующим образом:

```
gz-backup-2019-05-17 (1495004926) .tar.gz
```

## 3. Перезагрузите устройство.

Восстановление базы данных завершено.

**Восстановление базы данных из выведенных из эксплуатации виртуальных машин GravityZone**

### Требования к системе

- Свежая установка виртуальной машины GravityZone
  - С тем же IP-адресом, что и предыдущее устройство
  - Имея ТОЛЬКО установленную роль сервера баз данных.

Вы можете скачать образ виртуального устройства GravityZone отсюда [here](#).

- SSH-подключение к виртуальной машине GravityZone с полномочиями **root**.
- Инфраструктура GravityZone не меняется во время резервного копирования.
- Резервная копия более поздняя, чем 30 апреля 2017 года.
- В распределенной архитектуре GravityZone не должен использовать репликацию баз данных (Replica Set).

Если вы используете репликацию в среде GravityZone, у вас также должна быть роль сервера базы данных, установленная на другой машине.

Для восстановления базы данных с включенной функцией репликации перейдите к «[Восстановление базы данных в среде с репликацией](#)» (р. 70).

### Восстановление базы данных

1. Подключитесь к устройству GravityZone через SSH и переключитесь на **root**.
2. Остановите VASync:

```
# stop vasync
```

3. Остановить CLI:

```
# # killall -9 perl
```

4. Перейдите в место, где находится резервная копия:

```
# cd /directory-with-backup
```

, где Каталог-с резервной копией - это путь к месту, где вы сохранили файлы резервной копии.

Например:

```
# cd /tmp/backup
```

## 5. Восстановление базы данных.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password  
--authenticationDatabase=admin --gzip --drop \  
--archive='/home/bdadmin/gz-backup-$YYYYMMDDtimestamp
```

### Важно

Убедитесь, что вы заменили строку GZ\_db\_password настоящим паролем от Базы данных GravityZone и заменили переменную отметку времени в имени архива на актуальную дату.

Например, актуальная дата должна выглядеть следующим образом:

```
gz-backup-2019-05-17(1495004926).tar.gz
```

## 6. Восстановление ID старого устройства:

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ-db_password  
--eval print(db.applianceInstalls.findOne({name:'db'}).\  
applianceId)" --quiet > /opt/bitdefender/etc/applianceid
```

### Важно

Убедитесь, что вы заменили строку GZ\_db\_password настоящим паролем от Базы данных GravityZone.

## 7. Удалите соотношение со старыми ролями.

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ_db_password  
'db.applianceInstalls.remove({ip:db.applianceInstalls.findOne(  
{name:"db"}).ip,name:{$ne: "db"}});' --quiet devdb
```

### Важно

Убедитесь, что вы заменили строку GZ\_db\_password настоящим паролем от Базы данных GravityZone.

## 8. Запустите VASync:

```
# start vasync
```

## 9. Начать CLI:

```
# /opt/bitdefender/eltiw/installer
```

## 10. Установите остальные роли.

```
# dpkg -l gz*
```

Обратите внимание - схема базы данных успешно обновлена до последней версии:

