Positive Technologies MaxPatrol VM

Версия 1.0

Руководство по внедрению

POSITIVE TECHNOLOGIES

Дата редакции документа: 11.11.2020

Версия документа: 3

Содержание

1. Об этом документе

Руководство по внедрению содержит информацию для планирования и выполнения развертывания Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM) в инфраструктуре организации. В руководстве вы найдете типовые схемы развертывания MaxPatrol VM, а также инструкции по установке, первоначальной настройке, обновлению и удалению продукта.

Руководство адресовано руководителям и специалистам IT-подразделения организации, которые планируют и выполняют развертывание MaxPatrol VM.

Комплект документации MaxPatrol VM включает в себя следующие документы:

- Этот документ.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство оператора безопасности — содержит сценарии использования продукта для управления информационными активами организации.
- Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol VM для аудита активов.
- Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol VM.
- PDQL-запросы для анализа активов — содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в MaxPatrol VM.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о MaxPatrol VM (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия

Пример текста с условным обозначением	Описание
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о MaxPatrol VM

Вы можете найти дополнительную информацию о MaxPatrol VM на сайте ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 5).

2. О MaxPatrol VM

Positive Technologies MaxPatrol VM (MaxPatrol VM) обеспечивает комплексное управление уязвимостями в IT-инфраструктуре предприятия. MaxPatrol VM позволяет автоматизировать:

- управление активами;
- анализ защищенности активов ИБ;
- приоритизацию и проверку устранения уязвимостей на активах ИБ.

MaxPatrol VM можно развернуть и использовать как самостоятельно, так и в рамках единой интегрированной системы обеспечения информационной безопасности предприятия. В этом случае MaxPatrol VM поддерживает взаимодействие с другими продуктами (MaxPatrol SIEM, PT NAD), что позволяет полнее и своевременнее актуализировать модель IT-инфраструктуры предприятия, более точно оценивать защищенность предприятия и использовать эти данные при работе с сетевым трафиком.

MaxPatrol VM позволяет:

- в любой момент предоставлять пользователю и другим системам актуальную информацию об IT-инфраструктуре, полученную путем активного и пассивного сбора данных;
- объединять активы в группы по различным критериям, чтобы упростить управление активами;
- оценивать степень влияния активов на информационную безопасность предприятия в целом;
- на основе постоянно обновляемой со стороны "Позитив Текнолоджиз" базы знаний предоставлять пользователю и другим системам актуальную информацию об уязвимостях, обнаруженных на активах, и отображать степень защищенности активов;
- определять способы устранения уязвимостей и настраивать политики контроля;
- выбирать среди уязвимостей те, которые необходимо устранять в первую очередь;
- контролировать степень защищенности IT-инфраструктуры и отслеживать информацию об уязвимостях на интерактивных дашбордах;
- выгружать данные для внешних систем и выпускать отчеты для различных подразделений и должностных лиц.

В этом разделе

Архитектура MaxPatrol VM (см. раздел 2.1)

Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов (см. раздел 2.2)

2.1. Архитектура MaxPatrol VM

MaxPatrol VM состоит из программных компонентов, которые вы можете размещать как на одном сервере, так и на нескольких. Такая структура обеспечивает масштабирование и позволяет внедрять систему в компаниях любого размера.

В этом разделе

2.1.1. Компонент PT MaxPatrol 10 Core

Компонент PT MaxPatrol 10 Core (далее также — MP 10 Core) является основным компонентом системы, ее управляющим сервером. MP 10 Core устанавливается в центральном офисе компании или в крупных территориальных и функциональных подразделениях и выполняет следующие функции:

- централизованное хранение конфигурации активов;
- централизованное управление всеми компонентами системы;
- оперативное реагирование на инциденты информационной безопасности;
- обеспечение взаимодействия подразделений организации при расследовании инцидентов;
- автоматизацию процесса управления уязвимостями;
- поддержку веб-интерфейса системы.

В состав компонента входят следующие службы:

- Core Application Registration;
- Core Assets Identification;
- Core Assets Premerger;
- Core Assets Processing;
- Core Assets Projections;
- Core Assets Scans;
- Core Assets Temporal Read Model;
- Core Assets Triggers;
- Core Authorization Decision Point;

- Core Deployment Configuration;
- Core Events;
- Core Events Sources Monitoring;
- Core Events Triggers;
- Core Groups;
- Core Health Monitoring;
- Core Incidents Management;
- Core Incidents Read Model;
- Core Licensing;
- Core Notifications Management;
- Core Policies;
- Core Printing;
- Core Query Aggregator;
- Core Reporting;
- Core Reporting Delivery;
- Core Scanning;
- Core Scopes;
- Core Tables;
- Core Telemetry Collector;
- Core Topology;
- Core Topology Analyzer;
- Core Triggers;
- Core Usage Monitoring;
- Core Users Settings;
- Core Watchdog;
- Core Widgets.

2.1.2. Компонент PT MaxPatrol 10 Agent

Компонент PT MaxPatrol 10 Agent (далее также — MP 10 Agent) имеет модульную структуру и сканирует активы системы в режимах черного и белого ящика. Модули сканирования позволяют обнаруживать узлы и их открытые сетевые сервисы и проводить специализированные проверки в режиме теста на проникновение.

MP 10 Agent в режиме активного и пассивного сканирования собирает следующую информацию об активах: название, версию и производителя операционной системы, установленные обновления ОС, список установленного ПО, параметры ОС и ПО, учетные записи пользователей и их привилегии, данные об аппаратном обеспечении, запущенных сетевых сервисах и службах ОС, параметрах сети и средств защиты.

В состав компонента входят следующие модули:

— Audit — сканирование актива методом белого ящика;

— Hostdiscovery — поиск узлов методами ICMP ping, TCP ping;

— MP8ScanImporter — импорт информации об активах, обнаруженных MP8;

— Pentest — сканирование актива методом черного ящика;

— Remote Executor — удаленное исполнение сценариев одновременно на нескольких узлах и сбор результатов их выполнения.

Примечание. Существует возможность подключения модулей, разработанных сторонними производителями.

Компонент MP 10 Agent управляет перечисленными модулями и обеспечивает мониторинг их состояния, а также передачу данных между модулями и компонентом MP 10 Core. Собранные данные используются компонентом MP 10 Core для расчета уязвимости активов.

К одному компоненту MP 10 Core можно подключать несколько компонентов MP 10 Agent. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты).

В состав компонента входит служба Core Agent.

2.1.3. Компонент PT Management and Configuration

Компонент PT Management and Configuration (далее также — PT MC) обеспечивает:

— сервис единого входа в продукты "Позитив Текнолоджиз", развернутые в инфраструктуре организации;

— управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;

— журналирование действий пользователей.

В состав компонента входят следующие службы:

— MC Application Registration Management Service;

— MC Identity and Access Management Service;

— MC Notifications service;

— MC Tenant Manager Service;

— MC User Action Logging Service.

2.1.4. Компонент Knowledge Base

Компонент Knowledge Base — это единая база знаний для продуктов "Позитив Текнолоджиз". Knowledge Base содержит сведения об уязвимостях (об условиях их возникновения и способах устранения), бюллетенях безопасности и возможном ПО на активах.

В состав компонента входят следующие службы:

- KB ApiGateway service;
- KB Candidates Service;
- KB Platform Registration Service;
- KB Portal service;
- KnowledgeBase service.

2.1.5. Компонент PT Update and Configuration Service

Компонент PT Update and Configuration Service (далее также — PT UCS) — это сервис онлайн-обновления компонентов MaxPatrol VM. PT UCS обеспечивает проверку наличия, загрузку и установку новых версий компонентов, а также обновление базы данных по уязвимостям.

