Bitdefender

GravityZone

РУКОВОДСТВО ПО УСТАНОВКЕ

Bitdefender GravityZone
Руководство по установке

Дата публикации 2021.02.03

Правовое положение

Правовое положение

Digitally signed by Celonenco Vitalie
Date: 2021.04.22 10:07:43 EEST
Reason: MoldSign Signature
Location: Moldova

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 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.
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. viii)	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 (в том числе мобильных), виртуальных машин в частных и общедоступных облаках, а также почтовых серверов Exchange.

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 безопасности для конечных точек, почтовых серверов Microsoft Exchange: защита от вредоносного ПО с мониторингом поведения, защита от угроз нулевого дня, контроль приложений и "песочница", межсетевой экран, управление устройствами, управление контентом, антифишинг и антиспам.

2. УРОВНИ ЗАЩИТЫ GRAVITYZONE

GravityZone обеспечивает следующие уровни защиты:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Обнаружение гипервизора
- Advanced Anti-Exploit
- Брандмауэр
- Контроль контента
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Security for Exchange
- Контроль приложений
- Sandbox Analyzer
- Обнаружение и отклик конечной точки (EDR)
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

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).**

* Когда используются двойные движки сканирования - если первый движок не доступен, резервный движок может быть задействован. Потребление ресурсов и утилизация сети будет зависеть от используемых движков.

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. Обнаружение гипервизора

Bitdefender HyperDetect - дополнительный уровень безопасности, разработанный специально для обнаружения продвинутых атак и подозрительной активности ещё до выполнения процессов. HyperDetect содержит модели машинного обучения и технологии обнаружения скрытых атак против угроз, таких как: атаки нулевого дня, продвинутые устойчивые угрозы (APT), скрытое вредоносное ПО, безфайловые атаки (злоупотребление PowerShell, инструментарием управления Windows и т. д.), кража учетных данных, целевые кибератаки, специализированное вредоносное ПО, атаки на основе сценариев, эксплойты, инструменты взлома, подозрительный сетевой трафик, потенциально нежелательные приложения (PUA), вымогатели.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. 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.

2.9. 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.).

2.10. 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.

2.11. Security for Exchange

Bitdefender обеспечивает защиту Security for Exchange от вредоносных программ, антиспам, антифишинг, фильтрацию контента и содержимого писем, полностью интегрирована с серверами Microsoft Exchange, для обеспечения безопасной среды обмена сообщениями и повышения производительности. Используя признанные технологии защиты от вредоносных программ и спама, программа защищает пользователей Exchange от новейших, самых сложных вредоносных программ и от попыток украсть конфиденциальные и ценные данные пользователей.

Важно
Security for Exchange разработан для защиты всей Exchange-организации, к которой принадлежит защищаемый Exchange-сервер. Это означает, что происходит защита всех активных почтовых ящиков, включая user/room/equipment/shared mailboxes.
В дополнение к защите Microsoft Exchange, эта лицензия также покрывает установленные на сервере модули защиты конечных точек.

2.12. Контроль приложений

Модуль Управления приложениями предотвращает активность вредоносных программ, атаки "нулевого дня" и повышает безопасность, не влияя на производительность. Управление приложениями обеспечивает гибкое соблюдение политик для приложений из "белого" списка, который идентифицирует, предотвращает установку и выполнение каких-либо нежелательных, ненадежных или вредоносных приложений.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от продвинутых угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусным движком Bitdefender. В «песочнице» используется обширный набор технологий Bitdefender для выполнения полезных нагрузок в изолированной виртуальной среде, размещенной в Bitdefender или развернутой локально, анализа их поведения и сообщения о любых тонких системных изменениях, которые свидетельствуют о противоправных действиях.

Sandbox Analyzer использует серию датчиков для детонации контента с управляемых конечных точек, потоков сетевого трафика, централизованного карантина и серверов ICAP.

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

Примечание
Функциональность этого модуля может быть предоставлена Sandbox Analyzer Cloud и Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises доступен с отдельным лицензионным ключом.

2.14. События

Характеристика инцидента - это компонент корреляции событий, способный выявлять сложные угрозы или активные атаки. В рамках корпоративной интегрированной платформы характеристика инцидентов объединяет возможности всех устройств, работающих в корпоративной сети. Это решение приходит на помощь в случаях, когда группы немедленного реагирования распознают и отвечают на серьезные угрозы.

Посредством Bitdefender Endpoint Security Tools Вы можете активировать защитный модуль, который называется датчиком инцидентов, в управлении конечной точки, чтобы объединять данные компьютера и операционной системы. Сбор и обработка метаданных с обеих сторон идет на платформе клиент-сервер.

Этот компонент несет детальную информацию по обнаруженным происшествиям, интерактивной карте происшествий, действиям по исправлению и интеграции с Sandbox Analyzer и HyperDetect.

2.15. Hypervisor Memory Introspection (HVI)

Широко известно, что высоко организованные, ориентированные на извлечение прибыли, злоумышленники, ищут неизвестные уязвимости (уязвимости нулевого дня) или используют разовые, специально встроенные эксплойты (эксплойты нулевого дня) и другие инструменты. Злоумышленники также используют передовые методы, чтобы задерживать и последовательно атаковать полезную нагрузку, для маскировки вредоносной активности. Более новые, управляемые атаки, в целях извлечения прибыли, построены

таким образом, чтобы быть незаметными и обходить традиционные средства безопасности.

Для виртуальных сред проблема теперь решена, HVI защищает дата-центры с высокой плотностью виртуальных машин против передовых и сложных угроз, что не могут сделать движки на основе сигнатурного анализа. Это достигается соблюдением строгой изоляции, что обеспечивает обнаружение атак в реальном масштабе времени, их блокировку, как только они происходят, и немедленное удаление угроз.

Будет ли защищенная машина на Windows или Linux, сервер или рабочая станция, HVI даст представление на уровне, который невозможно достичь на уровне гостевой операционной системы. Подобно тому, как гипервизор контролирует доступ к оборудованию от имени каждой гостевой виртуальной машины, HVI имеет глубокое "понимание" как оба режима - пользователя и ядра, ведут себя в "гостевой" памяти. В результате HVI имеет полное представление о гостевой памяти, и, следовательно, ее полный контекст. В то же время, HVI изолирован от защищенных гостей, так же, как изолирован и сам гипервизор. Действуя на уровне гипервизора и используя функциональные возможности гипервизора, HVI превосходит технические возможности традиционных систем безопасности для выявления вредоносной активности в дата-центрах.

HVI идентифицирует методы атаки, а не шаблоны атаки. Таким образом, технология может идентифицировать, информировать и предотвращать общие методы взломов. Ядро защищено от методов взлома, типа руткит, которые используются во время атаки цели, чтобы обеспечить незаметность. Пользовательские процессы также защищены от внедрения кода, функции обхода и выполнения кода из стека.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

2.16. 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.

2.17. Security for Storage

GravityZone Security for Storage предоставляет защиту в реальном времени для ведущих систем обмена файлами и сетей хранения. Система и алгоритмы обнаружения угроз обновляются автоматически - без каких-либо усилий с вашей стороны или создания помех для конечных пользователей.

Два или более GravityZone Security Servers Multi-Platform выполняет роль сервера ICAP выполнять роль сервера ICAP, предоставляющего службы защиты от вредоносных программ для устройств сетевого хранилища (NAS) и систем совместного использования файлов, соответствующих протоколу Internet Content Adaptation Protocol (ICAP, как определено в RFC 3507).

Когда пользователь делает запрос на открытие, чтение, запись или закрытие файла с ноутбука, рабочей станции, мобильного или другого устройства, клиент ICAP (NAS или система обмена файлами) отправляет запрос на сканирование к Security Server и получает результат относительно данного файла. В зависимости от результата, Security Server разрешает доступ, запрещает доступ или удаляет файл.

Примечание
Этот модуль - это дополнение, доступное при наличии отдельного лицензионного ключа

2.18. Security for Mobile

Унифицирует управление безопасностью всего предприятия и контроль iPhone, iPad и Android устройств, обеспечивая надежность программного обеспечения и предоставление обновлений через онлайн-магазины Apple или Android. Решение было разработано для возможности управления личными устройствами (BYOD), последовательно продвигая политику использования любых портативных устройств. Функции безопасности включают блокировку

экрана, контроль подлинности, местоположение устройства, удаленную очистку, обнаружение root или jailbrake устройств и профили безопасности. На устройствах Android уровень безопасности расширен сканированием в режиме реального времени и шифрованием съемных носителей. В результате, мобильные устройства находятся под контролем и важная для бизнеса информация, находящаяся на них, защищена.

2.19. 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
- Security Server
- Дополнительный пакет HVI
- 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. Сервер обновлений GravityZone

Сервер инцидентов - это связующее звено между агентами безопасности и базой данных, собирающее данные конечных точек и генерирующее инциденты на основе угроз, которые обнаружены с помощью технологий предотвращения и алгоритмов машинного обучения.

3.1.5. Веб-консоль (GravityZone Control Center)

Решения безопасности Bitdefender управляются из единой точки управления, веб-консоли Control Center. Это упрощает управление и доступ к общей системе безопасности, обеспечивает контроль над всеми модулями безопасности, защищающими виртуальные и физические компьютеры, серверы и мобильные устройства от глобальных угроз. Работая на архитектуре Gravity, Control Center способна удовлетворить потребности даже самых крупных организаций.

Control Center интегрируется в существующие системы управления и системы мониторинга, чтобы упростить и автоматически применять защиту для неуправляемых рабочих станций, серверов и мобильных устройств, которые появляются в Microsoft Active Directory, VMware vCenter, Nutanix Prism Element или Citrix XenServer, или которые просто обнаружены в сети.

3.2. Security Server

Security Server является специализированной виртуальной машиной, которая дедуплицирует и централизует большую часть функциональностей защиты от вредоносных программ, агентов защиты от вредоносных программ, действуя в качестве сервера сканирования.

Существуют три версии Security Server, для каждого типа сред виртуализации:

- **Security Server for VMware NSX.** Эта версия автоматически устанавливается на каждом хосте в кластере, где был развернут Bitdefender.
- **Security Server for VMware vShield Endpoint.** Эта версия должна быть установлена на каждом хосте, которые должны быть защищены.
- **Security Server Multi-Platform.** Эта версия предназначена для других виртуальных сред и она должна быть установлена на одном или нескольких хостах, чтобы соответствовать количеству защищаемых виртуальных машин. При использовании HVI, Security Server должен быть установлен на каждом хосте, содержащем виртуальные машины, которые должны быть защищены.

3.3. Дополнительный пакет HVI

Пакет HVI обеспечивает связь между гипервизором и Security Server, расположенным на одном хосте. Таким образом, Security Server может контролировать используемую память на хосте, где он установлен, на основе политик безопасности GravityZone.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

3.4. 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
- GravityZone Mobile Client

- Bitdefender Tools (vShield)

3.4.1. 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).

В дополнение к защите файлов системы,Bitdefender Endpoint Security Tools также включает защиту почтовых серверов Microsoft Exchange.

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)
- Обнаружение гипервизора
- Брандмауэр
- Контроль контента
- Network Attack Defense
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Security for Exchange
- Sandbox Analyzer
- Контроль приложений

Роли конечных точек

- Привилегированный пользователь
- Ретранслятор
- Сервер кэширования патчей
- Защита Exchange

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. 31).

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 большими распределенными сетями, агент-ретранслятор помогает снизить использование полосы пропускания, предотвращая защищаемые конечные устройства и серверы безопасности от прямого взаимодействия с машинами 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.
- 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.

Защита Exchange

Bitdefender Endpoint Security Tools с ролью защитника Exchange может быть установлен на сервере Microsoft Exchange с целью защиты пользователей Exchange от угроз передаваемых по электронной почте.

Bitdefender Endpoint Security Tools с ролью защитника Exchange защищает как сам сервер, так и сервисы Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac - это агент безопасности, созданный для защиты устройств на базе Macintosh. 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

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client распространяет политики безопасности на любое количество Android и iOS устройств, защищая их от несанкционированного использования, от потенциально опасных программ и потери конфиденциальных данных. Функции безопасности включают блокировку экрана, контроль подлинности, местоположение устройства, удаленную очистку, обнаружение root или jailbrake устройств и профили безопасности. На устройствах Android уровень безопасности расширен сканированием в режиме реального времени и шифрованием съемных носителей.

GravityZone Mobile Client распространяется через Apple App Store и Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools является облегченным агентом для виртуальных сред VMware, который интегрирован с конечными точками vShield. Агент безопасности устанавливается на виртуальные машины, защищенные Security Server, что позволяет вам получить дополнительные функциональные возможности, которые он обеспечивает:

- Позволяет запускать задачи сканирования памяти и процессов на компьютере.
- Информирует пользователя об обнаруженных инфекциях и принятых в их отношении мерах.
- Добавляет больше возможностей для создания исключений при сканировании от вредоносных программ.

3.5. 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.

Sandbox Analyzer доступен в двух вариантах:

- Sandbox Analyzer Cloud , размещенный в Bitdefender.
- Sandbox Analyzer On-Premises , доступный как виртуальное устройство, которое можно развернуть локально.

Sandbox Analyzer Облако

Sandbox Analyzer Cloud содержит следующие компоненты:

- **Sandbox Analyzer Portal** - размещенный коммуникационный сервер связи, используемый для передачи запросов между конечными точками и кластером безопасной среды Bitdefender.
- **Sandbox Analyzer Cluster** - размещенная инфраструктура безопасной среды, в которой происходит выборочный анализ поведения объектов. На этом уровне отправленные файлы проверяются на виртуальных машинах под управлением Windows 7.

GravityZone Control Center – функционирует как консоль управления и отчетов, где вы настраиваете политики безопасности, просматриваете отчеты анализа и уведомления.

Bitdefender Endpoint Security Tools (BEST) - агент безопасности, установленный на конечных точках, действует как датчик подачи данных в Sandbox Analyzer.

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.

ЭкземплярSandbox 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:

- **Датчик конечной точки** . Bitdefender Endpoint Security Tools для Windows действует как датчик подачи, установленный на конечных точках. Агент Bitdefender использует передовые алгоритмы машинного обучения и нейронной сети для определения подозрительного контента и отправки его в Sandbox Analyzer, включая объекты из централизованного карантина.
- **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» (p. 113).

Bitdefender HVI также запрашивает значительное количество ресурсов. Если вы используете эту услугу, пожалуйста, ознакомьтесь с таблицами с конкретными данными. Для просмотра всех требований данной услуги, перейдите к разделу «HVI» (p. 53).

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
Базовые функции GravityZone								
Сервер обновлений*	10	14	16	18	4	4	6	8
Веб-консоль**					6	10	12	12
Коммуникационный Сервер					6	10	12	18
База данных***					6	6	9	12
Инциденты сервера					4	4	6	6
Общее количество	**10**	**14**	**16**	**18**	**26**	**34**	**45**	**56**
GravityZone с Bitdefender HVI								
Сервер обновлений*	10	4	4	4	4	4	6	8

Компонент	Количество машин							
	250	500	1000	3000	5000	10000	25000	50000
Веб-консоль**		6	8	8	10	10	12	12
Коммуникационный Сервер		6	8	8	10	10	16	20
База данных***		6	6	6	6	6	9	12
Инциденты сервера		2	2	2	4	4	6	6
Общее количество	**10**	**24**	**28**	**28**	**34**	**34**	**49**	**58**

* 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
Базовые функции GravityZone								
Сервер обновлений	18	18	20	22	2	2	3	3
Веб-консоль*					8	8	12	16
Коммуникационный Сервер					6	12	12	16
База данных**					8	10	12	12
Инциденты сервера					2	2	4	4
Общее количество	**18**	**18**	**20**	**22**	**26**	**34**	**43**	**51**
GravityZone с Bitdefender HVI								
Сервер обновлений	18	2	2	2	2	2	3	3
Веб-консоль*		8	10	10	10	10	12	16

Компонент	Количество машин							
	250	500	1000	3000	5000	10000	25000	50000
Коммуникационный Сервер		8	10	10	12	12	16	20
База данных**		8	8	8	8	12	12	12
Инциденты сервера		2	2	2	2	2	4	4
Общее количество	**18**	**28**	**32**	**32**	**36**	**40**	**47**	**55**

* 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
Базовые функции GravityZone									
Сервер обновлений	150	**190**	190	230	230	80	80	80	80
Веб-консоль						80	80	80	80
Коммуникационный Сервер						80	80	80	80
База данных**						110	150	230	530
Общее количество	**150**	**190**	**190**	**230**	**230**	**350**	**390**	**470**	**770**
GravityZone с Bitdefender HVI									
Сервер обновлений	150	190	80	80	80	80	80	80	80
Веб-консоль			80	80	80	80	80	80	80
Коммуникационный Сервер			80	80	80	80	80	80	80
База данных**			110	110	130	130	190	330	730
Общее количество	**150**	**190**	**350**	**350**	**370**	**370**	**430**	**570**	**970**

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.

Примечание
При установке роли сервера инцидентов для базы данных требуется дополнительное пространство размером не менее 30 ГБ. Дополнительное количество пространства уже было добавлено в базу данных, расположенную в приведённой выше таблице.

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 агенты безопасности GravityZone на конечных рабочих станциях сети. Для оптимизации защиты вы также можете установить серверы Security Server. Для этой цели вам нужен пользователь Control Center с полномочиями администратора в отношении служб, которые необходимо установить, и правами на управление конечными точками сети, находящимися 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» (p. 14).

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	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	

Предупреждение
Процессоры ARM в настоящее время не поддерживаются.

Свободная оперативная память

Во время установки (MB)

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 (MB) *

ОС	Антивирус (Одиночный процессор)			М	
	Локальный	Гибридный	Централизованный	Поведенческая проверка	Брандмауэ
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 (MB)

ОС	Один движок						Двойной	
	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 (MB) *

ОС	Антивирус (Одиночный процессор)			М	
	Локальный	Гибридный	Централизованный	Поведенческая проверка	Брандмауэ
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

- Процессоры ARM в настоящее время не поддерживаются.
- 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 ролью обменной защиты

Карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности.

Размер карантина зависит от количества хранящихся элементов и их размера.

По умолчанию, агент устанавливается на системном разделе.

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 доп 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.

Требования к средам VMware vShield

Это требования Bitdefender Tools для систем, интегрированных в среду VMware с vShield Endpoint.

Платформа	ОЗУ	Дисковое пространство
Windows	6-16* МБ (~ 10 МБ для GUI)	24 МБ
Linux	9-10 МБ	10-11 МБ

* 5 МБ, когда параметр "Тихий режим" включен и 10 МБ, когда он отключен. Когда "Тихий режим" включен, графический интерфейс пользователяBitdefender Tools не загружается автоматически при запуске системы, освобождая при этом соответствующие ресурсы.

