Bitdefender

GravityZone

РУКОВОДСТВО ПО УСТАНОВКЕ

Bitdefender GravityZone
Руководство по установке

Дата публикации 2021.09.29

Правовое положение

Bitdefender

Содержание

Предисловие

Это руководство предназначено IT-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 объясняет, как развернуть агенты безопасности Bitdefender на всех типах конечных точек в Вашей компании и как настроить решение GravityZone.

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.
http://www.bitdefender.com	Ссылки URL на внешние источники (http или ftp серверы).
gravityzone-docs@bitdefender.com	Адреса электронной почты в тексте приводятся в качестве контактной информации.
«Предисловие» (p. v)	В кавычках приводятся внутренние ссылки на другие материалы в пределах этого документа.
опция	Все параметры продукта выделены **жирным** шрифтом.

Виды шрифтов и стилей	Описание
ключевое слово	Опции интерфейса, ключевые слова или сочетания клавиш выделены с помощью **bold** 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
- Управление Рисками Конечной Точки (ERA)
- Email Security

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, руткитов 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).

ATC 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 управление 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. Управление Рисками Конечной Точки (ERA)

Управление Рисками Конечной Точки (ERA) определяет, оценивает и исправляет слабые стороны конечных точек Windows с помощью сканирования рисков (по запросу или по расписанию согласно политике), учитывая большое число индикаторов риска. После первого сканирования вашей сети с определенными индикаторами риска, вы получите обзор состояния риска вашей сети в панели **Управление рисками**, доступной из главного меню. Некоторые риски Вы можете разрешить автоматически из Control CenterGravityZone, а также просмотреть рекомендации по снижению ущерба конечной точки.

2.11. Email Security

С помощью Email Security вы можете контролировать доставку электронной почты, фильтровать сообщения и применять политики в масштабах всей компании, чтобы предотвращать нацеленные и сложные угрозы электронной почты, включая Нарушение безопасности деловой почты (BEC) и CEO мошенничество. Email Security требует предоставления учетной записи для доступа к консоли. Для получения дополнительной информации см. Руководство пользователя Bitdefender Email Security.

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

Решение GravityZone включает в себя следующие компоненты:

- Веб-Консоль (Control Center)
- Агенты безопасности

3.1. 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.

Веб-интерфейс Control Center интегрируется с существующими системами управления и мониторинга, чтобы упростить применение защиты для неуправляемых рабочих станций и серверов.

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
- Управление Рисками Конечной Точки (ERA)

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» (p. 14).

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 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.

  Эта функциональность имеет важное значение для развертывания агента безопасности в облачной среде GravityZone.
- Развертывание 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)

4. ТРЕБОВАНИЯ

Все решения GravityZone устанавливаются и управляются посредством Control Center.

4.1. 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

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.

4.2. 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.

4.2.1. 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	ОС MAK
	Apple M1	
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	

Свободное пространство на диске

Во время установки (MB)

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

Количество связанных конечных точек	Центральный процессор (CPU) для поддержки Сервера обновлений	ОЗУ	Свободное пространство на диске для Сервера обновлений
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.

4.2.2. 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

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 [2]
- SUSE Linux Enterprise Server 11 SP4 или выше
- OpenSUSE Leap 42.x
- Fedora 25 или выше[1]
- 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 / CentOS 6.0 или более поздней версии Ubuntu версия 14.04 или более поздняя версия SUSE Linux Enterprise Server 11 SP4 или выше 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	**Fanotify** (опция ядра) должна быть включена.
2.6.38 или выше	Debian 8	**Fanotify** должен быть включен и установлен в режим принудительного применения, затем необходимо перестроить пакет ядра. Для получения подробной информации смотрите эту статью базы знаний.
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender обеспечивает поддержку через **DazukoFS** помощью встроенных модулей ядра.
Все остальные ядра	Все другие поддерживаемые системы	Модуль **DazukoFS** должен быть скомпилирован вручную. Дополнительные сведения см. в разделе «Компиляция вручную модуля DazukoFS» (p. 37).

* С некоторыми ограничениями, описанными ниже.