```
> db.settings.findOne().database
{
  "previousVersion" : "000-002-009",
  "ranCleanUpVersions" : {
    "b0469c84f5bf0bec0b989ae37161b986" : "000-002-008"
  },
  "updateInProgress" : false,
  "updateTimestamp" : 1456825625581,
  "version" : "000-002-011"
}
```

## 11. Перезагрузите устройство.

Восстановление базы данных завершено.

### Восстановление базы данных в среде с репликацией

Если вы развернули базу данных в среде с репликацией, вы можете найти официальную процедуру восстановления в [MongoDB online manual](#) (только английская версия).

#### Примечание

Процедура требует продвинутых технических навыков и должна выполняться только обученным инженером. Если вы столкнулись с трудностями, пожалуйста, свяжитесь с нашим [Technical Support](#), чтобы помочь вам в восстановлении данных.

## Служба каталогов (Active Directory)

Благодаря интеграции с Active Directory вы можете импортировать в Control Center существующий инвентарь из локальной службы Active Directory и из Active Directory, размещенной в Microsoft Azure, упрощая развертывание защиты, управление, мониторинг и отчетность. Кроме того, пользователям, зарегистрированным в службе каталогов могут быть назначены различные роли через Control Center.

Для интеграции и синхронизации GravityZone с доменной службой каталогов:

1. Перейдите в **Настройки > Active Directory > Домены** и нажмите **+ Добавить**.
2. Настройте необходимые параметры:
  - Интервал синхронизации (в часах)
  - Имя домена Active Directory (в том числе расширение домена)
  - Имя пользователя и пароль администратора домена
  - Расположение в инвентаре сети, где отображаются конечные точки AD:
    - Сохраняйте структуру AD и игнорируйте пустые OU
    - Игнорировать структуру AD, импортировать в пользовательские группы
    - Сохранить структуру AD только с выбранными подразделениями
  - Контроллеры домена, с которыми выполняется синхронизация Control Center. Разверните раздел **Запрос контроллера домена** и выберите контроллеры из таблицы.
3. Нажмите **Сохранить**.

### Важно

Всякий раз, когда меняется пароль пользователя, не забудьте также обновить его в Control Center.

## Разрешения на доступ

С разрешениями доступа вы можете предоставить GravityZone Control Center доступ пользователям Active Directory (AD) на основе правил доступа. Чтобы интегрировать и синхронизировать домены AD, см. [Active Directory](#). Для дополнительной информации об управлении учетными записями пользователей через правила доступа, см. главу [Учетные записи пользователей](#) в Руководстве по установке GravityZone.

## Поставщики средств виртуализации

На данный момент GravityZone может быть интегрирована с VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 и Microsoft Azure.

- «Интеграция с vCenter Server» (п. 72)
- «Интеграция с XenServer» (п. 73)
- «Интеграция с Nutanix Prism Element» (п. 74)
- «Интеграция с Amazon EC2» (п. 76)
- «Интеграция с Microsoft Azure» (п. 77)
- «Управление Интеграцией с Платформами» (п. 78)



### Важно

Каждый раз, когда вы проводите новую интеграцию с другим сервером vCenter, XenServer, Nutanix Prism Element или Microsoft Azure, не забудьте также пересмотреть и обновить права доступа существующих пользователей.

## Интеграция с vCenter Server

Вы можете интегрировать GravityZone с одной или несколькими системами vCenter Server. Системы vCenter Server в подключенном режиме должны быть добавлены отдельно в Control Center.

Чтобы настроить интеграцию с vCenter Server:

1. Перейдите на страницу **Конфигурация** в Control Center и зайдите в раздел **Провайдеры виртуализации > Платформы управления**.
2. Нажмите кнопку **+ Add** в верхней части таблицы и выберите **vCenter Server** из меню. Появится окно настроек.
3. Укажите необходимые сведения о vCenter Server.
  - Имя системы vCenter Server в Control Center
  - Имя хоста или IP-адрес системы vCenter Server
  - Порт vCenter Server (по умолчанию 443)
4. Укажите учетные данные, которые будут использоваться для проверки подлинности в vCenter Server. Пользователь, чьи учетные данные вы предоставляете, должен иметь права администратора на сервере vCenter.
5. **Ограничить назначение политики из просмотра сети.** Используйте эту опцию, чтобы управлять разрешениями сетевым администраторам

изменять политики виртуальных машин через **Computers and Virtual Machines** на странице **Network**. Когда выбрана эта опция, администраторы могут изменять политики виртуальных машин только из раздела **Virtual Machines** сетевых элементов.

6. Нажмите **Сохранить**. Вам необходимо будет принять сертификаты безопасности для vCenter Server и NSX Manager. Эти сертификаты обеспечивают безопасную связь между компонентами GravityZone и VMware, устранивая риск атак среднего уровня.

Вы можете проверить, были ли установлены правильные сертификаты, проверив информацию сайта для всех компонентов VMware и информацию о сертификатах, отображаемую в Control Center.

7. Установите флагки для принятия использования сертификатов.
8. Нажмите **Сохранить**. Вы сможете просмотреть vCenter Server в списке активных интеграций.

В итоге вы можете увидеть, что происходит синхронизация vCenter Server. Подождите несколько минут, пока не завершится синхронизация.

## Интеграция с XenServer

Вы можете интегрировать GravityZone с одной или несколькими системами XenServer.

Чтобы настроить интеграцию с XenServer:

1. Перейдите на страницу **Конфигурация** в Control Center и кликните в раздел **Провайдеры виртуализации**.
2. Нажмите кнопку **+ Add** в верхней части таблицы и выберите **XenServer** из меню. Появится окно настроек.
3. Укажите необходимые сведения о XenServer.
  - Имя системы XenServer в Control Center
  - Имя хоста или IP-адрес системы XenServer
  - Порт XenServer (по умолчанию 443)
4. Укажите учетные данные, которые будут использоваться для проверки подлинности в XenServer. Вы можете выбрать: использовать учетные данные, предоставленные для интеграции службой каталогов или иной набор учетных данных.

5. **Ограничить назначение политики из просмотра сети.** Используйте эту опцию, чтобы управлять разрешениями сетевым администраторам изменять политики виртуальных машин через **Computers and Virtual Machines** на странице **Network**. Когда выбрана эта опция, администраторы могут изменять политики виртуальных машин только из раздела **Virtual Machines** сетевых элементов.
6. **Автоматическое обновление интеграции при смене хозяина в XenCenter.** Используйте этот параметр, чтобы поддерживать интеграцию без ручного вмешательства при изменении IP-адреса главного сервера пула.



### Примечание

Вы можете включить уведомление **Об автоматическом обновлении интеграции XenServer**, чтобы знать, когда происходят такие изменения, и настройки автоматически обновляются.

7. Нажмите **Сохранить**. Вы сможете просмотреть XenServer в списке активных интеграций и синхронизировать его. Подождите несколько минут, пока не завершится синхронизация.

## Интеграция с Nutanix Prism Element

Вы можете интегрировать GravityZone с одним из множества кластеров Nutanix Prism Element, независимо от того, зарегистрированы они в Nutanix Prism Central или нет.

Для настройки интеграции с Nutanix Prism Element:

1. Перейдите на страницу **Конфигурация** в Control Center и кликните в раздел **Провайдеры виртуализации**.
2. Нажмите кнопку **+ Добавить** в верхней части таблицы и выберите **Nutanix Prism Element** из меню. Появится окно настроек.
3. Укажите детали Nutanix Prism Element:
  - Название Nutanix Prism Element в Control Center.
  - IP-адрес Контроллера виртуальной машины (CVM) из Nutanix Prism Element кластера или IP-адрес Виртуального IP Кластера.
  - Порт Nutanix Prism Element (по умолчанию 9440).

4. Укажите учетные данные, которые будут использоваться для проверки подлинности в Nutanix Prism Element.



### Важно

Пользователь, чьи учетные данные вы предоставляете, должен иметь права Администратора Кластера (Cluster Admin) или Администратора-пользователя (User Admin) в Nutanix Prism Element.

5. **Ограничить назначение политики из просмотра сети.** Используйте данную функцию, чтобы управлять разрешениями сетевых администраторов для изменения политик виртуальных машин через страницу **Компьютеры и Виртуальные Машины** в разделе **Сеть**. Когда выбрана эта опция, администраторы могут изменять политики виртуальных машин только из раздела Virtual Machines сетевых элементов.
6. Нажмите **Сохранить**. Вам будет предложено принять сертификаты безопасности для Nutanix Prism. Эти сертификаты обеспечивают безопасную связь между компонентами GravityZone и Nutanix Prism Element, устранивая риск MITM-атак.

Вы можете проверить, были ли установлены правильные сертификаты, проверив информацию сайта для всех кластеров Nutanix Prism Element или CVM и информацию о сертификатах, отображаемую в Control Center.

7. Установите флагки для принятия использования сертификатов.
8. Нажмите **Сохранить**.

Если вы вошли в CVM IP для настройки интеграции, в новом окне вас спросят, хотите ли вы использовать Cluster Virtual IP вместо CVM IP:

- a. Нажмите **Да**, чтобы использовать Cluster Virtual IP для интеграции. Cluster Virtual IP заменит CVM IP в деталях Nutanix Prism Element.
- b. Нажмите **Нет**, чтобы дальше использовать CVM IP.



### Примечание

Рекомендуется использовать Cluster Virtual IP, а не CVM IP. В таком случае, интеграция останется активной даже если конкретный хост станет недоступен.

- c. В окне **Добавить Nutanix Prism Element** нажмите **Сохранить**.

Вы сможете просмотреть Nutanix Prism Element в списке активных интеграций. Подождите несколько минут, пока не завершится синхронизация.

## Интеграция с Amazon EC2

Вы можете интегрировать GravityZone в ваш инвентарь Amazon EC2 и защитить ваши экземпляры EC2, расположенные в Amazon cloud.

Требования к системе:

- Доступ к учетной записи AWS и секретные ключи
- Учетная запись должна иметь следующие разрешения:
  - IAMReadOnlyAccess
  - AmazonEC2ReadOnly для всех регионов AWS

Вы можете создать несколько интеграций Amazon EC2. Для каждой интеграции вам необходимо предоставить действительную учетную запись пользователя AWS.

### Примечание

Нельзя добавить несколько интеграций используя учетные данные ролей IAM, созданных для одной учетной записи AWS.

Для настройки интеграции с Amazon EC2:

1. Перейдите на страницу **Конфигурация** в Control Center и кликните в раздел **Провайдеры виртуализации**.
2. Нажмите на кнопку  **Добавить** в верхней части таблицы и выберите **Интеграция с Amazon EC2** из меню. Появится окно настроек.
3. Укажите дополнительную информацию интеграции с Amazon EC2:
  - Название интеграции. При добавлении нескольких интеграций Amazon EC2, вы сможете определить их по названию.
  - Доступ к учетной записи AWS и секретные ключи
4. **Ограничить назначение политики из просмотра сети.** Используйте эту опцию, чтобы управлять разрешениями сетевым администраторам изменять политики виртуальных машин через **Computers and Virtual Machines** на странице **Network**. Когда выбрана эта опция, администраторы

могут изменять политики виртуальных машин только из раздела **Virtual Machines** сетевых элементов.

5. Нажмите **Сохранить**. Если предоставленные учетные данные действительны, интеграция будет создана и добавлена в список.

Подождите, пока GravityZone проведет синхронизацию с инвентарем Amazon EC2.

## Интеграция с Microsoft Azure

Вы можете интегрировать GravityZone с Microsoft Azure и защитить ваши виртуальные машины, расположенные в Microsoft cloud.

Требования к системе:

- Приложение Azure с разрешением Reader
- Идентификатор Active Directory
- Идентификатор приложения
- Секретная фраза приложения

За подробной информацией о получении требуемых учетных данных и настройке приложения Azure, просмотрите данную [статью Базы знаний](#).

Вы можете создать несколько интеграций Microsoft Azure. Для каждой интеграции вы должны предоставить действительный Active Directory ID.

Для настройки интеграции с Microsoft Azure:

1. Перейдите на страницу **Конфигурация** в Control Center и кликните в раздел **Провайдеры виртуализации**.
2. Нажмите кнопку **+ Добавить** в верхней части таблицы и выберите **Интеграция Azure** из меню. Появится окно настроек.
3. Укажите дополнительную информацию интеграции с Azure:
  - **Название интеграции.** При добавлении нескольких интеграций Azure, вы сможете определить их по названию.
  - **Идентификатор Active Directory.** Каждый экземпляр Azure Active Directory имеет уникальный идентификатор, доступный в информации учетной записи Microsoft Azure.
  - **Идентификатор приложения.** Каждой приложение Azure имеет уникальный идентификатор, доступный в подробной информации приложения.

- **Секретная фраза приложения.** Секрет приложения это значение, доступное при сохранении ключа в настройках приложения Azure.
4. Выберите опцию **Ограничить назначение политики из просмотра сети**, чтобы изменить политику только для просмотра **Виртуальных машин**. Если не выбрано, вы сможете менять политику из просмотра **Компьютеров** и **Виртуальных Машин**.
  5. Нажмите **Сохранить**. Если предоставленные учетные данные действительны, интеграция будет создана и добавлена в список.

Подождите, пока GravityZone проведет синхронизацию с инвентарем Microsoft Azure.

## Управление Интеграцией с Платформами

Для изменения или обновления интеграции с платформами:

1. В Control Center, перейдите в раздел **Настройка > Виртуализация**.
2. Нажмите кнопку  **Изменить** в **Действие**.
3. Настройте нужные параметры правила. Для получения дополнительной информации обратитесь к одному из следующих разделов, в зависимости от того, что применимо:
  - [«Интеграция с vCenter Server» \(p. 72\)](#)
  - [«Интеграция с XenServer» \(p. 73\)](#)
  - [«Интеграция с Nutanix Prism Element» \(p. 74\)](#)
  - [«Интеграция с Amazon EC2» \(p. 76\)](#)
  - [«Интеграция с Microsoft Azure» \(p. 77\)](#)
4. Нажмите **Сохранить**. Подождите несколько минут, пока сервер не будет повторно синхронизирован.

Интеграции Nutanix Prism Element, Amazon EC2 and Microsoft Azure синхронизируются автоматически каждые 15 минут. Вы можете синхронизировать их вручную в любое время следующим образом:

1. В Control Center, перейдите в раздел **Настройка > Виртуализация**.
2. Нажмите кнопку  **Ресинхронизация** в столбце **Действие**.
3. Нажмите **Да**, чтобы подтвердить выбор.

Кнопка  **Ресинхронизация** особенно полезна в случае, когда статус интеграции меняется и требует синхронизации, как показано в следующих ситуациях:

- Для интеграции с Nutanix Prism Element:
  - Пользователь больше не имеет привилегий администратора.
  - Пользователь становится недействительным (смена или удаление пароля).
  - Сертификат безопасности становится недействительным.
  - Произошла ошибка соединения.
  - В кластере Nutanix Prism Element добавлен или удален хост.
- Для интеграции Microsoft Azure:
  - Добавления или удалена подписка в Microsoft Azure.
  - В Microsoft Azure добавлена или удалена виртуальная машина.

Вы также можете синхронизировать интеграцию, нажав кнопку  **Изменить**, а затем нажав **Сохранить**.

Чтобы убедиться, что отображается актуальная информация, нажмите кнопку **Refresh** в верхней части таблицы.

## Провайдеры Безопасности

GravityZone Security for Virtualized Environments интегрируется с VMware NSX-T Data Center с помощью NSX-T Manager.

### Интеграция с помощью NSX-T Manager

NSX-T Manager - это панель управления серверами vCenter, интегрированная с NSX-T Data Center. Чтобы интеграция работала, вам необходимо настроить интеграцию для серверов vCenter, связанных с NSX-T Manager. За дополнительной информацией, перейдите к разделу [Интеграция с сервером vCenter](#).

Для настройки интеграции с помощью NSX-T Manager:

1. В Control Center, перейдите в раздел **Конфигурация > Виртуализация> Провайдеры безопасности**.

2. Нажмите кнопку **Добавить** в верхней части таблицы. Появится окно настроек.
3. Укажите дополнительную информацию интеграции с NSX-T:
  - Название интеграции с NSX-T.
  - Имя хоста или IP-адрес связанной системы vCenter Server.
  - Порт NSX-T (по умолчанию - 433).
4. Укажите учетные данные, которые будут использоваться для проверки подлинности в vCenter Server. Вы можете выбрать: использовать учетные данные, предоставленные для интеграции службой каталогов или иной набор учетных данных. Пользователь, чьи учетные данные вы предоставляете, должен иметь права администратора на сервере vCenter.
5. Нажмите **Сохранить**.

Теперь Control Center интегрирована с NSX-T. Для установки защиты на ваши виртуальные машины через политику Guest Introspection GravityZone, просмотрите статью [Базы знаний Настройка и установка защиты на гостевые виртуальные машины VMware NSX-T с помощью политики GravityZone Guest Introspection](#).



### Примечание

GravityZone может быть использована только для защиты соответствующего сервера Server.

## NTSA

В этом разделе вы сможете настроить интеграцию с Bitdefender Network Traffic Security Analytics, решением безопасности предприятий, которое точно определяет бреши в защите и дает представление о сложных атаках путем анализа сетевого трафика. За подробной информацией о данном продукте, обратитесь к [документации Bitdefender NTSA](#).



### Важно

Раздел интеграции с NTSA доступен только после ввода действительного лицензионного ключа на странице [Конфигурация > Лицензии](#).

Для настройки интеграции NTSA, вам необходимо иметь решение NTSA в вашем окружении, а также иметь учетные данные для доступа к веб-консоли NTSA.

Во время интеграции, вам потребуется предоставить адрес (IP или имя хоста) веб-консоли NTSA и токен (ключ сопряжения), созданный в веб-консоли NTSA, о чём будет объяснено в дальнейшем.

## Настройка интеграции NTSA

1. Вход в GravityZone Control Center.
2. Перейдите на страницу **Конфигурация** и нажмите вкладку NTSA.
3. Активируйте опцию **Интеграция с Network Traffic Security Analytics (NTSA)**
4. Введите следующие данные:
  - Адрес веб-консоли NTSA (IP / имя хоста).
  - Порт, по которому GravityZone будет соединяться с NTSA (по умолчанию - 443).
  - Ключ сопряжения (токен), созданный в веб-консоли NTSA следующим образом:
    - a. Войдите в веб-консоль NTSA и перейдите на страницу **Лицензирование**
    - b. Выберите опцию **Интеграция с GravityZone**.
    - c. Нажмите **Создать Ключ Сопряжения**. Ключ появится автоматически.
    - d. Используйте кнопку **Скопировать в буфер обмена**, чтобы получить ключ сопряжения.
    - e. Нажмите **OK** для подтверждения.
5. Удостоверьтесь, что отображенный отпечаток хоста совпадает с хэшем сертификата SSL из устройства NTSA, затем активируйте опцию **Я принимаю сертификат**.
6. Нажмите **Сохранить**.

После успешного завершения настройки, интеграция отобразится со статусом **Синхронизировано**. Интеграция с NTSA может находиться в следующих состояниях:

- **N/A**: интеграция еще не настроена.
- **Синхронизировано**: интеграция настроена и включена.
- **Неверный токен**: ключ сопряжения из веб-консоли NTSA недействителен.

- **Ошибка соединения:** невозможно подключиться к указанному адресу веб-консоли NTSA (неверный IP / имя хоста).
- **Ошибка сертификата:** текущий отпечаток SSL сертификата из устройства NTSA не совпадает с изначально принятым отпечатком.
- **Неизвестная ошибка:** неизвестная ошибка соединения.

Поле **Последнее изменение статуса** отображает время и дату последнего успешного изменения настроек интеграции или смены статуса интеграции.

После настройки интеграции NTSA, вы можете включить / отключить интеграцию с помощью флагка в верхней части странице **NTSA**.

### Соединение ваших учетных записей GravityZone и NTSA

После настройки интеграции, ваши учетные записи GravityZone и NTSA будут соединены и вы сможете легко перейти в веб-консоль NTSA следующим образом:

1. В Control Center GravityZone, нажмите кнопку **NTSA**, расположенную в нижнем левом углу окна.
2. Вы будете перенаправлены на страницу авторизации веб-консоли NTSA. После ввода ваших учетных данных NTSA, вы сможете просмотреть веб-консоль NTSA.

Вам необходимо ввести учетные данные NTSA только один раз. Впоследствии, вы сможете заходить в веб-консоль NTSA автоматически, нажав кнопку **NTSA**, без необходимости снова вводить ваши учетные данные.

### Удаление интеграции NTSA

Удаление лицензионного ключа NTSA из страницы **Конфигурация > Лицензия** также удалит интеграцию NTSA.



#### Примечание

Ваша учетная запись NTSA и GravityZone будут разъединены в следующих случаях:

- Лицензионный ключ NTSA был удален.
- Пароль от NTSA был изменен.
- Пароль от GravityZone был изменен.

- Настройки интеграции NTSA были изменены.

## Сертификаты

Чтобы ваше развертывание GravityZone работало корректно и безопасно, вы должны создать и добавить сертификат безопасности в Control Center.

The screenshot shows the Bitdefender GravityZone Control Center interface. On the left, there's a sidebar with various navigation options: Dashboard, Network, Packages, Tasks, Policies, Assignment Rules, Reports, Quarantine, Accounts, User Activity, Configuration (which is selected and highlighted in blue), Update, and License. At the top right, there's a 'Welcome, Admin' message and a dropdown arrow. The main content area has a header with tabs: Mail Server, Proxy, Miscellaneous, Backup, Active Directory, Virtualization, and Certificates (which is also highlighted in blue). Below the tabs is a table with one row. The table columns are 'Certificate', 'Common Name', 'Issued By', and 'Expire Date'. The single row contains the text 'Control Center Security' under 'Certificate', and 'N/A' for all other columns.

Certificate	Common Name	Issued By	Expire Date
Control Center Security	N/A	N/A	N/A

Страница сертификатов

Control Center поддерживает следующие форматы сертификатов:

- PEM (.pem, .crt, .cer, .key)
- DER (.der, .cer)
- PKCS#7 (.p7b, .p7c)
- PKCS#12 (.p12, .pfx)

## Сертификаты безопасности Control Center

Сертификаты безопасности Control Center необходимы для того, чтобы веб-консоль Control Center отображалась в вашем веб-браузере как доверенный сайт. Control Center по умолчанию использует сертификат SSL, подписанный Bitdefender. Этот встроенный сертификат не признается веб-браузерами и, в результате, срабатывают предупреждения безопасности. Чтобы избежать предупреждений безопасности браузера, добавьте

сертификат SSL, подписанный вашей компанией или с помощью внешнего центра сертификации (CA).

Чтобы добавить или заменить сертификаты Control Center:

1. Перейдите на страницу **Configuration** и нажмите вкладку **Certificates**.
2. Нажмите на имя сертификата.
3. Выберите тип сертификата (с отдельным или встроенным личным ключом).
4. Нажмите кнопку **Add** рядом с полем **Certificate** и загрузите сертификат.
5. Для сертификата с отдельным личным ключом, нажмите кнопку **Add** рядом с полем **Private key** и загрузите личный ключ.
6. Если сертификат защищен паролем, введите пароль в соответствующем поле.
7. Нажмите **Сохранить**.

## Репозиторий

На этой вкладке отображается информация об обновлениях агента безопасности, включая версии продукта, хранящиеся на сервере обновлений, и версии, доступные в официальном репозитории Bitdefender, кольца обновлений, дата и время обновления и последняя проверка наличия новых версий.

### Примечание

Версии продукта недоступны для серверов безопасности.

## 5.1.5. Управление устройством GravityZone

GravityZone поставляется с базовой конфигурацией интерфейса, доступного из инструментария управления, который используется для управления средой виртуализации, в которой установлено устройство.

Это доступные основные параметры после первого развертывания устройства GravityZone:

- [Настройка параметров имени хоста](#)
- [Настройка сетевых параметров](#)
- [Настройка параметров прокси-сервера](#)



- Коммуникационный сервер MDM
- Дополнительные настройки
- Настройка языка

Используйте клавиши со стрелками и клавишу Tab для навигации по меню и опциям. Нажмите Enter для выбора определенных опций.

## Настройка имени хоста и параметров

Связь с ролями GravityZone осуществляется по IP-адресу или DNS-имени устройства, на которых они установлены. По умолчанию компоненты GravityZone связываются по IP-адресам. Если вы хотите обеспечить связь через имена DNS, необходимо настроить DNS-имена устройств GravityZone и убедиться, что они корректно разрешаются в IP-адреса, назначенные устройствам.

Требования к системе:

- Настройка DNS-записи на сервере DNS.
- DNS-имя должно корректно разрешаться в IP-адрес, назначенный устройству. Таким образом, вы должны убедиться, что устройство настроено на корректный IP-адрес.

Чтобы задать настройки имени хоста:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Выберите из главного меню **Configure Hostname Settings**.
3. Введите имя хоста устройства и имя домена службы каталогов (Active Directory, в случае необходимости).
4. Нажмите **OK**, чтобы сохранить изменения.

## Настройка сетевых параметров

Вы можете настроить устройство на автоматическое получение сетевых параметров от сервера DHCP или выбрать настройки параметров сети вручную. Если вы выберите использование DHCP, вы должны настроить DHCP-сервер, чтобы зарезервировать для устройства определенный IP-адрес.

Чтобы настроить сетевые параметры:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Выберите из главного меню **Configure Network Settings**.
3. Выберите сетевой интерфейс (по умолчанию eth0).
4. Выберите способ настройки:
  - **Настройка параметров сети вручную.** Вы должны указать IP-адрес, маску сети, адрес шлюза и DNS-сервера.
  - **Автоматическое получение сетевых настроек от сервера DHCP.** Используйте эту опцию только если вы настроили DHCP-сервер на резервирование определенного IP-адреса для устройства.
5. Вы можете проверить детали текущей IP-конфигурации или состояния соединения, выбрав соответствующие опции.

## Настройка параметров прокси-сервера

Если ваше устройство подключено к Интернету через прокси-сервер, вам необходимо настроить параметры прокси-сервера.

### Примечание

Настройки прокси-сервера также доступны из Control Center, на странице **Configuration > Proxy**. Изменение настроек прокси-сервера в одном месте автоматически обновит их и в других местах также.

Чтобы настроить параметры прокси-сервера:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Выберите из главного меню **Configure Proxy Settings**.
3. Выберите **Configure proxy settings**.
4. Введите адрес прокси-сервера. Используйте следующий синтаксис:
  - Если прокси-сервер не требует авторизации:  
`http(s)://<IP/hostname>:<port>`
  - Если прокси-сервер требует авторизацию:  
`http(s)://<username>:<password>@<IP/hostname>:<port>`

5. Нажмите **OK**, чтобы сохранить изменения.

Выберите **Show proxy information**, чтобы проверить настройки прокси-сервера.

## Коммуникационный сервер MDM



### Примечание

Эта конфигурация требуется только для управления мобильными устройствами, если ваш лицензионный ключ распространяется на службу Security for Mobile. Опция появится в меню после установки [Роль коммуникационного сервера](#).

При установке GravityZone по умолчанию, мобильные устройства могут управляться только тогда, когда они непосредственно связаны с корпоративной сетью (через Wi-Fi или VPN). Это происходит потому, что при регистрации мобильных устройств они настроены на подключение к коммуникационному серверу по локальным адресам.

Чтобы иметь возможность управлять мобильными устройствами через Интернет, независимо от того, где они находятся, необходимо настроить коммуникационный сервер на доступность с публичных адресов.

Для управления мобильными устройствами, когда они не подключены к сети компании, доступны следующие варианты:

- Настройте переадресацию портов на корпоративном шлюзе для устройства с ролью коммуникационного сервера.
- Добавьте дополнительный сетевой адаптер в устройство с ролью коммуникационного сервера и присвойте ему публичный IP-адрес.

В обоих случаях необходимо настроить коммуникационный сервер с внешним IP-адресом, чтобы управлять мобильными устройствами:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **MDM Communication Server**.
3. Нажмите **Configure MDM Server external address**.
4. Введите внешний адрес.

Используйте следующий синтаксис: `https://<IP/Domain>:<Port>`.

- Если вы используете перенаправление портов, необходимо ввести публичный IP-адрес или доменное имя и открыть нужный порт на шлюзе.
  - Если вы используете публичный IP-адрес для коммуникационного сервера, вам необходимо ввести публичный IP-адрес или доменное имя и порт, используемый коммуникационным сервером. По умолчанию порт 8443.
5. Нажмите **OK**, чтобы сохранить изменения.
  6. Нажмите **Show MDM Server external address**, чтобы проверить настройки.

## Дополнительные настройки

Расширенные настройки охватывают несколько вариантов ручного развертывания, расширения среды и усиления безопасности:

- Установка/удаление ролей
- Установка Security Server
- Задайте новый пароль базы данных.
- Сервер обновлений
- Конфигурирование роли балансировщика
- Репликация
- Включить Безопасный VPN-клuster
- Подключитесь к существующей базе данных
- Подключитесь к существующей базе данных (Безопасный VPN-клuster)
- Проверьте Безопасный VPN-клuster

Доступность опций зависит от установленных ролей и включенных служб. Например, если роль «Сервер базы данных» не установлена на устройстве, вы можете только установить роли или подключиться к базе данных GravityZone, развернутой в вашей сети. Как только роль сервера базы данных установлена на устройстве, опции подключения к другой базе данных становятся недоступными.

## Установка/удаление ролей

Устройство GravityZone может выполнять одну, несколько или все из перечисленных ролей:

- Сервер базы данных
- Сервер обновлений
- Веб-консоль
- Коммуникационный Сервер
- Инциденты сервера

Развертывание GravityZone требует выполнения по одному экземпляру каждой роли. Следовательно, в зависимости от предпочтений по распределению ролей GravityZone, вы будете развертывать от одного до четырех устройств GravityZone. Роль сервера баз данных должна быть установлена первой. В сценарии с несколькими устройствами GravityZone, вы будете устанавливать роль сервера базы данных на первом устройстве и настраивать все другие устройства на подключение к существующему экземпляру базы данных.



### Примечание

Вы можете установить дополнительные экземпляры определенных ролей, используя балансировщики ролей. Для получения более подробной информации, обратитесь к [«Конфигурирование роли балансировщика»](#) (р. 92).

Чтобы установить роли GravityZone:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.
3. Нажмите **Install/Uninstall Roles**.
4. Выберите **Add or remove roles**.
5. Выполните действия, соответствующие текущей ситуации:
  - Если это начальное развертывание GravityZone устройства, нажмите клавишу **Space**, а затем **Enter**, чтобы установить роль сервера базы данных. Вы должны подтвердить свой выбор, нажав **Enter** снова. Задайте пароль базы данных, а затем дождитесь завершения установки.

- Если вы уже развернули другое устройство с ролью сервера базы данных, выберите **Cancel** и вернитесь к меню **Add or remove roles**. Затем вы должны выбрать **Configure Database Address** и ввести адрес сервера базы данных. Убедитесь, что вы задали пароль базы данных перед доступом к этой опции. Если вы не знаете пароль базы данных, задайте новый, выбрав из главного меню **Advanced Settings > Set a new database password**.

Используйте следующий синтаксис: `http://<IP/Hostname>:<Port>`. По умолчанию порт базы данных 27017. Введите текущий пароль базы данных.

6. Установите другие роли, выбрав **Add or remove roles** из меню **Install/Uninstall Roles**, а затем роли для установки. Для каждой роли, которую вы хотите установить или удалить, нажмите клавишу **Space**, чтобы выбрать или отменить роль, и затем нажать **Enter** для выполнения. Вы должны подтвердить свой выбор, нажав клавишу **Enter** снова, а затем дождаться завершения установки.

#### Примечание

Каждая роль обычно устанавливается в течение нескольких минут. Во время установки, необходимые файлы загружаются из Интернет. Следовательно, установка занимает больше времени, если Интернет-соединение медленное. Если установка зависла, разверните устройство заново.

Вы можете просмотреть установленные роли и их IP-адреса, выбрав один из следующих вариантов из меню **Install/Uninstall Roles**:

- **Show locally installed roles**, для просмотра только ролей, установленных на этом устройстве.
- **Show all installed roles**, чтобы просмотреть все роли, установленные в вашей среде GravityZone.

#### Установка Security Server

#### Примечание

Security Server будет доступен для использования только если это позволяет лицензионный ключ.

Вы можете установить Security Server из GravityZone интерфейса конфигурации устройства, непосредственно на GravityZone устройстве или из Control Center, как самостоятельное устройство. Преимущества установки Security Server из устройства являются:

- Подходит для развертывания одного устройства GravityZone, выполняющего все роли.
- Вы можете видеть и использовать Security Server без интеграции GravityZone с платформой виртуализации.
- Для выполнения развертывания за меньшее число операций.

Требования к системе:

На машине GravityZone должна быть установлена роль сервера базы данных, или она может быть настроена на подключение к существующей базе данных.

Чтобы установить Security Server из интерфейса устройства:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.
3. Нажмите **Install Security Server**. Появится окно подтверждения.
4. Нажмите **Enter** для подтверждения и ожидайте окончания установки.

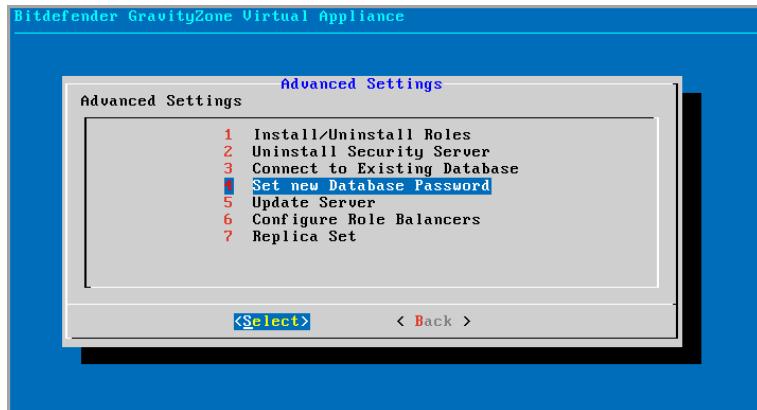


### Примечание

Вы можете деинсталлировать этот Security Server только из меню **Advanced Settings** интерфейса устройства.

**Задайте новый пароль базы данных.**

При установке роли сервера базы данных вы должны установить пароль для защиты базы данных. Если вы хотите изменить его, установите новый, выбрав **Расширенные настройки > Установите новый пароль базы данных** в главном меню.



Интерфейс консоли устройства: опция установки нового пароля базы данных

Следуйте инструкциям, чтобы установить надежный пароль.

### Настройка сервера обновлений

Устройство GravityZone по умолчанию настроено на обновление из Интернета. При желании, вы можете задать обновление установленных устройств с локального сервера обновлений Bitdefender (должна быть установлена машина GravityZone с ролью сервера обновлений).

Чтобы назначить адрес сервера обновлений:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.
3. Выберите **Update Server**.
4. Выберите **Configure update address**.
5. Введите IP-адрес или имя хоста устройства с ролью сервера обновлений. По умолчанию порт сервера обновлений 7074.

### Конфигурирование роли балансировщика

Для обеспечения надежности и масштабируемости, вы можете установить несколько экземпляров конкретных ролей (сервер инцидентов, коммуникационный сервер, веб-консоль).

Каждый экземпляр роли установлен на разных устройствах.

Все экземпляры конкретной роли должны быть подключены к другим ролям с помощью балансировщика ролей.

У каждой роли может быть только один балансировщик.