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 (1)(2)
- Windows 8 (3)
- Windows 7

Предупреждение
(1) платформа VMware vShield (версия без агентов) поддерживается для Windows 8.1 (32/64 бит) и доступна начиная с VMware vSphere 5.5 - ESXi build 1892794 и выше.
(2) В VMware NSX поддерживается версия ОС, начиная с vSphere 5. 5 Patch 2.
(3) В VMware NSX поддерживается версия ОС, начиная с vSphere 5. 5.

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(1)(2)
- Windows Server 2012(3)(4)
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2(4)

Предупреждение
(1) платформа VMware vShield (версия без агентов) поддерживается для Windows Server 2012 R2 (64 бит) и доступна начиная с VMware VSphere 5.5 - ESXi build 1892794 и выше.
(2) В VMware NSX поддерживается версия ОС, начиная с vSphere 5. 5 Patch 2.
(3) В VMware NSX поддерживается версия ОС, начиная с vSphere 5. 5.
(4) VMware NSX не поддерживает 32-разрядные версии Windows 2012 и 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	**Fanotify** (опция ядра) должна быть включена.

Версии ядра	Дистрибутивы Linux	Требования к доступу
	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	**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. 164).

* 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.

Поддержка обнаружения и отклика в конечной точке (EDR)

Перейдите на эту веб-страницу для получения полного и обновленного списка версий ядра и дистрибутивов Linux, поддерживающих датчик EDR.

ОС MAK

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Контроль контента не поддерживается в macOS Big Sur (11. 0).

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, 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 XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (включая Xen гипервизор)
- 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 или Windows Server 2008 R2, 2012, 2012 R2 (включая Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (включая KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

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

Требования для интеграции с VMware NSX-V

- ESXi 5. 5 или более поздняя для каждого сервера
- VCenter Server 5. 5 или новее
- NSX Manager 6. 2. 4 или более поздняя версия
- VMware Tools 9.1.0 или позже, с тонким агентом Guest Introspection.
  - Для Виртуальных Машин Windows обратитесь к Статье VMware Docs.
  - Для Виртуальных Машин Linux обратитесь к Статье VMware Docs.

Примечание
VMware рекомендует использовать следующие версии VMware Tools:
  - 10. 0. 8 или новее, чтобы разрешить работу с медленными виртуальными машинами после обновления VMware Tools в NSX / vCloud Безопасность и сети (VMware Knowledge Base, статья 2144236).
  - 10. 0. 9 и более поздних версий для поддержки Windows 10.

Важно
Рекомендуется хранить все продукты VMware, обновленные последними патчами.

Требования для интеграции с VMware NSX-T Data Center

- VMware NSX-T менеджер 2.4, 2.5 or 3.0
- ESXi совместимо с NSX-T версией менеджера
- vCenter Server & vSphere совместим с NSX-T версией менеджера
- VMware Tools при Guest Introspection thin agent совместим с NSX-T версией менеджера

Дополнительные сведения о совместимости см. на этих веб-страницах VMware:

- VMware Руководство по совместимости – GravityZone vs. NSX-T Менеджер
- Совместимость продукта VMware матриц- решение NSX-T с центром обработки данных и решения VMware vCenter и VMware и инструменты

Требования для интеграции с Nutanix Prism Element

- Учетные данные Nutanix Prism Element с правами администратора (Администратор кластера или Администратор пользователей)
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

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. Security Server

Security Server - это предварительно сконфигурированная виртуальная машина, работающая на сервере Ubuntu со следующими версиями:

- 16.04 (VMware NSX and Multi-Platform)
- 16.04 (VMware NSX and Multi-Platform)

Память и CPU

Распределение ресурсов памяти и CPU для Security Server зависит от количества и типа виртуальных машин, запущенных на хосте. В следующей таблице приведены рекомендуемые ресурсы, которые необходимо выделить:

Количество защищаемых виртуальных машин	ОЗУ	Процессоров
1-50 VMs	2 ГБ	2 CPUs
51-100 VMs	2 ГБ	4 CPUs
101-200 VMs	4 ГБ	6 CPUs

Security Server для NSX поставляется с предустановленной аппаратной конфигурацией (CPU и RAM), которую вы можете настроить в VMware vSphere Web Client, выключив компьютер, отредактировав его настройки, а затем снова включив его. Для получения дополнительной информации перейдите к «Установка Security Server для VMware NSX» (p. 132).

Свободное пространство жесткого диска

Среда	Запас свободного места на жестком диске
VMware NSX-V / NSX-T	40 GB
VMware с конечной точкой vShield	40 GB
Другое	16 ГБ

Распределение по хостам Security Server

Среда	Security Server vs. Хосты
VMware NSX-V / NSX-T	Security Server автоматически устанавливает на каждом узле ESXi в защищаемом кластере во время развертывания услуг Bitdefender.
VMware с конечной точкой vShield	Security Server должен быть установлен на каждом хосте ESXi, который должен быть защищен.
Другое	Хотя это и не обязательно, Bitdefender рекомендует установить Security Server на каждом физическом хосте для повышения производительности.

Сетевая задержка

Задержка связи между Security Server и защищенными конечными точками должна быть менее 50 мс.

Нагрузка модуля Защиты Хранилища

Влияние защиты хранилища на Security Server при сканировании 20 ГБ заключается в следующем:

Статус защиты хранилища	Ресурсы Security Server	Загрузка Security Server	Время передачи (мм:сс)
Отключено (базовый уровень)	Данные отсутствуют	Данные отсутствуют	10:10

Статус защиты хранилища	Ресурсы Security Server	Загрузка Security Server	Время передачи (мм:сс)
Включено	4 vCPU 4 GB RAM	Стандартный	10:30
Включено	2 vCPU 2 GB RAM	Тяжелый	11:23

Примечание
Эти результаты получены с образцом файлов различных типов (. Exe,. Txt,. Doc,. Eml,. Pdf,. Zip и т. Д.), от 10 КБ до 200 МБ. Длительность передачи соответствует 20 ГБ данных, содержащихся в 46 500 файлах.

4.3.7. Использование трафика

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

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

  - На Windows ОС: ~20 МБ
  - На Linux ОС: ~26 МБ
  - На ОС Mac: ~25 MB

- **Загружаемый трафик обновлений механизмов защиты между клиентом конечной точки и Сервером обновлений (MB / 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. Защита Exchange

Security for Exchange доставляется через Bitdefender Endpoint Security Tools, который может защитить как файловую систему, так и почтовый сервер Microsoft Exchange.

4.4.1. Поддерживаемое окружение Microsoft Exchange

Security for Exchange поддерживает следующие версии и роли Microsoft Exchange:

- Exchange Server 2019 с ролями Edge Transport или Mailbox
- Exchange Server 2016 с ролями Edge Transport или Mailbox
- Exchange Server 2013 с ролями Edge Transport или Mailbox
- Exchange Server 2010 с ролями Edge Transport, Hub Transport или Mailbox
- Exchange Server 2007 с ролями Edge Transport, Hub Transport или Mailbox

Security for Exchange совместим с Microsoft Exchange Database Availability Groups (DAGs).

4.4.2. Системные требования

Security for Exchange совместим с физическими или виртуальными 64-разрадяными серверами (Intel или AMD), работающих под управлением

поддерживаемой версией и ролью сервера Microsoft Exchange. Для получения подробной информации относительно системных требований Bitdefender Endpoint Security Tools, обратитесь к «Агент безопасности без ролей» (p. 28).

Рекомендуемые доступные ресурсы сервера:

- Свободной оперативной памяти: 1 Гб
- Свободное пространство жесткого диска: 1 Гб

4.4.3. Другие требования к программному обеспечению

- Для Microsoft Exchange Server 2013 с Service Pack 1: KB2938053 от Microsoft.
- Для Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 более поздняя версия

4.5. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises имеет конкретные требования 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.

4.5.1. 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» (p. 51).
- 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» (p. 51).
- 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.

4.5.2. 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» (p. 51))
- 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» (p. 233).

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 » (p. 234).

4.5.3. 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

4.5.4. 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 ва 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.

4.5.5. 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

Направление	Коммуникационные порты (на TCP)	Источник/назначение
	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.

4.6. HVI

HVI работает с помощью двух компонентов: Security Server и Дополнительный пакет HVI. Эти продукты должны быть установлены на хостах в вашем виртуальном окружении, где у вас есть виртуальные машины, которые вы хотите защитить.

Примечание
Функция HVI может быть доступна для вашего решения GravityZone с отдельным лицензионным ключом.

Перед развертыванием HVI на хостах убедитесь, что выполнены следующие требования:

Поддерживаемые виртуальные платформы

- Citrix XenServer 7. 1 Enterprise Edition или выше, с последними исправлениями

  Важно
  Для любого XenServer, начиная с версии 7.1, прекратившего жизненный срок, Bitdefender предоставляет поддержку HVI в течение двух дополнительных месяцев. По истечении этого периода мы рекомендуем обновить XenServer до версии, поддерживаемой Citrix. Для получения дополнительной информации смотрите Citrix Legacy Products Matrix и Citrix Product Matrix.

- Citrix Hypervisor 8. 0 Enterprise Edition или выше, с последними исправлениями

  Предупреждение
  Для Citrix Hypervisor 8.0 необходимо установить исправление XS80E004.

Поддерживаемые гостевые виртуальные машины

Виртуальные машины, которые вы хотите защитить с помощью [HIV], должны соответствовать следующим условиям:

1. Машины находятся в режиме виртуализации HVM, что означает, что они полностью виртуализированы.
2. Рабочие станции работают на поддерживаемой операционной системе:
   - **Настольные операционные системы Windows (32- и 64-битные)**

     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 (Restone 2)

Windows 10 Anniversary Update (Redstone 1)

Windows 10 November Update (Threshold 2)

Windows 10

Windows 8.1

Windows 8

Windows 7

- **Серверные операционные системы Windows (64-битные)**

  Windows Server 2019

  Windows Server 2016

  Windows Server 2012 / Windows Server 2012 R2

  Windows Server 2008 R2

- **Операционные системы Linux (64-битные)**

Дистрибутив	Версия	Версия ядра
Debian	10	4.19
Debian	9	4.9
Debian	8	3.16
Ubuntu	20. 04 LTS	5.4
Ubuntu	18.04 LTS	4.15
Ubuntu	16.04 LTS	4.4
Ubuntu	14.04 LTS	3.13.139 и позже
CentOS	8.2	4.18
CentOS	8	4.18
CentOS	7	3.10
Red Hat Enterprise Linux	8.2	4.18
Red Hat Enterprise Linux	8	4.18
Red Hat Enterprise Linux	7	3.10
Red Hat Enterprise Linux	6.8 / 6.9 / 6.10	2.36.32

Дистрибутив	Версия	Версия ядра
SUSE Linux Enterprise Server	15 SP1	4.12
SUSE Linux Enterprise Server	12 SP4	4.12
SUSE Linux Enterprise Server	12 SP3	4.4
SUSE Linux Enterprise Server	12 SP2	4.4
SUSE Linux Enterprise Server	12 SP1	3.12
Oracle Linux	Ранее чем 7.5	4. 1 (UEK / RHCK)
Oracle Linux	7.5 и позже	4.14 (UEK/RHCK)

Требования к оборудованию для GravityZone VA

- **Требуемый 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	
Сервер обновлений*	10	4	4	4	4	4	6	8	
Веб-консоль**		6	8	8	10	10	12	12	
Коммуникационный Сервер		6	8	8	10	10	16	20	
База данных ***		6	6	6	6	6	9	12	
Общее количество		**10**	**24**	**28**	**28**	**34**	**34**	**49**	**58**

  * 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.

- **Требуемое ОЗУ (ГБ)**

Компонент	Количество машин								
	250	500	1000	3000	5000	10000	25000	50000	
Сервер обновлений	18	2	2	2	2	2	3	3	
Веб-консоль*		8	10	10	10	10	12	16	
Коммуникационный Сервер		8	10	10	12	12	16	20	
База данных**		8	8	8	8	12	12	12	
Общее количество		**18**	**28**	**32**	**32**	**36**	**40**	**47**	**55**

* 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 место на жестком диске (ГБ)**

Сервер обновлений	150	190	80	80	80	80	80	80	80
Веб-консоль			80	80	80	80	80	80	80
Коммуникационный Сервер			80	80	80	80	80	80	80
База данных**			110	110	130	130	190	330	730
Общее количество	**150**	**190**	**350**	**350**	**370**	**370**	**430**	**570**	**970**

* 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.

Примечание
При установке роли сервера инцидентов для базы данных требуется дополнительное пространство размером не менее 30 ГБ. Дополнительное

количество пространства уже было добавлено в базу данных, расположенную в приведённой выше таблице.

Требования к оборудованию для хостов

- **Микроархитектура процессора:**
  - Любой процессор Intel® Sandy Bridge или более поздняя версия с поддержкой технологии виртуализации Intel®.
  - Расширения VT-x или VT-d должны быть включены в BIOS.
- **Свободное место на жестком диске:** Помимо пространства, необходимого для Security Server, HVI требует еще 9 МБ для дополнительного пакета на каждом узле.

Требования Security Server

Распределение ресурсов памяти и процессоров для Security Server зависит от количества и типа виртуальных машин, запущенных на хосте. В следующей таблице приведены рекомендуемые ресурсы, которые необходимо выделить:

Количество защищаемых виртуальных машин	ОЗУ	Процессоров
1-50 VMs	6 ГБ	4 CPUs
51-100 VMs	8 ГБ	6 CPUs
101-200 VMs	16 ГБ	8 CPUs

Свободное место на жестком диске: Вы должны обеспечить 8 ГБ дискового пространства на каждом узле для Security Server.

Для обеспечения оптимальной производительности в среде XenAPP выполните масштабирование ресурсов Security Server на основе конфигурации следующим образом:

Количество VDA XenApp	VDA		Security Server	
	Процессоров	ОЗУ (ГБ)	Процессоров	ОЗУ (ГБ)
1 VDA	4 / 8	12 / 24	2	4
2 VDA	4 / 8	12 / 24	2	8

Количество VDA XenApp	VDA		Security Server	
	Процессоров	ОЗУ (ГБ)	Процессоров	ОЗУ (ГБ)
4 VDA	8	24	2	16
8 VDA	4	12	4	16

Требования к гостевым виртуальным машинам

При обычной настройке окружения для оптимальной производительности и коэффициента консолидации виртуальной машины рекомендуется иметь следующую минимальную аппаратную конфигурацию для гостевых виртуальных машин:

- **vCPU:** 2 x vCPU
- **ОЗУ:** 3 ГБ

4.7. 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 (11.0)

- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

4.8. Защита хранилища

Поддерживаемые хранилища и файл-обменные решения:

- ICAP-совместимые системы сетевых хранилищ (NAS) и сети хранения данных (SAN) от Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle®, И другие
- Nutanix® Файлы 3.x до 3.6.2
- Citrix® ShareFile

4.9. Защита мобильных устройств

4.9.1. Поддерживаемые платформы

Security for Mobile поддерживает следующие типы мобильных устройств и операционных систем:

- Apple iPhones и iPad (iOS 8.1 и выше)
- Смартфоны и планшеты Google Android (4.2 и выше)

4.9.2. Требования к подключению

Мобильные устройства должны включить мобильную передачу данных или соединение Wi-Fi и иметь соединение с коммуникационным сервером.

4.9.3. Всплывающее уведомления

Security for Mobile использует push-уведомления, чтобы предупредить мобильных клиентов об обновлении политики и доступных задачах. Push-уведомления отправляются коммуникационным сервером через службы, предоставляемые производителем операционных систем:

- Служба Firebase Cloud Messaging (FCM) для Android устройств. Для работы FCM необходимо следующее:

  - Должен быть установлен Google Play Store.
  - Устройства под управлением Android 4.2 и выше.
  - Чтобы послать push-уведомление, a number of ports должен быть открыт.
- Apple Push Notifications service (APNs) для устройств iOS. Для получения более подробной информации, обратитесь к этой статье базы знаний Apple.

Вы можете проверить правильность работы push-уведомлений в разделе **Mobile Push Notifications Check** из меню **Configuration > Miscellaneous**.

Чтобы узнать больше о процессе управления мобильными устройствами в GravityZone, пожалуйста, смотрите эту статью базы знаний.

4.9.4. Управление сертификатами iOS

Чтобы настроить инфраструктуру для управления мобильными устройствами под управлением iOS, вы должны предоставить ряд сертификатов безопасности.

Для получения более подробной информации, обратитесь к «Сертификаты» (p. 106).

4.10. 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. Некоторые уровняи защиты требуют установки и настройки дополнительных компонентов.

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 для всех компонентов служб безопасности через веб-интерфейс Control Center.

Образ устройства GravityZone доступно в нескольких различных форматах, совместимых с основными платформами виртуализации. Вы можете получить лицензионный ключ сделав запрос на сайте Bitdefender Business Products Inquiry.

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
- Подробную информацию о vCenter Server, vShield Manager, 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 Веб-консоль Коммуникационный Сервер	Базовые (необходимые)	Хотя бы один экземпляр каждой роли. Устройство GravityZone может выполнять одну, несколько или все данные роли.
	Вспомогательные	Одно устройство на каждую роль
Security Server	Необязательные	Рекомендуется для малых сетей или для сетей с низкими ресурсами. В другом случае, установите отдельный от Control CenterSecurity Server, после успешной установки GravityZone.
Инциденты сервера	Необходимый	Может быть развернут как на универсальных, так и на распределенных устройствах. Используйте встроенное

Роль GravityZone	Тип роли	Установить
		программное обеспечение балансировщика при установке нескольких экземпляров.

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.

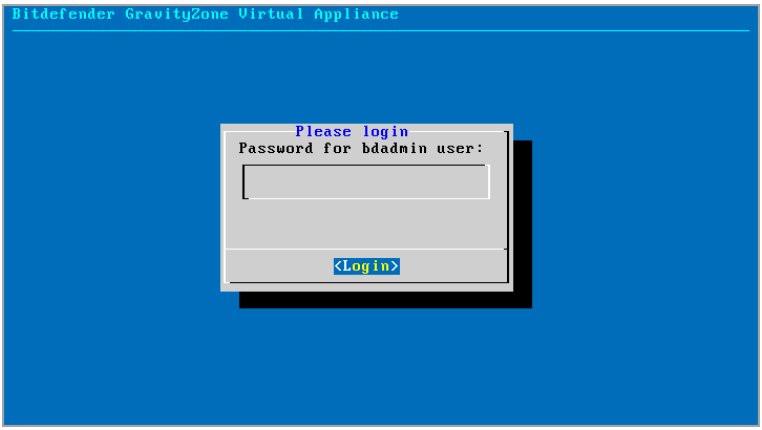
Вы можете установить несколько экземпляров ролей Базы данных, Веб-консоли и коммуникационного сервера. В данном случае, вам понадобится Набор Реплик (Replica Set) для Базы данных и Балансировщик нагрузки для Веб-консоли и коммуникационного сервера на устройствах GravityZone.

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`.