Для доставки компонентам новых версий PT UCS использует ПО SaltStack: модуль Salt Master находится на сервере PT UCS, модуль Salt Minion — на серверах компонентов MaxPatrol VM. PT UCS получает новые версии компонентов с глобального сервера обновлений "Позитив Текнолоджиз" и с помощью модуля Salt Master отправляет их модулям Salt Minion для установки.

2.2. Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов

Алгоритм работы MaxPatrol VM:

1. Модули компонента MP 10 Agent сканируют IT-инфраструктуру предприятия и собирают сведения о сетевых узлах. Собранные данные агенты передают в MP 10 Core.
2. Компонент MP 10 Core обрабатывает и хранит результаты сканирования с подробной информацией об обнаруженных ОС, ПО, службах, портах и прочих свойствах и связях между ними. Компонент сохраняет параметры заданий сбора данных, профили сканирования, справочники и другие параметры. MP 10 Core осуществляет контроль доступа к данным, связываясь с остальными компонентами системы для выполнения пользовательских запросов.
3. Компонент Knowledge Base содержит базу знаний, необходимых MP 10 Core для структурирования сведений об активах и обнаружения уязвимостей.
4. Используя данные Knowledge Base, компонент MP 10 Core рассчитывает уязвимости активов.

5. Компонент PT MC обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
6. Компонент PT UCS обеспечивает обновление компонентов системы и базы знаний.

Взаимодействие компонентов MaxPatrol VM отражено на схеме.

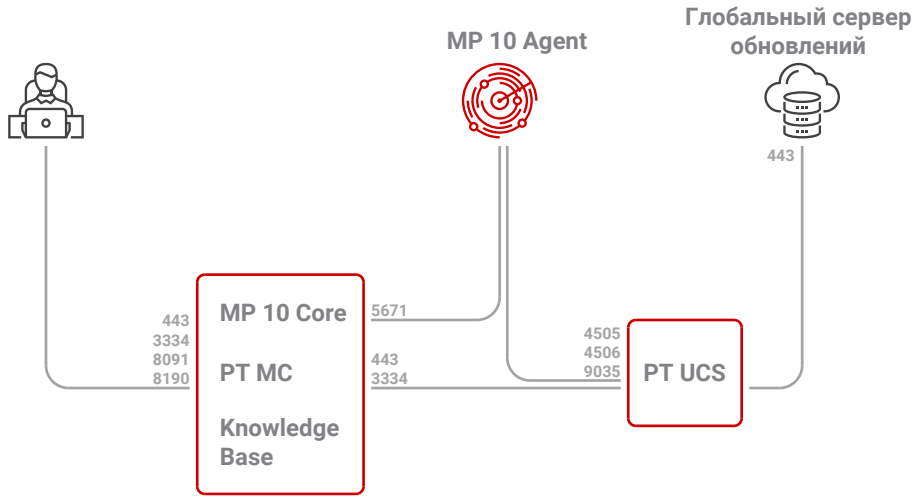

Рисунок 1. Схема взаимодействия компонентов MaxPatrol VM

Для получения обновлений межсетевой экран сервера компонента PT UCS не должен блокировать адрес глобального сервера обновлений "Позитив Текнолоджиз" — update.ptsecurity.com. Для обеспечения сетевого взаимодействия компонентов MaxPatrol VM должны быть доступны для входящих соединений перечисленные ниже порты.

Таблица 2. Компоненты и порты взаимодействия

Источник	Получатель	TCP-порт
Рабочая станция пользователя	MP 10 Core	443
MP 10 Agent	MP 10 Core	5671
PT UCS	MP 10 Core	443, 3334
Рабочая станция пользователя	PT MC	3334
Рабочая станция пользователя	Knowledge Base	8091, 8190
MP 10 Core, MP 10 Agent	PT UCS	4505, 4506, 9035
PT UCS	Глобальный сервер обновлений	443

Для исходящих соединений нет необходимости создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов рекомендуется разрешить соединения от рабочих станций администратора через порт 3389/TCP к серверам на Microsoft Windows, через порт 22/TCP — к серверам на Debian.

3. Развертывание MaxPatrol VM

Для развертывания MaxPatrol VM вам потребуется два сервера. На один сервер необходимо установить компоненты MP 10 Core , Knowledge Base, PT MC и MP 10 Agent, на другой — компонент PT UCS.

Компоненты системы могут быть установлены в виртуальной среде (см. раздел 3.3).

Если вы планируете развертывать MaxPatrol VM на базе уже развернутой системы MaxPatrol SIEM, вам не требуется устанавливать компоненты. Для работы MaxPatrol VM необходимо активировать лицензию (см. раздел 3.11), перезапустить службы компонента MP 10 Core с помощью команды `corecfg restart`, а затем выйти из системы и заново войти в нее. Вы можете развертывать MaxPatrol VM на базе MaxPatrol SIEM только в конфигурациях для средненагруженных или высоконагруженных систем.