Устройство GravityZone включает в себя встроенный балансировщик, который вы можете установить и использовать. Если в вашей сети уже имеется программный или аппаратный балансировщик, вы можете выбрать его вместо того, чтобы использовать встроенный.

Встроенная роль балансировщика не может быть установлена вместе с другими ролями на машине GravityZone.

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.
3. Выберите **Configure Role Balancers**.
4. Выберите желаемую опцию:

- **Использование внешнего балансировщика.** Выберите эту опцию, если ваша сетевая инфраструктура уже включает программный или аппаратный балансировщик, который вы можете использовать. Вы должны ввести адрес балансировщика для каждой роли, которую вы хотите сбалансировать. Используйте следующий синтаксис:

`http(s)://<IP/Hostname>:<Port>`.

- **Использование встроенного балансировщика.** Выберите эту опцию, чтобы установить и использовать встроенный программный балансировщик нагрузки.



### Важно

To install multiple instances of the Incidents Server role you may only use the built-in balancer.

5. Нажмите **OK**, чтобы сохранить изменения.

## Репликация

С помощью этой опции можно включить использование репликации базы данных, вместо единичного экземпляра сервера базы данных. Этот механизм

позволяет создавать несколько экземпляров баз данных в распределенном окружении GravityZone, обеспечивая высокую доступность базы данных в случае сбоев.



### Важно

Репликация базы данных доступна только для свежих установок устройств GravityZone, начиная с версии 5.1.17-441.

## Настройка репликации

Во-первых, вы должны включить репликацию на первом установленном устройстве GravityZone. Затем вы сможете добавить участников репликации, установив роли сервера базы данных на других экземплярах GravityZone в этом же окружении.



### Важно

- Набор Реплик (Replica Set) требует как минимум три экземпляра для корректной работы.
- Вы можете добавить до семи серверов с ролью сервера базы данных, как участников репликации (ограничения MongoDB).
- Рекомендуется использовать нечетное число экземпляров базы данных. Четное число участников будет потреблять больше ресурсов только для тех же результатов.

Чтобы включить репликацию баз данных в среде GravityZone:

1. Установите роль сервера базы данных на первом GravityZone устройстве. Для получения более подробной информации, обратитесь к «[Установка/удаление ролей](#)» (р. 89).
2. Настройте другие машины для подключения к первому экземпляру базы данных. Для получения более подробной информации, обратитесь к «[Подключитесь к существующей базе данных](#)» (р. 96).
3. Перейдите в главное меню первого устройства, выберите **Advanced Settings** и затем нажмите для активации **Replica Set**. Появится окно подтверждения.
4. Выберите **Yes** для подтверждения.
5. Установите роль сервера базы данных на других GravityZone устройствах.

Как только эти шаги будут завершены, все экземпляры базы данных начнут работать в режиме репликации:

- Выбирается основной экземпляр и только он способен принимать операции записи.
- Основной экземпляр записывает все изменения, внесенные в его данные и ведет журнал.
- Вторичные экземпляры реплицируют этот журнал и осуществляют те же изменения в собственных наборах данных.
- Когда основной экземпляр становится недоступным, механизм репликации выберет один из вторичных экземпляров в качестве основного.
- Когда первичный экземпляр теряет связь с другими участниками группы более чем на 10 секунд, механизм репликации будет пытаться выбрать другого участника, чтобы сделать его основным.

### Удаление участников репликации

Для удаления экземпляров Набора Реплик, в меню устройства (в консольном интерфейсе) просто выберите **Установить/Удалить Роли > Добавить или Удалить Роли** и отменить роли **Базы данных**.

#### Примечание

Вы можете удалить участника репликации, только если по крайней мере, четыре экземпляра базы данных установлены в сети.

### Включить Безопасный VPN-клuster

Роли GravityZone имеют несколько внутренних служб, которые взаимодействуют только между собой. Для более безопасной среды вы можете изолировать эти сервисы, создав для них VPN-клuster. Находятся эти службы на одном и том же устройстве или на нескольких, затем они будут связываться по безопасному каналу.

#### Важно

- Эта функция требует стандартного развертывания GravityZone, без каких-либо установленных пользовательских инструментов.
- Как только кластер включен, вы не можете его отключить.

Для защиты внутренних служб на устройствах:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.
3. Выберите Включить **Безопасный VPN-кластер**.

Сообщение информирует вас об изменениях, которые будут сделаны.

4. Выберите **Да**, чтобы подтвердить и продолжить установку VPN.
- По завершении отобразится сообщение с подтверждением.

С этого момента все роли на устройстве устанавливаются в защищенном режиме, и службы будут взаимодействовать через интерфейс VPN. Любое новое устройство, которое вы добавляете в среду, должно присоединиться к VPN-кластеру. Для получения более подробной информации, обратитесь к «[Подключитесь к существующей базе данных \(Безопасный VPN-кластер\)](#)» (р. 97).

### **Подключитесь к существующей базе данных**

В распределенной архитектуре GravityZone необходимо установить роль сервера базы данных на первом устройстве, а затем настроить все другие устройства для подключения к существующему экземпляру базы данных. Таким образом, все устройства будут использовать одну базу данных.



#### **Важно**

Рекомендуется включить Безопасный VPN-кластер и подключиться к базе данных в таком кластере. Для получения более подробной информации, обратитесь к:

- [«Включить Безопасный VPN-кластер» \(р. 95\)](#)
- [«Подключитесь к существующей базе данных \(Безопасный VPN-кластер\)» \(р. 97\)](#)

Чтобы подключить устройство к базе данных GravityZone вне Безопасного VPN-кластера

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.

### 3. Выберите **Connect to Existing Database**.



#### Примечание

Убедитесь, что вы задали пароль базы данных перед доступом к этой опции. Если Вы не знаете пароль базы данных, задайте новый, выбрав в главном меню **Расширенные настройки > Залать новый пароль базы данных**.

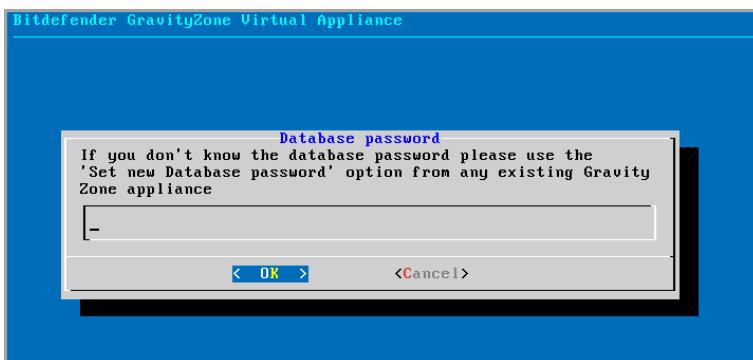
### 4. Выберите **Configure Database Server address**.

### 5. Введите адрес базы данных, используя следующий синтаксис:

<IP/Hostname>:<Port>

Указание порта необязательно. По умолчанию порт 27017.

### 6. Введите текущий пароль базы данных.



Интерфейс консоли устройства: ввод пароля базы данных

### 7. Нажмите **OK**, чтобы сохранить изменения.

### 8. Нажмите **Show Database Server address**, чтобы убедиться, что адрес был правильно настроен.

#### Подключитесь к существующей базе данных (Безопасный VPN-клuster)

Используйте эту опцию, когда вам нужно расширить развертывание GravityZone с помощью большего количества устройств, и Безопасный VPN-клuster включен. Таким образом, новое устройство будет совместно

использовать ту же базу данных с существующим развертыванием в безопасном режиме.

Для получения дополнительной информации о Безопасном VPN-кластере, обратитесь к [«Включить Безопасный VPN-кластер»](#) (р. 95).

### Требования к системе

Прежде чем продолжить, убедитесь, что у вас под рукой есть следующее:

- IP-адрес сервера базы данных
- Пароль для пользователя **bdadmin** на устройстве с ролью сервера базы данных

### Подключитесь к базе данных

Чтобы подключить устройство к базе данных GravityZone в Безопасном VPN-кластере:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.
3. Выберите **Подключиться к существующей базе данных (Безопасный VPN-кластер)**.  
Вы будете проинформированы о требованиях и альтернативах, если они не будут выполнены.
4. Выберите **OK**, чтобы подтвердить и продолжить.
5. Введите IP-адрес сервера базы данных в Безопасном VPN-кластере.
6. Введите пароль для пользователя **bdadmin** на устройстве с сервером базы данных.
7. Выберите **OK**, чтобы сохранить изменения и продолжить.

Когда процесс завершится, вы получите сообщение с подтверждением. Новое устройство становится членом кластера, и оно будет взаимодействовать с другими устройствами безопасным способом. Все устройства будут использовать одну базу данных.

## Проверьте статус Безопасного VPN-кластера

Эта опция доступна только после того, как вы ранее включили Безопасный VPN-кластер. Выберите эту опцию, чтобы проверить, какие устройства в вашем развертывании GravityZone еще не защитили свои службы. Возможно, вам придется провести дальнейшее расследование и проверить, что устройства онлайн и доступны.

## Настройка языка

Чтобы изменить язык конфигурационного интерфейса устройства:

1. Выберите **Configure Language** из главного меню.
2. Выберите язык из доступных вариантов. Появится окно подтверждения.



### Примечание

Вы должны прокрутить вниз, чтобы найти свой язык.

3. Нажмите **OK**, чтобы сохранить изменения.

## 5.2. Управление лицензиями

GravityZone лицензируется одним ключом для всех служб безопасности.

Помимо основных служб безопасности, GravityZone также предусматривает важные функции защиты в качестве дополнений. Каждое дополнение лицензируется с помощью отдельного ключа, вы можете использовать его только вместе с основной действительной лицензией. Если основная лицензия недействительна, вы будете видеть настройки функций, но не сможете применять их.

Вы можете выбрать GravityZone для тестирования и решить, это ли правильное решение для вашей организации. Для активации пробного периода, необходимо ввести лицензионный ключ пробной версии из регистрационного письма в Control Center.

Для продолжения использования GravityZone после завершения пробного периода, вы должны приобрести лицензионный ключ и использовать его для регистрации продукта.

Чтобы приобрести лицензию, свяжитесь с реселлером Bitdefender или свяжитесь с нами по электронной почте [enterprisesales@bitdefender.com](mailto:enterprisesales@bitdefender.com).

Лицензионным ключом GravityZone можно управлять на странице **License** в Control Center. Когда текущий лицензионный ключ подходит к концу, появится сообщение в консоли, чтобы сообщить вам, что он должен быть продлен. Чтобы ввести новый лицензионный ключ или просмотреть текущую информацию о лицензии, перейдите на страницу **License**.

### 5.2.1. Поиск реселлера

Наши реселлеры помогут вам со всей необходимой информацией и помогут выбрать лучший для вас вариант лицензирования.

Чтобы найти реселлера Bitdefender в вашей стране:

1. Перейдите на страницу [Partner Locator](#) на веб-сайте Bitdefender.
2. Выберите страну, в которой вы проживаете, чтобы просмотреть контактную информацию доступных партнеров Bitdefender.
3. Если не удалось найти реселлера Bitdefender в вашей стране, свяжитесь с нами по адресу электронной почты [enterprisesales@bitdefender.com](mailto:enterprisesales@bitdefender.com).

### 5.2.2. Ввод ваших лицензионных ключей

Регистрация лицензий GravityZone может быть сделана онлайн или оффлайн (когда интернет-соединение не доступно). В обоих случаях необходимо предоставить действительный лицензионный ключ.

Для оффлайн регистрации, вам также понадобится оффлайн регистрационный код, связанный с лицензионным ключом.

Чтобы изменить текущий лицензионный ключ или зарегистрировать надстройку:

1. Войдите в Control Center, используя учетную запись администратора компании.
2. Перейдите на страницу [Configuration > License](#).
3. Нажмите кнопку **Добавить** в верхней части таблицы.
4. Выберите тип регистрации:
  - **Online**. В этом случае, введите действующий лицензионный ключ в поле **License key**. Лицензионный ключ будет проверен и подтвержден онлайн.
  - **Offline**, когда подключение к интернету отсутствует. В этом случае, вы должны предоставить лицензионный ключ, а также его регистрационный код.

Если лицензионный ключ не действителен, ошибка проверки отобразится в виде подсказки над полем **License key**.

5. Нажмите **Добавить**. Лицензионный ключ будет добавлен на страницу **License**, где вы можете проверить подробности лицензии.
6. Нажмите **Сохранить**, чтобы сохранить изменения. Control Center перезагрузится и вы должны будете войти еще раз, чтобы просмотреть изменения.



### Примечание

Надстройки можно использовать до тех пор, пока действует совместимая базовая лицензия. В противном случае вы будете видеть функции, но не сможете их использовать.

## 5.2.3. Проверка текущих параметров лицензирования

Для просмотра подробностей лицензии:

1. Войдите в Control Center, используя учетную запись администратора компании.
2. Перейдите на страницу **Configuration > License**.

The screenshot shows the Bitdefender GravityZone Control Center interface. The top navigation bar includes the Bitdefender logo, the word "GravityZone", a search bar, and a user welcome message "Welcome, Admin". On the far right of the header is a bell icon for notifications. The left sidebar contains a vertical menu with links: Dashboard, Network, Packages, Tasks, Policies (with "Assignation Rules" under it), Reports, Quarantine, Accounts (with "User Activity" under it), Configuration (with "Update" under it), and License (which is highlighted in blue). The main content area has a title "Configuration > License". Below the title are four buttons: "+ Add", "(i) Reset", "(-) Delete", and "(r) Refresh". A table follows, with columns: Key, Status, Expiry Date, and Usage. There is one entry in the table:

	Key	Status	Expiry Date	Usage
<input type="checkbox"/>	[Redacted]	Active	21 Dec 2015, 195 days...	0/50 Entities, Available

Страница лицензии

3. В таблице вы можете просмотреть информацию о лицензионном ключе.

- Лицензионный ключ
- Статус лицензионного ключа
- Срок действия и оставшийся срок действия лицензии



### Важно

По истечении срока действия лицензии модули защиты установленных агентов отключены. В результате конечные точки больше не защищены, и вы не можете выполнять какую-либо задачу проверки. Любой новый установленный агент войдет в ознакомительный период.

- Подсчет используемых лицензий

## 5.2.4. Сброс счетчика использования лицензии

Вы можете найти информацию о использовании вашего лицензионного ключа на странице **License**, под столбцом **Usage**.

Если вам нужно обновить информацию об использовании, выберите лицензионный ключ и нажмите кнопку **Reset** в верхней части таблицы.

## 5.3. Установка агентов по безопасности

Чтобы защитить ваши физические и виртуальные конечные устройства, необходимо установить агента безопасности на каждом из них. Кроме управления защитой на локальной конечной точке, агент безопасности также взаимодействует с Control Center для приема команд администратора и отправляет результаты их действий.

Вы можете установить агента безопасности на физических и виртуальных конечных точках локально [by running installation packages locally](#) или удаленно [by running installation tasks remotely](#) из Control Center.

Очень важно внимательно прочитать и следовать инструкциям по подготовке к установке.

В нормальном режиме агенты безопасности имеют упрощенный пользовательский интерфейс. Он позволяет пользователям проверять только состояние защиты и выполнять основные задачи по обеспечению безопасности (обновления и сканирования), без предоставления доступа к настройкам.

По умолчанию, язык дисплея пользовательского интерфейса, на конечных точках, находящихся под защитой, выбирается во время установки, на основании языка вашей учетной записи GravityZone .

Чтобы установить пользовательский интерфейс на другом языке на некоторых конечных точках Windows, вы можете создать установочный пакет и выбрать язык в его опциях. Эта опция недоступна для конечных точек Mac и Linux. Для получения более подробной информации о создании пакетов установки, обратитесь к [«Создание инсталляционных пакетов» \(р. 104\)](#).

### 5.3.1. Подготовка к установке

Перед установкой выполните следующие подготовительные шаги, чтобы убедиться, что она пройдет без проблем:

1. Убедитесь, что выбранные конечные точки удовлетворяют [minimum system requirements](#). Для некоторых конечных точек вам, возможно, потребуется установить последний доступный пакет обновлений для операционной системы или освободить дисковое пространство. Составьте список конечных точек, не отвечающих необходимым требованиям, чтобы вы могли исключить их из управления.
2. Установка требует привилегий администратора и доступ в Интернет. Если целевые конечные точки находятся в домене Active Directory, вы должны использовать учетные данные администратора домена для удаленной установки. В противном случае убедитесь, что у вас есть необходимые полномочия для всех конечных точек.
3. Конечные точки должны иметь сетевое подключение к устройству GravityZone.
4. Рекомендуется использовать статический IP-адрес для Relay сервера. Если вы не установите статический IP-адрес, используйте имя хоста машины.

### 5.3.2. Локальная установка

Одним из способов установить агента безопасности на конечной точке является локальный запуск установочного пакета.

Вы можете создавать и управлять инсталляционными пакетами на странице **Network > Packages**.

The screenshot shows the Bitdefender Control Center interface. On the left, there's a sidebar with links for Dashboard, Network (which is selected and highlighted in blue), Tasks, and Policies. At the top right, there's a welcome message "Welcome, Admin" and a notification bell icon. Below the sidebar, there's a toolbar with buttons for Add (+), Download, Delete (-), and Refresh. The main area is a table titled "Packages". The columns are labeled Name, Type, Language, Description, and Status. There's one row visible in the table.

## Страница пакетов

После установки первого клиента, он будет использоваться для обнаружения других конечных точек в той же сети, используя механизм сетевого обнаружения. Для получения более подробной информации о сетевом обнаружении, обратитесь к [«Как работает сетевое обнаружение» \(р. 117\)](#).

Чтобы локально установить агента безопасности на конечной точке, выполните следующие действия:

1. [Create an installation package](#) в соответствии с вашими потребностями.



### Примечание

Этот шаг не является обязательным, если инсталляционный пакет уже был создан для сети под вашей учетной записью.

2. [Download the installation package](#) на выбранную конечную точку.

Вы можете поочередно [отправлять ссылки для загрузки установочного пакета по электронной почте](#) нескольким пользователям в вашей сети.

3. [Run the installation package](#) на выбранной конечной точке.

## Создание инсталляционных пакетов

Чтобы создать инсталляционный пакет:

1. Подключитесь и войдите в Control Center.
2. Перейдите на страницу **Network > Packages**.
3. Нажмите кнопку **+ Добавить** в верхней части таблицы. Появится окно настроек.

General

Name: \*

Description:

Language: English

Modules:

Antimalware  
 Advanced Threat Control  
 Advanced Anti-Exploit  
 Firewall  
 Network Protection  
 Content Control  
 Network Attack Defense  
 Device Control  
 Power User

## Создание пакета - Опции

4. Введите подходящее имя и описание для пакета, который вы хотите создать.
5. В поле **Language**, выберите нужный язык для интерфейса клиента.
6. Выберите роль целевой конечной точки:
7. **Разное.** Вы можете настроить следующие параметры для некоторых типов файлов на определенных конечных точках:
  - **Отправка аварийного дампа.** Выберите этот параметр, чтобы отправить файлы дампа памяти в лабораторию Bitdefender для анализа сбоя агента безопасности. Аварийные дампы помогут нашим инженерам найти причину, которая вызвала проблему, и предотвратить ее возникновение в дальнейшем. Никакая персональная информация не будет отправлена.
  - **Отправлять файлы карантина в лабораторию Bitdefender каждые (часы).** По умолчанию, файлы из карантина автоматически отправляются в лабораторию Bitdefender каждый час. Вы можете отредактировать интервал отправки файлов. Специалисты по вирусам Bitdefender проанализируют образцы файлов. Если наличие

вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

- **Отправлять подозрительные исполняемые файлы в Bitdefender.** Выберите этот параметр, чтобы отправить файлы, которые кажутся ненадежными или имеют подозрительное поведение, в Bitdefender Labs для анализа.

#### Примечание

Для получения информации о том, как этот параметр противоречит правилам HIPAA, обратитесь к «[Bitdefender GravityZone и HIPAA](#)» (п. 130).

#### 8. Важно

При использовании пользовательского пути убедитесь, что у вас есть правильный установочный пакет для каждой операционной системы.

9. При желании, вы можете установить пароль, чтобы запретить пользователям удалять защиту. Выберите **Set uninstall password** и введите желаемый пароль в соответствующие поля.
10. Если выбранные конечные точки находятся в инвентаризации сети под **Custom Groups**, вы можете переместить их в определенную папку сразу после завершения развертывания агентов безопасности.

Нажмите **Use custom folder** и выберите папку в соответствующей таблице.

11. В разделе **Установщик**, выберите объект, к которому выбранные конечные точки будут подключаться для установки и обновления клиента:

- **GravityZone Appliance**, если конечные точки будут подключаться непосредственно к устройству GravityZone.

В этом случае, вы также можете определить:

- Пользовательский коммуникационный сервер, набрав его IP-адрес или имя хоста, в случае необходимости.
- Настройки прокси-сервера, если требуемые конечные точки будут общаться с устройством GravityZone через прокси-сервер. В этом случае выберите **Использовать прокси для общения** и введите необходимые параметры прокси-сервера в полях ниже.

- **Ретранслятор безопасности конечной точки**, если вы хотите подключить конечные точки к клиенту Relay, установленному в вашей сети. Все

машины с ролью ретранслятора, обнаруженные в вашей сети, будут отображены в таблице ниже. Выберите компьютер с ролью ретранслятора, который Вам нужен. Подключенные конечные точки будут сообщаться при помощи Control Center только через выбранный компьютер с ролью ретранслятора.

## 12. Нажмите **Сохранить**.

Обновленный пакет будет добавлен в список пакетов.



### Примечание

Настройки, заданные в пакете установки будут применяться к конечным точкам сразу же после установки. Как только политика применится к клиенту, параметры, заданные политикой, будут применены, заменив некоторые параметры инсталляционного пакета (например, коммуникационные серверы или настройки прокси).

## Скачивание установочных пакетов

Чтобы скачать установочные пакеты агентов безопасности:

1. Ввойдите в Control Center из конечной точки, на которой вы хотите установить защиту.
2. Перейдите на страницу **Network > Packages**.
3. Выберите установочный пакет, который вы хотите загрузить.
4. Нажмите кнопку **Download** в верхней части таблицы и выберите тип установки, который вы хотите использовать. Доступны два типа установочных файлов:

- **Загрузчик.** Загрузчик в первую очередь загружает полный установочный комплект из облачных серверов Bitdefender, а затем начинает установку. Это небольшой по размеру файл и может быть запущена как на 32-битных, так и на 64-битных системах (что делает его легким в распространении). С другой стороны, это требует активного подключения к Интернету.
- **Full Kit.** Полные инсталляционные комплекты больше по размеру и они должны быть запущены для конкретного типа операционной системы. Полные комплексы предназначены для установки защиты на конечных точках с медленным Интернетом или без подключения к Интернету. Скачайте этот файл на конечную точку подключенную к интернету,

затем распространите его на другие конечные точки с использованием внешних носителей или сетевой папки.



### Примечание

Доступные полные версии комплектов:

- Windows OS: 32-бит и 64-бит системы

5. Сохраните файл на конечной точке.



### Предупреждение

- Скаченный исполняемый файл не должен быть переименован, в противном случае он не будет иметь возможность скачать установочные файлы из сервера Bitdefender.

6. Кроме того, если выбран Загрузчик, можно создать пакет MSI для конечных точек Windows. Для получения более подробной информации смотрите [этую статью базы знаний](#).

## Переслать ссылки на установочные пакеты по электронной почте

Возможно, вы захотите быстро сообщить другим пользователям, что инсталляционный пакет доступен для загрузки. В этом случае выполните действия, описанные ниже:

1. Перейдите на страницу **Network > Packages**.
2. Выберите нужный инсталляционный пакет.
3. Нажмите кнопку **Отправить ссылки для загрузки** в верхней части таблицы. Появится окно настроек.
4. Введите адрес электронной почты пользователя, которому вы хотите передать ссылку для загрузки установочного пакета. Нажмайте **Enter** после написания каждого электронного письма.  
Убедитесь, что каждый введенный адрес электронной почты действителен.
5. Если вы хотите просмотреть ссылки для скачивания перед отправкой их по электронной почте, нажмите кнопку **Установочные ссылки**.
6. Нажмите **Отправить**. На каждый указанный адрес электронной почты отправляется письмо, содержащее ссылку на установку.

## Запуск установочных пакетов

Для запуска процесса инсталляции, пакет установки должен быть запущен с правами администратора.

Для каждой операционной системы пакет устанавливается по-разному, как указано ниже:

- На операционных системах Windows и MAC:
  1. На выбранную конечную точку, скачайте установочный файл из Control Center или скопируйте его из сетевой папки.
  2. Если вы скачали полный комплект, извлеките файлы из архива.
  3. Запустите исполняемый файл.

После установки агента безопасности, конечная точка будет отображаться в Control Center как управляемая (страница **Network**) в течение нескольких минут.

### 5.3.3. Удаленная установка

Control Center позволяет удаленно установить агента безопасности на конечных точках из сред интегрированных с Control Center и на других конечных точках, обнаруженных в сети с помощью задач установки. В среде VMware, удаленная установка опирается на инструменты VMware, а в среде Citrix XenServer и Nutanix Prism Element, она опирается на общие административные системные ресурсы Windows и SSH.

После установки агента безопасности на конечной точке, может понадобится несколько минут для остальных конечных точек сети, чтобы стать видимыми в Control Center.

Bitdefender Endpoint Security Tools включает в себя автоматический механизм сетевого обнаружения, что позволяет обнаруживать конечные точки, которые не находятся в Active Directory. Обнаруженные конечные точки отображаются в виде **unmanaged** на странице **Network**, в обзоре **Computers**, под **Custom Groups**. Control Center автоматически удаляет конечные устройства Active Directory из списка обнаруженных устройств.

Чтобы включить сетевое обнаружение, вы должны иметь установленный Bitdefender Endpoint Security Tools, по крайней мере, на одной конечной точке в сети. Эта конечная точка будет использоваться для сканирования сети и

установки Bitdefender Endpoint Security Tools на незащищенных конечных точках.

Для получения более подробной информации о сетевом обнаружении, обратитесь к [«Как работает сетевое обнаружение» \(р. 117\)](#).

## Требования для удаленной установки

Для запуска удаленной установки:

- Для Windows :
  - Административный ресурс admin \$ должен быть включен. Настройте каждую целевую рабочую станцию, чтобы не использовать расширенный общий доступ к файлам.
  - Настройте контроль учетных записей (UAC) в зависимости от операционной системы, работающей на целевых конечных точках. Если конечные точки находятся в домене Active Directory, вы можете использовать групповую политику для настройки контроля учетных записей. Для получения подробной информации смотрите [этую статью базы знаний](#).



### Примечание

Удаленное развертывание работает только в современных операционных системах, начиная с Windows 7 / Windows Server 2008 R2, для которых Bitdefender предоставляет полную поддержку. Для получения более подробной информации, обратитесь к [«Поддерживаемые операционные системы» \(р. 24\)](#).

- На Linux SSH должен быть включен.
- В macOS: удаленный вход и обмен файлами должны быть включены.

## Выполнение задач удаленной установки

Чтобы запустить задачу удаленной установки:

1. Подключитесь и войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. Выберите **компьютеры и виртуальные машины** из меню видов сетей.

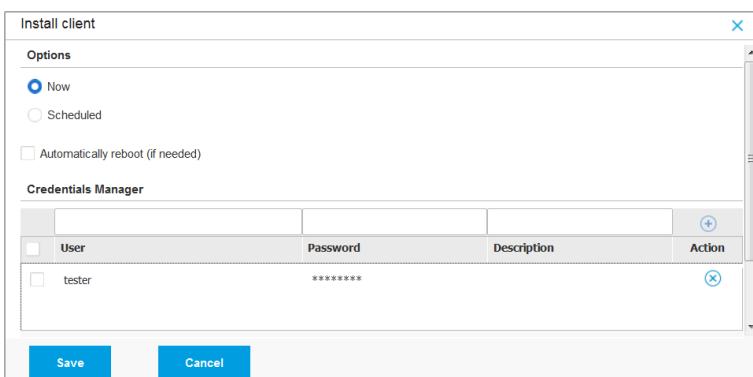
4. Выберите нужную группу в левой панели. Объекты, содержащиеся в выбранной группе, будут отображены в таблице правой панели.

### Примечание

При желании, вы можете применять фильтры для отображения только неуправляемых конечных точек. Нажмите меню **Фильтры** и выберите следующие параметры: **Неуправляемые** на вкладке **Безопасность** и **Все предметы рекурсивно** на вкладке **Глубина**.

5. Выберите объекты (конечные точки или группы конечных точек), на которых вы хотите установить защиту.  
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить**.

Отобразится мастер установки **Install Client**.



7. В разделе **Опции**, настройте время установки:
- **Сейчас**, чтобы немедленно начать развертывание.
  - **Запланировано**, настроить интервал повторения развертывания. В этом случае, выберите желаемый интервал времени (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.



### Примечание

Например, когда некоторые операции требуется выполнить на нужной машине перед установкой клиента (например, удаление другого программного обеспечения и перезагрузки ОС), вы можете запланировать запуск задачи развертывания каждые 2 часа. Задача будет запускаться на каждом компьютере каждые 2 часа до тех пор, пока развертывание не будет завершено.

8. Если вы хотите, чтобы заданные конечные точки перезапустились после завершения установки, выберите **Автоматическая перезагрузка (при необходимости)**.
9. В разделе **Диспетчер учетных задач**, укажите учетные данные администратора, необходимые для удаленной аутентификации на заданных конечных точках. Вы можете добавить учетные данные, набрав имя пользователя и пароль, для каждой выбранной операционной системы.



### Важно

Для станций под Windows 8.1, необходимо предоставить учетные данные встроенной учетной записи администратора или учетной записи администратора домена. Для получения подробной информации смотрите [эту статью базы знаний](#).

Чтобы добавить необходимые учетные данные ОС:

- a. Введите имя пользователя и пароль учетной записи администратора в соответствующих полях заголовка таблицы.

Если компьютеры находятся в домене, достаточно ввести учетные данные администратора домена.

Используйте правила именования Windows при вводе имени учетной записи:

- Для машин из службы каталогов Active Directory используйте следующий синтаксис: `username@domain.com` и `domain\username`. Чтобы быть уверенным, что введенные учетные данные будут работать, добавьте их в обоих видах (`username@domain.com` и `domain\username`).
- Для машин из рабочей группы достаточно ввести только имя пользователя без имени рабочей группы.

При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт.

- b. Нажмите кнопку **Добавить**. Учетная запись будет добавлена в список учетных данных.



### Примечание

Указанные учетные данные автоматически сохраняются в [Менеджере учетных данных](#), так что вам не придется вводить их в следующий раз. Для доступа к диспетчеру учетных данных, просто укажите ваше имя пользователя в правом верхнем углу консоли.



### Важно

Если предоставленные учетные данные являются недействительными, развертывание клиента на соответствующих конечных точках не произойдет. Не забудьте обновить учетные данные введенной ОС в диспетчере учетных данных, если они изменились на конечных точках.

10. Установите флагки на соответствующие аккаунты, которые вы хотите использовать.



### Примечание

Предупреждающее сообщение будет отображаться до тех пор, пока вы не выберите какие-нибудь учетные данные. Этот шаг является обязательным для удаленной установки агента безопасности на конечных точках.

11. В разделе **Установщик**, выберите объект, к которому выбранные конечные точки будут подключаться для установки и обновления клиента:

- **GravityZone Appliance**, если конечные точки будут подключаться непосредственно к устройству GravityZone.

В этом случае, вы также можете указать:

- Пользовательский коммуникационный сервер, набрав его IP-адрес или имя хоста, в случае необходимости.
- Настройки прокси-сервера, если требуемые конечные точки будут общаться с устройством GravityZone через прокси-сервер. В этом случае выберите **Использовать прокси для общения** и введите необходимые параметры прокси-сервера в полях ниже.

- Ретранслятор безопасности конечной точки, если вы хотите подключить конечные точки к клиенту Relay, установленному в вашей сети. Все машины с ролью ретранслятора, обнаруженные в вашей сети, будут отображены в таблице ниже. Выберите компьютер с ролью ретранслятора, который Вам нужен. Подключенные конечные точки будут сообщаться при помощи Control Center только через выбранный компьютер с ролью ретранслятора.

**Важно**

При развертывании через агента ретранслятора, должен быть открыт 7074 порт.

Deployer				
Deployer:		Endpoint Security Relay		
Name	IP	Custom Server Name/IP	Label	
CO_SUPA	192.168.0.183		N/A	
FC-WIN7-X64-01	192.168.3.80		N/A	

First Page ← Page 1 of 1 → Last Page 20 ▾ 2 items

12. Используйте раздел **Дополнительные цели**, если вы хотите развернуть клиента на определенных машинах в вашей сети, которые не отображаются в сетевом содержимом. Раскройте раздел и введите через запятую IP-адреса или имена хостов этих машин в специальном поле. Вы можете добавить столько IP-адресов, сколько вам нужно.
13. Вы должны выбрать один установочный пакет для текущего развертывания. Нажмите на список **Использовать пакет** и выберите установочный пакет, который вам нужен. Вы можете найти здесь все инсталляционные пакеты, созданные ранее под вашей учетной записью, а также пакеты установки по умолчанию, доступные в Control Center.
14. При необходимости, вы можете изменить некоторые настройки выбранного пакета установки с помощью кнопки **Настроить**, рядом с полем **Использовать пакет**.

Настройки инсталляционного пакета появятся ниже и вы сможете сделать необходимые изменения. Чтобы узнать больше о редактировании инсталляционных пакетов, обратитесь к [«Создание инсталляционных пакетов» \(р. 104\)](#).

Если вы хотите сохранить изменения как новый пакет, выберите опцию **Сохранить как пакет**, расположенную в нижней части списка параметров пакета, и введите имя для нового пакета установки.

15. Нажмите **Сохранить**. Появится окно подтверждения.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**.

### 5.3.4. Подготовка систем Linux для сканирования при доступе

Bitdefender Endpoint Security Tools для Linux включает возможности сканирования при доступе, которые работают с конкретными дистрибутивами Linux и версиями ядра. Для получения дополнительных сведений обратитесь к разделу [системные требования](#).

Далее вы узнаете, как вручную скомпилировать модуль DazukoFS.

#### Компиляция вручную модуля DazukoFS

Выполните следующие действия для компиляции DazukoFS для нужной версии ядра системы, а затем загрузите модуль:

1. Загрузка подходящих ядер.

- На системах **Ubuntu**, запустите эту команду:

```
$ sudo apt-get install linux-headers-`uname -r`
```

- На системах **RHEL/CentOS**, запустите эту команду:

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. На системах **Ubuntu**, вам необходим `build-essential`:

```
$ sudo apt-get install build-essential
```

3. Скопируйте и извлеките исходный код DazukoFS в предпочтительном каталоге:

```
# mkdir temp  
# cd temp  
# cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz  
# tar -xzvf dazukofs-source.tar.gz  
# cd dazukofs-3.1.4
```

4. Компиляция модуля:

```
# make
```

5. Установка и загрузка модуля:

```
# make dazukofs_install
```

## Требования по использованию сканирования при доступе с DazukoFS

Для совместной работы DazukoFS и сканирования при доступе, несколько условий должно быть выполнено. Пожалуйста, проверьте, применимы ли любые заявления ниже, к вашей системе Linux и следуйте инструкциям, чтобы избежать проблем.

- Политика SELinux должна быть отключена или установлена на **permissive**. Чтобы проверить и скорректировать настройки политики SELinux, отредактируйте файл `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools эксклюзивно совместим с версией DazukoFS, включенной в инсталляционный пакет. Если DazukoFS уже установлен в системе, удалите его перед установкой Bitdefender Endpoint Security Tools.
- DazukoFS поддерживает определенные версии ядра. Если пакет DazukoFS поставляемый с Bitdefender Endpoint Security Tools не совместим с версией ядра системы, модуль не загрузится. В таком случае, вы можете обновить ядро до поддерживаемой версии или перекомпилировать модуль DazukoFS для вашей версии ядра. Вы можете найти пакет DazukoFS в каталоге установки Bitdefender Endpoint Security Tools:

/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz

- Когда для обмена файлами используются специальные серверы, такие как NFS, UNFSv3 или Samba, вы должны запустить службы в следующем порядке:

1. Включение сканирования при доступе через политику из Control Center.

Для получения более подробной информации, обратитесь к Руководству администратора GravityZone.

2. Запуск службы сетевого обмена.

Для NFS:

```
# service nfs start
```

Для UNFSv3:

```
# service unfs3 start
```

Для Samba:

```
# service smbd start
```



### Важно

Для службы NFS, DazukoFS совместим только с пользовательским сервером NFS.

#### 5.3.5. Как работает сетевое обнаружение

Кроме интеграции с Active Directory, GravityZone также включает в себя автоматический механизм сетевого обнаружения, предназначенный для обнаружения компьютеров рабочей группы.

GravityZone использует службу **Microsoft Computer Browser** и инструмент **NBTscan** для обнаружения сети.

Служба просмотра компьютеров является сетевой технологией, используемой компьютерами на базе Windows, для хранения и обновления списков доменов, рабочих групп и компьютеров в них, а также для предоставления этих списков

клиентам-компьютерам по запросу. Компьютеры, обнаруженные в сети с помощью службы просмотра компьютеров (Computer Browser service), можно просмотреть запуском команды **net view**, набранной в командной строке.