Интерфейс консоли устройства: введите новый пароль

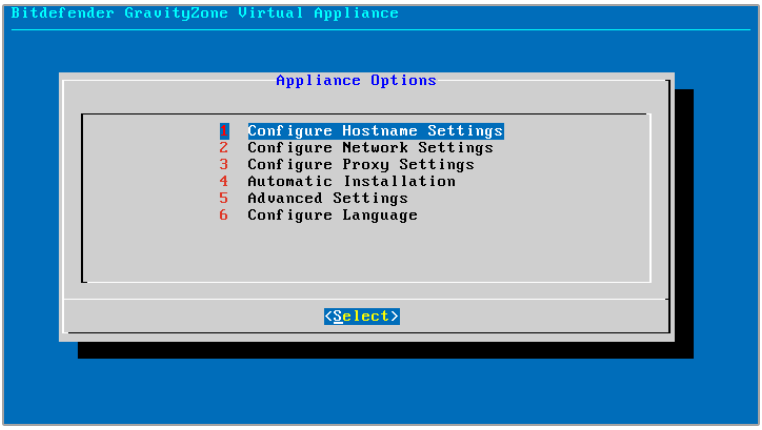
6. Войдите с помощью заданного пароля.



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» (p. 74).
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» (p. 113).

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.

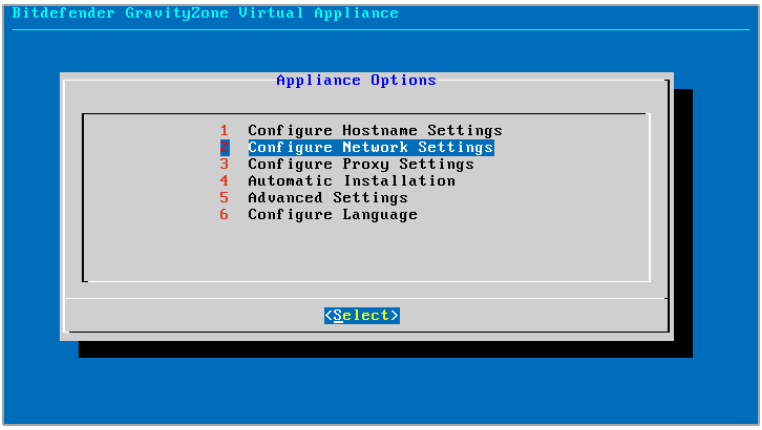
Чтобы задать настройки имени хоста:

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

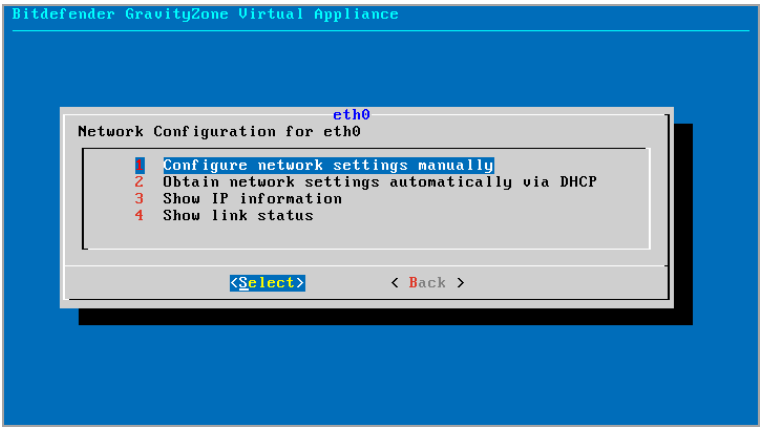
Вы можете настроить устройство на автоматическое получение сетевых параметров от сервера DHCP или выбрать настройки параметров сети вручную. Если вы выберите использование DHCP, вы должны настроить DHCP-сервер, чтобы зарезервировать для устройства определенный IP-адрес.

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.



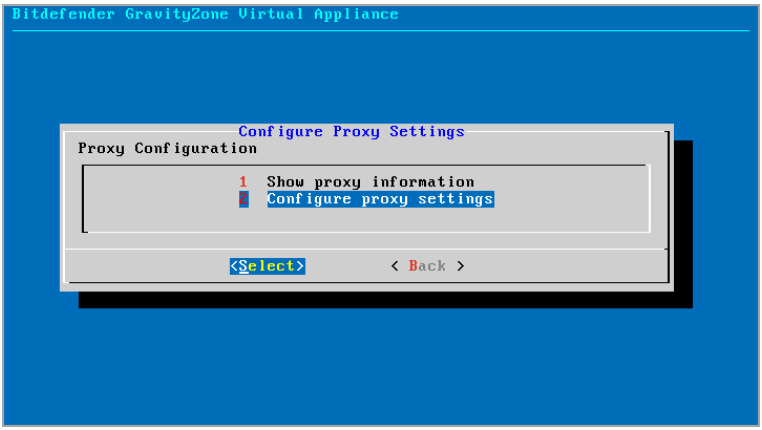
Интерфейс консоли устройства: настройка сети

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

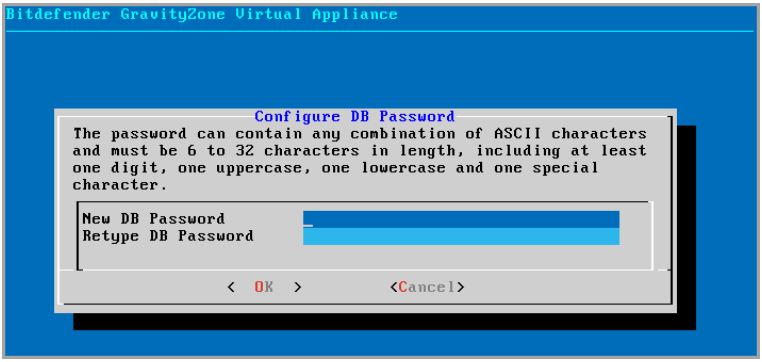
Во время автоматической установки все базовые роли устанавливаются на одно и тоже устройство. Для распределенной установки GravityZone, перейдите к «Дополнительные настройки» (p. 72).

Важно
Автоматическая установка также развернет Security Server, встроенный в устройство GravityZone. Для информации о Security Server, обратитесь к разделу «Архитектура GravityZone» (p. 12).
Опция автоматической установки доступна только при первоначальной настройке GravityZone.

Чтобы автоматически установить роли:

1. Из главного меню выберите **Automatic Installation**.
2. Прочитайте 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

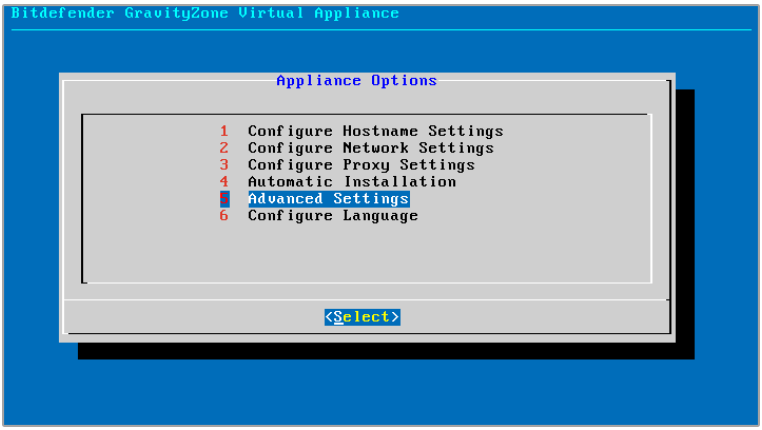
5. Дождитесь завершения процесса установки.

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» (p. 125) или «Подключитесь к существующей базе данных (Безопасный VPN-кластер)» (p. 126)

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).

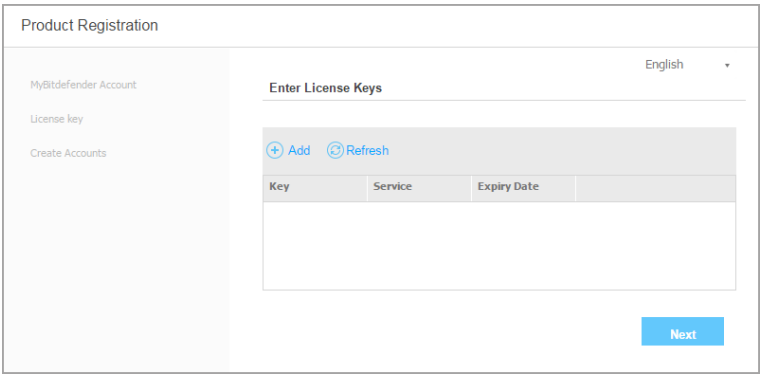
   c. Введите лицензионный ключ в поле **License key**. Для регистрации в офф-лайн режиме, вы должны также предоставить регистрационный код.

   d. Подождите пока лицензионный ключ проверяется. Нажмите **Add** для завершения.

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

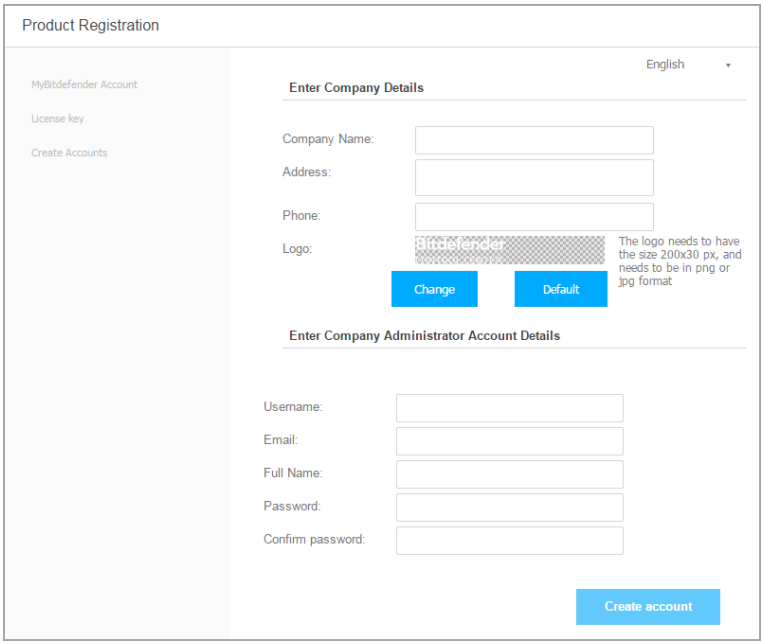
Примечание

- 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.



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.



Первоначальная настройка - Параметры вашей учетной записи

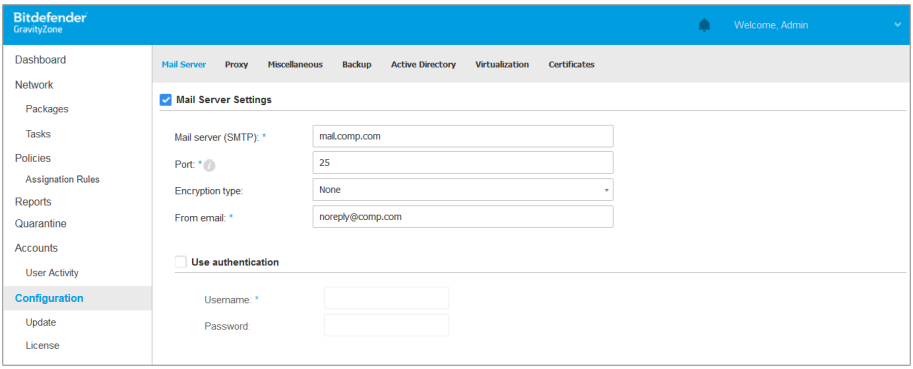
7. Нажмите **Create account**.

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.



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:

1. Перейдите к странице **Configuration**.
2. Выберите вкладку **Mail Server**.
3. 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:

- **Когда необходим недоступный образ Security Server.** В устройстве GravityZone по умолчанию не отображаются образы виртуальной машины Security Server. Если администратор попытается загрузить образ Security Server или выполнить задачу установки Security Server, действие будет прервано. Вы можете настроить автоматическое действие для такой ситуации, выбрав один из следующих вариантов:
  - **Загрузить образ автоматически**

- **Предупредите администратора и не выполняйте загрузку**

> **Примечание**
>
> Чтобы не создавать помех работе администратора, вы можете вручную загрузить необходимые пакеты Security Server со страницы **Обновление** в **Обновление продукта** . Для получения более подробной информации, обратитесь к «Загрузка обновлений продуктов» (p. 200).

- **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 функцию 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 событияGravityZone.

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 флажок **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":"companyname",
         "user_name":"username",
         "os":"osname",
         "browser_version":"browserversion",
         "browser_name":"browsername",
         "request_time":"DD MMM YYYY, hh:mm:ss +hh:ss",
         "device_ip":"computerip"
     }
     ```

     Для дополнительной информации, см. 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=companyname suser=username
     ```

```
BitdefenderGZLoginOS=osname
BitdefenderGZAuthenticationBrowserName=browsername
BitdefenderGZAuthenticationBrowserVersion=browserversion
dvchost=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:

1. Перейдите на страницу **Configuration** в Control Center и нажмите вкладку **Backup**.
2. Нажмите кнопку **Backup Now** в верхней части таблицы. Появится окно настроек.
3. 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 копии 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» (p. 91).

- 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 команду:

```
# /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» (p. 91).

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 дрступа, 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» (p. 93)
- «Интеграция с XenServer» (p. 96)
- «Интеграция с Nutanix Prism Element» (p. 97)
- «Интеграция с Amazon EC2» (p. 98)
- «Интеграция с Microsoft Azure» (p. 99)
- «Управление Интеграцией с Платформами» (p. 100)

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 виртуализаци > 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. 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. Выберите платформу VMware, установленную в вашей среде, и соответствующим образом настройте параметры:
   - **Ограничения**. Выберите данную опцию для NSX-T, или же если отсутствует какая-либо определенная платформа VMware и нажмите **Сохранить**. Принятие самозаверяющего сертификата безопасности требуется для интеграции.

     Для настройки интеграции NSX-T Manager и применения защиты на ваши Виртуальные Машины через политику GravityZone Guest Introspection, обратитесь к данной статье Базы знаний.
   - **vShield**. Укажите сведения о системе vShield Manager, интегрированной с сервером vCenter.
     - Имя хоста или IP-адрес системы vShield Manager
     - Порт vShield Manager (по умолчанию `443`)
   - **NSX-V**. Укажите сведения о NSX Manager, интегрированном с сервером vCenter.

Примечание
Для перехода с VMWare vShield на NSX смотрите эту статью базы знаний.

- Имя хоста или IP-адрес диспетчера NSX
- Порт диспетчера NSX (по умолчанию `443`)
- Имя пользователя и пароль, используемые для аутентификации в NSX Manager.

  Эти учетные данные будут сохранены в защищенном объекте, а не в диспетчере учетных данных.
- Установите флажок **При обнаружении вируса**, чтобы использовать теги безопасности NSX по умолчанию при обнаружении вредоносного ПО на виртуальной машине.

  Машина может быть помечена тремя различными тегами безопасности в зависимости от уровня угрозы:

  - `ANTI_VIRUS.VirusFound.threat=low`, применяется к машине, когда Bitdefender находит вредоносное ПО с низким уровнем риска, которое он может удалить.
  - `ANTI_VIRUS.VirusFound.threat=medium`, применяется к машине, если Bitdefender не может удалить инфицированный файл, но вместо этого пытается вылечить его.
  - `ANTI_VIRUS.VirusFound.threat=high`, применяется к машине, если Bitdefender не может ни удалить, ни вылечить зараженные файлы, но блокирует доступ к ним.

  При обнаружении угроз с разными уровнями риска на одном компьютере все связанные теги будут применены. Например, машина, на которой обнаружены вредоносные программы с высоким и низким уровнем риска, будет иметь оба тега безопасности.

  Примечание
  Вы можете найти теги безопасности в разделе VMware vSphere, **Сетевое оборудование & Безопасность > Управление NSX >** `Менеджер NSX` **> Управление > Теги безопасности**.

  Хотя вы можете создать столько тэгов, сколько захотите, только три из них будут работать с Bitdefender..

6. **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.
7. Нажмите **Сохранить**. Вам необходимо будет принять сертификаты безопасности для vCenter Server и NSX Manager. Эти сертификаты обеспечивают безопасную связь между компонентами GravityZone и VMware, устраняя 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.
8. Установите флажки для принятия использования сертификатов.
9. Нажмите **Сохранить**. Вы сможете просмотреть vCenter Server в списке активных интеграций.
10. Если вы используете платформу NSX-V:
    a. Перейдите на вкладку **Обновление > Компоненты** .
    b. Загрузите и опубликуйте пакет **Security Server (VMware with NSX)** . Для получения дополнительной информации о том, как обновить компоненты GravityZone, обратитесь к «Обновление GravityZone» (p. 196).
    c. Перейдите в раздел **Конфигурация > Провайдеры для виртуализации**.
    d. В столбце **Action**нажмите конпку **Регистрация** , соответствующую vCenter, интегрированному с NSX, для регистрации службы Bitdefender в VMware NSX Manager.

Предупреждение
Когда сертификат безопасности истечет, и vCenter попытается синхронизироваться, всплывающее окно предложит вам обновить его. Войдите в окно конфигурации интеграции с vCenter Server, нажмите **Сохранить** , примите новые сертификаты и снова нажмите **Сохранить** .

После регистрации Bitdefender добавляет в консоль VMware vSphere:
- Услуги Bitdefender

- Управление услугами Bitdefender
- Три новых профиля службы по умолчанию для разрешенных, нормальных и агрессивных режимов сканирования.

> **Примечание**
> Эти профили служб можно просмотреть также на странице **Политики** в Control Center. Нажмите кнопку **Столбцы** в верхней правой части правой панели, чтобы просмотреть дополнительную информацию.

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 виртуализаци**.
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. Нажмите **Сохранить**. Вы сможете просмотреть vCenter Server 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 виртуализаци**.
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, устраняя 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 флажки 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 виртуализаци**.
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 виртуализаци**.
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. 93)
   - «Интеграция с XenServer» (p. 96)
   - «Интеграция с Nutanix Prism Element» (p. 97)
   - «Интеграция с Amazon EC2» (p. 98)
   - «Интеграция с Microsoft Azure» (p. 99)
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**.

Для удаления интеграции с vShield, XenServer, Nutanix Prism Element, Amazon EC2 или Microsoft Azure:

1. В Control Center, перейдите в раздел **Настройка > Виртуализация**.
2. Нажмите кнопку ⊗ **Удалить** в **Действие** , соответствующую удаляемой интеграции.
3. Нажмите **Да**, чтобы подтвердить выбор.

Чтобы удалить интеграцию NSX:

1. Войдите в консоль VMware vSphere и удалите все политики Bitdefender и Security Server.
2. В Control Center, перейдите в раздел **Настройка > Виртуализация**.
3. В столбце **Действие**, соответствующем удаляемой интеграции, нажмите ⊗ **Отменить регистрацию** , а затем ⊗ **Удалить** .
4. Нажмите **Да**, чтобы подтвердить выбор.