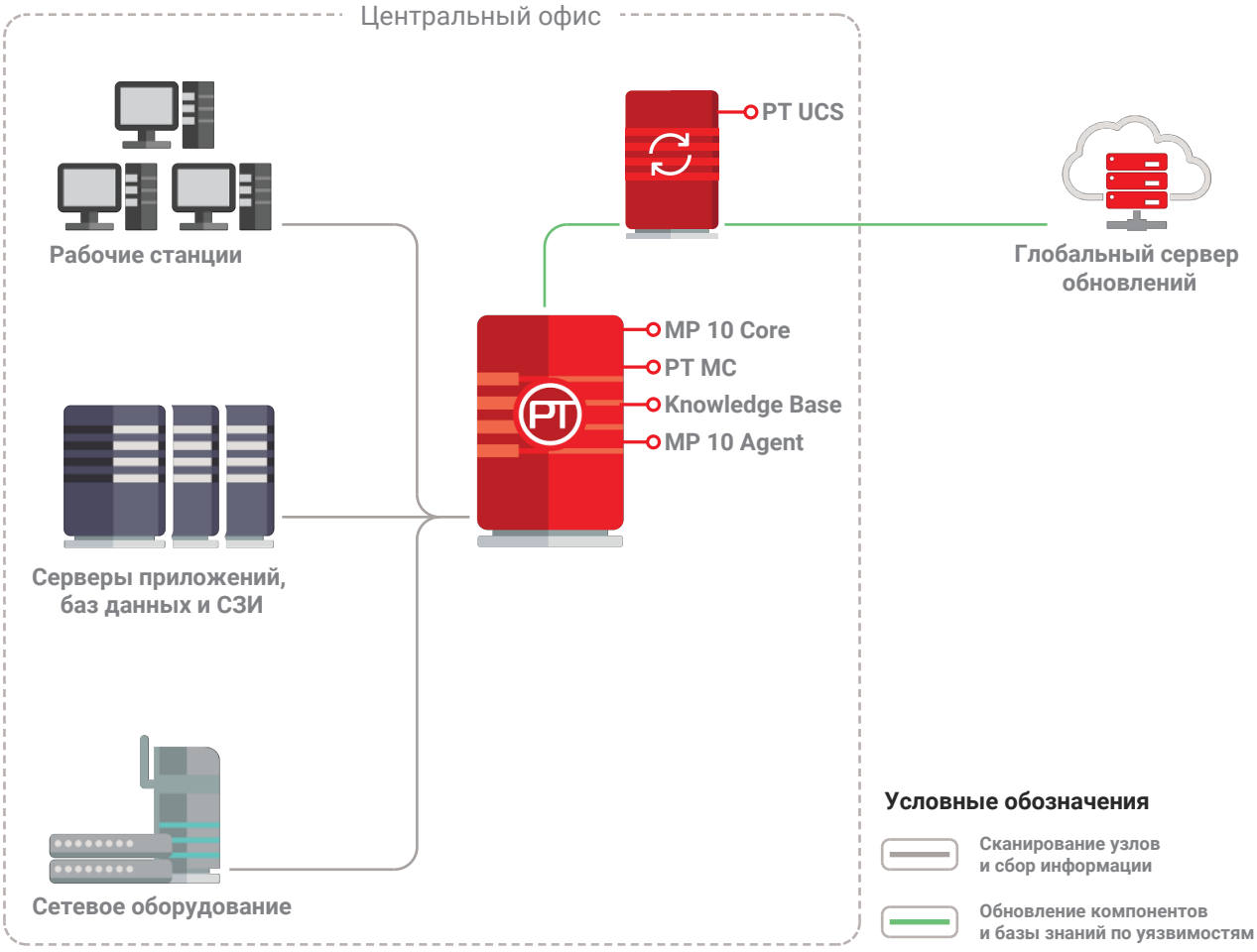

Рисунок 2. Схема развертывания MaxPatrol VM

В зависимости от физической или логической топологии IT-инфраструктуры предприятия может потребоваться сканировать узлы, расположенные в отдельных сетевых сегментах. В этом случае на каждый сегмент рекомендуется устанавливать отдельный агент. Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных агентов.

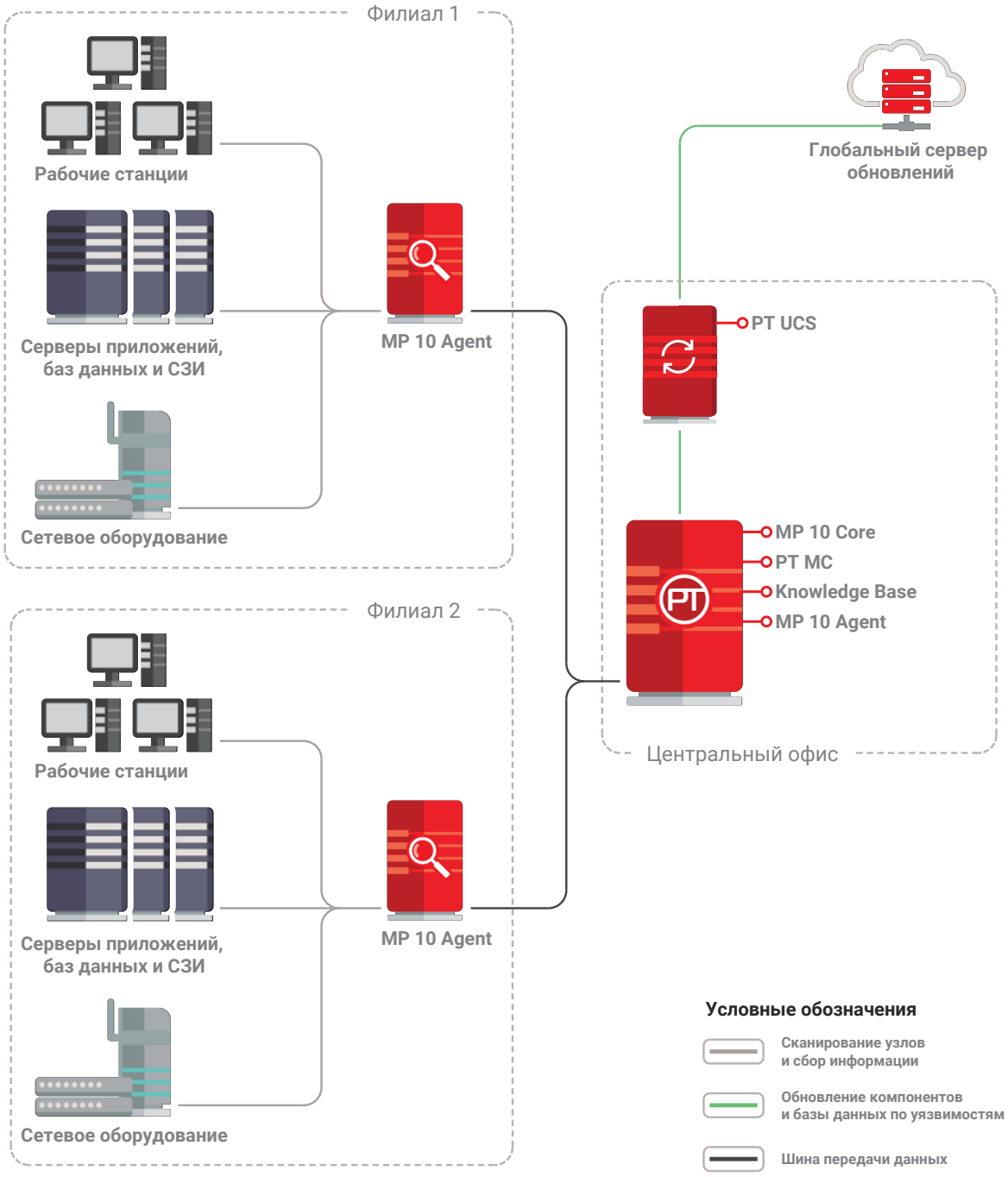

Рисунок 3. Схема развертывания MaxPatrol VM на филиальной сети

В этом разделе

3.1. Аппаратные требования к развертыванию MaxPatrol VM

Компоненты системы необходимо устанавливать на сервера, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 3. Аппаратные требования к серверу MP 10 Core, PT MC, Knowledge Base и MP 10 Agent

Компонент сервера	Минимальное требование
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 48 логических ядра
Память (ОЗУ)	64 ГБ
Сетевой адаптер	2 порта RJ-45 со скоростью 1 Гбит/с каждый
Жесткие диски и свободное дисковое пространство	Файловая система жестких дисков — NTFS, интерфейс обмена данными — SATA. Для работы ОС, установки компонентов и баз данных — RAID 10 (10 000 об./мин.), 4 диска емкостью не менее 1,2 ТБ каждый

Таблица 4. Аппаратные требования к серверу компонента MP 10 Agent, размещенному в отдельном сегменте сети

Компонент сервера	Минимальное требование
Центральный процессор	Тактовая частота 3,5 ГГц, суммарно 8 логических ядер
Память (ОЗУ)	32 ГБ

Компонент сервера	Минимальное требование
Сетевой адаптер	2 порта RJ-45 со скоростью 1 Гбит/с каждый, дополнительная сетевая карта на базе Intel i350 (2 порта RJ-45 со скоростью 1 Гбит/с каждый)
Жесткие диски и свободное дисковое пространство	Файловая система жестких дисков — NTFS, интерфейс обмена данными — SATA. Для работы ОС и установки компонентов — RAID 1 (7200 об./мин.), 2 диска емкостью не менее 1,2 ТБ каждый

3.2. Программные требования к развертыванию MaxPatrol VM

Поддерживаемые операционные системы для MP 10 Core, PT MC, Knowledge Base и MP 10 Agent:

- Microsoft Windows Server 2012;
- Microsoft Windows Server 2012 R2;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2019.

  Примечание. При развертывании компонента MP 10 Agent устанавливается драйвер WinPcap 4.1.3. Не рекомендуется дополнительно устанавливать другие версии драйвера WinPcap, поскольку работа другой версии драйвера может привести к некорректной работе модуля hostdiscovery.

Поддерживаемая операционная система для PT UCS — Debian 10.x.

Примечание. Для установки или обновления Debian необходимо использовать полный установочный образ. Он содержит необходимый набор пакетов и не требует подключения к интернету (подробнее см. на сайте debian.org).

Компоненты на Debian не поддерживают пакеты SaltStack, установленные помимо указаний "Позитив Текнолоджиз".