Ограничения сканирования при доступе

Версии ядра	Дистрибутивы Linux	Подробная информация
2.6.38 или выше	Все поддерживаемые системы	Сканирование при доступе контролирует подключенные сетевые ресурсы только в следующих условиях: • **Fanotify** включается как на удаленных, так и на локальных системах. • Общий ресурс основан на файловых системах CIFS и NFS. **Примечание** Сканирование при доступе не сканирует сетевые ресурсы, установленные с помощью SSH или FTP.
Все ядра	Все поддерживаемые системы	Сканирование при доступе не поддерживается в системах с **DazukoFS** 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)

4.2.3. 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.

4.2.4. 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+

4.2.5. Использование трафика

- **Трафик обновления продукта между клиентом конечного устройства и сервером обновлений**
  - На Windows ОС: ~20 МБ
- **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.

4.3. 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 Server смотрите 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

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

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)

4.4. 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

Чтобы защитить вашу сеть с Bitdefender, вы должны установить агентов безопасности GravityZone на конечных точках. Для этого под вашим управлением должен быть пользователь GravityZone Control Center с правами администратора для конечных точек.

5.1. Управление лицензиями

GravityZone лицензируется одним ключом для всех служб безопасности, за исключением полного шифрования диска, который для ежегодной лицензии поставляется с отдельным ключом.

Бесплатное тестирование GravityZone в течение 30 дней. В течение пробного периода все функции полностью доступны, и вы можете использовать эту услугу на любом количестве компьютеров. До истечения пробного периода, если вы хотите продолжать пользоваться услугами, вы должны выбрать платный тарифный план и совершить покупку.

Чтобы приобрести лицензию, свяжитесь с рессейлером Bitdefender или свяжитесь с нами по электронной почте enterprisesales@bitdefender.com.

Ваша подписка управляется Bitdefender или партнером Bitdefender, который предоставляет данную услугу. Поставщиками услуг безопасности в некоторых случаях являются партнеры Bitdefender. В зависимости от выбранных Вами условий подписки ежедневные данные по функционированию GravityZone могут обрабатываться либо внутри вашей компании, либо внешним поставщиком услуг безопасности.

5.1.1. Поиск рессейлера

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.

5.1.2. Активация лицензии

Когда вы впервые приобретаете план платной подписки, вам выдается лицензионный ключ. Подписка GravityZone активируется с помощью этого лицензионного ключа.

Предупреждение
Активация лицензии НЕ добавляет ее функции к текущей активной лицензии. Вместо этого новая лицензия отменяет прежнюю. Например, активация лицензии на 10 конечных точек поверх лицензии на 100 конечных точек не приведет к подписке на 110 конечных точек. Напротив, это уменьшит количество охваченных конечных точек от 100 до 10.

После покупки, лицензионный ключ отправляется вам по электронной почте. В зависимости от соглашения об обслуживании, после того Ваш лицензионный ключ был выпущен, ваш провайдер услуг может активировать его для вас. В качестве альтернативы вы можете активировать свою лицензию вручную, выполнив следующие шаги:

1. Войдите в Control Center, используя свою учетную запись.
2. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **My Company**.
3. Проверьте информацию о текущей лицензии в разделе **Лицензия**.
4. В разделе **Лицензия** выберите тип **Лицензия**.
5. В поле **Лицензионный ключ** введите свой лицензионный ключ.
6. Нажмите кнопку **Check** и подождите пока Control Center не получит информацию о введенном лицензионном ключе.
7. В поле **Добавочный ключ** введите ключ для определенного дополнения, например «Шифрование».
8. Нажмите **Добавить**. Дополнительные сведения отображаются в таблице: тип, лицензионный ключ и опция удаления ключа.
9. Нажмите **Сохранить**.
10. Чтобы использовать надстройку, необходимо выйти из Control Center, а затем снова войти в систему. Это сделает дополнительные функции видимыми в GravityZone.

5.1.3. Проверка текущих параметров лицензирования

Для просмотра подробностей лицензии:

1. Войдите в Control Center , используя электронную почту и пароль, полученные по электронной почте.
2. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **My Company**.
3. Проверьте информацию о текущей лицензии в разделе **Лицензия**. Вы также можете нажать кнопку **Проверить** и подождать, пока Control Center не извлечет последнюю информацию о текущем лицензионном ключе.