```
Z:\>net view
Server Name      Remark
\\SCIREFDL
\\SCIREFJM
\\SCIREFLL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

Команда "net view"

Средство NBTscan сканирует компьютерные сети, используя NetBIOS. Он запрашивает каждую конечную точку в сети и добывает такую информацию, как IP-адрес, имя компьютера NetBIOS и MAC-адрес.

### Важно

Control Center не использует информацию о сети из Active Directory или из функции карты сети. Кarta сети использует другую технологию обнаружения сети: Протокол обнаружения топологии канального уровня (LLTD).

Control Center обрабатывает список ресурсов, добавляя новые обнаруженные компьютеры в свой **Unmanaged Computers** список. Ранее обнаруженные компьютеры, не удаляются после нового запроса обнаружения сети, так что вы должны вручную исключить & удалить компьютеры, которые больше не в сети.

- Если Relay установлен на компьютере рабочей группы, то только компьютеры из этой рабочей группы будут отображены в Control Center.
- Если Relay установлен на доменном компьютере, то только компьютеры этого домена будут отображены в Control Center. Компьютеры от других доменов могут быть обнаружены, если есть доверительные отношения с доменом, где установлен Relay.

Последующие запросы сетевого обнаружения выполняются регулярно каждый час. Для каждого нового запроса Control Center делит пространство управляемых компьютеров на области видимости и затем назначает один Relay в каждой области для выполнения задачи. Область видимости представляет собой группу компьютеров, которые обнаруживают друг друга.

Как правило, зона видимости определяется рабочей группой или доменом, но это зависит от топологии сети и конфигурации. В некоторых случаях, область видимости может состоять из нескольких доменов и рабочих групп.

Если выбранному Relay не удается выполнить запрос, Control Center ожидает следующего запланированного запроса, не выбирая другой Relay, чтобы повторить попытку.

## Подробнее о службе "Обозреватель компьютеров" Microsoft

Краткие сведения о службе Обозреватель компьютеров:

- Работает независимо от Active Directory.
- Работает исключительно в сетях IPv4 и действует независимо в пределах сетевой группы (рабочей группы или домена). Список просмотра составляется и поддерживается для каждой сетевой группы.
- Обычно используют широковещательный сервер без установления соединения для связи между узлами.
- Использование NetBIOS поверх TCP/IP (NetBT).
- Требуется разрешение имен NetBIOS. Рекомендуется иметь Windows Internet Name Service (WINS) инфраструктуру, работающую в сети.
- Не включен по умолчанию в Windows Server 2008 и 2008 R2.

Для получения более подробной информации о службе обозревателя (Computer Browser), проверьте [Computer Browser Service Technical Reference](#) на Microsoft TechNet.

## Требования сетевого обнаружения

Для того, чтобы успешно обнаружить все компьютеры (серверы и рабочие станции), которые будут управляться из Control Center, требуется следующее:

- Компьютеры должны быть включены в рабочую группу или домен и подключены через локальную сеть IPv4. Служба Обозреватель компьютеров не работает в сетях IPv6.
- На нескольких компьютерах в каждой LAN группе (рабочая группа или домен) должен быть запущен сервис Обозреватель компьютеров. Должна быть запущена служба первичного контроллера домена.

- NetBIOS поверх TCP/IP (NetBT) должен быть включен на компьютерах. Локальный брандмауэр должен разрешать NetBT-трафик.
- Если вы используете ретранслятор Linux для обнаружения других конечных точек Linux или Mac, вы должны либо установить Samba на целевые конечные точки, либо присоединиться к ним в Active Directory и использовать DHCP. Таким образом, NetBIOS будет автоматически настроен на них.
- Общий доступ к файлам должен быть включен на компьютерах. Локальный брандмауэр должен разрешать общий доступ к файлам.
- Windows Internet Name Service (WINS) инфраструктура должна быть настроена и работать правильно.
- Сетевое обнаружение должно быть включено (**Control Panel > Network and Sharing Center > Change Advanced Sharing Settings**). Чтобы включить эту функцию, должны быть запущены следующие службы:
  - DNS клиент
  - Публикация ресурсов функции обнаружения
  - Обнаружение SSDP
  - Устройства UPnP
- В средах с несколькими доменами, рекомендуется установить доверительные отношения между доменами так, чтобы компьютеры могли получить доступ к спискам просмотра из других доменов.

## 5.4. Установка Sandbox Analyzer On-Premises

Чтобы убедиться, что установка идет без проблем, выполните следующие действия:

1. Подготовка к установке
2. Разверните виртуальное устройство Sandbox Analyzer
3. Разверните виртуальное устройство сетевой безопасности

### 5.4.1. Подготовка к установке

Перед установкой Sandbox Analyzer On-Premises убедитесь, что:

- Гипервизор VMWare ESXi установлен и настроен. Подробнее смотрите в документации [Установка и настройка vSphere](#), раздел 2: «Установка и настройка ESXi».
- Виртуальное устройство Bitdefender GravityZone развернуто и настроено.



### Примечание

Что касается гипервизора VMWare ESXi, убедитесь, что:

- Версия ESXi - 6.5 или более поздняя.
- Версия хранилища данных VMFS - 5.
- SSH включен в **политике запуска** с конфигурацией **запуск и остановка с хоста**.
- Служба NTP активна и настроена.

Лицензионный ключ Sandbox Analyzer On-Premises контролирует количество максимальных одновременных детонаций. Поскольку для каждой детонации требуется работающий экземпляр виртуальной машины, количество одновременных детонаций отражается в количестве созданных виртуальных машин. Подробнее о добавлении лицензионных ключей в Control Center GravityZone смотрите [«Ввод ваших лицензионных ключей»](#) (р. 100).

## 5.4.2. Разверните виртуальное устройство Sandbox Analyzer

Чтобы развернуть виртуальное устройство Sandbox Analyzer:

- Войдите в Control Center GravityZone.
- Перейдите на страницу **Network > Packages**.
- Установите флажок **Sandbox Analyzer** из таблицы.
- Нажмите кнопку **Скачать** в верхнем левом углу страницы. Выберите опцию **Устройство безопасности (автономная версия ESXi)**.
- Используйте инструмент управления виртуализацией (например, vSphere Client), чтобы импортировать загруженный файл OVA в вашу виртуальную среду.



### Примечание

При развертывании файла OVA настройте сети следующим образом:

- **Сеть Bitdefender** - это сеть, в которой находятся другие компоненты Bitdefender (eth0 interface) Sandbox Analyzer и GGravityZone устройство должны относиться к одной сети и соединены путем eth0
- **Частная сеть детонации** - Sandbox Analyzer использует данную сеть для международных коммуникаций (eth1interface) Эта сеть должна быть изолирована от любых других сегментов сети.
- **Сеть доступа в Интернет** - Sandbox Analyzer использует эту сеть для получения последних обновлений (eth2interface) eth1interface не следует иметь тот же самый IP или сеть как eth0.

6. Включите устройство.
7. Из инструмента управления виртуализацией откройте консольный интерфейс виртуального устройства Sandbox Analyzer.
8. При запросе учетных данных используйте `root` для имени пользователя и `sve` для пароля.
9. Войдите в меню конфигурации, выполнив следующую команду:

```
/opt/bitdefender/bin/sandbox-setup
```

10. В меню **Настройки песочницы** выполните следующие настройки:

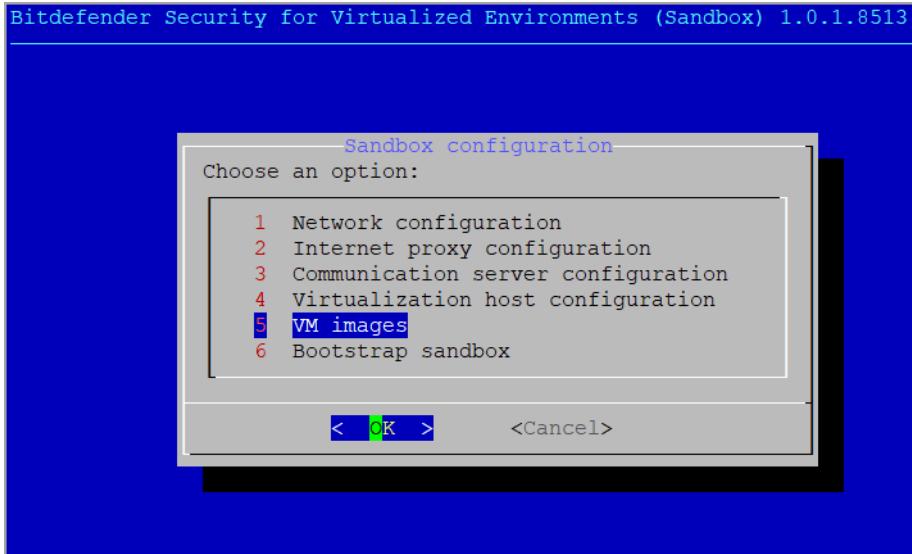
- a. **Конфигурация сети.** Выберите эту опцию для настройки сетевой карты управления. Sandbox Analyzer будет использовать этот сетевой интерфейс для связи с GravityZone.

IP-адрес может быть указан вручную или автоматически через DHCP.



### Примечание

Если GravityZone устройство имеет отношение не к той сети, что eth0, Вы должны добавить статистический маршрут в **Конфигурацию сети > BitDefender Network > маршрут** для Sandbox Analyzer



Консоль устройства Sandbox Analyzer

- b. **Настройка интернет-прокси.** Для успешной установки Sandbox Analyzer требуется подключение к Интернету. В этом случае вы можете настроить Sandbox Analyzer на использование прокси-сервера, указав следующие данные:
- **Хост** - IP-адрес или полное доменное имя прокси-сервера. Используйте следующий синтаксис: `http://<IP/Hostname>:<Port>`.
  - **Пользователь и пароль** - вам нужно ввести пароль дважды.
  - **Домен** - домен Active Directory в соответствующих случаях.
- c. **Конфигурация коммуникационного сервера.** Укажите либо IP-адрес, либо имя хоста устройства, выполняющего роль коммуникационного сервера.
- Используйте следующий синтаксис: `http://<IP/Hostname>:<Port>`. По умолчанию порт 8443.



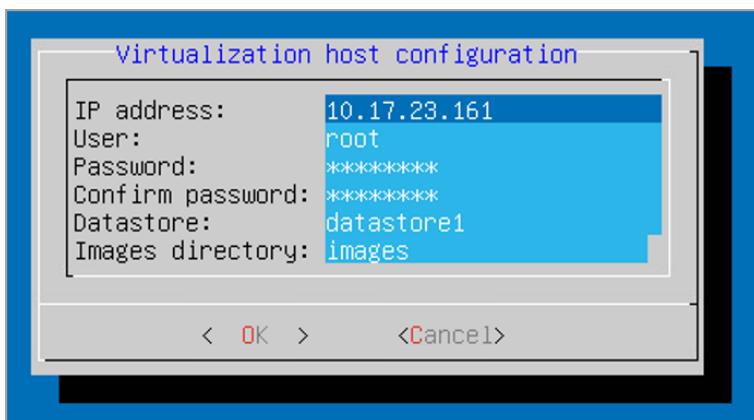
### Примечание

Как только IP-адрес или имя хоста указаны и конфигурация сохранена, экземпляр Sandbox Analyzer станет видимым в Control Center GravityZone, на странице **Sandbox Analyzer > Инфраструктура**.

- d. **Конфигурация виртуализированного хоста.** Sandbox Analyzer использует сервер ESXi для осуществления анализа вредоносных программ. Используя **Конфигурацию виртуализированного хоста**, вы подключаете устройство Sandbox Analyzer к хосту ESXi, предоставляя следующую информацию:

- IP-адрес сервера ESXi.
- Корневые учетные данные для доступа к хосту ESXi.
- Хранилище данных, посвященное Sandbox Analyzer.  
Ведите имя хранилища данных, отображаемое ESXi.
- Имя папки, используемой в хранилище данных для хранения образов виртуальных машин.

Если эта папка не существует, вы должны создать ее в хранилище данных перед сохранением конфигурации Sandbox Analyzer.



Sandbox Analyzer консоль устройства

e. **Образы виртуальной машины.** Чтобы создать детонационные виртуальные машины для Sandbox Analyzer, вам необходимо скопировать файлы VMDK, содержащие нужные образы, в папку **Образы**, указанную в меню **Конфигурации виртуального хоста**. Для каждого образа в меню **Образы виртуальной машины** вы можете выполнить следующие настройки:

- i. В меню **Конфигурация образа** укажите имя образа (как оно будет отображаться в Control Center GravityZone) и операционную систему.



#### Примечание

Папка, содержащая образы виртуальной машины, периодически сканируется, и о новых записях сообщается GravityZone. Эти записи отображаются в Control Center на странице **Sandbox Analyzer > Инфраструктура > Управление образом**.

В определенных ситуациях при использовании Sandbox Analyzer могут возникнуть проблемы с детонационными виртуальными машинами. Для решения этих проблем необходимо отключить функцию защиты от цифровых отпечатков. Дополнительные сведения см. в разделе «[Методы защиты от цифровых отпечатков](#)» (р. 125).

- ii. В меню **хостов DMZ** вы можете внести в белый список имена хостов, которые сторонним сервисам и компонентам, встроенным в виртуальные машины, необходимы для взаимодействия с Sandbox Manager. Подробностисмотрите в [«Хости DMZ» \(р. 126\)](#)
- iii. В меню **Очистка** вы можете удалить образы виртуальной машины, которые вам больше не нужны.
- f. **Загрузочная песочница.** После добавления сведений о конфигурации Sandbox Analyzer продолжите установку, выбрав эту опцию. Статус установки будет отражен в Control Center GravityZone на странице [Sandbox Analyzer > Инфраструктура](#)

### Методы защиты от цифровых отпечатков

По умолчанию, во время процесса создания образа, Sandbox Analyzer включает различные методы защиты от цифровых отпечатков. Определенные типы вредоносных программ способны определять, работают ли они

самостоятельно в среде «песочницы», и, если это так, то они не будут активировать свои вредоносные процедуры.

Целью методов защиты от цифровых отпечатков является моделирование различных условий с целью имитации реальной окружающей среды. Из-за виртуально исключенной комбинации развернутого программного обеспечения и конфигурации среды, комбинация, которую нельзя предвидеть заранее или контролировать, возможно, что определенные методы не будут совместимы с программным обеспечением, установленным в золотом образе. Вы можете распознать такие редкие ситуации по следующим признакам:

- Ошибки в процессе создания образа.
- Ошибки при попытке запустить программное обеспечение внутри образа.
- Сообщения об ошибках при детонации образцов.
- Лицензионное программное обеспечение больше не работает из-за неверных лицензионных ключей.

Быстрое решение таких редких случаев заключается в восстановлении образа с отключенными методами защиты от цифровых отпечатков. Для этого выполните следующие действия:

1. Войдите в Control Center GravityZone и удалите образ.
2. Войдите в устройство Sandbox Analyzer и запустите консоль устройства Sandbox Analyzer, выполнив следующую команду:

```
/opt/bitdefender/bin/sandbox-setup
```

3. Перейдите на **Образы виртуальной машины > Конфигурация образа**.
4. Выберите образ, который вызывает проблемы.
5. Перейдите к опции **Защита от цифровых отпечатков**.
6. Снимите соответствующий флажок, чтобы отключить методы защиты от цифровых отпечатков.

## Хосты DMZ

В процессе создания образа будет создана виртуальная инфраструктура для облегчения связи между Sandbox Manager и виртуальными машинами. С точки зрения сети это приводит к изолированной сетевой среде, которая

будет содержать все потенциальные связи, которую может создать детонированный образец.

Меню серверов DMZ позволяет вносить в белый список имена хостов, с которыми должны взаимодействовать сторонние сервисы и компоненты, встроенные в виртуальные машины, для правильной работы.

Примером такой ситуации могут служить серверы лицензирования KMS, используемые лицензированием Windows, если на поставляемых виртуальных машинах применяется корпоративная лицензия.

## 5.5. Установка полного шифрования диска

GravityZone Полное шифрование диска - это служба, требующая активации на основе лицензионного ключа. Для этого вам необходимо перейти к **Конфигурация > Лицензия** и ввести лицензионный ключ.

Для получения дополнительной информации по лицензионным ключам, перейдите к [«Управление лицензиями» \(р. 99\)](#).

Агенты безопасности Bitdefender поддерживают Полношне шифрование диска, начиная с версии 6. 2. 22. 916 на Windows и 4. 0. 0173876 на Mac. Чтобы убедиться, что агенты полностью совместимы с этим модулем, у вас есть два варианта:

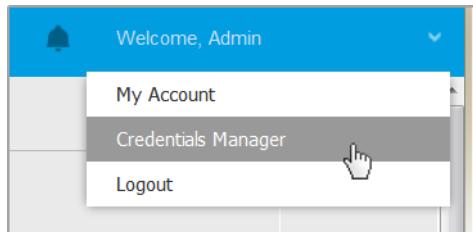
- Установите агентов безопасности с включенным модулем шифрования.
- Используйте задачу **Переконфигурировать**.