Примечание. Если такие пакеты установлены на сервере, перед развертыванием компонентов необходимо удалить пакеты с помощью команды `apt-get --purge autoremove salt-minion`, а также удалить ссылки на репозиторий salt с помощью команды `rm /etc/apt/sources.list.d/saltstack*`.

Поддерживаемые браузеры:

- Google Chrome 49 и выше;
- Mozilla Firefox 45 и выше.

3.3. Рекомендации по развертыванию MaxPatrol VM в виртуальной среде

Рекомендуется использовать версию 11 виртуальной машины VMware vSphere и версию 6.0 гипервизора VMware ESXi с приведенными ниже параметрами распределения ресурсов.

Настройка гипервизора

Рекомендуется использовать технологию Storage I/O Control при обмене данными между гипервизором и хранилищами, содержащими виртуальные машины, на которых будут развернуты компоненты системы.

Настройка центрального процессора

В аппаратных требованиях к центральному процессору указано минимальное количество логических ядер. Если сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить вдвое меньше физических ядер. Если технология Hyperthreading не используется, количество выделенных физических ядер должно быть равно количеству логических. Например, если виртуальной машине требуется 56 логических ядер и сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить два процессора по 14 ядер каждый.

Для повышения производительности виртуальной машины рекомендуется в блоке параметров **Hyperthreaded Core Sharing** выбрать режим **None**, в блоке параметров **Resource Allocation** передвинуть максимально вправо ползунок **Reservation** и установить флажок **Unlimited**.

Настройка оперативной памяти

Объем оперативной памяти, выделяемой каждой виртуальной машине, не должен быть меньше значения, указанного в аппаратных требованиях. Также необходимо учитывать, что часть оперативной памяти сервера (до 8% от общего объема) должна быть зарезервирована для работы гипервизора.

Для работы виртуальной машины рекомендуется зарезервировать постоянный объем оперативной памяти, установив в блоке параметров **Resources Allocation** флажок **Reserve all guest memory (All locked)**.

Настройка виртуальных жестких дисков

Объем и производительность виртуальных жестких дисков не должны быть меньше значений, указанных в аппаратных требованиях.

При создании виртуального жесткого диска на шаге **Create a Disk** в блоке параметров **Disk Provisioning** рекомендуется выбрать вариант **Thick Provision Eager Zeroed**, на шаге **Advanced Options** в блоке параметров **Mode** рекомендуется установить флажок **Independent**, а затем выбрать вариант **Persistent**.

3.4. Подготовка к развертыванию MaxPatrol VM

Для развертывания MaxPatrol VM вам потребуются следующие файлы из комплекта поставки:

- `MPXCoreSetup_<Номер версии>.exe` — дистрибутив компонентов MP 10 Core, PT MC и Knowledge Base;
- `MPXAgentSetup_<Номер версии>.exe` — дистрибутив компонента MP 10 Agent;
- `ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar` — архив с дистрибутивами компонента PT UCS.

Развертывание MaxPatrol VM делится на следующие этапы:

1. Установка компонентов MP 10 Core, PT MC и Knowledge Base.
2. Установка компонентов MP 10 Agent.
3. Установка и настройка компонента PT UCS.
4. Настройка MaxPatrol VM для обеспечения его безопасной работы.
5. Активация лицензии.

Перед началом развертывания необходимо:

- разместить папку `packages` и файл `setup.json` в одной папке с файлом `MPXCoreSetup_<Номер версии>.exe`;
- выделить не менее 4 ГБ свободного места на жестком диске сервера для файла подкачки;
- убедиться, что учетная запись администратора ОС сервера MP 10 Core имеет привилегии SeSecurity, SeBackup и SeDebug.

  Примечание. Вы можете проверить наличие указанных привилегий, выполнив команду `whoami /priv` в командной строке Microsoft Windows от имени администратора.

3.5. Установка компонентов MP 10 Core, PT MC и Knowledge Base

Если мастер установки предложит перезагрузить операционную систему, вам необходимо подтвердить перезагрузку. После перезагрузки установка будет продолжена автоматически.

► Чтобы установить компоненты MP 10 Core, PT MC и Knowledge Base:

1. Запустите файл `MPXCoreSetup_<Номер версии>.exe`.

   Откроется окно мастера установки.

2. Если вы даете согласие на сбор, хранение и передачу в "Позитив Текнолоджиз" данных о срабатывании правил корреляции и версиях служб, установите флажок **Я разрешаю передачу обезличенных данных об использовании системы**.

Примечание. Передаваемые данные используются для повышения качества поставляемой экспертизы.

3. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
4. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
5. Укажите пути для установки.

   Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.
6. Нажмите кнопку **Продолжить**.
7. В поле **Адрес сервера PT MaxPatrol 10 Core** укажите IP-адрес или FQDN сервера MP 10 Core.
8. Если вы хотите активировать лицензию при установке компонентов системы, установите флажок **Активировать лицензию**, укажите путь к файлу лицензии и введите ключ активации лицензии.

   Примечание. Для активации лицензии во время установки компонентов системы необходим доступ к интернету. Также вы можете активировать лицензию (см. раздел 3.11) после установки компонентов — как при наличии доступа к интернету, так и при его отсутствии.
9. В раскрывающемся меню **Язык интерфейса MaxPatrol VM** выберите желаемый язык интерфейса MaxPatrol VM.
10. Нажмите кнопку **Продолжить**.

    Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

    Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. Вам необходимо вернуться, нажимая кнопку **Назад**, и указать корректные значения параметров.
11. Нажмите кнопку **Установить**.
12. По завершении установки нажмите кнопку **Закрыть**.

Компоненты MP 10 Core, PT MC и Knowledge Base установлены.

3.6. Установка компонента MP 10 Agent

Если мастер установки предложит перезагрузить операционную систему, вам необходимо подтвердить перезагрузку. После перезагрузки установка будет продолжена автоматически.

► Чтобы установить компонент MP 10 Agent:

1. Запустите файл `MPXAgentSetup_<Номер версии>.exe`.

Откроется окно мастера установки.

2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
4. Укажите пути для установки.

   Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.
5. Нажмите кнопку **Продолжить**.
6. В поле **Имя агента** введите имя агента, которое будет отображаться в интерфейсе MaxPatrol VM.
7. В поле **Адрес сервера PT MaxPatrol 10 Core** укажите IP-адрес или FQDN сервера MP 10 Core.
8. Нажмите кнопку **Продолжить**.

   Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

   Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. Вам необходимо вернуться, нажимая кнопку **Назад**, и указать корректные значения параметров.
9. Нажмите кнопку **Установить**.
10. По завершении установки нажмите кнопку **Закрыть**.

Компонент MP 10 Agent установлен.

3.7. Установка компонента PT UCS

► Чтобы установить компонент PT UCS:

1. Распакуйте архив `ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar`:

   ```
   tar -xf ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar -C <Путь к каталогу для распаковки архива>
   ```
2. Запустите сценарий:

   ```
   <Путь к каталогу для распаковки архива>/siem-ucs-debian<Номер версии Debian>-<Номер версии MaxPatrol VM>/install.sh
   ```

   Откроется окно **UCS configuration**.
3. Выберите вариант **Basic**.

   Откроется страница со списком основных параметров.

4. Укажите значение параметра SaltMasterHost:
   ```
   SaltMasterHost: <IP-адрес или FQDN сервера компонента PT UCS>
   ```
5. Нажмите кнопку **Yes**.

   Запустится установка PT UCS. По завершении установки интерфейс терминала Debian отобразит сообщение:
   ```
   Done installing ucs-pt
   ```

Компонент PT UCS установлен.