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 чем 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 соединятся 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 **ОК** 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 флажка 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

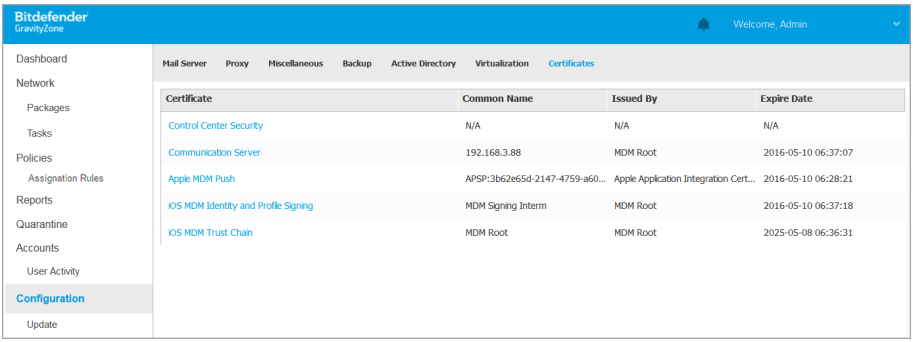
Удаление лицензионного ключа NTSA из страницы **Конфигурация > Лицензия** также удалит интеграцию NTSA.

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

Для правильного и безопасного развертывания вашего GravityZone, необходимо создать и добавить ряд сертификатов безопасности в Control Center.



Страница сертификатов

Control Center поддерживает следующие форматы сертификатов:

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

Примечание

Следующие сертификаты требуются исключительно для управления безопасностью на устройствах Apple iOS:

- Сертификат коммуникационного сервера
- Сертификат сервера инцидентов
- Apple MDM Push-Сертификат
- Сертификат подлинности и профиля подписания iOS MDM
- Цепочка доверенных сертификатов iOS MDM

Если вы не планируете разворачивать управление мобильными устройствами iOS, вам не нужно предоставлять эти сертификаты.

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**.

Конечные точки - Сертификат коммуникационного сервера Security Server

Этот сертификат гарантирует безопасную связь между агентами безопасности и назначенным им Security Server (Multi-Platform).

Во время его развертывания, Security Server генерирует по умолчанию самоподписанный сертификат. Вы можете заменить встроенный сертификат, добавив другой на ваш выбор, в Control Center.

Для добавления или замены коммуникационного сертификата между конечной точкой и Security Server:

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**. Может появится предупреждающее сообщение если сертификат самоподписанный или истекший. Если сертификат истек, пожалуйста обновите его.
8. Нажмите **Yes** для продолжения выгрузки сертификата. Незамедлительно после завершения выгрузки, Control Center вышлет сертификат безопасности Security Servers.

В случае необходимости, вы можете вернуться к исходным встроенным сертификатам каждого Security Server следующим образом:

1. Нажмите на название сертификата в разделе **Certificates**.
2. Выберите в качестве типа сертификатов **No certificate (use default)**.
3. Нажмите **Сохранить**.

Сертификат коммуникационного сервера

Сертификат коммуникационного сервера используется для защиты канала связи между коммуникационным сервером и мобильными устройствами iOS.

Требования:

- Этот сертификат SSL может быть подписан либо в вашей компании, либо с помощью внешнего центра сертификации.

  Предупреждение
  Сертификат может быть признан недействительным, если он не был выдан общедоступным/доверенным центром сертификации (например, самозаверяющие сертификаты).

- Публичное имя сертификата должно в точности совпадать с именем или IP-адресом вашего домена, используемым мобильными клиентами для подключения к коммуникационному серверу. Это настраивается как внешние MDM-адреса в конфигурационном интерфейсе консоли GravityZone.

- Мобильные клиенты должны доверять этому сертификату. Для этих целей вы должны добавить iOS MDM Trust Chain.

Чтобы добавить или заменить сертификаты коммуникационного сервера:

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**.

Сертификат сервера инцидентов

Добавить или заменить лицензию сервера инцидентов:

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**.

Apple MDM Push-Сертификат

Устройства Apple требуют наличие MDM Push-сертификата для обеспечения безопасной связи между коммуникационным сервером и службой Apple Push Notifications service (APNs), при отправке push-уведомлений. Push-уведомления используются, чтобы подсказать устройствам о необходимости подключения к коммуникационному серверу, когда доступны новые задачи или изменения в политике.

Apple выпускает сертификат непосредственно для вашей компании, но требуется ваш запрос на подписание сертификата (Certificate Signing Request - CSR), для его подписания Bitdefender. Центр управления имеет специальный мастер, который поможет вам облегчить процедуру получения сертификата Apple MDM Push certificate.

Важно

- Вам понадобится Apple ID для получения и управления сертификатом. Если у вас нет Apple ID, вы можете создать его странице My Apple ID. Используйте общий адрес электронной почты компании, а не адрес электронной почты сотрудника, чтобы зарегистрировать Apple ID, так как он понадобится позже, чтобы обновить сертификат.
- Сайт Apple не работает должным образом в Internet Explorer. Мы рекомендуем использовать последние версии Safari или Chrome.
- Apple MDM Push certificate действителен только один год. Когда сертификат истечет, вы должны обновить его и импортировать обновленный сертификат в Control Center. Если вы допустили просрочку сертификата, вам необходимо создать новый и реактивировать все ваши устройства.

Добавление нового сертификата Apple MDM Push Certificate

Чтобы получить Apple MDM Push certificate и импортировать его в Control Center:

1. Перейдите на страницу **Configuration** и нажмите вкладку **Certificates**.
2. Нажмите на имя сертификата и следуйте подсказкам мастера, как описано ниже:

   Шаг 1 - Получение запроса на подпись сертификата (CSR), подписанного Bitdefender

   Выберите подходящие опции:

   - **I need to generate a certificate signing request signed by Bitdefender** (рекомендуется)
     a. Введите название компании, ваше полное имя и адрес электронной почты в соответствующих полях.
     b. Нажмите **Generate** для загрузки CSR-файла, подписанного Bitdefender.
   - **У меня уже есть запрос на подпись сертификата (CSR), и мне нужно получить его подписанным Bitdefender**

a. Загрузите файл CSR и соответствующий личный ключ, нажав кнопку **Add** рядом с обоими полями.

   Коммуникационному серверу необходим личный ключ для аутентификации с серверами APNs.
b. Укажите пароль, защищающий личный ключ, если необходимо.
c. Нажмите кнопку **Sign** для загрузки CSR-файла, подписанного Bitdefender.

Шаг 2 - Запрос push-сертификата от Apple.

a. Нажмите ссылку **Apple Push Certificates Portal** и войдите в него, используя Apple ID и пароль.
b. Нажмите кнопку **Create a Certificate** и примите условия использования.
c. Нажмите **Choose file**, выберите CSR-файл и затем нажмите **Upload**.

   Примечание
   Вы можете увидеть кнопку **Choose file** под другим именем, таким как **Choose** или **Browse**, в зависимости от используемого браузера.

d. На странице подтверждения нажмите кнопку **Download**, чтобы получить ваш MDM Push certificate.
e. Вернитесь обратно к мастеру Control Center.

Шаг 3 - Импорт Apple push-сертификата

Нажмите кнопку **Add Certificate**, чтобы загрузить файл сертификата с вашего компьютера.

Вы можете проверить сведения о сертификате в поле ниже.

3. Нажмите **Сохранить**.

Возобновление сертификата Apple MDM Push Certificate

Чтобы продлить Apple MDM push-сертификат и обновить его в Control Center:

1. Перейдите на страницу **Configuration** и нажмите вкладку **Certificates**.
2. Нажмите на название сертификата, чтобы открыть мастер импорта.
3. Получение запроса на подпись сертификата (CSR), подписанного Bitdefender. Процедура такая же, как и для получения нового сертификата.
4. Нажмите на ссылку **Apple Push Certificates Portal** и зайдите на него с тем же Apple ID, используемым при создании сертификата.
5. Найдите MDM Push certificate for Bitdefender и нажмите соответствующую клавишу **Renew**.

6. Нажмите **Choose file**, выберите CSR-файл и затем нажмите **Upload**.
7. Нажмите **Download**, чтобы сохранить сертификат на вашем компьютере.
8. Вернитесь в Control Center и импортируйте новый Apple push-сертификат.
9. Нажмите **Сохранить**.

Сертификат подлинности и профиля подписания iOS MDM

Сертификат подлинности и профиля подписания iOS MDM используется коммуникационным сервером, чтобы подписывать сертификаты, удостоверяющие подлинность и профили конфигурации, отправляемые на мобильные устройства.

Требования:

- Это должен быть промежуточный сертификат или сертификат конечной точки, подписанный либо вашей компанией либо внешним центром сертификации.
- Мобильные клиенты должны доверять этому сертификату. Для этих целей вы должны добавить iOS MDM Trust Chain.

Чтобы добавить или заменить Сертификат подлинности и профиля подписания iOS MDM:

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**.

Цепочка доверенных сертификатов iOS MDM

Цепочка доверенных сертификатов iOS MDM необходима мобильным устройствам чтобы они доверяли Сертификату коммуникационного сервера и Сертификату подлинности и профиля подписания iOS MDM.

Коммуникационный сервер отправляет этот сертификат на мобильные устройства во время активации.

Цепочка доверенных сертификатов iOS MDM должна содержать все промежуточные сертификаты и до корневого сертификаты вашей компании или промежуточные сертификаты подписанные внешним центром сертификации.

Чтобы добавить или заменить цепочку доверенных сертификатов iOS MDM:

1. Перейдите на страницу **Configuration** и нажмите вкладку **Certificates**.
2. Нажмите на имя сертификата.
3. Нажмите кнопку **Add** рядом с полем **Certificate** и загрузите сертификат.
4. 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-кластер
- Подключитесь к существующей базе данных
- Подключитесь к существующей базе данных (Безопасный VPN-кластер)
- Проверьте Безопасный VPN-кластер

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» (p. 121).

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 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.

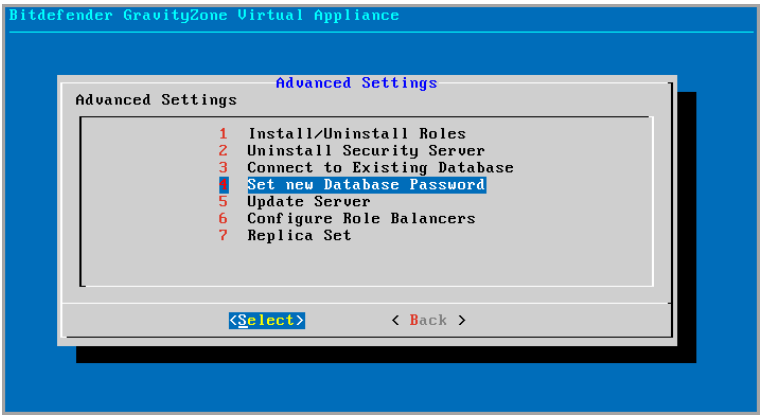
Чтобы установить Security Server из интерфейса устройства:

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.

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» (p. 117).
2. Настройте другие машины для подключения к первому экземпляру базы данных. Для получения более подробной информации, обратитесь к «Подключитесь к существующей базе данных» (p. 125).
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-кластер

Роли GravityZone имеют несколько внутренних служб, которые взаимодействуют только между собой. Для более безопасной среды вы можете изолировать эти сервисы, создав для них VPN-кластер. 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)» (p. 126).

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» (p. 124)
- «Подключитесь к существующей базе данных (Безопасный VPN-кластер)» (p. 126)

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

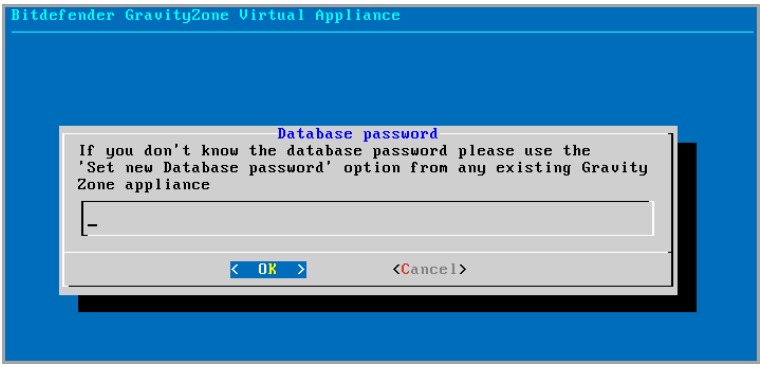
1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Из главного меню выберите **Advanced Settings**.
3. Выберите **Connect to Existing Database**.

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-кластер)

Используйте эту опцию, когда вам нужно расширить развертывание GravityZone с помощью большего количества устройств, и Безопасный VPN-кластер 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» (p. 124).

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.

Примечание
Control Center предоставляется бесплатно с любой службой безопасности GravityZone.

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

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

Клавишами GravityZone можно управлять со страницы **Настройки конфигурации > Лицензия** 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 сведения о текущей лицензии, перейдите на страницу **Конфигурация > Лицензия**

5.2.1. 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.

5.2.2. 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**.

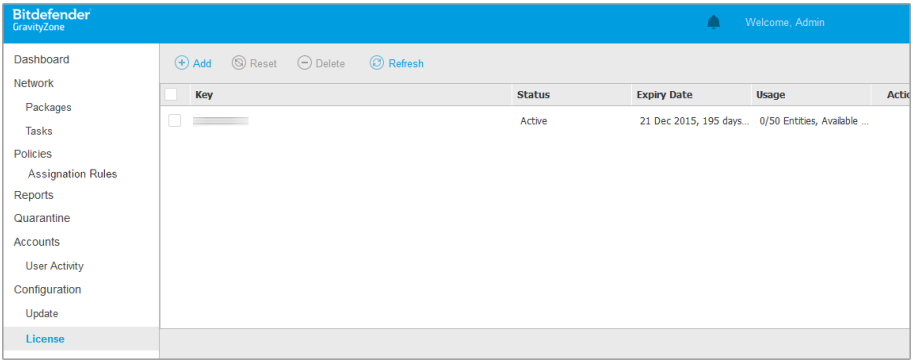
5. Нажмите **Добавить**. Лицензионный ключ будет добавлен на страницу **License**, где вы можете проверить подробности лицензии.
6. Нажмите **Сохранить**, чтобы сохранить изменения. Control Center перезагрузится и вы должны будете войти еще раз, чтобы просмотреть изменения.

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**.



Страница лицензии

3. В таблице можно просмотреть подробные сведения о существующих лицензионных ключах.

- 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 кнобку **Reset** в верхней части таблицы.

5.2.5. Удаление лицензионных ключей

Вы можете удалить удаленные или устаревшие ключи лицензии со страницы **Лицензия**.

> **Предупреждение**
> Удаление лицензионного ключа приведет к удалению соответствующей службы безопасности из Control Center. Вы не сможете устанавливать и управлять защитой, предоставляемой этой службой, на конечных точках вашей сети. Тем не менее, конечные точки остаются защищенными до тех пор, пока действительный лицензионный ключ действителен.
> Если вы введете новый действующий лицензионный ключ, который включает ранее удаленный сервис, он вернет все функции этой службы в Control Center.

Чтобы удалить лицензионный ключ:

1. Войдите в Control Center, используя учетную запись администратора компании.
2. Перейдите на страницу **Configuration > License**.
3. Выберите лицензионный ключ, который хотите удалить, и нажмите **Удалить** На верхней стороне стола.

5.3. Установка защиты для конечных точек

В зависимости от конфигурации компьютеров и сетевой среды вы можете выбрать установку только агентов безопасности или также использовать Security Server. В последнем случае вам нужно сначала установить Security Server, а затем агентов безопасности.

Рекомендуется использовать Security Server в виртуализированных средах, таких как Nutanix, VMware или Citrix Xen, или если у компьютеров мало аппаратных ресурсов.

Важно
Только Bitdefender Endpoint Security Tools и Bitdefender Tools поддерживает подключение к Security Server. Для получения более подробной информации, обратитесь к «Архитектура GravityZone» (p. 12).

5.3.1. Установка Security Server

Security Server является специализированной виртуальной машиной, которая дедуплицирует и централизует большую часть функций защиты клиентов от вредоносных программ, действуя в качестве сервера сканирования.

Развертывание Security Server зависит от среды, в которой оно установлено. Процедуры установки описаны ниже:

- Security Server для VMware NSX
- Security Server Multi-Platform или для VMware vShield
- Security Server для Amazon EC2
- Security Server для Microsoft Azure

Установка Security Server для VMware NSX

В средах VMware с установленным NSX необходимо развернуть службу Bitdefender в каждом защищаемом кластере. Специально созданное устройство будет автоматически развертываться на всех узлах кластера. Все виртуальные машины на узле автоматически подключаются через гостевую интроспекцию к экземпляру Security Server, установленному на этом хосте.

Развертывание Security Server должно выполняться исключительно из vSphere Web Client.

Чтобы установить службу Bitdefender:

1. Войдите в веб-клиент vSphere.
2. Перейдите на страницу **Сеть и безопасность> Установка** и нажмите вкладку **Развертывания служб** .
3. Нажмите кнопку **Новое развертывание службы** (значок знака «плюс»). Откроется окно конфигурации.
4. Выберите **Интроспекция гостей** и нажмите **Далее** .
5. Выберите центр данных и кластеры для развертывания службы, а затем нажмите **Далее** .
6. Выберите сеть хранения и управления, нажмите **Далее** , а затем **Готово** .
7. Повторите шаги с 3 по 6, на этот раз выбрав службу **Bitdefender**

   Прежде чем продолжить установку, убедитесь, что у вас есть сетевое соединение между выбранной сетью и Control Center GravityZone.

   После установки службы Bitdefender она автоматически развернет Security Server на всех хостах ESXi в выбранных кластерах.

Предупреждение
Для правильной работы служб очень важно, чтобы вы установили их в этом порядке, сначала в Самоанализ Компьютеров, а затем в Bitdefender, а не в обоих одновременно.

Примечание
Дополнительную информацию о добавлении партнерских сервисов в NSX см. В VMware NSX Центр Документации .
Если для хранения и управления сетью вы выбрали **, указанный на хосте** , убедитесь, что на виртуальных машинах установлена хост-служба для автоматического анализа гостей и служб Bitdefender.

Security Server имеет конкретные требования, которые зависят от количества виртуальных машин, которые он должен защищать. Чтобы настроить аппаратную конфигурацию по умолчанию для Security Server:

1. Войдите в VMware vSphere Web Client.
2. Перейдите на страницу **Хосты и кластеры** .