Для получения подробной информации об использовании полного шифрования диска в вашей сети см. Главу **Политики безопасности и шифрование** в Руководстве администратора GravityZone.

## 5.6. Диспетчер учетных данных (Credentials Manager)

Диспетчер учетных данных поможет вам определить учетные данные, необходимые для доступа к имеющимся ресурсам vCenter Server, а также для удаленной аутентификации в различных операционных системах вашей сети.

Чтобы открыть диспетчер учетных данных, нажмите на имя пользователя в правом верхнем углу страницы и выберите **Диспетчер учетных данных**.



Меню диспетчера учетных данных

Окно **Диспетчер учетных данных** содержит две вкладки:

- Операционная система
- Виртуальная среда

### 5.6.1. Операционная система

На вкладке **Operating System**, вы можете управлять учетными данными администратора, необходимыми для удаленной аутентификации во время установки, отправки задач для компьютеров и виртуальных машин в вашей сети.

Чтобы добавить набор учетных данных:

A screenshot of the "Credentials Manager" section. It shows a table with columns for "Username", "Password", and "Description". There are two rows: one for "User" and one for "User". To the right of the table is a sidebar with links: "My Account", "Credentials Manager" (which is highlighted in blue), "Help &amp; Support", "Feedback", "Logout", and "Action".

Диспетчер учетных данных (Credentials Manager)

1. Введите имя пользователя и пароль учетной записи администратора для каждой требуемой операционной системы в соответствующих полях в верхней части над заголовком таблицы. При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт. Если компьютеры находятся в домене, достаточно ввести учетные данные администратора домена.

Используйте правила именования Windows при вводе имени учетной записи:

- Для машин из службы каталогов Active Directory используйте следующий синтаксис: `username@domain.com` и `domain\username`. Чтобы быть уверенным, что введенные учетные данные будут работать, добавьте их в обоих видах (`username@domain.com` и `domain\username`).
  - Для машин из рабочей группы достаточно ввести только имя пользователя без имени рабочей группы.
2. Нажмите кнопку  **Добавить** в верхней части таблицы. Новый набор учетных данных будет добавлен в таблицу.



#### Примечание

Если вы не указали учетные данные, вам будет необходимо ввести их при запуске задачи установки. Указанные учетные данные автоматически сохраняются в диспетчере учетных данных, так что вам не придется вводить их в следующий раз.

### 5.6.2. Виртуальная среда

На вкладке **Virtual Environment** вы можете управлять учетными данными для доступных виртуальных серверных систем.

Для доступа к виртуальной инфраструктуре, интегрированной с Control Center, вы должны указать свои учетные данные для каждой доступной серверной системы. Control Center использует ваши учетные данные для подключения к виртуальной инфраструктуре, отображая только те ресурсы, к которым у вас есть доступ (задается на виртуальном сервере).

Чтобы задать учетные данные, необходимые для подключения к виртуальному серверу:

1. Выберите сервер из соответствующего меню.



#### Примечание

Если меню недоступно, значит интеграция еще не была выполнена или все необходимые учетные данные уже настроены.

2. Введите имя пользователя, пароль и подходящее описание.

3. Нажмите кнопку Добавить. Новый набор учетных данных будет добавлен в таблицу.

### Примечание

Если вы не настроили учетные данные в диспетчере учетных данных, вам будет необходимо ввести их, когда вы будете пытаться просмотреть ресурсы любой виртуализованной серверной системы. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дальнейшем.



### **Важно**

Всякий раз, когда вы изменяете свой пароль пользователя виртуального сервера, не забудьте также обновить его в диспетчере учетных данных.

## 5.6.3. Удаление учетных данных из диспетчера учетных данных

Чтобы удалить устаревшие учетные данные из диспетчера учетных данных:

1. Нажмите на строку таблицы, содержащую учетные данные, которые вы хотите удалить.
2. Нажмите кнопку Удалить с правой стороны соответствующей строки таблицы. Выбранный аккаунт будет удален.

## 5.7. Bitdefender GravityZone и HIPAA

Одним из главных приоритетов Bitdefender является обеспечение безопасной обработки и хранения персональных данных клиентов. В связи с этим Bitdefender разработал специальные политики конфиденциальности для домашних и бизнес-решений. Bitdefender найти политики конфиденциальности можно здесь <https://www.bitdefender.com/site/view/legal-privacy.html>.

В рамках защиты персональных данных клиентов Bitdefender стремится помочь своим клиентам, в том числе медицинским работникам, соблюдать правила Закона США о переносимости и подотчетности медицинского страхования 1996 года (HIPAA).

### 5.7.1. GravityZone облачное решение

Для обеспечения защиты от угроз GravityZone собирает и хранит данные с управляемых конечных точек на серверах Bitdefender. Однако данные о

состоянии здоровья не доступны, не хранятся и не обрабатываются каким-либо другим способом. Вся информация, полученная GravityZone, анонимизирована или, по крайней мере, псевдонимизирована. Этот технический подход означает, что использование нашего облачного решения GravityZone не гарантирует Вашего соответствия правилам HIPAA.

## 5.7.2. GravityZone облачное решение

Локальное решение GravityZone было разработано для хранения Ваших данных внутри Вашей организации. Однако для более высокой защиты некоторые функции GravityZone требуют взаимодействия с облачными серверами Bitdefender для выполнения задач. Чтобы соответствовать правилам HIPAA, Вам необходимо отключить эти функции в консоли GravityZone (Control Center), как описано ниже.

### Настройки политик безопасности

Измените параметры политики безопасности в Control Center следующим образом:

1. Перейдите в раздел **Политики** и нажмите, чтобы изменить существующую политику или создать новую.
2. Перейдите в раздел **Общие > Настройки**.
3. В разделе **Параметры** снимите следующие флагки:
  - **Отправлять отчеты о сбоях в Bitdefender.**
  - **Отправьте подозрительные исполняемые файлы для анализа.**
  - **Используйте Bitdefender Global Protective Network для усиления защиты.**
4. Перейдите в раздел **Antimalware > Настройки**.
5. В разделе **Карантин** снимите флагок **Отправлять файлы на карантин в лаборатории Bitdefender каждые (часы)**.
6. Перейдите к **Sandbox Analyzer**.

При использовании облака Sandbox Analyzer в качестве среды детонации необходимо отфильтровать отправленные типы файлов, чтобы они не содержали медицинских данных или какой-либо личной информации (PII). Для этого в разделе **Предварительная фильтрация содержимого** укажите

в поле **Исключения** расширения файлов, которые Вы не хотите автоматически отправлять.

Если Вы не уверены в том, какие данные Вы можете отправлять в Sandbox Analyzer, чтобы быть в безопасности с точки зрения HIPAA, Вы можете полностью отключить эту функцию, сняв флажок **Автоматическая отправка образцов с управляемых конечных точек**.

7. Нажмите **Сохранить**, чтобы сохранить изменения.

## Пакеты установки

Измените установочные пакеты в Control Center следующим образом:

1. Перейдите в раздел **Сетевые пакеты** и нажмите, чтобы отредактировать существующий установочный пакет или создать новый.
2. В разделе **Разное** снимите эти флажки:
  - **Отправка аварийного дампа**.
  - **Отправлять файлы карантина в лабораторию Bitdefender каждые (часы)**.
  - **Отправлять подозрительные исполняемые файлы в Bitdefender**.
  - **Используйте Bitdefender Global Protective Network для усиления защиты**.
3. В разделе **Настройки** снимите флажок **Сканировать перед установкой**.
4. Нажмите **Сохранить**, чтобы сохранить изменения.

## Sandbox Analyzer Ручное управление

Хотя Вы можете настроить автоматическую отправку в облако Sandbox Analyzer в настройках политики безопасности, отправка вручную зависит исключительно от операций, которые Вы выполняете в разделе **Sandbox Analyzer > Отправка вручную** главного меню Control Center. Чтобы соответствовать правилам HIPAA, убедитесь, что Вы не отправляете в Sandbox Analyzer облачные файлы, которые могут содержать медицинские данные или персональные данные.

## Правовое положение

Пожалуйста, имейте в виду, что Вы полностью несете ответственность за проверку соблюдения Вами любого законодательства, включая HIPAA, и,

предоставляя вышеуказанную информацию, Bitdefender напрямую отказывается от любой ответственности в отношении Вашего соблюдения HIPAA и поведения в отношении HIPAA или любых других юридических требований, которые могут на Вас распространяться. Во избежание каких-либо сомнений, используя решения Bitdefender, в том числе GravityZone, Bitdefender никаким образом не гарантирует соблюдение Вами какого-либо законодательства, включая HIPAA. Вышеизложенное не является юридическим руководством, и Вам рекомендуется обратиться за юридической консультацией по вышеуказанному или любой другой правовой теме.



## 6. ОБНОВЛЕНИЕ GRAVITYZONE

Bitdefender публикует все обновления продукта и механизмов защиты через серверы Bitdefender в Интернете. Все обновления зашифрованы и имеют цифровую подпись, чтобы их нельзя было подделать.

GravityZone включает в себя роль сервера обновлений, предназначеннной для централизованного распространения обновлений в вашем окружении GravityZone. Сервер обновлений проверяет и загружает все доступные для GravityZone обновления от серверов обновлений Bitdefender в Интернете, что делает их доступными в локальной сети. Компоненты GravityZone могут быть настроены на автоматическое обновление с локального сервера обновлений вместо серверов в Интернете.

Когда доступно новое обновление, устройство или агент безопасности GravityZone проверяет цифровую подпись обновления для аутентификации и содержимое пакета для обеспечения целостности. Затем каждый файл обновления анализируется, и его версия проверяется на соответствие установленной. Более новые файлы загружаются локально и проверяются на соответствие хэшу MD5, чтобы убедиться, что они не изменены.

Если в какой-то момент проверка не была пройдена, процесс обновления останавливается, возвращая ошибку. В противном случае обновление считается действительным и готовым к установке.

Чтобы обновить приборы GravityZone, установленные в вашей среде, и пакеты установки компонентов GravityZone, войдите в систему с учетной записью администратора компании и перейдите к **Configuration > Update**.

### 6.1. Обновление устройств GravityZone

Через обновления устройств GravityZone Bitdefender выпускает новые функции и улучшает уже существующие. Их можно увидеть в Control Center.

Перед обновлением, вам необходимо проверить следующее:

- Состояние обновления
- Любую информацию или появляющиеся предупреждающие сообщения
- Журнал изменений

Для проверки состояния обновления:

1. Перейдите в раздел **Конфигурация > Обновления > Роли GravityZone**.

2. Под разделом **Текущий статус** просмотрите сообщение, указывающее на общий статус обновления. Если GravityZone нуждается в обновлении, кнопка **Обновить** станет активной.
3. Под разделом **Инфраструктура**, просмотрите детали для каждой роли GravityZone, развернутой в вашей сети. Так как роли обновляются отдельно, для каждой роли вы можете увидеть: имя устройства с данной ролью, его IP-адрес, текущую версию, последнее доступное обновление и состояние обновления.

Чтобы просмотреть журнал изменений:

1. Перейдите в раздел **Конфигурация > Обновления > Роли GravityZone**.
2. Нажмите на ссылку **Просмотреть журнал изменений**. Появившееся окно отобразит список со всеми версиями и изменениями, которые они включают.

Примечания к выпуску каждой новой версии продукта также публикуются на [Bitdefender Support Center](#).

Вы можете обновить GravityZone двумя способами:

- [Вручную](#)
- [Автоматически](#)

### **6.1.1. Обновление вручную.**

Выберите данные метод чтобы иметь полный контроль над процессом обновления.

Для ручного обновления GravityZone:

1. Перейдите в раздел **Конфигурация > Обновления > Роли GravityZone**.
2. Нажмите кнопку **Обновить** (если активна).

Обновление может занять некоторое время. Пожалуйста, дождитесь окончания обновления.

3. Очистите кэш браузера.

Во время обновления Control Center выводит из системы всех пользователей и информирует их о проведении обновления. Вы сможете просмотреть детальный прогресс процесса обновления.

После завершения обновления Control Center отобразит страницу входа в учетную запись.

## 6.1.2. Автоматическое обновление

При установке обновлений автоматически, вы будете уверены, что на GravityZone всегда установлены новейшие функции и механизмы защиты.

В GravityZone имеются два типа автоматических обновлений:

- [Обновления продуктов](#)
- [Обновления стороннего программного обеспечения](#)

### Обновления продуктов

Данные обновления привносят новые функции в GravityZone и устраняют проблемы, связанные с этими функциями.

Так как обновления мешают пользователям GravityZone, они могут быть запущены по расписанию. Вы можете запланировать обновление в удобные вам часы. По умолчанию автоматические обновления продукта отключены.

Чтобы включить и запланировать обновления продукта:

1. Перейдите в раздел **Конфигурация > Обновления > Роли GravityZone**.
2. Выберите **Включить автоматическое обновления продукта GravityZone**.
3. Установите **Повторение** на **Ежедневно , Еженедельно** (выберите один или несколько дней недели) Или **Ежемесячно**.
4. Определите **Интервал**. Вы можете запланировать время начала процесса обновления, когда доступно новое обновление.

По умолчанию, GravityZone выводит предупреждающее сообщение всем пользователям Control Center за 30 минут до начала автоматического обновления. Для отключения оповещения, снимите флажок с **30-минутное оповещение остоях перед обновлением**.

### Обновления стороннего программного обеспечения

Виртуальное устройство GravityZone поддерживает серии программных продуктов от сторонних поставщиков. Данный тип обновлений нацелен скорейшее на исправления такого ПО, исключая возможные риски безопасности.

Данные обновления запускаются бесшумно и не прерывают работу с Control Center.

По умолчанию данная функция включена. Для отключения функции:

1. Перейдите в раздел **Конфигурация > Обновления > Роли GravityZone**.
2. Снимите флажок с опции **Включить автоматическую загрузку обновлений безопасности для сторонних компонентов GravityZone**.

В данном случае исправления для стороннего ПО будут опубликованы вместе с обновлением продукта GravityZone.

## 6.2. Настройка сервера обновлений

По умолчанию, сервер обновлений загружает обновления из Интернета каждый час. Не рекомендуется изменять настройки по умолчанию сервера обновлений.

Для проверки и настройки параметров сервера обновлений:

1. Перейдите на страницу **Обновление** в Control Center и откройте вкладку **Компоненты**.
2. Нажмите кнопку **Настройки** в верхней части панели слева, чтобы отобразить окно **Параметры сервера обновлений**.
3. В разделе **Обновить конфигурацию сервера** вы можете проверить и настроить основные параметры
  - **Адрес пакета.** Адрес загрузки пакета
  - **Обновить адрес.** Сервер обновлений настроен для проверки и загрузки обновлений с помощью обновления обновл. Bitdefender.com: 80. Это общий адрес, который автоматически определяет ближайший к вам сервер, хранящий обновления Bitdefender в вашем регионе.
  - **Порт.** При настройке различных компонентов GravityZone, для обновления с сервера обновлений, вы должны предоставить этот порт. По умолчанию порт 7074.
  - **IP-адрес.** IP-адрес сервера обновлений.
  - **Период обновления (часы).** Если требуется изменить периодичность обновления, введите в этом поле новое значение. Значение по умолчанию - 1.

4. Вы можете настроить сервер обновлений для автоматической загрузки наборов конечных точек.
5. Сервер обновлений может выступать в качестве шлюза для данных, отправляемых клиентскими продуктами Bitdefender, установленными в сети, на серверы Bitdefender. Эти данные могут включать в себя анонимные отчеты о вирусной активности, отчеты о сбоях продукта и данных, используемых для онлайн-регистрации. Включение ролей шлюза может оказаться полезным в целях контроля трафика, а также в сетях без доступа в Интернет.



#### Примечание

Вы можете в любое время по желанию отключить модули продукта, которые отправляют в лабораторию Bitdefender статистику и данные о сбоях. Вы можете использовать политики для удаленного управления этими параметрами на компьютерах и виртуальных машинах, управляемых Control Center.

6. Нажмите **Сохранить**.

### 6.3. Загрузка обновлений продуктов

Вы можете просмотреть информацию о существующих пакетах компонентов GravityZone на вкладке **Компоненты**. Доступная информация включает текущую версию, обновленную версию (если таковые имеются) и статус выполнения операций обновления.

Чтобы обновить компонент GravityZone:

1. Перейдите на страницу **Обновление** в Control Center и откройте вкладку **Компоненты**.
2. Выберите компонент, который вы хотите обновить, в списке **Продукты**. Все доступные версии будут отображаться в таблице **Пакеты**. Установите флажок, соответствующий версии, которую вы хотите загрузить.



#### Примечание

Новые пакеты будут находиться в состоянии **Не загруженные**. Как только более новая версия будет выпущена Bitdefender, самая старая незагруженная версия будет удалена из таблицы.

3. Нажмите **Действия** в верхней части таблицы и выберите **Опубликовать**. Будет загружена выбранная версия, статус изменится соответствующим образом. Обновите содержимое таблицы, нажав кнопку **Refresh** и проверьте соответствующий статус.

## 6.4. Обновление продукта в автономном режиме

GravityZone использует по умолчанию систему обновлений, подключенную к Интернету. Для изолированных сетей Bitdefender предлагает альтернативу, которая делает доступными автономные компоненты и механизмы безопасности.

### 6.4.1. Требования к системе

Чтобы использовать автономные обновления, вам необходимо:

- Установленное устройство GravityZone в сети с доступом в Интернет ("онлайн-экземпляры"). Онлайн-экземпляр должен иметь:
  - Прямое Интернет соединение
  - Доступ к портам 80 и 443. За подробной информацией о портах, используемых GravityZone, обратитесь к [статье из Базы знаний](#).
  - Только установленные роли Базы Данных и Сервера Обновлений
- Один или несколько устройств GravityZone, развернутые в сети без доступа в Интернет ("автономные экземпляры").
- Оба экземпляра GravityZone должны иметь одинаковую версию устройства.

### 6.4.2. Настройка онлайн экземпляра GravityZone

На этой стадии необходимо установить экземпляр GravityZone в сеть с доступом в Интернет, а затем настроить его как автономный сервер обновлений.

1. Установите последнее GravityZone изображение на машину с доступом в Интернет.
2. Установите только роли Базы Данных и Сервера Обновлений.
3. Получите доступ к TTY-терминалу машины в вашей виртуальной среде (или подключитесь к нему через SSH).

4. Войдите под учетной записью `bdadmin`, используя установленный пароль.
5. Запустите команду `sudo su`, чтобы получить привилегии `root`.
6. Выполните данную команду для установки автономного пакета `gzou-mirror`:

```
# apt update # gzcli update # apt install gzou-mirror
```

`gzou-mirror` имеет следующие роли:

- Настройте Сервер Обновлений для автоматической генерации автономных пакетов обновления.
- Настройте веб-сервис для онлайн-экземпляра для предоставления конфигураций и загружаемых опций для автономных архивов обновлений.

### 6.4.3. Настройка и загрузка начальных файлов обновлений

На данном этапе необходимо настроить параметры архивов обновлений через веб-сервис, установленный на онлайн-экземпляре, а затем создать файлы, требуемые для [настройки автономного экземпляра](#). После этого вам необходимо загрузить файлы обновлений и поместить их на портативное мультимедийное устройство (USB-накопитель).

1. Получите доступ к веб-службе по следующему URL-адресу: `https://Update-Server-IP-or-Hostname`, с именем пользователя `bdadmin` и паролем, который вы установили.



### Appliance Status

Current job:

Next archive will be created on: Tue Aug 14 2018 17:55:07 GMT+0300 (Eastern European Summer Time) [Create...](#)

Free disk space: 86.59 GiB

Kits	Settings
<input checked="" type="checkbox"/> Bitdefender Security Tools (BEST)	Archive creation interval (in hours): 2
<input type="checkbox"/> Bitdefender Security Tools (BEST) Legacy	Number of FULL archives to keep on disk: 1
<input checked="" type="checkbox"/> Bitdefender Security Tools (BEST)	Number of LITE archives to keep on disk: 1
<input type="checkbox"/> Bitdefender Endpoint Security	
<input type="checkbox"/> Bitdefender Endpoint Security	
<input type="checkbox"/> Bitdefender Tools	
<input type="checkbox"/> Bitdefender Tools	

[Apply](#)

Онлайн-экземпляр - Веб-Служба

2. Настройте автономный архив обновлений как описано ниже:
  - Обновите **Пакеты**: выберите пакеты с агентами конечных точек, чтобы включить их в архив автономного обновления.
  - В разделе **Настройки**, измените параметры архива обновлений.  
Задание CRON, установленное в онлайн-экземпляре, каждую минуту будет проверять наличие новых файлов обновлений и наличие свободного дискового пространства более 10 ГБ. В каждый период, заданный параметром **Интервал создания архива (в часах)**, задание CRON создает следующие файлы:
    - **Полный архив (обновления продукта + механизмы защиты)**, если доступны новые файлы обновлений
    - **Легкий архив** (только механизмы защиты), если новые файлы обновлений недоступны

Архивы будут созданы в следующей директории:

<https://Online-Instance-Update-Server-IP-or-Hostname/snapshots>

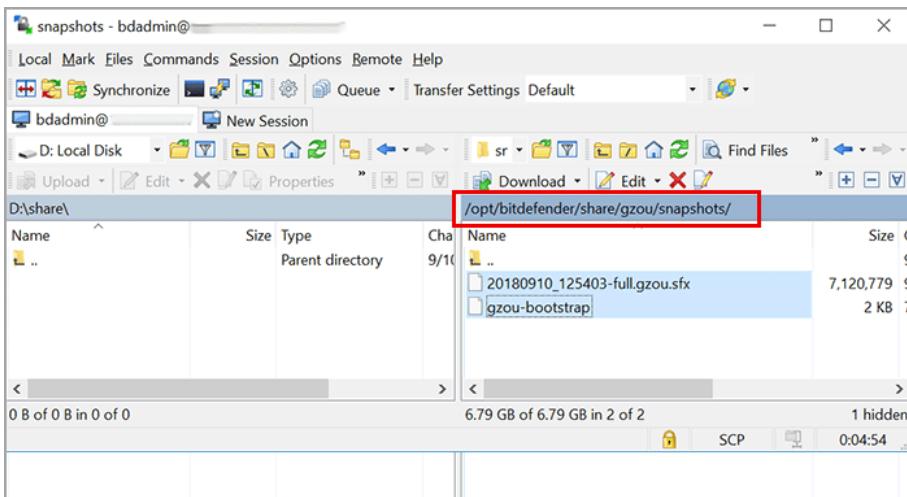
3. Нажмите **Создать > Полный архив**, чтобы создать первый полный архив. Подождите, пока создается архив.

The screenshot shows the Bitdefender GravityZone web interface. At the top left is the Bitdefender GravityZone logo. At the top right are links for 'Logout' and 'unfollow the traditional'. Below the header, the page title is 'Appliance Status'. On the right side, there are two buttons: 'Download archives' and 'Generate support bundle'. In the center, there's a section titled 'Current job:' with a progress bar. Below it, a message says 'Next archive will be created on: Tue Aug 14 2018 17:55:07 GMT+0300 (Eastern European Summer Time)'. A 'Create...' button has a dropdown menu open, showing 'Full archive' (which is highlighted in blue) and 'Lite archive'.

Онлайн-экземпляр - Веб-Сервис: Создание архива

4. Загрузите полный архив обновления и файл `gzou-bootstrap` с онлайн-экземпляра. Это можно сделать несколькими способами:
  - Через веб-сервис: нажмите **Загрузить архивы**, чтобы перейти к странице со ссылками на файлы обновлений. Нажмите на ссылки для полного архива обновлений и `gzou-bootstrap`, чтобы загрузить их на машину.
  - Используйте удобный вам клиент SCP/SCTP (например, WinSCP), чтобы установить SCP-сессию с онлайн-экземпляром и перенести вышеупомянутые файлы в любое местоположение в вашей сети. Путь по умолчанию:

`/opt/bitdefender/share/gzou/snapshots`



Перенос файлов обновления с помощью SCP

- Через файлового обмена SAMBA. Используйте файлообменник SAMBA для того, чтобы получить архивы автономного обновления из следующий путей:  
\\Online-Instance-Update-Server-IP-or-Hostname\\gzou-snapshots



#### Примечание

Учетные данные для доступа к общему ресурсу SAMBA, если они запрошены, совпадают с учетными данными сетевого экземпляра (пользователь `bdadmin` и пароль).

### 6.4.4. Настройка автономного экземпляра GravityZone

На этом шаге необходимо установить и настроить автономный экземпляр для получения обновления через архивы, созданные на онлайн-экземпляре. Если не указано иное, все команды должны выполняться как `root`.

- Установите GravityZone на машину из изолированной среды.
- Установите только роли Базы Данных и Сервера Обновлений.

3. Перенесите архивы обновлений и файл `gzou-bootstrap`, загруженные с онлайн-экземпляра, в расположение `/home/bdadmin` на автономном экземпляре используя переносное мультимедийное устройство (USB накопитель).

! **Важно**

Для корректной работы автономного обновления, удостоверьтесь, что:

- Архив обновления и файл `gzou-bootstrap` находятся в одной папке.
- Архив обновления является **полным**.

4. Выполните файл `gzou-bootstrap` как описано ниже:

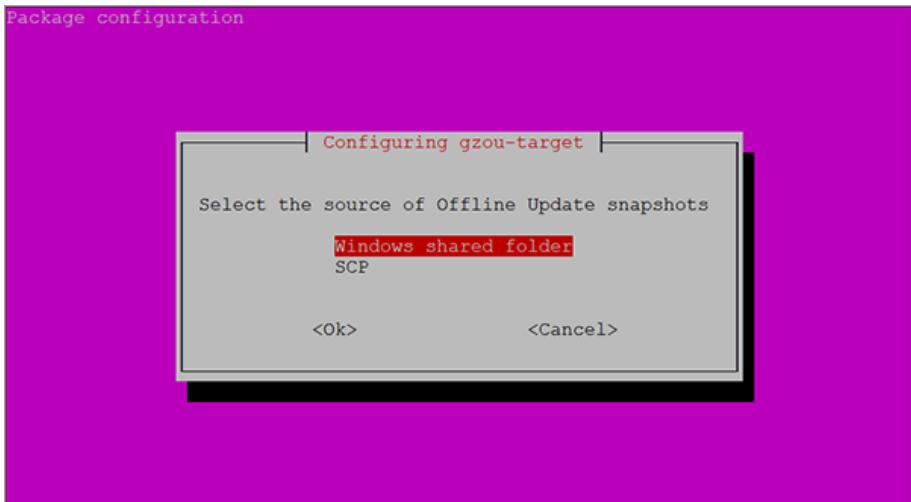
- a. Получите доступ к TTY-терминалу машины в вашей виртуальной среде (или подключитесь к нему через SSH).
- b. Трансформировать `gzou-bootstrap` в исполняемый файл:

```
#  
chmod +x gzou-bootstrap
```

- c. Запустить: `./gzou-bootstrap`

5. Выберите метод переноса архивов обновления на автономный экземпляр:

- Выберите **Общая папка Windows** (Samba). В данном случае вам необходимо указать путь к общей папке Windows из изолированной сети, к которой автономный экземпляр автоматически подключится для загрузки архивов обновления. Введите запрашиваемые учетные данные для доступа к указанному местоположению.
- Выберите SCP, если вы хотите вручную перенести файлы в папку `/opt/bitdefender/share/gzou/snapshots/` на автономный экземпляр через SCP.



Автономный экземпляр GravityZone - настройка режима передачи файлов обновлений



### Примечание

Если в дальнейшем вы хотите изменить режим:

- a. Получите доступ к TTY-терминалу машины в вашей виртуальной среде (или подключитесь к нему через SSH).
- b. Войдите под учетной записью `bdadmin`, используя установленный пароль.
- c. Запустите команду `sudo su`, чтобы получить привилегии `root`.
- d. Выполнение:

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

Появится окно настроек, в котором вы сможете внести желаемые действия.

6. Переключитесь на командную строку консоли автономной GravityZone и установите остальные роли.
7. Откройте автономную консоль в своем веб-браузере и вставьте свой лицензионный ключ (в автономном режиме).

## 6.4.5. Использование автономных обновлений

После установки экземпляров GravityZone, выполните следующие шаги для обновления вашей автономной установки:

1. Скачайте образ виртуального устройства GravityZone отсюда [here](#).
2. Установите онлайн-экземпляр, как это описано [here](#).
3. Загрузите последний архив обновлений с онлайн-экземпляра на удобный вам сетевой файлообменник. Дополнительные сведения см. в разделе [«Настройка и загрузка начальных файлов обновлений»](#) (р. 140).
4. Используйте USB устройство для переноса архива обновлений на файлообменник Samba в изолированной сети. Дополнительные сведения см. в разделе [«Настройка автономного экземпляра GravityZone»](#) (р. 143).

Файлы будут автоматически перенесены в указанную директорию на автономном экземпляре:

/opt/bitdefender/share/gzou/snapshots/

## 6.4.6. Использование веб-консоли

Войдите в веб-консоль, указав IP-адрес / имя хоста устройства в веб-браузере. Вы можете изменить доступные параметры:

- [Центр управления](#)
- [Общие настройки](#)

### Центр управления

**Состояние устройства** отображает детали последнего выполненного задания (тип архива, дата и время) и следующее запланированное задание.

Вам доступны следующие действия:

- **Создать Архив Механизмов Защиты**
- **Создать полный архив**

В разделе **Созданные Архивы**, вы можете загрузить архивы с механизмами защиты и полные архивы.

Выберите архив (ы) из доступного списка и нажмите кнопку **Загрузить**.

Вы также можете просмотреть доступное пространство на диске устройства.

## Общие настройки

Вы можете определить расписание загрузки для наборов GravityZone.

1. Нажмите кнопку **Изменить настройки**.
2. Выберите один или несколько наборов из списка **Доступные комплекты**.
3. В разделе **Расписание**, вы можете указать интервал создания архивов, а также количество архивов, сохраняемых на диске.
4. Нажмите кнопку **Применить**, чтобы сохранить изменения.

## 7. УДАЛЕНИЕ ЗАЩИТЫ

Вы можете удалить и повторно установить компоненты GravityZone в случаях, когда вам нужно использовать лицензионный ключ для другого компьютера, чтобы исправить ошибки или при обновлении.

Чтобы правильно удалить защиту Bitdefender конечных рабочих станций в вашей сети, следуйте инструкциям, описанным в этой главе.

- Удаление защиты конечных рабочих станций
- Удаление Ролей GravityZone

### 7.1. Удаление защиты конечных рабочих станций

У вас есть два варианта удаления агентов безопасности:

- **удаленно** в Control Center
- **Вручную** на целевой машине

#### Удаленная deinсталляция

Чтобы удаленно удалить защиту Bitdefender с любой управляемой конечной рабочей станции:

1. Перейдите на страницу **Сеть**.
2. Выберите **компьютеры и виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Выберите конечные точки, из которых вы хотите удалить агент безопасности Bitdefender.
5. Нажмите **Задачи** в верхней части таблицы и выберите **Удалить клиента**. Появится окно конфигурации.
6. В окне задачи **Удалить агент** вы можете выбрать, сохранять ли файлы в карантине на конечной рабочей станции или удалять их.

Для интегрированных сред VMware vShield вы должны выбрать необходимые учетные данные для каждой машины, в противном случае удаление не произойдет. Выберите **Использовать учетные данные для**

интеграции vShield , затем добавьте необходимые данные в таблицу диспетчера учетных данных, отображаемую ниже.

7. Нажмите **Сохранить**, чтобы создать задачу. Появится сообщение с подтверждением.

Вы можете просматривать задачу и управлять ею в **Сеть > Задачи**

Если вы хотите переустановить агентов безопасности, обратитесь к «[Установка агентов по безопасности](#)» (p. 102).

## Локальная deinсталляция

Чтобы вручную удалить агент безопасности Bitdefender с компьютера с ОС Windows:

1. В зависимости от вашей операционной системы:
  - В Windows 7 перейдите к **Пуск > Панель управления > Удалить программу** в разделе **Программы** .
  - В ОС Windows 8 перейдите к **Настройки > Панель управления > Удалить программу** в разделе **Программы** .
  - В ОС Windows 8.1, кликните правой кнопкой мыши **Старт**, затем выберите **Панель управления > Программы & Функции** .
  - В ОС Windows 10, go to **Старт > Настройки > Система > Приложения & Свойства**.
2. Выберите агент Bitdefender из списка программ.
3. Щелкните **Deинсталляция**.
4. Введите пароль Bitdefender, если он предусмотрен политикой безопасности. Вы можете просмотреть ход выполнения задачи во время удаления.

Чтобы вручную удалить агент безопасности Bitdefender с компьютера с ОС Linux:

1. Откройте терминал.
2. Получите коневой доступ (root) с помощью команд `su` или `sudo su` .
3. Перейдите с помощью команды `cd` на следующий путь:  
`/opt/BitDefender/bin`
4. Запустите скрипт:

```
# ./remove-sve-client
```

5. Чтобы продолжить, введите пароль Bitdefender, если он предусмотрен политикой безопасности.

Чтобы вручную удалить агент Bitdefender с компьютера с ОС Mac:

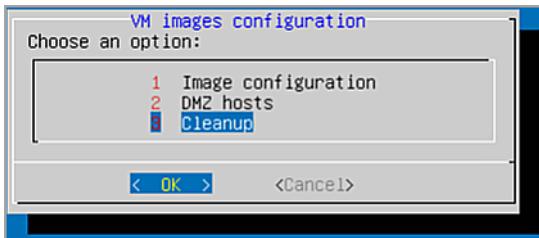
1. Откройте **Finder > Applications**.
2. Откройте папку Bitdefender.
3. Перепроверьте **Bitdefender Mac Деинсталляция**.
4. В окне подтверждения щелкните **Проверить** и **Удалить**, чтобы продолжить.

Если вы хотите переустановить агентов безопасности, обратитесь к [«Установка агентов по безопасности» \(п. 102\)](#).

## 7.2. Удаление Sandbox Analyzer On-Premises

Чтобы удалить Sandbox Analyzer On-Premises:

1. Удалите образы виртуальной машины (VM) из консоли устройства Sandbox Analyzer.
  - a. Войдите в интерфейс устройства Sandbox Analyzer.  
Используйте клавиши со стрелками и клавишу Tab для навигации по меню и опциям.  
Нажмите Enter для выбора определенных опций.
  - b. В меню **Конфигурации песочницы** перейдите к параметру **образы виртуальной машины**.
  - c. В меню **Конфигурация образов виртуальной машины** перейдите к опции **Очистка**.



Консоль устройства Sandbox Analyzer - Настройки песочницы - Очистка

- d. Подтвердите, что вы хотите удалить установленные образы виртуальных машин.

Подождите, пока это действие не завершится. Во время этого действия также будут удалены данные, связанные с образами виртуальной машины.

2. Удалите виртуальное устройство Sandbox Analyzer:

- Выключите виртуальное устройство Sandbox Analyzer.
- Удалите устройство из инвентаря ESXi.

### 7.3. Удаление ролей виртуального устройства GravityZone

Вы можете удалить роли виртуального устройства GravityZone через меню интерфейса. Даже если вы удалите один из них, ваша сеть по-прежнему будет защищена. Тем не менее, для работы GravityZone необходимо как минимум один экземпляр каждой роли.

В сценарии с одним устройством со всеми ролями GravityZone при удалении одной роли конечные точки будут оставаться защищенными, хотя некоторые функции устройства недоступны, в зависимости от каждой роли.

В сценарии с несколькими устройствами GravityZone можно безопасно удалить роль, пока доступен другой экземпляр одной и той же роли. По дизайну несколько экземпляров ролей Коммуникационного сервера и Веб консоли могут быть установлены на разных устройствах и подключены к другим ролям с помощью балансировщика ролей. Следовательно, если вы удаляете один экземпляр определенной роли, его функция перехватывается другими.

При необходимости вы можете удалить коммуникационный сервер из одного устройства, назначив его функцию другому экземпляру этой роли. Для плавного перехода выполните следующие действия:

1. В Control Center перейдите на страницу **Политики**.
2. Выберите существующую политику или нажмите **Добавить**, чтобы создать новую.
3. В разделе **Общие** перейдите к **Связь**.
4. В окне **Назначение связи конечной точки**, нажмите на поле **Имя**. Появится список обнаруженных коммуникационных серверов.
5. Выберите коммуникационный сервер, который вы хотите привязать к конечным точкам.
6. Нажмите кнопку **Добавить** в верхней части таблицы. Если у вас в списке более одного коммуникационного сервера, вы можете настроить их приоритет, используя стрелки вверх и вниз в правой части каждого объекта.
7. Нажмите **Сохранить**, чтобы создать политику. Конечные точки связуются с Control Center через указанный коммуникационный сервер.
8. В интерфейсе командной строки GravityZone удалите старую роль сервера связи.