3.8. Настройка компонента PT UCS

- Чтобы настроить компонент PT UCS:

1. На серверах компонентов MaxPatrol VM под управлением Microsoft Windows выполните команду:
   ```
   saltcfg set -p SaltMasterHost <IP-адрес или FQDN компонента PT UCS>
   ```
2. На сервере PT UCS выполните команду:
   ```
   salt-key -L
   ```
   Интерфейс терминала Debian в списке `Unaccepted Keys` выведет названия неавторизованных модулей Salt Minion (по умолчанию в качестве названий используются FQDN серверов).
3. Авторизуйте модули Salt Minion:
   ```
   salt-key -a <FQDN сервера с модулем Salt Minion>
   ```
4. На сервере MP 10 Core измените параметр `SaltMasterHost`:
   ```
   corecfg set -p SaltMasterHost <IP-адрес или FQDN компонента PT UCS>
   ```

Компонент PT UCS настроен.

3.9. Настройка MaxPatrol VM для обеспечения его безопасной работы

Компоненты системы рекомендуется разместить в доверенном сегменте сети. Доступ к ним из других сегментов рекомендуется ограничить с помощью межсетевого экрана.

► Чтобы настроить MaxPatrol VM:

1. На серверах MP 10 Core и MP 10 Agent удалите все правила удаленного доступа по протоколу RDP:

   ```
   netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389
   netsh advfirewall firewall delete rule name=all protocol=udp localport=3389
   ```

2. Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:

   ```
   netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in action=allow
   protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>
   netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in action=allow
   protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>
   ```

3. На сервере MP 10 Core удалите все правила доступа для входящих соединений через TCP-порты 443, 3333, 3334, 8091, 8190, 5671, 5672, 8703, 8704, 8740, 8721 и 8799:

   ```
   for %P IN (443,3333,3334,8091,8190,5671,5672,8703,8704,8740,8721,8799) DO (netsh
   advfirewall firewall delete rule name=all protocol=tcp localport=%P)
   ```

4. Разрешите доступ к веб-интерфейсу системы только с рабочих станций пользователей:

   ```
   netsh advfirewall firewall add rule name="Allow MaxPatrol VM for users" dir=in
   action=allow protocol=tcp localport=443,3334,8091,8190 remoteip=<IP-адреса рабочих станций
   пользователей>
   ```

5. Разрешите входящие соединения от агентов через TCP-порт 5671:

   ```
   netsh advfirewall firewall add rule name="Allow MP 10 Core for agents" dir=in action=allow
   protocol=tcp localport=5671 remoteip=<IP-адрес сервера агента>
   ```

6. Разрешите входящие соединения от сервера PT UCS через TCP-порты 443, 3334:

   ```
   netsh advfirewall firewall add rule name="Allow MP 10 Core for PT UCS" dir=in action=allow
   protocol=tcp localport=443,3334 remoteip=<IP-адрес сервера PT UCS>
   ```

7. На сервере MP 10 Agent удалите все правила для входящих соединений через TCP-порты 514, 1468 и UPD-порты 514, 2055:

   ```
   for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all protocol=tcp
   localport=%P)
   for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all protocol=udp
   localport=%P)
   ```

8. На сервере PT UCS добавьте правила межсетевого экрана:

   ```
   iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
   iptables -A INPUT -i lo -j ACCEPT
   iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
   iptables -A INPUT -s <IP-адрес рабочей станции администратора или маска подсети, где
   находятся рабочие станции, в формате CIDR> -p tcp --dport 22 -m conntrack --ctstate NEW -m
   comment --comment "SSH admin access" -j ACCEPT
   iptables -A INPUT -s <IP-адрес сервера MP 10 Core> -p tcp -m multiport --dports
   4505,4506,9035 -m conntrack --ctstate NEW -m comment --comment "from MP 10 Core to PT UCS"
   -j ACCEPT
   ```

9. Заблокируйте все входящие соединения, кроме разрешенных:

   ```
   iptables -A INPUT -j DROP
   ```

10. Установите пакет iptables-persistent:

    ```
    apt-get install iptables-persistent
    ```

11. Сохраните правила межсетевого экрана:
    ```
    netfilter-persistent save
    ```
12. Смените пароли служебных учетных записей в MaxPatrol VM (подробнее см. Руководство администратора).
13. Убедитесь, что пароли для входа в операционные системы серверов MP 10 Core и MP 10 Agent соответствуют требованиям к сложности, установленным на предприятии.
14. Установите собственные доверенные сертификаты (см. раздел 3.10) для MP 10 Core, Knowledge Base, PT MC и RabbitMQ.
15. На сервере PT UCS для каждого администратора MaxPatrol VM создайте отдельную учетную запись:
    ```
    adduser <Логин администратора>
    ```
16. На рабочих станциях администраторов MaxPatrol VM сгенерируйте ключевую пару.

    Примечание. Для генерации ключевой пары на Debian вы можете использовать утилиту ssh-keygen, на Microsoft Windows — PuTTygen.
17. На сервере PT UCS добавьте открытый ключ в файл `/home/<Логин администратора>/.ssh/authorized_keys`.
18. В файле `/etc/ssh/sshd_config` раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):
    ```
    PubkeyAuthentication yes
    RhostsRSAAuthentication no
    HostbasedAuthentication no
    PermitEmptyPasswords no
    PasswordAuthentication no
    ```
19. В файле `/etc/sudoers` измените значение параметра:
    ```
    <Логин администратора> ALL=(ALL) ALL
    ```
20. Для каждого пользователя MaxPatrol VM создайте отдельную учетную запись.
21. Смените пароль учетной записи Administrator.

MaxPatrol VM настроен.

3.10. Установка доверенных сертификатов для компонентов MP 10 Core, Knowledge Base и PT MC

При установке компонентов MP 10 Core, Knowledge Base и PT MC для их веб-сайтов автоматически устанавливаются самоподписанные сертификаты, поставляемые в составе дистрибутива. Поэтому при попытке подключения к веб-сайту вы получите предупреждение о том, что создаваемое подключение не защищено.

Для компонента PT MC также автоматически устанавливается самоподписанный сертификат для подписи маркера временного доступа. Этот сертификат необходим для взаимодействия PT MC с другими продуктами "Позитив Текнолоджиз".

Вы можете установить собственные доверенные сертификаты. Такие сертификаты должны отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- иметь длину закрытого ключа не менее 2048 бит;
- включать область применения сертификата: Digital Signature или Key Encipherment;
- иметь следующие значения параметров SAN: `DNS:localhost`, `IP:127.0.0.1`, `DNS:<FQDN сервера MP 10 Core>`, `DNS:<IP-адрес сервера MP 10 Core>`, `IP:<IP-адрес сервера MP 10 Core>`.

► Чтобы установить доверенные сертификаты для компонентов MP 10 Core, Knowledge Base и PT MC:

1. Разместите сертификаты в хранилище Local Computer\Personal.
2. Если вы хотите установить доверенный сертификат для веб-сайтов компонентов MP 10 Core и PT MC, выполните команду:
   ```
   corecfg set -p SSLCertificateThumb <Отпечаток сертификата>
   ```
   При установке сертификата утилита `corecfg.exe` выдает пользователю права на его чтение (NT AUTHORITY\NETWORK SERVICE).
3. Если вы хотите установить доверенный сертификат для веб-сайта компонента Knowledge Base, выполните команду:
   ```
   kbcfg set -p SSLCertificateThumb <Отпечаток сертификата>
   ```
4. Если вы хотите установить доверенный сертификат для подписи маркера временного доступа, выполните команду:
   ```
   mccfg set -p TokensCertificateThumb <Отпечаток сертификата>
   ```

Доверенные сертификаты для компонентов MP 10 Core, Knowledge Base и PT MC установлены.