5.2. 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 упращенный 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» (p. 27).

5.2.1. Подготовка к установке

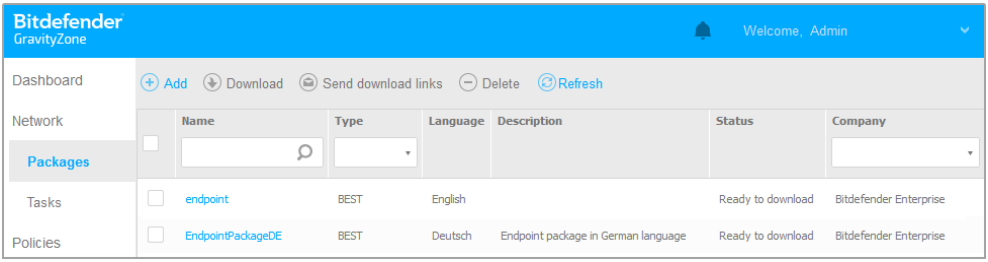
Перед установкой выполните следующие подготовительные шаги, чтобы убедиться, что она пройдет без проблем:

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 подключение к Control Center.
4. Рекомендуется использовать статический IP-адрес для Relay сервера. Если вы не установите статический IP-адрес, используйте имя хоста машины.

5.2.2. 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**.



Страница пакетов

Предупреждение

- Первая машина, на которой установлена защита, должна иметь роль ретранслятора, иначе вы не сможете применить агент безопасности на других рабочих станциях в той же сети.
- Компьютер-ретранслятор должна быть включена и находится в состоянии он-лайн, чтобы клиенты могли подключаться к Control Center.

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» (p. 39).

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.

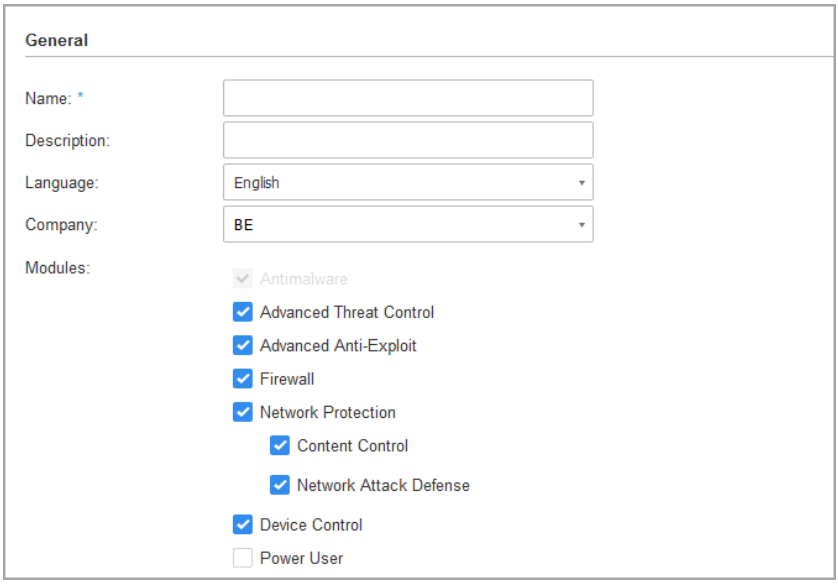
2. Download the installation package на выбранную конечную точку.

   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.



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. **Важно**
   При использовании пользовательского пути убедитесь, что у вас есть правильный установочный пакет для каждой операционной системы.
8. При желании, вы можете установить пароль, чтобы запретить пользователям удалять защиту. Выберите **Set uninstall password** и введите желаемый пароль в соответствующие поля.
9. 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.

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

    - **Облако Bitdefender**, если необходимо обновлять клиентов непосредственно из Интернета.

      В этом случае вы также можете определить параметры прокси-сервера, если конечные точки конечных пользователей подключаются к Интернету через прокси-сервер. Выберите **Использовать прокси для связи** 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
      Порт 7074 должен быть открыт для правильного развертывания через Bitdefender Endpoint Security Tools Relay.

11. 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, будет 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 комплекты 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 эту 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. Нажимайте `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:

- 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.