3. Выберите кластер, на котором установлен Security Server, а затем выберите вкладку **Связанные объекты > Виртуальные машины** .
4. Отключите устройство **Bitdefender** .
5. Щелкните правой кнопкой мыши имя устройства и выберите **Изменить параметры ...** в контекстном меню.
6. На вкладке **Виртуальное оборудование** настройте значения CPU и RAM в соответствии с вашими потребностями, а затем нажмите **OK** , чтобы сохранить изменения.
7. Включите устройство.

Примечание
Для перехода с VMWare vShield на NSX смотрите эту статью базы знаний.

Установка Security Server Multi-Platform или для VMware vShield

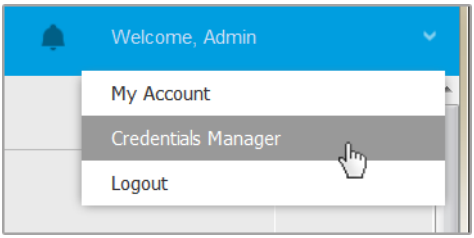
1. Подключитесь к платформе виртуализации
2. Установка Security Server на хостах

Подключение к платформе виртуализации

Для доступа к виртуальной инфраструктурой, интегрированной с Control Center, вы должны предоставить ваши учетные данные пользователя для каждой доступной виртуализированной серверной системы. Control Center использует ваши учетные данные для подключения к виртуальной инфраструктуре, отображая только те ресурсы, к которым у вас есть доступ (задается в vCenter Server).

Чтобы указать учетные данные для подключения к системам виртуализации сервера:

1. Нажмите на ваше имя пользователя в правом верхнем углу страницы и выберите **Credentials Manager**.



The Network > Packages menu

2. Перейдите на вкладку **Virtual Environment**.
3. Укажите необходимые данные аутентификации.
   a. Выберите сервер из соответствующего меню.

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

   b. Введите имя пользователя, пароль и подходящее описание.
   c. Нажмите кнопку ⊕ **Добавить**. Новый набор учетных данных добавляется в таблицу.

Примечание
Если вы не указали свои учетные данные, вам будет необходимо ввести их, когда вы попытаетесь просмотреть перечень элементов любой системы vCenter Server. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дельнейшем.

Установка Security Server на хостах

Вы должны установить Security Server на хостах следующим образом:

- В среде VMware с vShield Endpoint, необходимо установить специализированное устройство на каждом защищаемом хосте. Все виртуальные машины на хосте автоматически подключаются через vShield Endpoint к экземпляру Security Server, установленному на хосте.

- В окружении Citrix с помощью задачи удаленной установки вы должны установить Security Server на каждом хосте, который хотите защитить с помощью HVI,
- В среде Nutanix Prism Element вам необходимо установить Сервер безопасности на каждый хост с помощью задачи установки.
- Во всех других средах, необходимо установить Security Server на одном или нескольких хостах, чтобы обеспечить защиту всех виртуальных машин. Вы должны учитывать количество защищаемых виртуальных машин и ресурсы, доступные Security Server на хостах, такие как пропускная способность между Security Server и защищаемыми виртуальными машинами. Агент безопасности, установленный на виртуальных машинах подключается к Security Server по протоколу TCP/IP, используя настройки, заданные при установке или с помощью политики.

Если Control Center интегрирована с vCenter Server, XenServer and Nutanix Prism Element, вы сможете автоматически установить Security Server на хостах из Control Center. Вы также можете скачать пакеты Security Server для автономной установки из Control Center.

Примечание
Для сред VMware с vShield Endpoint, вы можете развернуть Security Server на хостах исключительно с помощью задач установки.

Локальная установка

Во всех виртуализированных средах, которые не интегрированы с Control Center, необходимо установить Security Server на хостах вручную, с помощью установочного пакета. Пакет Security Server доступен для загрузки из Control Center в различных форматах, совместимых с основными платформами виртуализации.

Скачать установочные пакеты Security Server

Чтобы скачать установочные пакеты Security Server:

1. Перейдите на страницу **Network > Packages**.
2. Выбор пакета Security Server по умолчанию.
3. Нажмите кнопку **Download** в верхней части таблицы и выберите тип пакета из меню.

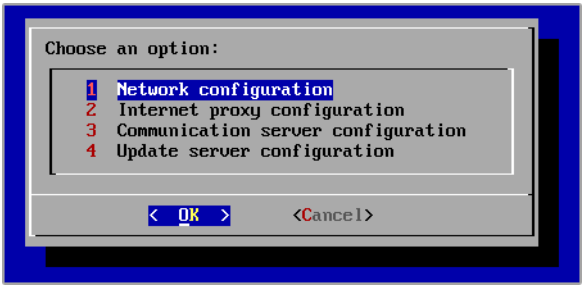
4. Сохранить выбранный пакет в нужное место.

Развертывание установочных пакетов Security Server

Если у вас есть установочный пакет, разверните его на хосте, используя свой предпочтительный инструмент развертывания виртуальной машины.

После развертывания настройте Security Server следующим образом:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client). Кроме того, вы можете подключиться к устройству с помощью SSH.
2. Войдите, используя учетные данные по умолчанию.
   - Имя пользователя: `root`
   - Пароль: `sve`
3. Запустите команду `sva-setup`. Вы получите доступ к интерфейсу конфигурации устройства.



Конфигурационный интерфейс Security Server (главное меню)

Для навигации по меню и опциям, используйте `Tab` и клавиши со стрелками. Для выбора конкретного параметра нажмите `Enter`.

4. Настройка сетевых параметров.

   Security Server использует протокол TCP/IP для связи с другими компонентами GravityZone. Вы можете настроить устройство на автоматическое получение сетевых параметров от сервера DHCP или выбрать настройки параметров сети вручную, как описано здесь:

   a. Из главного меню, выберите **Network configuration**.

b. Выберите сетевой интерфейс.

c. Выберите режим конфигурации IP:

- **DHCP**, если вы хотите, чтобы Security Server автоматически получил параметры сети от DHCP-сервера.
- **Static**, если DHCP-сервер отсутствует или резервирование IP-адреса для устройства было сделано на DHCP-сервере. В этом случае, вы должны вручную настроить сетевые параметры.

  i. Введите имя хоста, IP-адрес, маску сети, шлюз и DNS-серверы в соответствующих полях.

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

Примечание
Если вы подключены к устройству с помощью клиента SSH, изменение сетевых настроек будет немедленно прекращать сеанс.

5. Настройка параметров прокси-сервера.

   Если в сети используется прокси-сервер, вы должны указать его параметры, чтобы Security Server мог общаться с GravityZone Control Center.

   Примечание
   Поддерживается только прокси с базовой аутентификацией.

   a. Выберите из меню **Internet proxy configuration**.

   b. Введите имя хоста, имя пользователя, пароль и домен в соответствующих полях.

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

6. Настройка адреса коммуникационного сервера.

   a. Выберите из меню **Конфигурация коммуникационного сервера**.

   b. Введите адрес коммуникационного сервера, включая номер порта 8443, используя следующий формат:

   ```
   https://Communication-Server-IP:8443
   ```

   Кроме того, вы можете использовать имя хоста коммуникационного сервера вместо IP-адреса.

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

Удаленная установка

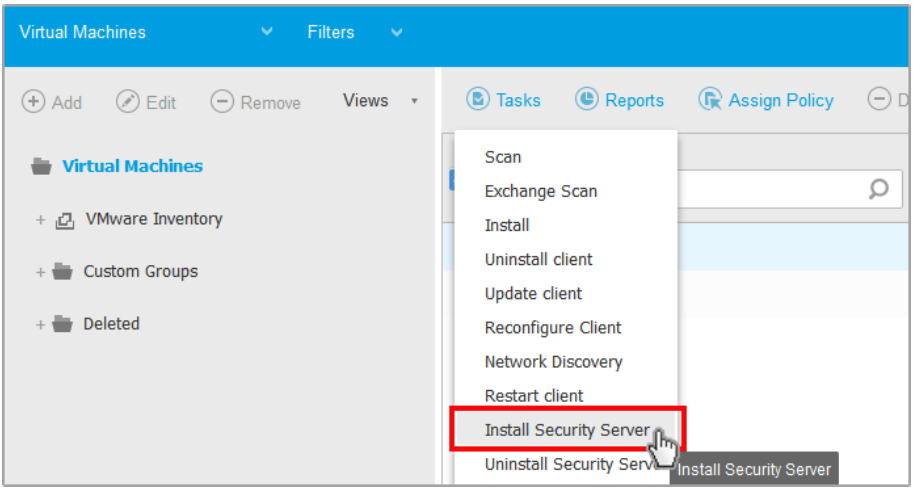
Control Center позволяет удаленно устанавливать Security Server на видимых хостах с помощью задач установки.

Чтобы установить Security Server удаленно на одном или нескольких хостах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Virtual Machines** из меню выбора просмотров.
3. Просмотрите инвентарь VMware, Citrix or Nutanix и установите флажки на соответствующих хостах или контейнерах (Nutanix Prism, vCenter Server, XenServer или дата-центр). Для быстрого выбора, вы можете сразу выбрать корневой контейнер (Nutanix, VMware или Citrix). Вы сможете выбрать хосты самостоятельно в мастере установки.

   Примечание
   Вы не можете выбрать хосты из разных папок.

4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **УстановитьSecurity Server** в меню. Отобразится окно установки **Security Server Установка**.



Установка Security Server из меню задач

5. Выберите хосты, на которых вы хотите установить экземпляр Security Server.
6. Выберите параметры конфигурации, которые вы хотите использовать.

   Важно
   Использование общих настроек, при развертывании нескольких экземпляров Security Server одновременно, требует: одно общее хранилище для хостов; наличие собственных IP-адресов, назначенных с помощью DHCP-сервера; находится в одной сети.

   При выборе разных настроек для каждого Security Server, вы сможете определить параметры, которые необходимы для каждого хоста в следующем шаге мастера установки. Описанные далее шаги применяются в случае, когда используется опция **Configure each Security Server**.
7. Нажмите **Далее**.
8. Введите подходящее имя для Security Server.
9. Для среды VMware, выберите контейнер, в который вы хотите включить Security Server из меню **Установить контейнер**.
10. Выберите расположение хранилища.

11. Выберите тип диска (provisioning type). Рекомендуется развернуть устройство на "толстых" дисках (thick provisioning).

    Важно
    Если вы используете "тонкие" диски (thin provisioning) и дисковое пространство в хранилище данных закончится, Security Server заморозится и, следовательно, хосты останутся незащищенными.

12. Настройте распределение памяти и ресурсов процессора, основанное на коэффициенте консолидации виртуальной машины на хосте. Выберите **Низкий**, **Средний** или **Высокий**, чтобы загрузить рекомендуемые параметры распределения ресурсов или **настройка вручную**, чтобы настроить распределение ресурсов вручную.
13. Задайте пароль администратора для консоли Security Server. Установка пароля администратора перезаписывает пароль по умолчанию ("sve").
14. Установите часовой пояс устройства.
15. Выберите тип конфигурации сети для сети Bitdefender. IP-адрес Security Server не должен изменяться со временем, так как он используется агентами Linux для общения.

    Если вы выберите DHCP, убедитесь, что настроили DHCP-сервер на резервирование IP-адреса для устройства.

    Если вы выберите статический, вы должны ввести информацию о IP-адресе, маске подсети, шлюзе и DNS.
16. Выберите сеть vShield и введите учетные данные vShield. По умолчанию метка для vShield сети `vmservice-vshield-pg`.
17. Нажмите **Сохранить**.

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

Примечание
Чтобы перейти с VMWare vShield на NSX, смотрите эту статью базы знаний.

Важно
Установка Security Server на Nutanix через удаленную задачу может окончиться неудачей, когда кластер Prism Element зарегистрирован на Prism Central или по другой причине. В данной ситуации, рекомендуется произвести ручную

установку Security Server. За подробной информацией, обратитесь к этой статье Базы знаний.

Установка Security Server на Amazon EC2

Вы можете использовать Security Server для защиты вашей Amazon EC2 среды как описано ниже:

- Настройте Security Server, установленный в вашей локальной сети для коммуникации с Amazon EC2. Таким образом, вы сможете использовать ресурсы локальных устройств, как физических, так и виртуальных, для защиты инвентаря Amazon EC2.
- Установите один или несколько экземпляров Security Server в вашей среде Amazon EC2, в соответствии с вашими потребностями. В данном случае, следуйте процедуре, описанной в данной статье Базы знаний.

Важно

- Для коммуникации между вашими машинами EC2 и Серверами безопасности, установленными в вашей сети Amazon EC2, вам необходимо настроить Amazon VPC (Virtual Private Cloud) и подключения Amazon. Для получения дополнительной информации обратитесь к документации Amazon VPC.
- Рекомендуется устанавливать Security Server в том же регионе Amazon EC2, в котором находятся экземпляры для защиты.

Режим сканирования по умолчанию для экземпляров EC2 - «Локальное сканирование» (механизмы защиты хранятся в установленном агенте безопасности, а сканирование выполняется локально на компьютере). Если вы хотите сканировать ваши экземпляры EC2 с помощью Security Server, вам необходимо соответствующим образом настроить пакет установки агента безопасности и применяемую политику.

Установка Security Server для Microsoft Azure

Вы можете использовать Security Server для защиты ваших виртуальных машин Microsoft Azure как описано ниже:

- Настройте Security Server, установленный в вашей локальной сети для коммуникации с виртуальными машинами Microsoft Azure. Таким образом,

вы сможете использовать ресурсы локальных устройств, как физических, так и виртуальных, для защиты инвентаря Microsoft Azure.

- Установите один или несколько экземпляров Security Server в вашей среде Microsoft Azure, в соответствии с вашими потребностями. В данном случае, следуйте процедуре, описанной в данной статье Базы знаний.

  Важно

  – Для работы коммуникации между виртуальными машинами Microsoft Azure и Серверами безопасности, установленными в вашей сети Microsoft Azure, вам необходимо правильно настроить ваши виртуальные сети/подсети. Для детальной информации обратитесь к Документации Microsoft Azure Virtual Network.

  – Рекомендуется устанавливать Security Server в том же регионе Microsoft Azure, в котором находятся экземпляры для защиты.

Режим сканирования по умолчанию для виртуальных машин Microsoft Azure - «Локальное сканирование» (механизмы защиты хранятся в установленном агенте безопасности, а сканирование выполняется локально на компьютере). Если вы хотите сканировать ваши виртуальные машины Microsoft Azure с помощью Security Server, вам необходимо соответствующим образом настроить пакет установки агента безопасности и применяемую политику.

5.3.2. 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.

Чтобы узнать о доступных агентах безопасности, обратитесь к «Агенты безопасности» (p. 14).

На компьютерах под управлением Windows и Linux агент безопасности может иметь две роли, и вы можете установить его следующим образом:

1. В качестве простого агента безопасности для конечных точек.
2. Как Relay, действующего в качестве агента безопасности, а также связи, прокси и сервера обновлений для других конечных точек в сети.

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.

Если через установочный пакет и политики безопасности администратором сети разрешено, то агент безопасности может также работать в режиме Power User mode на конечных точках Windows, позволяя пользователю конечной точки просматривать и изменять параметры политик. Тем не менее, администратор Control Center всегда может контролировать, какие параметры политик применять, перекрывая режим привилегированного пользователя.

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

На Mac язык отображения пользовательского интерфейса выбирается во время установки на основе языка операционной системы конечной точки. На Linux агент безопасности не имеет локального пользовательского интерфейса.

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. 147).

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. Удалить (не просто отключить) любую существующую защиту от вредоносных программ или программное обеспечение для Интернет-безопасности на целевых конечных точках. Запуск агента безопасности одновременно с другим программным обеспечением по безопасности на конечной точке может повлиять на их работу и вызвать серьезные проблемы с системой.

   Многие из несовместимых программ безопасности автоматически обнаруживаются и удаляются во время установки.

   Чтобы узнать больше и проверить список программного обеспечения безопасности, обнаруженного Bitdefender Endpoint Security Tools для текущих операционных систем Windows, см. эту статью базы знаний .

   Важно
   Если вы хотите развернуть агент безопасности на компьютере с Антивирусом Bitdefender для Mac 5. X, сначала необходимо удалить его вручную. Для инструкции для выполнения смотрите эту статью базы знаний.

3. 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.
4. Конечные точки должны иметь сетевое подключение к устройству GravityZone.
5. Рекомендуется использовать статический IP-адрес для Relay сервера. Если вы не установите статический IP-адрес, используйте имя хоста машины.
6. При развертывании агента через Linux Relay должны выполняться следующие дополнительные условия:

   - На конечной точке с Relay ролью должен быть установлен пакет Samba (`smbclient`) версии 4.1.0 или выше и `net` binary/command для развертывания агентов на Windows.

     Примечание
     `net` binary/command обычно используется с samba-клиентом и/или стандартными пакетами samba. В некоторых дистрибутивах Linux

(например CentOS 7.4) `net` command устанавливается только, когда установлен Samba Samba suite (Common + Client + Server). Убедитесь, что на конечной точке с Relay ролью доступна `net` command.

- Целевые конечные точки Windows должны иметь доступ к ресурсам администрирования и сети.
- В целевых конечных точках Linux and Mac должно быть включено SSH.

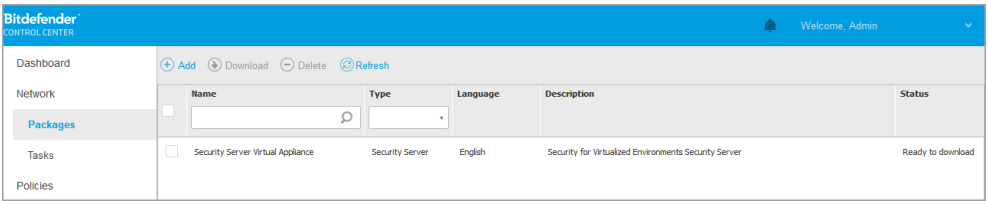
7. Начиная с macOS High Sierra (10. 13), после установки Endpoint Security for Mac вручную или удаленно, пользователям предлагается утвердить расширения ядра Bitdefender на своих компьютерах. Пока пользователи не утвердят расширения ядра Bitdefender, некоторые функции Endpoint Security for Mac не будут работать. Чтобы исключить вмешательство пользователя, вы можете предварительно утвердить расширения ядра Bitdefender, занеся их в белый список с помощью инструмента управления мобильными устройствами.
8. При установке агента в Amazon EC2, настройте группы безопасности, связанные с экземплярами, которые вы хотите защищать в Amazon EC2 в **Панели управления > Сеть & Безопасность** как описано ниже:
   - Для удаленной установки, разрешите SSH-подключение* с экземпляра EC2.
   - Для локальной установки, разрешите подключение по SSH и RDP (Remote Desktop Protocol) для компьютера, с которого вы пытаетесь подключиться.

   * Для удаленной установки на Linux, вам необходимо разрешить SSH-подключение, используя имя пользователя и пароль.
9. При установке агента в Microsoft Azure:
   - Целевая виртуальная машина должна быть в той же виртуальной сети, что и устройство GravityZone.
   - Целевая виртуальная машина должна находиться в одной виртуальной сети с ретранслятором, который связывается с устройством GravityZone, когда оно находится в другой сети.