3.11. Активация лицензии MaxPatrol VM

Для работы MaxPatrol VM необходимо активировать лицензию. Активацию лицензии необходимо выполнять на сервере с компонентом MP 10 Core при развертывании MaxPatrol VM или по истечении срока действия предыдущей лицензии.

Лицензия поставляется вместе с дистрибутивами системы и представляет собой файл, содержащий информацию о типе лицензии и сроке ее действия.

Для активации MaxPatrol VM вам потребуются следующие файлы из комплекта поставки:

- `GuardantActivationWizard.exe` — мастер активации лицензии Guardant;
- `<Имя файла>.grdvd` — файл лицензии;
- `<Имя файла>.txt` — текстовый файл с серийным номером лицензии.

Перед активацией лицензии необходимо установить драйверы электронных ключей Guardant (подробное описание см. на сайте производителя) и разместить мастер активации лицензии и файл лицензии в одной папке.

> **Примечание.** Перед активацией новой лицензии рекомендуется удалить ключ предыдущей лицензии (см. раздел 3.11.3).

После изменения аппаратной конфигурации сервера MP 10 Core (например, по причине замены центрального процессора) необходимо повторно активировать лицензию. Количество повторных активаций, причиной которых явилось изменение аппаратной конфигурации, ограничено — не более пяти раз. Дальнейшие попытки активации приведут к ошибке мастера активации "Количество активаций для введенного серийного номера исчерпано". Для получения новой лицензии необходимо обращаться в службу технической поддержки (см. раздел 5). Если вы повторно активировали лицензию (например, после переустановки ОС или компонента MP 10 Core) и при этом не изменяли аппаратную конфигурацию сервера, счетчик активаций не уменьшается (количество таких повторных активаций не ограничено).

В этом разделе

3.11.1. Активация лицензии при наличии доступа к интернету

- Чтобы активировать лицензию MaxPatrol VM:

  1. Запустите файл `GuardantActivationWizard.exe`.

     Откроется окно мастера активации лицензий Guardant.

  2. Нажмите кнопку **Далее**.

  3. Введите серийный номер лицензии и нажмите кнопку **Далее**.

     Запустится процесс активации лицензии MaxPatrol VM. По завершении активации окно мастера активации лицензий Guardant отобразит сообщение об успешной активации MaxPatrol VM.

  4. Нажмите кнопку **Готово**.

  Лицензия активирована.

3.11.2. Активация лицензии при отсутствии доступа к интернету

► Чтобы активировать лицензию MaxPatrol VM:

1. На сервере с компонентом MP 10 Core запустите файл `GuardantActivationWizard.exe`.

   Откроется окно мастера активации лицензий Guardant.

2. Установите флажок **Режим offline** и нажмите кнопку **Далее**.

3. Введите серийный номер лицензии и нажмите кнопку **Далее**.

   Мастер активации лицензий Guardant создаст файл `<Имя файла>.toserver`. Папка с файлом откроется автоматически.

4. Нажмите кнопку **Готово**.

5. Переместите файлы `GuardantActivationWizard.exe` и `<Имя файла>.toserver` в одну папку на рабочую станцию с доступом в интернет.

6. На рабочей станции запустите файл `GuardantActivationWizard.exe`.

   Откроется окно мастера активации лицензий Guardant.

7. Нажмите кнопку **Указать файл лицензии**.

8. В открывшемся окне выберите файл `<Имя файла>.toserver` и нажмите кнопку **Открыть**.

9. Нажмите кнопку **Далее**.

   Мастер активации лицензий Guardant создаст файл `<Имя файла>.fromserver`. Папка с файлом откроется автоматически.

10. Нажмите кнопку **Готово**.

11. Переместите файл `<Имя файла>.fromserver` на сервер с компонентом MP 10 Core в папку с файлом `GuardantActivationWizard.exe`.

12. На сервере с компонентом MP 10 Core запустите файл `GuardantActivationWizard.exe`.

    Откроется окно мастера активации лицензий Guardant.

13. Нажмите кнопку **Указать файл лицензии**.

14. В открывшемся окне выберите файл `<Имя файла>.fromserver` и нажмите кнопку **Открыть**.

15. Нажмите кнопку **Далее**.

Запустится процесс активации лицензии MaxPatrol VM. По завершении активации окно мастера активации лицензий Guardant отобразит сообщение об успешной активации MaxPatrol VM.

16. Нажмите кнопку **Готово**.

Лицензия активирована.

3.11.3. Удаление лицензии

Перед удалением лицензии необходимо убедиться, что на сервере MP 10 Core установлено ПО Guardant SDK (подробнее см. на сайте guardant.ru).

► Чтобы удалить лицензию:

1. Запустите утилиту диагностики `C:\Program Files (x86)\Guardant\SDK7\Bin\grddiag.exe`.

   Откроется окно **Поиск и проверка ключей**, содержащее список установленных ключей.

2. В контекстном меню ключа удаляемой лицензии выберите пункт **Удалить ключ Guardant SP из системы** и подтвердите удаление.

Лицензия удалена.

4. Удаление MaxPatrol VM

Для удаления MaxPatrol VM вы можете запустить сценарий или удалить компоненты продукта стандартными средствами Microsoft Windows. При удалении MaxPatrol VM вы можете также удалить пользовательские данные и установленные при развертывании MaxPatrol VM компоненты сторонних производителей.

В этом разделе

4.1. Удаление компонента MaxPatrol VM стандартными средствами Microsoft Windows

- Чтобы удалить компонент MaxPatrol VM стандартными средствами Microsoft Windows:

  1. В контекстном меню кнопки **Пуск** выберите пункт **Программы и компоненты**.
  2. В списке установленных программ выберите компонент MaxPatrol VM и нажмите кнопку **Удалить/Изменить**.

     Откроется окно мастера удаления компонента MaxPatrol VM.
  3. Нажмите кнопку **Удалить**.
  4. Если требуется удалить пользовательские данные, установите флажок **Удалить данные приложений**.
  5. Нажмите кнопку **Удалить**.

     Запустится процесс удаления компонента MaxPatrol VM.
  6. По завершении удаления нажмите кнопку **Закрыть**.

  Компонент MaxPatrol VM удален.

4.2. Удаление MaxPatrol VM с помощью сценария

Сценарий необходимо запускать в интерфейсе командной строки Windows PowerShell от имени администратора.

- Чтобы удалить MaxPatrol VM с помощью сценария:

  1. Запустите сценарий удаления:

     ```
     powershell -ExecutionPolicy ByPass -File <Путь к папке со сценарием>\ProductCleanUp.ps1
     ```

Сценарий удаления соберет информацию о путях установки компонентов, расположении пользовательских данных и сохранит ее в файле `ProductCleanUpSettings.json`. По завершении сбора информации интерфейс командной строки Windows PowerShell отобразит сообщение:

```
Select a delete mode:
1 - Delete only MaxPatrol VM components
2 - Delete all (full cleanup)
0 - Cancel operation
```

Примечание. При повторном запуске сценария удаления вы можете загружать информацию о путях установки из файла `ProductCleanUpSettings.json`, созданного при первоначальном запуске сценария.

2. Выберите вариант удаления:

   - Если необходимо удалить только компоненты MaxPatrol VM, введите `1`.
   - Если необходимо удалить компоненты MaxPatrol VM, пользовательские данные и установленные компоненты сторонних производителей (полное удаление продукта), введите `2`.

3. Для подтверждения удаления введите `Yes`.

   Запустится процесс удаления MaxPatrol VM. По завершении удаления интерфейс командной строки Windows PowerShell отобразит сообщение:

   ```
   Execution finished
   ```

Компонент MaxPatrol VM удален.

5. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

5.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

5.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по телефону +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языках.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

5.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

5.4. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

Предоставление информации для технической поддержки (см. раздел 5.4.1)

Типы запросов (см. раздел 5.4.2)

Время реакции и приоритизация запросов (см. раздел 5.4.3)

Выполнение работ по запросу (см. раздел 5.4.4)

5.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

5.4.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

5.4.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 5).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 5. Время реакции на запрос и время его обработки

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

5.4.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение А. Параметры конфигурации компонентов MaxPatrol VM на Microsoft Windows

Раздел содержит описание параметров конфигурации компонентов MaxPatrol VM на Microsoft Windows. Инструкции по изменению параметров приведены в Руководстве администратора.

Таблица 6. Параметры конфигурации компонента MP 10 Core

Параметр	Описание	Значение по умолчанию
`CollectCorrelationTelemetry`	Если запущен сбор данных (параметр `CollectTelemetry` равен `True`), собираются (`True`) или не собираются (`False`) данные о срабатывании правил корреляции	`True`
`CollectProductTelemetry`	Если запущен сбор данных (параметр `CollectTelemetry` равен `True`), собираются (`True`) или не собираются (`False`) данные о версиях служб MaxPatrol VM	`True`
`CollectTelemetry`	Система собирает (`True`) или не собирает (`False`) данные о своей работе	`False`
`ConsiderEventsImportance`	В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (`True`) или по расписанию (`False`)	`True`
`DefaultAssetTtl`	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	`90.00:00:00`
`DefaultLocale`	Интерфейс MaxPatrol VM отображается на русском (`ru-RU`) или английском (`en-US`) языке	`ru-RU`
`EmailNotificationRetryCount`	Максимальное количество попыток отправки сообщения на SMTP-сервер	`10`

Параметр	Описание	Значение по умолчанию
EmailNotificationRetryPeriodSeconds	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	60
HostAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
MicroservicesCertificateThumb	Отпечаток сертификата, используемого службами MP 10 Core для взаимодействия между собой	7EA87DDE95A95FD2D2BA8C9C1237110A9177DA46
MongoDbAuthSource	Имя базы данных, где хранятся учетные данные пользователей СУБД MongoDB	admin
MongoDbHost	IP-адрес или FQDN сервера СУБД MongoDB	localhost
MongoDbLogin	Логин служебной учетной записи для подключения MP 10 Core к СУБД MongoDB	admin
MongoDbPassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД MongoDB	P@ssw0rd
MongoDbPort	Порт сервера СУБД MongoDB для входящих подключений от MP 10 Core	27017
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	pt_system
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	—
PtkbFeatureHost	IP-адрес или FQDN сервера Knowledge Base	localhost

Параметр	Описание	Значение по умолчанию
PtmcHostAddress	IP-адрес или FQDN сервера PT MC	localhost
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd
RMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O
RMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	C:\Program Files\Positive Technologies\MaxPatrol 10 Core \.install\scripts\Certificates \RMQ_Core_Client.p12
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SaltMasterHost	IP-адрес или FQDN сервера с модулем SaltMaster	—
SaltMasterPort	Порт сервера с модулем SaltMaster для входящих подключений от MP 10 Core	9035
SendTelemetry	Система отправляет (True) или не отправляет (False) собранные данные в "Позитив Текнолоджиз"	False
ServicesRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
ServicesRMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd
ServicesRMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O

Параметр	Описание	Значение по умолчанию
ServicesRMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	C:\Program Files\Positive Technologies\MaxPatrol 10 Core\.install\scripts\Certificates\RMQ_Core_Client.p12
ServicesRMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
ServicesRMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
ServicesRMQVirtualHost	Имя виртуального узла RabbitMQ	/
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpPassword	Пароль служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от MP 10 Core	25
SmtpSender	Значение поля "Отправитель" в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtpSslEnabled	Для подключения к SMTP-серверу службы MP 10 Core используют защищенное (True) или незащищенное (False) соединение	False
SmtpUseDefaultCredentials	Для аутентификации на SMTP-сервере используются логин и пароль служебной учетной записи Network Service (True) или логин и пароль, указанные в параметрах SmtpUser и SmtpPassword (False)	True
SmtpUser	Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—

Параметр	Описание	Значение по умолчанию
SSLCertificateThumb	Отпечаток сертификата для веб-сайта компонентов MP 10 Core и PT MC	805A6F12A9BF2978BCC718D718DB7E9F269E2D53
SsoClientId	Идентификатор для регистрации приложения MaxPatrol 10 в PT MC	mpx
SsoClientSecret	Ключ для регистрации приложения MaxPatrol 10 в PT MC	eea74278-ff80-4268-9934-51de0a2c8d7e
StopOnMicroserviceError	Службы MP 10 Core останавливаются (True) или не останавливаются (False) при возникновении ошибки в их работе	False
TtlCheckPeriod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsePtbkServer	MP 10 Core проверяет (True) или не проверяет (False) наличие обновления базы знаний об уязвимостях в Knowledge Base	True

Таблица 7. Параметры конфигурации компонента MP 10 Agent

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode1	—

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode1	—
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	20480M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	—
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди сообщений. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди сообщений. При достижении порогового значения агент переходит в режим SafeMode1	—
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	—

Параметр	Описание	Значение по умолчанию
AgentName	Имя агента в веб-интерфейсе MaxPatrol VM	FQDN сервера MP 10 Agent
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	C:\Program Files (x86)\Positive Technologies\MaxPatrol 10 Agent\.install\scripts\Certificates\rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	C:\Program Files (x86)\Positive Technologies\MaxPatrol 10 Agent\.install\scripts\Certificates\RMQ_Agent_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	C:\Program Files (x86)\Positive Technologies\MaxPatrol 10 Agent\.install\scripts\Certificates\RMQ_Agent_Client.key
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Agent к RabbitMQ	P@ssw0rd
RMQPort	Порт сервера RabbitMQ для входящих подключений от MP 10 Agent	5671
RMQUser	Логин служебной учетной записи для подключения MP 10 Agent к RabbitMQ	mpx_agent
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SSLEnabled	MP 10 Agent подключается к RabbitMQ через защищенное (True) или незащищенное (False) соединение	True

Таблица 8. Параметры конфигурации компонента Knowledge Base

Параметр	Описание	Значение по умолчанию
`ClientId`	Идентификатор для регистрации приложения Knowledge Base в PT MC	`ptkb`
`ClientSecret`	Ключ для регистрации приложения Knowledge Base в PT MC	`secret`
`CoreAddress`	IP-адрес или FQDN сервера MP 10 Core	`localhost`
`DatabaseBackupFolder`	Путь к папке для хранения резервной копии БД	`C:\ProgramData\Positive Technologies\Knowledge Base\ \data\backup`
`DatabaseConnectionString`	Строка для подключения к БД PostgreSQL	—
`DefaultLocale`	Интерфейс Knowledge Base отображается на русском (`ru-RU`) или английском (`en-US`) языке	—
`DeploymentType`	Тип развертывания Knowledge Base	—
`DisplayName`	Название приложения Knowledge Base в PT MC	`Knowledge Base`
`EnableMPXAuth`	Аутентификация пользователей выполняется локально (`True`) или через LDAP (`False`)	`True`
`FrontendBindingPort`	Порт для подключения к веб-интерфейсу Knowledge Base	`8091`
`HostAddress`	IP-адрес или FQDN сервера Knowledge Base	`localhost`
`IamPort`	Порт сервера PT MC для входящих подключений от Knowledge Base к службе MC Identity and Access Management Service	`3334`
`IdentityServerAddress`	IP-адрес или FQDN сервера PT MC	`localhost`