5.2.3. Удаленная установка

Control Center позволяет удаленно установить агент безопасности на конечные рабочие станции, обнаруженные в сети, с помощью задач установки.

После установки первого клиента с ролью Relay может потребоваться несколько минут, чтобы остальные конечные рабочие станции сети стали видимыми в Control Center. С этого момента вы можете удаленно установить

агент безопасности на конечную рабочую станцию под управлением с помощью задач установки из Control Center.

Bitdefender Endpoint Security Tools включает механизм автоматического обнаружения сети, который позволяет обнаруживать другие конечные рабочие станции в данной сети. Обнаруженные конечные точки отображаются как **неуправляемые** на странице **Сеть** .

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» (p. 39).

Требования для удаленной установки

Для запуска удаленной установки:

- В вашей сети должен быть установлен Bitdefender Endpoint Security Tools Relay.
- 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 эту 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» (p. 14).

Выполнение задач удаленной установки

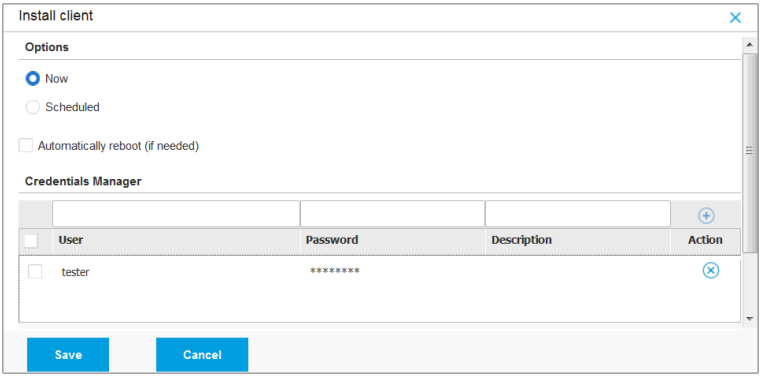
Чтобы запустить задачу удаленной установки:

1. Подключитесь и войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. 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**.

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

   Отобразится мастер установки **Install Client**.



6. 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.

7. Если вы хотите, чтобы заданные конечные точки перезапустились после завершения установки, выберите **Автоматическая перезагрузка (при необходимости)** .
8. 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.

9. Установите флажки на соответствующие аккаунты, которые вы хотите использовать.

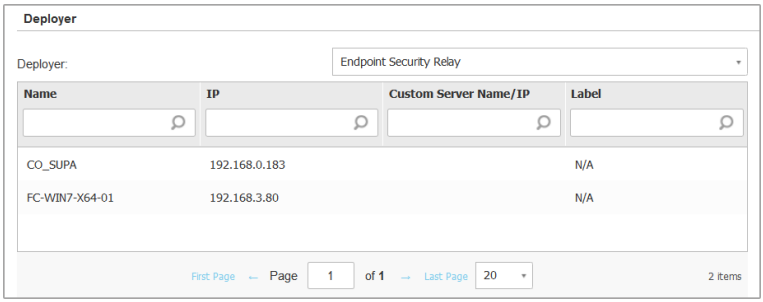
Примечание
Предупреждающее сообщение будет отображаться до тех пор, пока вы не выберите какие-нибудь учетные данные. Этот шаг является обязательным для удаленной установки агента безопасности на конечных точках.

10. В разделе **Участник операции** настройте Relay, к которому будут подключаться целевые конечные точки для установки и обновления клиента:

- Все компьютеры с ролью Relay, обнаруженные в сети, будут отображаться в таблице, доступной в разделе **Участник операции**. Каждый новый клиент должен быть подключен в той же сети по меньшей мере к одному Relay, который будет служить в качестве коммуникационного и сервера обновлений. Выберите Relay, к которому

вы хотите подключить выбранные конечные точки. 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.



- Если выбранные конечные точки связаны с Relay через прокси-сервер, вам необходимо также задать параметры прокси-сервера. В этом случае выберите **Использовать прокси для общения** и введите необходимые параметры прокси-сервера в полях ниже.

11. 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.
12. 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» (p. 27).

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.

13. Нажмите **Сохранить**. Появится окно подтверждения.

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

5.2.4. 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.

5.2.5. 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.

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.

Чтобы включить автоматическое обнаружение сети, у вас должен быть установлен Bitdefender Endpoint Security Tools Relay на хотя бы одном компьютере в сети. Этот компьютер будет использоваться для сканирования сети.

Важно

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

Control Center не принимает активного участия в работе службы просмотра компьютеров. Только Bitdefender Endpoint Security Tools опрашивает службу просмотра компьютеров для построения списка рабочих станций и серверов, доступных в настоящее время в сети (известный как список просмотра), и затем отправляет его на Control Center. 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.

Начальный запрос для просмотра списка осуществляется первым Bitdefender Endpoint Security Tools, установленым 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.

Для полной видимости сети, Relay должен быть установлен, по крайней мере, на одном компьютере в каждом домене или рабочей группе в сети. В идеале, Bitdefender Endpoint Security Tools должен быть установлен по крайней мере на одном компьютере в каждой подсети.

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
  - Обноружение 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.

Компьютеры, с которых Bitdefender Endpoint Security Tools опрашивает службу просмотра компьютеров, должны быть в состоянии разрешать имена NetBIOS.

Примечание
Механизм сетевого обнаружения работает для всех поддерживаемых операционных систем, в том числе версий Windows Embedded, при выполнении ряда требований.

5.3. Установка полного шифрования диска

Для полного шифрования диска требуется активация на основе лицензионного ключа.

Для получения дополнительной информации по лицензионным ключам, перейдите к «Управление лицензиями» (p. 23).

Агенты безопасности Bitdefender поддерживают Полноше 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:

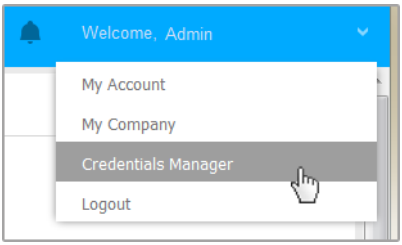
- Установите агентов безопасности с включенным модулем шифрования.
- Используйте задачу **Переконфигурировать** .

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

5.4. Диспетчер учетных данных (Credentials Manager)

Диспетчер учетных данных позволяет определить необходимые учетные данные для удаленной аутентификации на различных операционных системах в вашей сети.

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

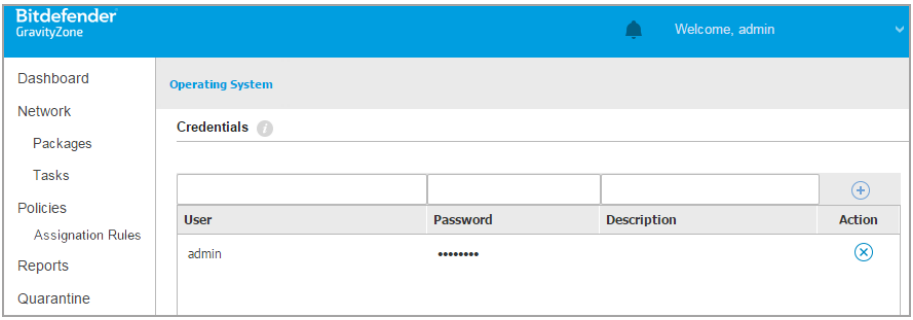


Меню диспетчера учетных данных

5.4.1. Добавление учетных данных в диспетчер учетных данных

С помощью Диспетчера учетных данных можно управлять учетными данными администратора, необходимыми для удаленной аутентификации, во время выполнения задач установки, отправленных на компьютеры и виртуальные машины в вашей сети.

Чтобы добавить набор учетных данных:



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.

5.4.2. 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.

5.5. 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).

5.5.1. 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.

5.5.2. 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 флажки:
   - **Отправлять отчеты о сбоях в Bitdefender**.
   - **Отправьте подозрительные исполняемые файлы для анализа**.
   - **Используйте Bitdefender Global Protective Network для усиления защиты**.
4. 111 Перейдите в раздел **Antimalware > Настройки**.
5. В разделе **Карантин** снимите флажок **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.

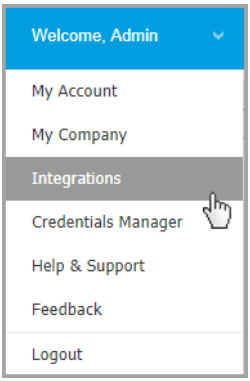
Правовое положение

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 распространиться. 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. ИНТЕГРАЦИЯ

GravityZone предоставляет возможность интеграции Control Center со сторонними решениями.

Вы можете настроить интеграцию стороннего решения на странице **Integrations**, на которую можно получить доступ, указав ваше имя пользователя в правом верхнем углу консоли и выбрав **Integrations**.



На этой странице вы можете добавлять, редактировать или удалять интеграции в соответствии с вашими потребностями.

6.1. Интеграция с Amazon EC2

Если ваша компания имеет лицензию на обслуживание Bitdefender Security for AWS или вы используете пробную подписку Bitdefender Security for AWS, вы можете настроить интеграцию с этой службой из GravityZone Control Center и централизованно развернуть, управлять и контролировать безопасность Bitdefender в своем инвентаре. Собственные серверы сканирования размещаются Bitdefender в облаке AWS, чтобы обеспечить оптимальный результат на защищаемых экземплярах и чтобы уменьшить использование ресурсов при сканировании, что обычно происходит при использовании традиционного программного обеспечения по безопасности.

Для получения полной информации об архитектуре Bitdefender Security for AWS, предварительных условиях, режиме подписки, создании и управлении интеграцией с Amazon EC2 см. Руководство по интеграции Amazon EC2.

7. УДАЛЕНИЕ ЗАЩИТЫ КОНЕЧНЫХ РАБОЧИХ СТАНЦИЙ

У вас есть два варианта удаления агентов безопасности:

- удаленно в Control Center
- Вручную на целевой машине

Предупреждение
Агенты безопасности и необходимы для обеспечения безопасности конечных точек от любых видов угроз, поэтому их удаление может поставить под угрозу всю сеть.

Удаленная деинсталляция

Чтобы удаленно удалить защиту Bitdefender с любой управляемой конечной рабочей станции:

1. Перейдите на страницу **Сеть** .
2. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
3. Выберите конечные точки, из которых вы хотите удалить агент безопасности Bitdefender.
4. Нажмите **Задачи** в верхней части таблицы и выберите **Удалить клиента** . Появится окно конфигурации.
5. В окне задачи **Удалить агент** вы можете выбрать, сохранять ли файлы в карантине на конечной рабочей ставнции или удалять их.
6. 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. 25).

Локальная деинсталляция

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 конпкой мыши **Старт**, затем выберите **Панель управления > Программы & Функции** .
- В ОС Windows 10, go to **Старт > Настройки> Сист ема > Приложения & Свойства**.

2. Выберите агент Bitdefender из списка программ.
3. Щелкните **Деинсталляция**.
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» (p. 25).

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

1. Чтобы загрузить Инструмент поддержки BEST, нажмите здесь.
2. Запустите исполняемый файл от имени администратора. Появится окно.
3. 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/epag` 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
Центр поддержки:http://www.bitdefender.com/support/business.html
Документация: gravityzone-docs@bitdefender.com
Местные дистрибьюторы:http://www.bitdefender.com/partners
Партнерские программы: partners@bitdefender.com
Отдел по связям со СМИ: pr@bitdefender.com
Вирусная лаборатория: virus_submission@bitdefender.com
Спам-лаборатория: spam_submission@bitdefender.com
Сообщение о нарушениях: abuse@bitdefender.com
Веб-сайт: http://www.bitdefender.com

8.4.2. Местные дистрибьюторы

Местные дистрибьюторы Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции.

Чтобы найти дистрибьютора Bitdefender в вашей стране:

1. Перейдите к http://www.bitdefender.com/partners.
2. Перейдите к **Поиск партнеров**.
3. Контактная информация местных дистрибьюторов Bitdefender будет отображена автоматически. Если это не произошло, выберите вашу страну, чтобы просмотреть информацию.
4. Если не удалось найти дистрибьютора Bitdefender в вашей стране, свяжитесь с нами по адресу электронной почты 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
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
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 1ª
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
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
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
Продажи: 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
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
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; 3g2; 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; fxp; 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; ocx; 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; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; 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
```