### **Предупреждение**

Если вы удалите старый Коммуникационный сервер без предварительной настройки политики, связь будет потеряна навсегда, и вам потребуется переустановить агентов безопасности.

Чтобы удалить роли виртуального устройства GravityZone:

1. Войдите в интерфейс консоли из средства управления виртуализацией (например, vSphere Client). Используйте клавиши со стрелками и клавишу **Tab** для навигации по меню и опциям. Нажмите **Enter** для выбора определенных опций.
2. Выберите **Дополнительные настройки**.
3. Нажмите **Install/Uninstall Roles**.
4. Перейдите к **Добавить или удалить роли**.

5. Используя `Space`, отмените выбор любой роли, которую вы хотите удалить, затем нажмите клавишу `Enter`. Появится окно подтверждения, информирующее вас о том, что роль будет удалена.
6. Нажмите `Enter`, чтобы продолжить и дождитесь завершения удаления.

Если вы хотите переустановить роль, обратитесь к [«Установка/удаление ролей» \(р. 89\)](#).

## 8. ПОЛУЧЕНИЕ СПРАВКИ

Bitdefender стремится предоставить своим клиентам быструю и качественную техподдержку. Если у вас возникли проблемы или если у вас есть какие-либо вопросы о продуктах Bitdefender, перейдите в наш [Онлайн центр поддержки](#). В нем доступны ресурсы, с помощью которых можно быстро найти решение или ответ. Или при необходимости можно обратиться в службу поддержки клиентов Bitdefender. Представители службы поддержки быстро ответят на все вопросы и окажут необходимую помощь.



### Примечание

В центре техподдержки можно найти информацию о предоставляемых услугах техподдержки, а также правилах их предоставления.

## 8.1. Центр поддержки Bitdefender

[Bitdefender Центр поддержки](#) это раздел, где вы найдете всю необходимую помощь по продуктам Bitdefender.

Доступные ресурсы можно использовать для быстрого нахождения решения или ответа:

- Статьи базы знаний
- Форум поддержки Bitdefender
- Документация по продукту

Также можно воспользоваться поисковой системой для получения дополнительных сведений о компьютерной безопасности, продуктах Bitdefender и самой компании.

### Статьи базы знаний

База знаний Bitdefender - онлайн хранилище информации о продуктах Bitdefender. Здесь хранятся в удобном для доступа формате отчеты о результатах текущих операций по технической поддержке и исправлению ошибок, выполняемых службой поддержки и разработки Bitdefender, а также статьи по предотвращению заражения вирусами, управлению решениями Bitdefender с подробными разъяснениями, а также другая информация.

База знаний Bitdefender открыта для общего доступа с возможностью свободного поиска. Bitdefender содержит обширную информацию,

предоставляя клиентам необходимые технические сведения. Все действующие информационные запросы или отчеты об ошибках, поступающие от клиентов Bitdefender, могут быть найдены в базе знаний Bitdefender, такие как отчеты по исправлениям, устранению неполадок и информационные статьи, дополняющие файлы справок продуктов.

База знаний Bitdefender для бизнес-продуктов доступна в любое время - <http://www.bitdefender.com/support/business.html>.

## Форум поддержки Bitdefender

Форум техподдержки Bitdefender предоставляет пользователям Bitdefender простой способ не только получить необходимую помощь, но и помочь другим. Можно опубликовать любую проблему или вопрос, связанные с продуктом Bitdefender.

Специалисты Службы технической поддержки Bitdefender отслеживают новые сообщения на форуме, что позволяет своевременно реагировать на все вопросы пользователей. На форуме также есть возможность получить ответ или узнать о способах решения проблемы от более опытных пользователей Bitdefender.

Перед публикацией своего сообщения о проблеме или вопроса, выполните поиск похожих или связанных тем на форуме.

Форум техподдержки Bitdefender доступен по адресу <http://forum.bitdefender.com>, на пяти различных языках: английском, немецком, французском, испанском и румынском. Нажмите ссылку **Защита бизнеса**, чтобы перейти в раздел продуктов для бизнеса.

## Документация по продукту

Документация по продукту является самым полным источником информации о продукте.

Самый простой способ получить документацию - перейти на страницу **Справка и поддержка** в Control Center. Нажмите свое имя пользователя в верхнем правом углу консоли, выберите **Справка и поддержка**, а затем ссылку интересующего вас руководства. Руководство откроется на новой вкладке вашего браузера.

Вы также можете проверить и загрузить документацию в разделе [Центр поддержки](#) во вкладке [Документация](#), доступной на каждой странице поддержки продукта.

## 8.2. Обращение за помощью

Вы можете обратиться за помощью в наш онлайн Центр поддержки. Заполните [контактная форма](#) и примите.

## 8.3. Использование инструментов поддержки

Инструменты поддержки GravityZone созданы, чтобы помочь пользователям и специалистам поддержки упростить предоставление необходимой информации для устранения неполадок. Запустите инструмент поддержки на действующих компьютерах и отправьте архив с информацией о выявленных неполадках в представительство поддержки Bitdefender.

### 8.3.1. Использование инструмента поддержки на операционных системах Windows

#### Запуск приложения Инструмент поддержки

Чтобы создать журнал на зараженном компьютере, используйте один из следующих способов:

- [Командная строка](#)

Для любых проблем с BEST, установленным на компьютере.

- [Проблема с установкой](#)

Для ситуаций, когда BEST не установлен на компьютере и установка завершается неудачно.

#### Метод командной строки

Используя командную строку, вы можете собирать журналы прямо с зараженного компьютера. Этот метод полезен в ситуациях, когда у вас нет доступа к Центру управления GravityZone или компьютер не взаимодействует с консолью.

1. Откройте командную строку с правами администратора.

2. Перейдите в папку установки продукта. Путь по умолчанию:

C:\Program Files\Bitdefender\Endpoint Security

3. Соберите и сохраните журналы, выполнив эту команду:

```
Product.Support.Tool.exe collect
```

Журналы по умолчанию сохраняются в C:\Windows\Temp.

При желании, если вы хотите сохранить журнал средства поддержки в произвольном месте, используйте путь к параметру:

```
Product.Support.Tool.exe collect [path=<path-to-file>]
```

Пример:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Пока команда выполняется, вы можете заметить индикатор выполнения на экране. Когда процесс завершен, в выходных данных отображается имя архива, содержащего журналы, и его местоположение.

Чтобы отправить журналы в службу поддержки Bitdefender Enterprise, перейдите в C:\Windows\Temp или в пользовательское местоположение и найдите архивный файл с именем ST\_[computername]\_[currentdate]. Прикрепите архив к заявке в службу поддержки для дальнейшего устранения неполадок.

## Проблема с установкой

- Чтобы загрузить Инструмент поддержки BEST, нажмите [здесь](#).
- Запустите исполняемый файл от имени администратора. Появится окно.
- Выберите место для сохранения архива журналов.

Пока журналы собираются, вы увидите на экране индикатор выполнения. Когда процесс завершен, в выходных данных отображается имя архива и его местоположение.

Чтобы отправить журналы в службу поддержки Bitdefender Enterprise, перейдите в выбранное местоположение и найдите архивный файл с именем

ST\_[computername]\_[currentdate]. Прикрепите архив к заявке в службу поддержки для дальнейшего устранения неполадок.

### 8.3.2. Использование инструмента поддержки на операционных системах Linux

Для операционных систем Linux инструмент поддержки интегрирован в агент безопасности Bitdefender.

Для сбора информации о системе Linux с использованием инструмента поддержки, запустите следующую команду:

```
# /opt/BitDefender/bin/bdconfigure
```

используя следующие доступные опции:

- --help составить список всех команд инструмента поддержки
- enablelogs для включения журналирования продукта и коммуникационного модуля (все сервисы будут автоматически перезапущены)
- disablelogs для отключения журналирования продукта и коммуникационного модуля (все сервисы будут автоматически перезапущены)
- deliverall чтобы создать:
  - Архив, содержащий журналы продукта и модуля связи, доставленный в папку /tmp в следующем формате: bitdefender\_machineName\_timeStamp.tar.gz.

После того как создан архив:

1. При отключении журналирования вам будет выдан запрос. При необходимости службы автоматически перезапустятся.
  2. При удалении журналов вам будет выдан соответствующий запрос.
- deliverall -default предоставляет такую же информацию, как и в предыдущей опции, но действия по умолчанию будут отображены в логах без запроса пользователя (журналы отключены и удалены).



Вы также можете запустить команду `/bdconfigure` прямо из пакета [BEST\_SHORT] (полный или загрузчик) без установки продукта.

Для сообщения о проблеме GravityZone, воздействующей на вашу систему Linux, выполните следующие шаги, используя ранее описанные опции:

1. Включите журналирование продукта и коммуникационного модуля.
2. Попытайтесь воспроизвести проблему.
3. Отключите журналы.
4. Создайте архив журналов.
5. Откройте обращение в службу поддержки, используя форму, которая доступна на странице **Помощь & Поддержка** в Control Center, с описанием проблемы и прикрепленным архивом журналов.

Инструмент поддержки для Linux предоставляет следующую информацию:

- `etc`, `var/log`, `/var/crash` (если доступно) и `var/erag` папки из папки `/opt/BitDefender`, которые содержат журналы и настройки Bitdefender
- Файл `/var/log/BitDefender/bdinstall.log` содержит информацию по установке
- Файл `network.txt`, который содержит информацию о сетевых настройках / о доступности машин
- Файл `product.txt`, включая содержимое всех файлов `update.txt` из `/opt/BitDefender/var/lib/scan` и полный рекурсивный список всех файлов из `/opt/BitDefender`
- Файл `system.txt`, который содержит общую системную информацию (версия дистрибутива и ядра, доступная оперативная память и свободное место на жестком диске)
- Файл `users.txt`, который содержит информацию о пользователе
- Другую системную информацию, касающуюся продукта, такую как внешнее сетевое взаимодействие процессов и использование процессора
- Системные журналы

### 8.3.3. Использование инструментов поддержки на операционных системах Mac

При отправке запроса в группу технической поддержки Bitdefender, необходимо предоставить следующую информацию:

- Подробное описание проблемы, с которой вы столкнулись.
- Скриншот (если возможно) сообщения об ошибке, которое появляется.
- Журнал инструмента поддержки.

Чтобы собрать информацию о Mac-системе с помощью инструмента поддержки:

1. Скачайте [ZIP-архив](#), содержащий инструмент поддержки.
2. Извлеките файл **BDProfiler. Tool** из архива.
3. Откройте окно терминала.
4. Перейдите к папке, содержащей файл **BDProfiler.tool**.

Например:

```
cd /Users/Bitdefender/Desktop;
```

5. Добавьте разрешение на выполнение файла:

```
chmod +x BDProfiler.tool;
```

6. Запустите инструмент.

Например:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Нажмите Y и введите пароль, когда появится запрос ввода пароля администратора.

Подождите пару минут, пока инструмент не закончит создание журнала. Полученный файл архива ( **Bitdefenderprofile\_output. Zip** ) появится на рабочем столе.

## 8.4. Контактная информация

Эффективное взаимодействие с клиентами является залогом успешного бизнеса. За последние 18 лет Bitdefender удалось завоевать бесспорный авторитет среди своих клиентов и партнеров за счет опережения их ожиданий и постоянного улучшения отношений с ними. Мы будем рады ответить на все ваши вопросы и решить ваши проблемы – не стесняйтесь, обратитесь к нам за помощью.

### 8.4.1. Адреса веб-сайтов

Отдел продаж: [enterprisesales@bitdefender.com](mailto:enterprisesales@bitdefender.com)

Центр поддержки: <http://www.bitdefender.com/support/business.html>

Документация: [gravityzone-docs@bitdefender.com](mailto:gravityzone-docs@bitdefender.com)

Местные дистрибуторы: <http://www.bitdefender.com/partners>

Партнерские программы: [partners@bitdefender.com](mailto:partners@bitdefender.com)

Отдел по связям со СМИ: [pr@bitdefender.com](mailto:pr@bitdefender.com)

Вирусная лаборатория: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)

Спам-лаборатория: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)

Сообщение о нарушениях: [abuse@bitdefender.com](mailto:abuse@bitdefender.com)

Веб-сайт: <http://www.bitdefender.com>

### 8.4.2. Местные дистрибуторы

Местные дистрибуторы Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции.

Чтобы найти дистрибутора Bitdefender в вашей стране:

1. Перейдите к <http://www.bitdefender.com/partners>.
2. Перейдите к **Поиск партнеров**.
3. Контактная информация местных дистрибуторов Bitdefender будет отображена автоматически. Если это не произошло, выберите вашу страну, чтобы просмотреть информацию.
4. Если не удалось найти дистрибутора Bitdefender в вашей стране, свяжитесь с нами по адресу электронной почты [enterprisesales@bitdefender.com](mailto:enterprisesales@bitdefender.com).

### 8.4.3. Офисы Bitdefender

Офисы компании Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции. Ниже приведены адреса и контактная информация офисов.

#### США

##### Bitdefender, LLC

PO Box 667588  
Pompano Beach, FL 33066  
United States  
Телефон (продажи & техническая поддержка): 1-954-776-6262  
Продажи: [sales@bitdefender.com](mailto:sales@bitdefender.com)  
Сайт: <http://www.bitdefender.com>  
Центр поддержки: <http://www.bitdefender.com/support/business.html>

#### Франция

##### Bitdefender

49, Rue de la Vanne  
92120 Montrouge  
Факс: +33 (0)1 47 35 07 09  
Телефон: +33 (0)1 47 35 72 73  
E-mail: [b2b@bitdefender.fr](mailto:b2b@bitdefender.fr)  
Веб-сайт: <http://www.bitdefender.fr>  
Центр поддержки: <http://www.bitdefender.fr/support/business.html>

#### Испания

##### Bitdefender España, S.L.U.

Avda. Diagonal, 357, 1º 1<sup>a</sup>  
08037 Barcelona  
España  
Факс: (+34) 93 217 91 28  
Телефон (office & sales): (+34) 93 218 96 15  
Телефон (техническая поддержка): (+34) 93 502 69 10  
Продажи: [comercial@bitdefender.es](mailto:comercial@bitdefender.es)  
Веб-сайт: <http://www.bitdefender.es>  
Центр поддержки: <http://www.bitdefender.es/support/business.html>

## Германия

### **Bitdefender GmbH**

Technologiezentrum Schwerte  
Lohbachstrasse 12  
D-58239 Schwerte  
Deutschland

Телефон (office & sales): +49 (0) 2304 94 51 60

Телефон (техническая поддержка): +49 (0) 2304 99 93 004

Продажи: [firmenkunden@bitdefender.de](mailto:firmenkunden@bitdefender.de)

Веб-сайт: <http://www.bitdefender.de>

Центр поддержки: <http://www.bitdefender.de/support/business.html>

## Великобритания и Ирландия

Genesis Centre Innovation Way  
Stoke-on-Trent, Staffordshire  
ST6 4BF  
UK

Телефон (продажи & техническая поддержка): (+44) 203 695 3415

E-mail: [info@bitdefender.co.uk](mailto:info@bitdefender.co.uk)

Продажи: [sales@bitdefender.co.uk](mailto:sales@bitdefender.co.uk)

Веб-сайт: <http://www.bitdefender.co.uk>

Центр поддержки: <http://www.bitdefender.co.uk/support/business.html>

## Румыния

### **BITDEFENDER SRL**

Orhideea Towers  
15A Orhideelor Street  
060071 Bucharest, Sector 6  
Факс: +40 21 2641799

Телефон (продажи & техническая поддержка): +40 21 2063470

Продажи: [sales@bitdefender.ro](mailto:sales@bitdefender.ro)

Веб-сайт: <http://www.bitdefender.ro>

Центр поддержки: <http://www.bitdefender.ro/support/business.html>

## Объединенные Арабские Эмираты

### **Bitdefender FZ-LLC**

Dubai Internet City, Building 17

Office # 160

Dubai, UAE

Телефон (продажи & техническая поддержка): 00971-4-4588935 / 00971-4-4589186

Факс: 00971-4-44565047

Продажи: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Сайт: <http://www.bitdefender.com>

Центр поддержки: <http://www.bitdefender.com/support/business.html>

## A. Приложения

### A.1. Поддерживаемые типы файлов

Механизмы сканирования на наличие вредоносных программ, включенные в решения безопасности Bitdefender, могут сканировать все типы файлов, которые могут содержать угрозы. Список ниже включает наиболее распространенные типы файлов, которые анализируются.

```
{*; 386; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx;drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; ffp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; oox; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rlx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; slidx; smm;.snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; tdo; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;
```

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;  
xsn; xtp; xz; z; zip; zl?; zoo

## A.2. Объекты Sandbox Analyzer

### A.2.1. Поддерживаемые Типы и Расширения Фалов для Отправки Вручную

Поддерживаются следующие расширения, которые могут быть проверены вручную в Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer может обнаруживать вышеупомянутые типы файлов, если они включены в архивы следующих типов: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

### A.2.2. Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке

Предварительная фильтрация контента определит конкретный тип файла с помощью комбинации, которая включает в себя содержимое объекта и расширение. Это означает, что исполняемый файл с расширением .tmp будет распознан как приложение и, если он окажется подозрительным, будет отправлен в Sandbox Analyzer.

- Приложения - файлы формата PE32, включая, но не ограничиваясь следующими расширениями: exe, dll, com.
- Документы - файлы формата документа, включая, но не ограничиваясь следующими расширениями: xlsx, xls, ppt, doc, docx, dot, chm,

xlm, docm, dotm, potm, potx, pparam, ppax, pps, ppssm, pptx, sldm, sldx, xlam, xlm, xltx, rtf, pdf.

- **Сценарии:** ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.
- **Архивы:** zip, jar, 7z, bz, bz2, tgz, msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.
- **Почту (сохраненную в файловой системе):** eml, tnef.

### A.2.3. Исключения По Умолчанию в Автоматической Отправке

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.

### A.2.4. Рекомендуемые приложения для детонации виртуальных машин

Sandbox Analyzer On-Premises требует, чтобы определенные приложения были установлены на виртуальных машинах детонации, чтобы они открывали отправленные образцы.

Приложения	Типы файлов.
Пакет Microsoft Office	xls, xltx, ppt, doc, dotx, docm, potm, potx, pparam, ppax, pps, ppssm, ppsx
Adobe Flash Player	swf
Программа Adobe Acrobat Reader	pdf
Windows по умолчанию	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pup

Приложения	Типы файлов.
Mozilla Thunderbird	eml
Microsoft Outlook	