Параметр	Описание	Значение по умолчанию
IdentityServerPort	Порт сервера PT MC для входящих подключений от Knowledge Base к службе MC User Action Logging Service	3333
InternalServicePort	Порт для подключения к API Knowledge Base	8190
MaxPortalPort	Порт сервера MP 10 Core для входящих подключений от Knowledge Base	443
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RegistrationId	Идентификатор Knowledge Base для регистрации в службе MC Tenant Manager Service	50dfcc46-fbf1-48f5-909b-ac90ca45567c
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpPassword	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от Knowledge Base	25

Параметр	Описание	Значение по умолчанию
SmtpSender	Значение поля "Отправитель" в уведомлении, отправляемом по электронной почте	Knowledge Base Notification System <NoReply@knowledgebase.com>
SmtpUseDefaultCredentials	Для аутентификации на SMTP-сервере используются логин и пароль служебной учетной записи Network Service (True) или логин и пароль, указанные в параметрах SmtpUser и SmtpPassword (False)	True
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
SSLCertificateThumb	Отпечаток сертификата для веб-сайта компонента Knowledge Base	805A6F12A9BF2978BCC718D718DB7E9F269E2D53
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics
TempDataDir	Путь к папке для хранения временных файлов Knowledge Base	C:\ProgramData\Positive Technologies\Knowledge Base\\tmp
TmPort	Порт сервера PT MC для входящих подключений от Knowledge Base к службе MC Tenant Manager Service	8703

Таблица 9. Параметры конфигурации компонента PT MC

Параметр	Описание	Значение по умолчанию
ActionLogBatchSize	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service единовременно отправляет службе MC User Action Logging Service	100

Параметр	Описание	Значение по умолчанию
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
DataProtectionFilePath	Путь к папке с ключами для шифрования файлов cookies	/ptmc-shared-keys
DefaultLocale	Интерфейс PT MC отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
HostAddress	IP-адрес или FQDN сервера PT MC	localhost
IamCookieLifetime	Продолжительность жизни неактивной сессии в MaxPatrol VM (в часах)	168
IamSecret	Идентификатор для регистрации приложения Management and Configuration в PT MC	—
LdapTimeout	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	60000
LogCleanLimit	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	1000000
LogCleanTimeout	Период между проверками количества сохраненных записей о действиях пользователей (в миллисекундах)	5000
MasterRedirectEnabled	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (True) или на локальной (False) площадке	True
MicroservicesCertificateThumb	Отпечаток сертификата, используемого службами MP 10 Core при взаимодействии между собой	7EA87DDE95A95FD2D2BA8C9C1237110A9177DA46
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost

Параметр	Описание	Значение по умолчанию
PostgrePassword	Пароль служебной учетной записи для подключения PT MC к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для подключения PT MC к СУБД PostgreSQL	pt_system
SSLCertificateThumb	Отпечаток сертификата для веб-сайта компонентов MP 10 Core и PT MC	805A6F12A9BF2978BCC718D718DB7E9F269E2D53
TmSiteAlias	Псевдоним площадки	SITE
TmSiteId	Идентификатор площадки	—
TmTenantManagerId	Идентификатор службы MC Tenant Manager Service	—
TokensCertificateThumb	Отпечаток сертификата для подписи и валидации маркеров доступа	805A6F12A9BF2978BCC718D718DB7E9F269E2D53

Таблица 10. Параметры конфигурации утилиты rabbitmqcfg

Параметр	Описание	Значение по умолчанию
AdminPassword	Пароль администратора RabbitMQ	guest
CACertFile	Путь к файлу корневого сертификата	C:\ProgramData\RabbitMQ/tls/rootCA.crt
CertFile	Путь к файлу публичного сертификата	C:\ProgramData\RabbitMQ/tls/RMQ_Server.crt
KeyFile	Путь к файлу закрытого ключа сертификата	C:\ProgramData\RabbitMQ/tls/RMQ_Server.pem

Параметр	Описание	Значение по умолчанию
MEMORY_HIGH_WATERMARK	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений	10GB
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах). **Примечание.** Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	20
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	0.5

Таблица 11. Параметры конфигурации утилиты mongodbcfg

Параметр	Описание	Значение по умолчанию
CacheSizeGB	Максимальный размер кэша (в гигабайтах)	1
DBPath	Путь к папке для хранения данных	C:\ProgramData\MongoDB\data\
ListenOnlyLocal	СУБД MongoDB доступна как для локальных, так и для удаленных подключений (False) или только для локальных (True)	True

Параметр	Описание	Значение по умолчанию
LogrotateCommonParamsDir	Путь к файлам конфигурации утилиты logrotate	C:\ProgramData\Positive Technologies\Logrotate\config\ComponentConfigs
SuperuserPassword	Пароль суперпользователя	P@ssw0rd

Таблица 12. Параметры конфигурации утилиты logrotatecfg

Параметр	Описание	Значение по умолчанию
CommonParamsDir	Путь к файлам конфигурации утилиты	C:\ProgramData\Positive Technologies\Logrotate\config\ComponentConfigs
RotateCount	Максимальное количество файлов журналов для компонентов сторонних производителей	10
RotateSize	Максимальный размер файла журнала для компонентов сторонних производителей (G для гигабайтов, M для мегабайтов, k для килобайтов)	200M

Таблица 13. Параметры конфигурации утилиты saltcfg

Параметр	Описание	Значение по умолчанию
SaltMasterHost	IP-адрес или FQDN сервера с модулем SaltMaster	—
SaltMinionLogLevel	Уровень журналирования для службы salt-minion (возможные значения — fatal, error, warn, info, debug или trace)	info

Приложение Б. Параметры конфигурации компонента PT UCS

Раздел содержит описание параметров конфигурации компонента PT UCS. Инструкция по изменению параметров приведена в Руководстве администратора.

Таблица 14. Параметры конфигурации компонента PT UCS

Параметр	Описание	Значение по умолчанию
`AutoAcceptMinions`	SaltMaster автоматически утверждает запрос на подключение от модулей SaltMinion (флажок установлен) или модули необходимо подключать вручную (флажок снят)	Флажок снят
`AutoDownloadProductsList`	PT UCS автоматически загружает с глобального сервера "Позитив Текнолоджиз" обновления для следующих объектов: — `KB VM DATA` — уязвимостей, условий их возникновения и закрытия, бюллетеней, возможного ПО на активах; — `KB BINARY` — дистрибутивов Knowledge Base; — `SIEM BINARY` — дистрибутивов компонентов на Microsoft Windows.	Установлены флажки `KB VM DATA` и `KB BINARY`
`LogLevel`	Уровень журналирования для служб PT UCS	`info`
`ProxyAddress`	IP-адрес или FQDN прокси-сервера	`proxy.server.fqdn.or.ip`
`ProxyEnabled`	PT UCS использует (флажок установлен) или не использует (флажок снят) прокси-сервер для подключения к глобальному серверу обновлений "Позитив Текнолоджиз"	Флажок снят
`ProxyPassword`	Пароль служебной учетной записи для подключения PT UCS к прокси-серверу	—

Параметр	Описание	Значение по умолчанию
`ProxyPort`	Порт прокси-сервера для входящего подключения от PT UCS	`8080`
`ProxyUser`	Логин служебной учетной записи для подключения PT UCS к прокси-серверу	—
`SaltMasterHost`	IP-адрес или FQDN сервера с модулем SaltMaster	—
`SaltMinionLogLevel`	Уровень журналирования для модуля SaltMinion (возможные значения — `fatal`, `error`, `warn`, `info`, `debug` или `trace`)	`info`
`TelemetrySendPeriod`	Расписание отправки в "Позитив Текнолоджиз" собранных данных о работе системы (в формате планировщика заданий cron)	`30 0 * * *`

О компании

"Позитив Текнолоджиз" уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга "Эксперт-400".

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com