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

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. 167).

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.

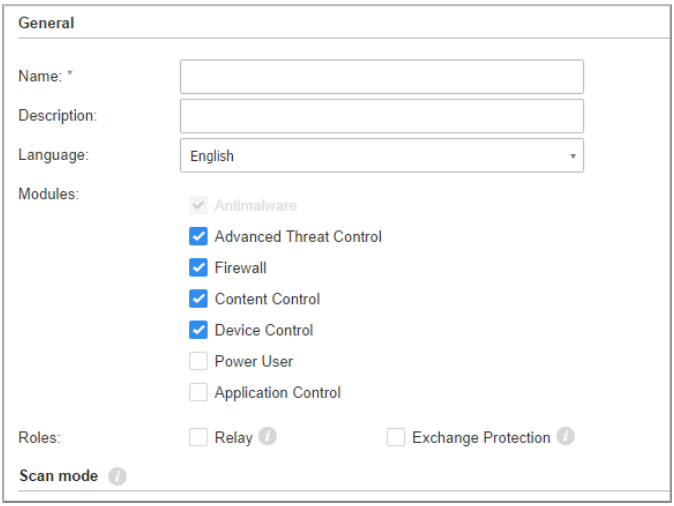
2. Download the installation package на выбранную конечную точку.

   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.

> **Примечание**
> Эта опция доступна только для ОС Windows.

6. Выберите модули защиты, которые вы хотите установить.

> **Примечание**
> Будут установлены только поддерживаемые модули для каждой операционной системы. Для получения более подробной информации, обратитесь к «Агенты безопасности» (p. 14).

7. Выберите роль целевой конечной точки:
   - **Relay**, чтобы создать пакет для конечной точки с ролью ретранслятора. Для получения более подробной информации, обратитесь к «Ретранслятор» (p. 16)

- **Сервер кэширования исправлений** , чтобы назначить ретранслятор внутренним сервером для распространения исправлений программного обеспечения. Эта роль отображается при выборе роли ретранслятора. Для получения более подробной информации, обратитесь к «Сервер кэширования патчей» (p. 17)
- **Exchange Protection**, чтобы установить модули защиты для серверов Microsoft Exchange, включая защиту от вредоносного ПО, антиспама, фильтрацию контента и вложений для трафика электронной почты Exchange и сканирование по запросу баз данных Exchange. Для получения более подробной информации, обратитесь к «Установка защиты Обмена» (p. 179).

8. **Удалить конкурентов**. Рекомендуется оставить этот флажок установленным, чтобы автоматически удалять любое несовместимое программное обеспечение безопасности, пока агент Bitdefender устанавливается в конечной точке. При отмене выбора этого параметра, агент Bitdefender будет установлен рядом с существующим решением безопасности. Вы можете вручную удалить ранее установленное решение безопасности на свой страх и риск.

   Важно
   Запуск агента Bitdefender одновременно с другим программным обеспечением безопасности на конечной точке может повлиять на их работу и вызвать серьезные проблемы с системой.

9. **Scan Mode**. Выберите технологию сканирования, которая наилучшим образом соответствует вашему сетевому окружению и ресурсам своих конечных точек. Вы можете определить режим сканирования, выбрав один из следующих типов:
   - **Автоматически**. В этом случае агент безопасности автоматически определяет конфигурацию конечных точек и соответственно адаптирует технологию сканирования:
     – Центральное сканирование в общедоступном или частном облаке (с Security Server) с запасным вариантом для гибридного сканирования (Light Engines), для физических компьютеров с низкой производительностью оборудования и для виртуальных машин. В этом случае требуется, по крайней мере, один Security Server развернутый в сети.

- Локальное сканирование (с полным движком) для физических компьютеров с высокой производительностью оборудования.
- Локальное сканирование для экземпляров EC2 и виртуальных машин Microsoft Azure.

Примечание
Считается, что компьютеры с низкой производительностью имеют частоту процессора менее 1,5 ГГц или оперативную память менее 1 ГБ.

- **Custom**. В этом случае, вы можете настроить режим сканирования, выбирая между несколькими технологиями сканирования для физических и виртуальных машин:
  - Центральное сканирование в общедоступном или частном облаке (с Security Server), которое может использоваться в качестве резервного * при локальном сканировании (с полным двигателем) или при гибридном сканировании (с легким двигателем).
  - Комбинированное сканирование (с облегченными движками)
  - Локальное сканирование (с полными движками)

  Режим сканирования по умолчанию для экземпляров EC2 - «Локальное сканирование» (механизмы защиты хранятся в установленном агенте безопасности, а сканирование выполняется локально на компьютере). Если вы хотите сканировать ваши экземпляры EC2 с помощью Security Server, вам необходимо соответствующим образом настроить пакет установки агента безопасности и применяемую политику.

  Режим сканирования по умолчанию для виртуальных машин Microsoft Azure - «Локальное сканирование» (механизмы защиты хранятся в установленном агенте безопасности, а сканирование выполняется локально на компьютере). Если вы хотите сканировать ваши виртуальные машины Microsoft Azure с помощью Security Server, вам необходимо соответствующим образом настроить пакет установки агента безопасности и применяемую политику.

  * Когда используются двойные движки сканирования - если первый движок не доступен, резервный движок может быть задействован. Потребление ресурсов и утилизация сети будет зависеть от используемых движков.

Для получения более подробной информации о доступных технологиях сканирования, обратитесь к«Сканирующие движки» (p. 3)

10. **Deploy endpoint with vShield when a VMware environment integrated with vShield is detected**. Эта опция может быть использована, когда инсталляционный пакет разворачивается на виртуальной машине из среды VMware интегрированной с vShield. В этом случае, VMware vShield Endpoint будет установлен на выбранной машине, вместо агента безопасности Bitdefender.

   Важно
   Эта опция предназначена только для удаленного развертывания, а не для локальных установок. При локальной установке в среде VMware, интегрированной с vShield, у вас есть возможность загрузить пакет vShield-Integrated.

11. При настройке модулей сканирования с использованием сканирования в публичном или частном облаке (Security Server) необходимо выбрать локально установленные Security Server, которые вы хотите использовать, и настроить их приоритет в разделе **. Раздел Security Server Assignment** :

    a. Нажмите список Security Server в заголовке таблицы. Появится список обнаруженных Security Server.

    b. Выберите объект.

    c. Нажмите кнопку ⊕ **Add** в заголовке столбца **Actions**.

       Security Server добавится в список.

    d. Выполните те же действия, чтобы добавить несколько серверов безопасности, если таковые имеются. В этом случае, вы можете настроить их приоритет, используя стрелки вверх ⌃ и вниз ⌄, доступные в правой стороне каждого объекта. Когда первый Security Server недоступен, будет использоваться следующий и так далее.

    e. Для удаления одного объекта из списка, нажмите соответствующую кнопку ⊗ **Delete** в верхней части таблицы.

    Вы можете выбрать для шифрования соединения с Security Server, следующую опцию **Use SSL**.

12. **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.

13. Выберите **Scan before installation**, если вы хотите убедиться, что машины "чисты" перед установкой клиента на них. Быстрое сканирование в облаке будет выполнено на целевых машинах перед началом установки.
14. Bitdefender Endpoint Security Tools устанавливается в каталог установки по умолчанию. Выберите **Использовать пользовательский путь установки** если вы хотите установить агента Bitdefender в другое место. Если указанная папка не существует, она будет создана во время установки.
    - В Windows по умолчанию используется путь `C:\Program Files\`. Чтобы установить Bitdefender Endpoint Security Tools в произвольном месте, используйте соглашения Windows при вводе пути. Например, `D:\folder`.
    - В Linux Bitdefender Endpoint Security Tools по умолчанию устанавливается в папку `/opt`. Чтобы установить агент Bitdefender в произвольном месте, используйте соглашения Linux при вводе пути. Например, `/folder`.

      Bitdefender Endpoint Security Tools не поддерживает установку по следующим пользовательским путям:

- Любой путь, который не начинается с косой черты (/). Единственным исключением является местоположение Windows `%PROGRAMFILES%`, которое агент безопасности интерпретирует как папку Linux по умолчанию `/opt`.
- Любой путь в `/tmp` или `/proc`.
- Любой путь, который содержит следующие специальные символы: `$, !, *, ?, ", ', `, \, (,), [,], {, }`.
- Спецификатор `systemd` (%).

В Linux для установки по пользовательскому пути требуется glibc 2.21 или выше.

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

15. При желании, вы можете установить пароль, чтобы запретить пользователям удалять защиту. Выберите **Set uninstall password** и введите желаемый пароль в соответствующие поля.
16. 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.
17. 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 общаются 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
  Порт 7074 должен быть открыт для правильного развертывания через Bitdefender Endpoint Security Tools Relay.

18. 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
  - **Linux OS:** 32-бит и 64-бит системы
  - **macOS:** только 64-битные системы

  Удостоверьтесь, что используете правильную версию для системы, на которую вы устанавливаете продукт.

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:

- 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.
  4. Следуйте инструкциям на экране.

  Примечание
  В macOS после установки Endpoint Security for Mac пользователям предлагается утвердить расширения ядра Bitdefender на своих компьютерах. Пока пользователи не утвердят расширения ядра Bitdefender, некоторые функции агента безопасности не будут работать. Для получения подробной информации смотрите эту статью базы знаний.

- На операционных системах Linux:
  1. Подключитесь и войдите в Control Center.

2. Загрузите или скопируйте установочный файл на целевую конечную точку.
3. Если вы скачали полный комплект, извлеките файлы из архива.
4. Получите привилегии суперпользователя, выполнив команду `sudo su`.
5. Измените права доступа к файлу установки, так чтобы вы могли запустить его:

```
# chmod +x installer
```

6. Запустите установочный файл:

```
# ./installer
```

7. Чтобы проверить установку агента на конечной точке, выполните следующую команду:

```
$ service bd status
```

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

Важно
При использовании VMware Horizon View Persona Management рекомендуется настроить групповую политику Active Directory, чтобы исключить следующие процессы Bitdefender (без полного пути):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Эти исключения должны применяться до тех пор, пока агент безопасности работает в конечной точке. Подробнее см. на этой странице документации VMware Horizon .

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» (p. 167).

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 эту статью базы знаний.
- Отключите брандмауэр Windows или настройте его для разрешения трафика через протокол общего доступа к файлам и принтерам.

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. 31).

- 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:

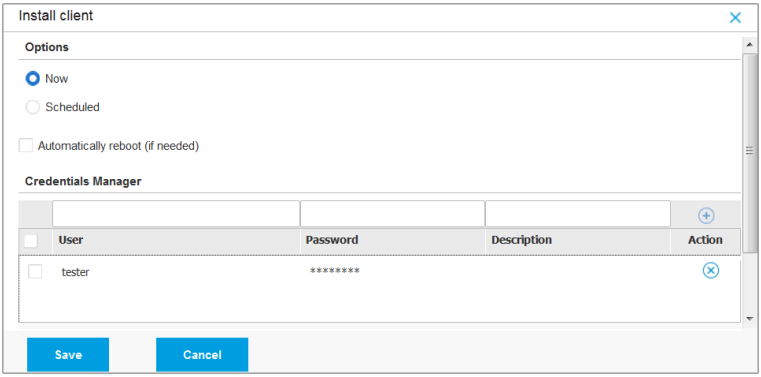
1. Подключитесь и войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. Выберите **компьютеры и виртуальные машины** из меню видов сетей.
4. Выберите нужную группу в левой панели. Объекты, содержащиеся в выбранной группе, будут отображены в таблице правой панели.

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**.



Установка Bitdefender Endpoint Security Tools из меню задач

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 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.

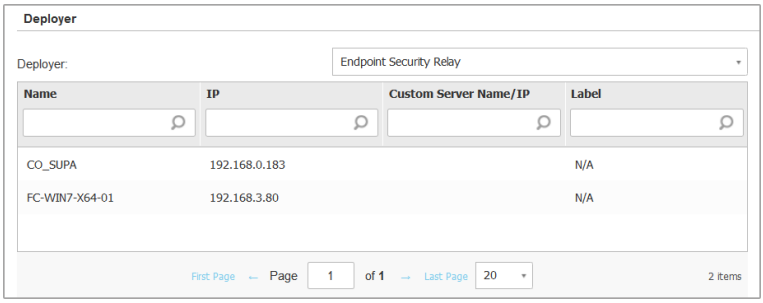
11. В разделе **Установщик**, выберите объект, к которому выбранные конечные точки будут подключаться для установки и обновления клиента:
    - **GravityZone Appliance**, если конечные точки будут подключаться непосредственно к устройству GravityZone.

      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 общаются 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.



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» (p. 147).

    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**.

Важно
При использовании VMware Horizon View Persona Management рекомендуется настроить групповую политику Active Directory, чтобы исключить следующие процессы Bitdefender (без полного пути):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Эти исключения должны применяться до тех пор, пока агент безопасности работает в конечной точке. Подробнее см. на этой странице документации VMware Horizon .

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.

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.

5.4. Установка обнаружения и отклика в конечной точке

Этот модуль поставляется по умолчанию с установочным комплектом Bitdefender Endpoint Security Tools и требует активации Датчика Инцидентов при первом вводе лицензионного ключа.

Перед установкой убедитесь, что целевые конечные точки удовлетворяют минимальным требованиям. Минимальные требования к инцидентам соответствуют требованиям агента безопасности.

Для защиты ваших конечных точек с помощью EDR вы можете выбрать один из двух вариантов:

- Установите агенты безопасности с датчиком EDR при вводе лицензионного ключа. Ссылайтесь на Активацию Вашей лицензии.
- Используйте задачу **Reconfigure** .

Важно
The Incidents Sensor no longer provides support for Internet Explorer.

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

5.5. 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

5.5.1. 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» (p. 129).

5.5.2. Разверните виртуальное устройство Sandbox Analyzer

Чтобы развернуть виртуальное устройство Sandbox Analyzer:

1. Войдите в Control Center GravityZone.
2. Перейдите на страницу **Network > Packages**.

3. Установите флажок **Sandbox Analyzer** из таблицы.
4. Нажмите кнопку **Скачать** в верхнем левом углу страницы. Выберите опцию **Устройство безопасности (автономная версия ESXi)**.
5. 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 (`eth1`interface) Эта сеть должна быть изолирована от любых других сегментов сети.
   - **Сеть доступа в Интернет** - Sandbox Analyzer использует эту сеть для получения последних обновлений (`eth2`interface) `eth1`interface не следует иметь тот же самый IP или сеть как `eth0`.

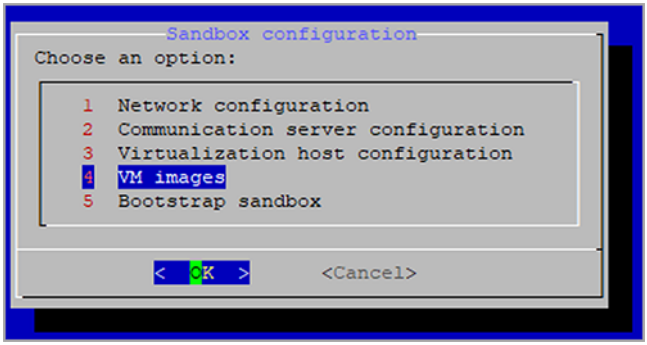
6. Включите устройство.
7. Из инструмента управления виртуализацией откройте консольный интерфейс виртуального устройства Sandbox Analyzer.
8. При запросе учетных данных используйте `root` для имени пользователя и `sve` для пароля.
9. Войдите в меню конфигурации, выполнив следующую команду:

   ```
   /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 статистически й 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`.

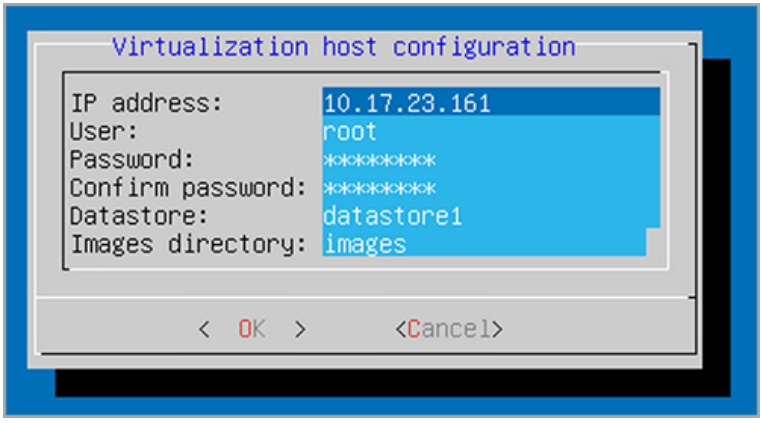
Примечание
Как только IP-адрес или имя хоста указаны и конфигурация сохранена, экземпляр Sandbox Analyzer станет видимым в Control Center GravityZone, на странице **Sandbox Analyzer > Инфраструктура**.

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.

  Введите 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» (p. 175).

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. Подробности смотрите в «Хосты DMZ» (p. 176)

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.

5.5.3. Разверните виртуальное устройство сетевой безопасности

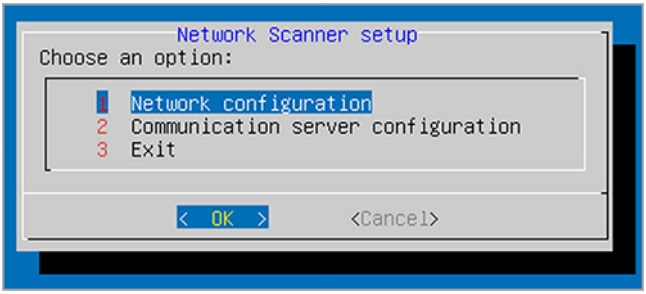
В этом разделе описывается, как развернуть виртуальное устройство сетевой безопасности, компонент Sandbox Analyzer, который захватывает сетевой трафик и передает подозрительные образцы для анализа поведения.

Чтобы развернуть виртуальное устройство сетевой безопасности:

1. Войдите в Control Center GravityZone.
2. Перейдите на страницу **Network > Packages**.
3. Выберите флажок **Виртуальное устройство сетевой безопасности** из таблицы.
4. Нажмите кнопку **Скачать** в верхнем левом углу страницы и выберите опцию **(VMware OVA)**.
5. Используйте инструмент управления виртуализацией (например, vSphere Client), чтобы импортировать загруженный файл OVA в вашу виртуальную среду.
6. В мастере развертывания выберите сетевую карту (NIC), используемую для связи с GravityZone, и сетевую карту, используемую для захвата трафика.
7. Включите устройство.
8. С помощью инструмента управления виртуализацией откройте консольный интерфейс виртуального устройства сетевой безопасности SVE SVA GravityZone.
9. При запросе учетных данных используйте `root` для имени пользователя и `sve` для пароля.

10. Войдите в меню конфигурации, выполнив следующую команду:

```
/opt/bitdefender/bin/nsva-setup
```



Консоль устройства сетевой безопасности

11. Перейдите к опции меню **Настройка коммуникационного сервера**.
12. Укажите IP-адрес или имя хоста и порт коммуникационного сервера GravityZone.

    Используйте следующий синтаксис: `http://<IP/Hostname>:<Port>`. По умолчанию порт `8443`.
13. Сохраните конфигурацию.

Настройте сетевой датчик для детонации файлов pcap

Датчик сети может извлекать содержимое из файлов захвата сети (pcap) и автоматически отправлять его для детонации в экземпляр Sandbox Analyzer.

Чтобы детонировать контент из файлов pcap:

1. Войдите в виртуальное устройство сетевой безопасности.
2. При запросе учетных данных используйте `root` для имени пользователя и `sve` для пароля.
3. Выполните следующую команду:

```
/opt/bitdefender/bin/scan-pcap <local pcap path>
```

В приведенной выше команде <локальный путь pcap< представляет местоположение, куда загружается файл pcap в виртуальном устройстве сетевой безопасности.

Дополнительные сведения об использовании датчика сети смотрите в главе **Политики > Sandbox Analyzer** из Руководства администратора GravityZone.

5.6. 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» (p. 128).

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.

5.7. Установка защиты Обмена

Security for Exchange автоматически интегрируется с серверами Exchange, в зависимости от роли сервера. Для каждой роли устанавливаются только совместимые компоненты, как описано в настоящем документе:

Особенности	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Ограничения	Почтовый ящик	Ограничения	Хаб	Почтовый ящик
Транспортный уровень					
Фильтрация вредоносных программ	x	x	x	x	
Фильтрация спама	x	x	x	x	
Фильтрация контента	x	x	x	x	
Фильтрация вложений	x	x	x	x	
Хранилище Exchange					
Антивирусное сканирование по требованию		x			x

5.7.1. Подготовка к установке

Перед установкой Security for Exchange, убедитесь, что все requirements выполнены, в противном случае Bitdefender Endpoint Security Tools может быть установлен без модуля защиты Exchange.

Для того, чтобы модуль защиты Exchange работал бесперебойно и предотвращал конфликты и нежелательные результаты, удалите всю защиту от вредоносных программ и всех агентов фильтрации электронной почты.

Bitdefender Endpoint Security Tools автоматически определяет и удаляет большинство антивирусных продуктов и отключает агентов защиты от вредоносного ПО, встроенных в сервер Exchange, начиная с версии 2013. Для получения подробной информации относительно списка обнаруживаемого программного обеспечения по безопасности, обратитесь к this KB article.

Вы можете повторно вручную включить встроенного в Exchange агента защиты от вредоносного ПО в любое время, однако, это не рекомендуется делать.

5.7.2. Установка защиты на серверах Exchange

Чтобы защитить ваши сервера Exchange, необходимо установить Bitdefender Endpoint Security Tools с ролью защитника Exchange на каждом из них.

У вас есть несколько вариантов развертывания Bitdefender Endpoint Security Tools на серверах Exchange:

- Локальная установка, скачав и запустив установочный пакет на сервере.
- Удаленная установка, путем запуска задачи **Install**.
- Удаленная, запустив задачу **Reconfigure Client**, если Bitdefender Endpoint Security Tools уже предлагает защиту файловой системы на сервере.

Для получения подробных инструкций по установке, обратитесь к «Установка агентов по безопасности» (p. 143).

5.8. Установка HVI

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Чтобы использовать HVI на виртуальных машинах с хостов Xen, вы должны выполнить следующие шаги:

1. Проверьте предварительные условия для установки
2. Установка Security Server
3. Установка дополнительного пакета HVI

Требования к системе

- XenServer интегрирован с GravityZone.
- XenCenter установлен на вашем компьютере.

Установка Security Server

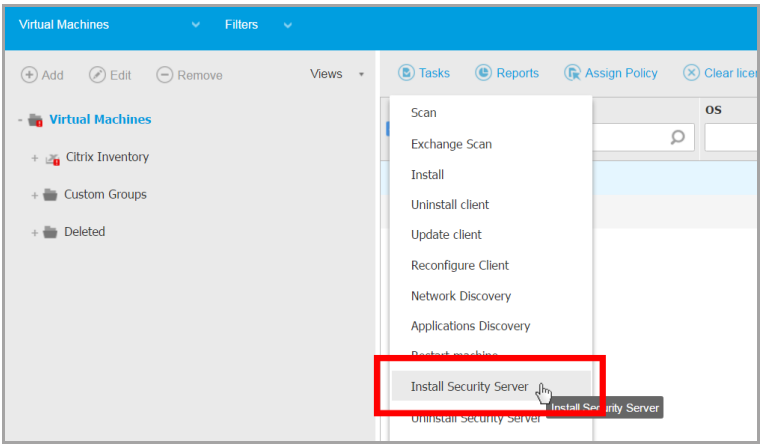
Чтобы установить Security Server на одном или нескольких хостах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Virtual Machines** из меню выбора просмотров.

3. Просмотрите инвентаризацию Citrix и установите флажки, соответствующие требуемым хостам. Для быстрого выбора вы можете напрямую выбрать корневой контейнер (Citrix Inventory). Вы сможете выбрать хосты самостоятельно в мастере установки.

Примечание
Вы не можете выбрать хосты из разных папок.

4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **УстановитьSecurity Server** в меню. Отобразится окно установки **Security Server Установка**.



Установка Security Server

5. Выберите хосты, на которых вы хотите установить экземпляр Security Server.
6. Выберите параметры конфигурации, которые вы хотите использовать.

Важно
Использование общих настроек, при развертывании нескольких экземпляров Security Server одновременно, требует: одно общее хранилище для хостов; наличие собственных IP-адресов, назначенных с помощью DHCP-сервера; находится в одной сети.

При выборе разных настроек для каждого Security Server, вы сможете определить параметры, которые необходимы для каждого хоста в следующем шаге мастера установки. Описанные далее шаги применяются в случае, когда используется опция **Configure each Security Server**.

7. Нажмите **Далее**.

   Примечание
   В зависимости от ранее сделанного выбора некоторые из описанных здесь вариантов могут не применяться к вашей ситуации.

8. Введите подходящее имя для Security Server.
9. Выберите контейнер, в который вы хотите включить Security Server из меню **Контейнер**.
10. Выберите расположение хранилища.
11. Выберите тип диска (provisioning type). Рекомендуется развернуть устройство на "толстых" дисках (thick provisioning).

    Важно
    Если вы используете "тонкие" диски (thin provisioning) и дисковое пространство в хранилище данных закончится, Security Server заморозится и, следовательно, хосты останутся незащищенными.

12. Настройте распределение памяти и ресурсов процессора, основанное на коэффициенте консолидации виртуальной машины на хосте. Выберите **Низкий**, **Средний** или **Высокий**, чтобы загрузить рекомендуемые параметры распределения ресурсов или **настройка вручную**, чтобы настроить распределение ресурсов вручную.
13. Установите часовой пояс устройства.
14. Задайте пароль администратора для консоли Security Server. Установка пароля администратора перезаписывает пароль по умолчанию ("sve").
15. Выберите тип конфигурации сети для сети Bitdefender. IP-адрес Security Server не должен изменяться со временем, так как он используется агентами Linux для общения.

    Если вы выберите DHCP, убедитесь, что настроили DHCP-сервер на резервирование IP-адреса для устройства.

Если вы выберите статический, вы должны ввести информацию о IP-адресе, маске подсети, шлюзе и DNS.

16. Нажмите **Сохранить**.

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

Установка дополнительного пакета HVI

1. Перейдите на страницу **Настройки > Обновить**.
2. Выберите Дополнительный пакет HVI в списке **Компоненты** и нажмите кнопку **Загрузить** в верхней части таблицы.
3. Перейдите на страницу **Сеть** и выберите **Виртуальные машины** в переключателе обзора.
4. Выберите **Сервер** из меню **Виды** в левой панели.
5. Выберите один или несколько Xen-хостов в сетевом содержимом. Вы можете легко просмотреть список доступных хостов, выбрав опцию **Type > Hosts** из меню **Filters**.
6. Нажмите кнопку **Задачи** в правой панели и выберите **Установить HVI Дополнительный пакет**. Откроется окно установки.
7. Вы можете запланировать задачу установки. Вы можете сразу же запустить задачу после сохранения задания или в определенное время. В случае если установка не может быть завершена в указанное время, задача автоматически повторится в соответствии с настройками повторения. Например, если вы выбрали несколько хостов и один хост недоступен в запланированное время, задание будет запущено снова в заданное время.
8. Хост должен перезагрузиться, чтобы применить изменения и завершить установку. Если вы хотите, чтобы хост перезагрузился без запроса, выберите **Automatically reboot host**.
9. Нажмите **Сохранить**. Появится окно подтверждения.

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

5.9. Установка защиты хранилища

Security for Storage - это услуга Bitdefender, предназначенная для защиты устройств сетевого хранилища (NAS) и систем обмена файлами, совместимых

с протоколом адаптации контента Интернета (ICAP). Для поддерживаемых систем обмена файлами, см. «Защита хранилища» (p. 61).

Чтобы использовать Security for Storage с вашим решением GravityZone, вам необходимо:

1. Установите и настройте как минимум два Security Servers в вашей среде для работы в качестве ICAP-серверов. Bitdefender Security Servers анализируют файлы, отправляют вердикты в системы хранения и при необходимости принимают соответствующие меры. В случае перегрузки первый Security Server перенаправляет избыток данных на второй.

   Примечание
   В качестве передового опыта установите специальные Security Server для защиты хранилища отдельно от Security Server, используемых для других ролей, таких как сканирование на наличие вредоносных программ.

   Подробнее о процедуре установки Security Server см. в главе **Установка Security Server** этого руководства.

2. Настройте модуль **Защита хранилища** из параметров политики GravityZone.

   Для получения дополнительной информации см. Главу **Политика безопасности> Политика в отношении компьютеров и виртуальных машин> Защита хранилища** из Руководства администратора GravityZone.

Подробнее о настройке и управлении серверами ICAP на определенном устройстве NAS или в системе общего доступа к файлам см. Документацию для этой конкретной платформы.

5.10. Установка защиты мобильных устройств

Security for Mobile это мобильное решение для управления устройствами, предназначеное для iPhone, iPad и Android устройств. Для получения полного списка поддерживаемых версий операционной системы, проверьте system requirements.

Для управления Security for Mobile из Control Center, вы должны добавить мобильные устройства в Active Directory или назначить пользователям, а затем установить приложение GravityZone Mobile Client на устройствах. После настройки службы, вы можете запустить административные задачи на мобильных устройствах.

Прежде чем начать, убедитесь, в выполненной настройке публичного (внешнего) адреса для коммуникационного сервера.

Чтобы установить Security for Mobile:

1. Если у вас нет интеграции с Active Directory, вы должны создать пользователей create users for mobile device owners.
2. Добавить устройства пользователям.
3. Установить GravityZone Mobile Client на устройствах и активировать его.

5.10.1. Настройка внешнего адреса для 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.

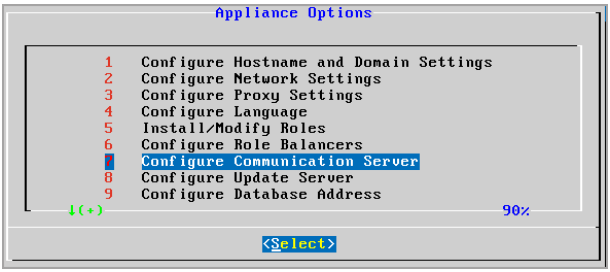
Чтобы иметь возможность управлять мобильными устройствами через Интернет, независимо от того, где они находятся, необходимо настроить коммуникационный сервер на доступность с публичных адресов.

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.

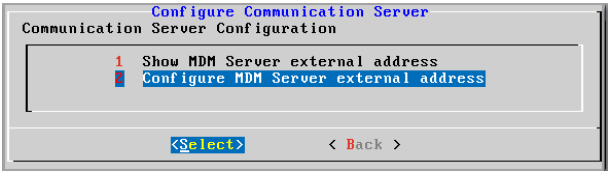
В обоих случаях необходимо настроить коммуникационный сервер с внешним IP-адресом, чтобы управлять мобильными устройствами:

1. Доступ к консоли устройства из вашего инструментария управления виртуализацией (например, vSphere Client).
2. Выберите из главного меню **Configure Communication Server**.



Окно параметров приложения

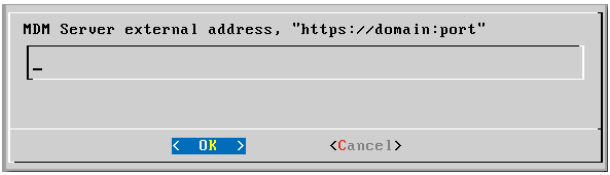
3. Нажмите **Configure MDM Server external address**.



Окно настройки коммуникационного сервера

4. Введите внешний адрес.

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



Окно ввода внешнего адреса сервера MDM

- 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.

5.10.2. Создание и организация настраиваемых пользователей

В ситуациях без Active Directory, вы должны сначала создать настраиваемых пользователей для того, чтобы иметь возможность идентифицировать владельцев мобильных устройств. Указанные мобильные устройства пользователей не связаны каким-либо образом с Active Directory или с другими пользователями, определенными в Control Center.

Создание настраиваемых пользователей

Чтобы создать настраиваемых пользователей:

1. Перейдите в раздел **Сеть**.
2. Выберите **Mobile Devices** из селектора просмотров.
3. В левой панели выберите **Пользовательские группы**.
4. Нажмите иконку **Add User** на панели инструментов. Появится окно настроек.
5. Укажите необходимые сведения о пользователе:
   - Подходящее имя пользователя (например, полное имя пользователя)
   - Адрес электронной почты пользователя

   Важно
   - Убедитесь, что это действительный адрес электронной почты. Пользователю по электронной почте будет выслана инструкция по установке, когда вы добавите устройство.
   - Каждый адрес электронной почты может быть связан только с одним пользователем.

6. Нажмите **OK**.

Организация настраиваемых пользователей

Чтобы организовать настраиваемых пользователей:

1. Создание настраиваемых групп.

a. Выберите **Custom Groups** в левой боковой панели и нажмите иконку ⊕ **Add** на панели инструментов (вверху панели).

b. Введите подходящее имя группы и нажмите **OK**. Появится новая группа в **Пользовательские группы**.

2. Переместите настраиваемых пользователей в соответствующие настраиваемые группы.

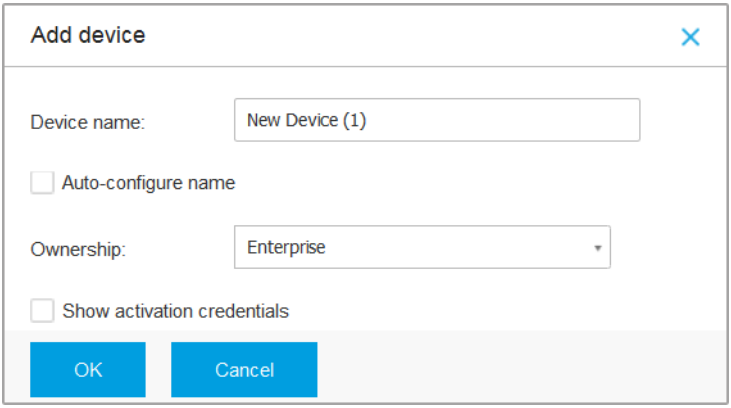
a. Выберите пользователей в правой боковой панели.

b. Перетащите выбранное в нужную группу в левой боковой панели.

5.10.3. Добавить устройства пользователям

Чтобы добавить устройство пользователю:

1. Перейдите в раздел **Сеть**.
2. Выберите **Mobile Devices** из селектора просмотров.
3. Найдите пользователя в папках Active Directory или настраиваемых группах.
4. Нажите иконку ⊕ **Add Device** в верхней части таблицы сети. Появится окно настроек.



Добавление мобильного устройства пользователю

5. Введите подходящее имя для устройства.

6. Используйте опцию **Автоматическая настройка имени**, если вы хотите, чтобы имя устройства назначалось автоматически. При добавлении устройство имеет обобщенное имя. После активации устройству автоматически будет присвоено имя, основанное на информации о производителе и модели устройства.
7. Выберите тип владельца устройства (предприятие или личное).
8. Выберите опцию **Show activation credentials** после нажатия кнопки **OK**, если вы собираетесь установить GravityZone Mobile Client на устройстве пользователя.
9. Нажмите **OK**. Пользователю будет незамедлительно отправлено письмо с инструкциями по установке, подробностями по активации и настройке устройства. Подробности активации включают маркер активации и адрес коммуникационного сервера (и соответствующий QR Code).

Примечание

- Вы можете просмотреть подробную информацию об активации устройства в любое время, нажав на ее имя в Control Center.
- Вы также можете добавить мобильные устройства к выбранным пользователям и группам. В этом случае окно конфигурации позволит определить только право собственности устройства. Мобильным устройствам, созданным ручным способом по умолчанию будет присвоено общее имя. Как только устройство зарегистрировано, его имя будет автоматически изменено, в том числе соответствующий изготовитель и модель.

5.10.4. Установка GravityZone Mobile Client на устройствах

Приложение GravityZone Mobile Client распространяется через Apple App Store и Google Play.

Чтобы установить GravityZone Mobile Client на устройстве:

1. Найдите приложение в официальном магазине приложений.
   - Ссылка Google Play
   - Ссылка Apple App Store
2. Скачайте и установите приложение на устройстве.
3. Запустите приложение и выполните необходимые настройки:

a. На устройствах Android, нажмите **Activate**, чтобы предоставить права GravityZone Mobile Client в качестве администратора устройства. Внимательно прочитайте предоставленную информацию.

Примечание

- Задача блокировки для устройств Android (7.0 или новее) будет применять пароль, установленный в консоли GravityZone только в том случае, если на устройстве не настроена защита блокировки. В ином случае для защиты устройства будут использоваться существующие параметры блокировки экрана, такие как PIN-код, пароль, отпечаток пальца или смарт-блокировка.
- Задача разблокировки больше недоступна для устройств Android (7.0 или новее).
- Из-за технических ограничений задачи блокировки и удаления недоступны на Android 11.

b. Введите маркер активации и адрес коммуникационного сервера или можете просканировать QR-код, полученный по электронной почте.

c. Нажмите **Trust**, когда будет предложено принять сертификат коммуникационного сервера. Таким образом, GravityZone Mobile Client проверяет коммуникационный сервер и будет принимать сообщения только от него, предотвращая атаки-посредники

d. Нажмите **Activate**.

e. На устройствах iOS, вам будет предложено установить профиль MDM. Если устройство защищено паролем, вам будет предложено указать этот пароль. Кроме того, вы должны разрешить GravityZone доступ к настройкам вашего устройства, иначе процесс установки вернется к предыдущему шагу. Следуйте инструкциям на экране, чтобы завершить установку профиля.

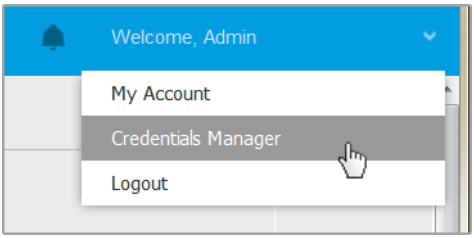
Примечание

Чтобы функция определения местоположения работала должным образом, пользователям необходимо разрешить фоновое определение местоположения на устройствах не только при использовании приложения.

5.11. 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

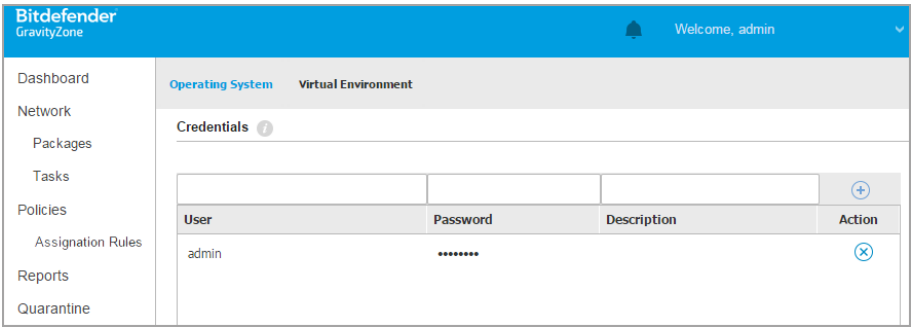
Окно **Диспетчер учетных данных** содержит две вкладки:

- Операционная система
- Виртуальная среда

5.11.1. 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:



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.

5.11.2. 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 дельнейшем.

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

5.11.3. 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.

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, предназначенной 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 Интернет.

Когда доступно новое обновление, GravityZone устройство, агент безопасности или Security Server 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 о простоях перед обновлением**.

Обновления стороннего программного обеспечения

Виртуальное устройство GravityZone поддерживает серии программных продуктов от сторонних поставщиков. Данные 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.ком: 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 Security Server и 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 компонет 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 ыыбранная версия , статус изменится соответствующим образом. Обновите содержимое таблицы, нажав кнопку **Refresh** и проверьте соответствующий статус.

Важно
Устройство GravityZone не включает в себя пакет Security Server по умолчанию. Вы должны вручную загрузить пакет Security Server, необходимый для вашей среды.

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 GravityZone 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
```

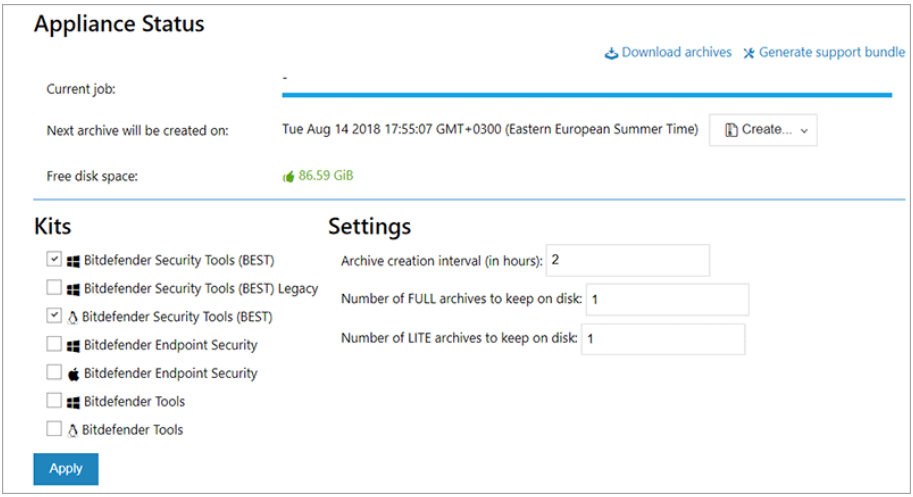
`gzou-mirror` имеет следующие роли:

- 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.



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.

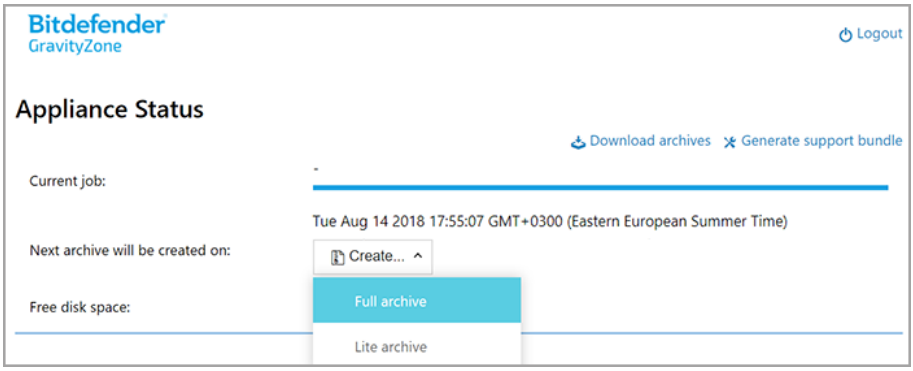
     Задание CRON, установленное в онлайн-экземпляре, каждую минуту будет проверять наличие новых файлов обновлений и наличие свободного дискового пространства более 10 ГБ. В каждый период, заданный параметром **Интервал создания архива (в часах)**, задание CRON создает следующие файлы:

     – **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:

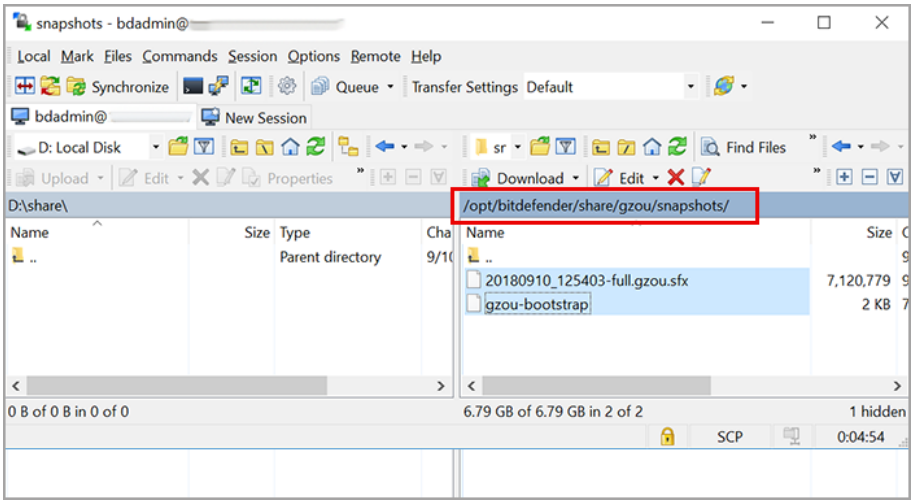
     `https://Online-Instance-Update-Server-IP-or-Hostname/snapshots`
3. Нажмите **Создать > Полный** архив, чтобы создать первый полный архив. Подождите, пока создается архив.



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** .

1. Установите GravityZone на машину из изолированной среды.
2. Установите только роли Базы Данных и Сервера Обновлений.

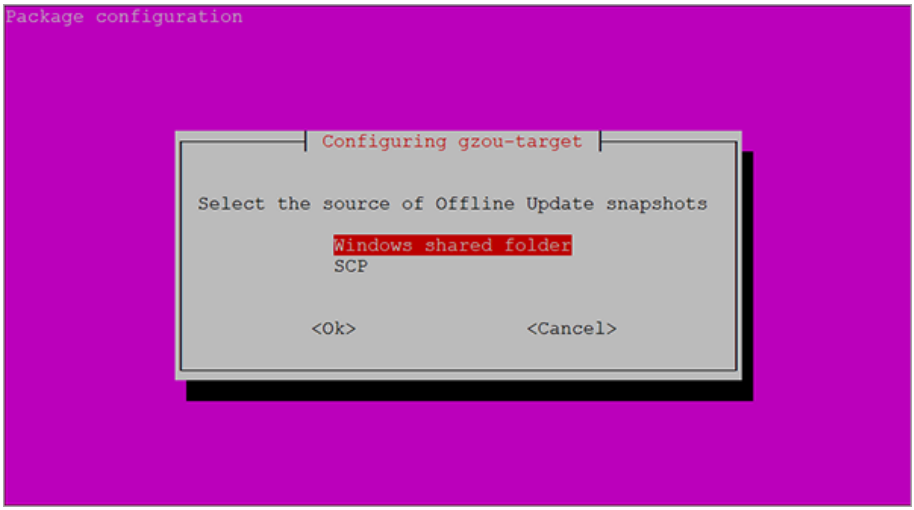
3. Перенесите архивы обновлений и файл `gzou-bootstrap`, загруженные с онлайн-экземпляра, в `расположение /home/bdadmin` на автономном экземпляре используя переносное мультимедийное устройство (USB накопитель).

   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. Загрузите последний архив обновлений с онлайн-экземпляра на удобный вам сетевой файлообменник. Дополнительные сведения см. в разделе «Настройка и загрузка начальных файлов обновлений» (p. 202).
2. Используйте USB устройство для переноса архива обновлений на файлообменник Samba в изолированной сети. Дополнительные сведения см. в разделе «Настройка автономного экземпляра GravityZone» (p. 205).

   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 HVI
- Удаление защиты Обмена
- Удаление защиты мобильных устройств
- Удаление Sandbox Analyzer On-Premises
- Удаление Ролей GravityZone

7.1. Удаление защиты конечных рабочих станций

Чтобы безопасно удалить защиту Bitdefender, сначала необходимо удалить агенты безопасности, а затем Security Server, если это необходимо. Если вы хотите удалить только Security Server, обязательно подключите его агентов к другому Security Server в первую очередь.

- Удаление агентов безопасности
- Удаление Security Server

7.1.1. Удаление агентов безопасности

У вас есть два варианта удаления агентов безопасности:

- удаленно в Control Center
- Вручную на целевой машине

Предупреждение
Агенты безопасности и Серверы безопасности 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 **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 ставнции 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 защиты для конечных точек» (р. 132).

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 защиты для конечных точек» (р. 132).

7.1.2. Удаление Security Server

Вы можете удалить Security Server так же, как он был установлен, либо в Control Center, либо в интерфейсе командной строки (CLI) виртуального устройства GravityZone.

Чтобы удалить Security Server в Control Center:

1. Перейдите в раздел **Сеть**.
2. Выберите **Virtual Machines** из меню выбора просмотров.
3. Выберите датацентр или папку, содержащую хост, на котором Security Server установлен. Конечные точки отображаются в правой панели.
4. Установите флажок в поле соответствующего хоста, на котором Security Server установлен.
5. В меню **Задачи** выберите **Удалить Security Server**.
6. Введите учетные данные vShield (если применимо) и нажмите **Да** , чтобы создать задачу.

Вы можете просматривать задачу и управлять ею в **Сеть > Задачи**

Если Security Server установлен на том же виртуальном устройстве, что и другие роли GravityZone, вы можете удалить его, используя интерфейс командной строки устройства. Следуйте инструкции:

1. Доступ к консоли устройства из вашего инструментария 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. В меню **Опции устройства** перейдите к **Расширенные настройки** .
3. Выберите **Удаление сервера безопасности** . Отобразится окно подтверждения.
4. Нажмите клавишу `Y` или нажмите клавишу `Ввод` , чтобы выбрать вариант **Да** , чтобы продолжить. . Подождите, идет удаление.

7.2. Удаление HVI

Чтобы удалить HVI с хоста, достаточно удалить HVI Дополнительный Пакет. Вы также можете использовать Security Server в качестве сервера

сканирования, если у вас есть действительный лицензионный ключ для Security for Virtualized Environments.

Если вы хотите полностью удалить Bitdefender, вам необходимо удалить как Дополнительный пакет HVI , так и Security Server.

Примечание
Модуль HVI может быть доступен для вашего решения GravityZone с отдельным лицензионным ключом.

Идет удаление дополнительного пакета HVI

У вас есть два варианта удаления Дополнительного пакета:

- Удаленно из Control Center, по выполнении задачи удаления.
- Удаленно из XenCenter, при запуске нескольких команд на целевом узле.

Чтобы удалить пакет HVI с помощью Control Center:

1. Войдите в Control Center.
2. Перейдите на страницу **Сеть** и выберите **Виртуальные машины** в переключателе обзора.
3. Выберите **Сервер** из меню **Виды** в левой панели.
4. Выберите один или несколько Xen-хостов в сетевом содержимом. Вы можете легко просмотреть доступные хосты, выбрав опцию **Тип > Хосты** в меню **Фильтры** .
5. Нажмите кнопку **Задачи** в правой панели и выберите **Удалить пакет HVI Supplemental Pack** . Откроется окно конфигурации.
6. Запланировать, когда удалить пакет. Вы можете сразу же запустить задачу после сохранения задания или в определенное время. В случае если удаление не может быть завершено в указанное время, задача автоматически повторится в соответствии с настройками повторения. Например, если вы выбрали несколько хостов и один хост недоступен в запланированное время, задание будет запущено снова в заданное время.
7. Хост должен перезапуститьсяб чтобы завершить удаление. Если вы хотите, чтобы хост перезагрузился без запроса, выберите **Автоматическая перезагрузка хоста(если необходимо)**.
8. Нажмите **Сохранить**. Появится окно подтверждения.

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

Чтобы удалить пакет HVI с помощью XenCenter:

1. Войдите в XenCenter.
2. Откройте консоль хоста Xen.
3. Введите пароль для хоста XenServer.
4. Выполните следующие команды:

```
# rpm -ebitdefender-xen-dom0 # rm -rf /etc//xensource/installed-r
  /bitdefender\:bitdefender-hvi/ # rm -rf/opt/bitdef* # Сервисxap
```

Удаление Security Server

Чтобы удалить Security Server с одного или нескольких хостов:

1. Войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. Выберите **Virtual Machines** из меню выбора просмотров.
4. Просмотрите инвентаризацию Citrix и установите флажки, соответствующие требуемым хостам. Для быстрого выбора вы можете фильтровать инвентарь сети для просмотра только серверов Security Server.
5. Нажмите кнопку **Задачи** в верхней части таблицы И выберите **Удалить Security Server** в меню. Появится окно подтверждения. Нажмите **Ок**, чтобы продолжить.

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

7.3. Удаление защиты Обмена

Вы можете удалить Защиту обмена с любого сервера Microsoft Exchange с Bitdefender Endpoint Security Tools с установленной ролью. Вы можете выполнить удаление в Control Center.

1. Перейдите в раздел **Сеть**.
2. Выберите **компьютеры и виртуальные машины** из меню видов сетей.

3. Выберите желаемый контейнер в левой панели. Объекты будут отображаться в правой панели таблицы.
4. Выберите конечную точку, с которой вы хотите удалить Защиту обмена.
5. Нажмите **Переконфигурировать клиента** в меню **Задачи** в верхней панели таблицы. Появится окно конфигурации.
6. В разделе **Общие** снимите флажок **Защита обмена** .

   Предупреждение
   В окне Конфигурации убедитесь, что вы выбрали все роли, которые активны на конечной рабочей станции. В противном случае они также будут удалены.

7. Нажмите **Сохранить**, чтобы создать задачу.

Вы можете просматривать задачу и управлять ею в **Сеть > Задачи**

Если вы хотите переустановить Защиту обмена, обратитесь к «Установка защиты Обмена» (p. 179).

7.4. Удаление Sandbox Analyzer On-Premises

Чтобы удалить Sandbox Analyzer On-Premises:

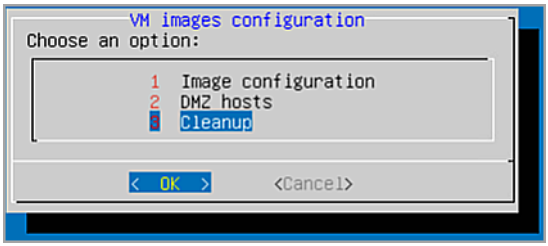
1. Удалите образы виртуальной машины (ВМ) из консоли устройства Sandbox Analyzer.
   a. Войдите в интерфейс устройства Sandbox Analyzer.

      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:
   a. Выключите виртуальное устройство Sandbox Analyzer.
   b. Удалите устройство из инвентаря ESXi.

7.5. Удаление защиты мобильных устройств

При удалении защиты Bitdefender с мобильного устройства вы должны сделать это как с помощью Control Center , так и с устройства.

При удалении устройства из Control Center:

- Мобильный клиент GravityZone отключен, но не удален с устройства.
- Все журналы, связанные с удаленным устройством, будут по-прежнему доступны.
- Ваша личная информация и приложения не будут затронуты.
- Для iOS-устройств MDM-профиль будет удален. Если устройство не подключено к сети Интернет, MDM-профиль останется в устройстве, пока не станет доступно новое соединение.

Предупреждение

- Вы не сможете восстановить удаленные мобильные устройства.

- Перед удалением убедитесь, что целевое устройство не заблокировано. Если вы случайно удалили заблокированное устройство, вам придется сбросить устройство к заводским установкам, чтобы его разблокировать.

1. Перейдите в раздел **Сеть**.
2. Выберите **Мобильные устройства** в селекторе просмотров.
3. Нажмите **Фильтры** в верхней части сетевой панели и выберите **Устройства** в категории **Просмотр** . Нажмите **Сохранить**.
4. Выберите желаемый контейнер в левой панели. Все устройства отображаются в таблице правой панели.
5. Отметьте флажком устройство, на котором вы хотите удалить защиту.
6. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Затем вам нужно удалить программное обеспечение с устройства.

Чтобы удалить защитуBitdefender с устройства Android:

1. Перейдите к **Безопасность > Администраторы устройств** .
2. Снимите флажок GravityZone. Появится окно подтверждения.
3. Нажмите **Деактивировать** . Появится предупреждающее сообщение, информирующее вас о том, что функции защиты от кражи не будут работать, и вы потеряете доступ к корпоративным сетям и данным.
4. Удалите Мобильный клиент GravityZone как любое другое приложение.

Чтобы удалить защиту Bitdefender с устройства iOS:

1. Перейдите на значокМобильный Клиент Bitdefender GravityZone и удерживайте его в течение нескольких секунд.
2. Коснитесь прикрепленного круга ⊗, когда он появится. Приложение удаляется.

Если вы хотите переустановить мобильную защиту, см.«Установка защиты мобильных устройств» (p. 185)

7.6. 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 свяжутся 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» (p. 117).

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.

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

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, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, 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, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, 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, pyp

Приложения	Типы файлов.
Mozilla Thunderbird Microsoft Outlook	eml

A.3. Ядра, поддерживаемые датчиком инцидентов

Датчик инцидентов поддерживает следующие ядра: