INFOWATCH

Документация для InfoWatch Device Monitor (Linux)

07/04/2025

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 InfoWatch Device Monitor for Linux. Руководство по установке 6
1.1 Аудитория 6
1.2 Комплект документов 6
1.3 Техническая поддержка пользователей 6
1.4 Аппаратно-программные требования 7
1.5 Установка Device Monitor 15
1.5.1 Состав дистрибутива 15
1.5.2 Схема развертывания Device Monitor 15
1.5.3 Подготовка окружения 18
Установка .NET на примере операционной системы Альт 20
Установка .NET на примере операционной системы Astra Linux 21
Установка .NET на примере операционной системы РЕД ОС 22
Установка conntrack и socat на примере операционной системы РЕД ОС 23
1.5.4 Новая установка 23
Возможные режимы установки Device Monitor: 24
Шаги установки в режиме "Все-в-одном": 24
Шаги распределенной установки Device Monitor: 29
Подготовка Сервера Device Monitor к миграции с ОС Windows на ОС семейства Linux 31
1.5.5 Настройка проверки сертификатов удаленных серверов 33
Чтобы настроить проверку сертификатов удаленных серверов при установлении SSL-сессии: 34
Чтобы установить сертификат службы XAPI Traffic Monitor: 34
Чтобы установить сертификат веб-сервера Traffic Monitor Traffic Monitor: 35
Чтобы установить сертификат службы EPEVENTS Платформы: 36
Просмотр логов 36
1.5.6 Установка Агентов Device Monitor 36
Локальная установка Агента на рабочей станции под управлением ОС Windows 40
Локальная установка Агента на рабочей станции под управлением ОС семейства Linux 45
Локальная установка Агента на рабочей станции под управлением Mac OS 47
Установка Агентов с помощью задачи распространения 48
1.6 Настройка сетевых правил доступа 49
1.7 Обновление Device Monitor 51
1.7.1 Обновление Сервера Device Monitor 51
1.7.2 Обновление Агентов Device Monitor 56
1.8 Удаление Device Monitor 58
1.8.1 Удаление Платформы и Сервера Device Monitor 58
1.8.2 Удаление Агентов Device Monitor 59

Локальное удаление Агента на рабочей станции под управлением ОС Windows ... 60
Локальное удаление Агента на рабочей станции под управлением ОС семейства Linux ... 62
Локальное удаление Агента на рабочей станции под управлением Mac OS ... 62

2 InfoWatch Device Monitor for Linux. Руководство пользователя ... 64
2.1 Аудитория ... 64
2.2 Комплект документов ... 64
2.3 Техническая поддержка пользователей ... 64
2.4 Обзор ... 65
2.5 Настройки пользователей ... 66
2.5.1 Пользователи ... 66
Создание нового пользователя ... 67
Просмотр профиля пользователя ... 68
Редактирование учетной записи ... 68
Смена пароля пользователя ... 68
Активация и деактивация пользователя ... 69
Удаление пользователя ... 69
2.5.2 Роли ... 69
2.6 Общие настройки ... 70
2.6.1 Управление безопасностью ... 70
2.6.2 Мониторинг состояния Системы ... 71
2.6.3 Интеграции ... 73
Интеграция с Active Directory ... 73
Редактирование и удаление интеграции ... 76
2.7 Настройка Device Monitor ... 76
2.7.1 Серверы DM ... 76
2.7.2 Синхронизации DM ... 79
2.7.3 Агенты ... 82
2.7.4 Каналы перехвата ... 84
2.7.5 Настройка отправки данных в продукты ... 85
2.7.6 Диагностика событий ... 86
2.7.7 Корпоративные сети ... 87
2.7.8 Уведомления ... 87
2.8 Интерфейс Центра Администрирования (Device Monitor) ... 90
2.8.1 Политики ... 92
2.8.2 Задачи ... 94
2.8.3 Справочники ... 94
2.8.4 Группы ... 100
2.9 Настройка Системы после установки ... 101
2.9.1 Создание и редактирование групп компьютеров ... 101
2.9.2 Настройка состава групп компьютеров ... 103

2.9.3 Просмотр сведений о компьютерах ... 105
2.9.4 Задача первичного распространения и обновления ... 108
2.10 Настройка схемы безопасности ... 111
2.10.1 Создание политик ... 111
2.10.2 Создание правил ... 113
Правило контроля съемных носителей ... 114
Правило контроля сетевых ресурсов ... 116
Правило контроля терминальной сессии ... 118
Правило контроля печати ... 120
Правило контроля внешних устройств ... 121
Правило контроля FTP ... 122
Правило контроля HTTP(S) ... 123
Правило контроля почты ... 124
Правило контроля облачных хранилищ ... 126
Правило контроля экрана ... 126
Правило контроля буфера обмена ... 127
Правило контроля мессенджера VK ... 129
Правило контроля мессенджера Telegram ... 130
Правило контроля Яндекс Мессенджера ... 131
Правило контроля мессенджера WhatsApp ... 132
Правило контроля мессенджера Skype ... 134
Правило контроля протокола XMPP ... 136
Правило контроля ввода текста с клавиатуры ... 137
Правило контроля активности сотрудника ... 139
2.10.3 Создание и изменение списков приложений ... 140
Создание списка приложения ... 140
Добавление приложений в список ... 140
Редактирование и удаление списка приложений ... 142
2.10.4 Создание и редактирование групп сотрудников ... 143
2.10.5 Настройка состава групп сотрудников ... 144
2.11 ПОЛЬЗОВАТЕЛЬСКОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ... 148

Руководство по установке ONLINE | PDF

Руководство пользователя ONLINE | PDF

1 InfoWatch Device Monitor for Linux. Руководство по установке

В настоящем документе содержится инструкция по установке компонентов InfoWatch Device Monitor for Linux (далее Система или Device Monitor).

1.1 Аудитория

Данное руководство предназначено для инженеров внедрения и офицеров безопасности, которые будут работать с Системой и заниматься ее администрированием. Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и СУБД PostgreSQL.

1.2 Комплект документов

В документацию входят:

- «InfoWatch Device Monitor for Linux. Руководство по установке». Документ содержит описание процесса установки Сервера, Веб-консоли и Агентов, входящих в Систему.
- «InfoWatch Device Monitor for Linux. Руководство пользователя». Содержит описание работы в Веб-консоли для решения задач.

Сопутствующая документация по системе InfoWatch Traffic Monitor (далее Traffic Monitor) включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию системы InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

1.3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера;
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Часы работы службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

1.4 Аппаратно-программные требования

Требования к аппаратной конфигурации сервера определяются на основании предполагаемой нагрузки на Систему и параметров сети, в которой происходит развертывание, поэтому спецификация оборудования для каждого случая рассчитывается отдельно.

Примерные минимальные программно-аппаратные требования приведены в следующей таблице. Подробный расчет конфигурации настоятельно рекомендуется проводить с участием специалистов InfoWatch или компании-партнера, у которой вы приобретаете продукт.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер Device Monitor на Платформе				
Не менее 100 GB свободного пространства для установки. Также понадобится свободное пространство для анализа данных, объем зависит от нагрузки на сервер	От 4 ядер (частота - 3.1 ГГц, разрядность - 64 bit, с поддержкой инструкций SSE 4.2)	От 16 GB	ОС: • РЕД ОС 7.3.3; • РЕД ОС 8; • Astra Linux 1.7.5 в редакциях "Орел" и "Смоленск" • Astra Linux 1.8 в редакциях "Орел", "Воронеж" и "Смоленск" • Альт Сервер Виртуализаци	• На сервере ТМ должен быть включен автозапуск процесса **iw_xapi_xapi** • Наличие локального DNS для перевода доменных имен в адреса • Режим FIPS должен быть отключен • Должен поддерживаться протокол TLS 1.2 • Если предполагается распространение агентов на рабочие станции под управлением ОС Windows, на сервере должен быть установлен Samba-клиент

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			и СП 10. • Альт Сервер Виртуализации 10.2. СУБД: PostgreSQL версии 11 и более поздних	
Агент Device Monitor для рабочих станций				
Не менее 1 GB свободного пространства для установки. Также понадобится свободное пространство для временного хранения файлов, предназначенных для передачи на анализ	От 2 ядер	От 2.5 GB	ОС: • [1]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • Microsoft Windows 11; • [1]Microsoft Windows Server 2008 R2; • Microsoft Window	**Поддерживаемые версии ядра Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"** • 5.4.0-54-generic • 5.4.0-54-hardened • 5.4.0-81-generic • 5.4.0-81-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.4.0-186.astra2+ci2 (начиная с версии 7.15.2) • 5.10.0-1045-generic • 5.10.0-1045-hardened • 5.10.142-1-generic • 5.10.176-1-generic • 5.10.216-1.astra2+ci2 (начиная с версии 7.15.2) • 5.15.0-33-generic • 5.15.0-33-hardened • 5.15.0-70-generic • 5.15.0-70-hardened • 5.15.0-83-generic

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			s Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows Server 2022; • Astra Linux Special Edition 1.7 в редакциях "Орел" (x64), "Воронеж" (x64) и "Смоленск" (x64); • Astra Linux Special Edition	• 5.15.0-111-generic (начиная с версии 7.15.1) • 6.1.50-1-generic#astra2+ci6 (до версии 7.13.5) • 6.1.50-1-generic#astra4+ci68 (начиная с версии 7.13.6) • 6.1.90-1-generic (начиная с версии 7.15.1) **Поддерживаемые версии ядра Astra Linux Special Edition 1.8 в редакциях "Орел", "Воронеж" и "Смоленск"** • 6.1.90-1-generic (начиная с версии 7.17) • 6.6.28-1-generic (начиная с версии 7.17) **Поддерживаемые версии ядра РЕД ОС 7.3** • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1 • 5.15.35-4 • 5.15.35-5 • 5.15.72-1 (начиная с версии 7.7.1) • 5.15.78-2 (начиная с версии 7.8) • 5.15.87-1 (начиная с версии 7.8.1) • 5.15.106-1 • 5.15.117-1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			1.8.1.16 в редакциях "Орел" (x64), "Воронеж" (x64) и "Смоленск" (x64); • РЕД ОС 7.3; • РЕД ОС 8.0; • Альт Рабочая станция 10; • Альт Сервер 10.1 с профилем "Офисный сервер"; • Альт Сервер 10.1 СП (сертифицированный);	• 5.15.125-1 • 5.15.131-1 • 5.15.161-1 (начиная с версии 7.14.1) • 6.1.20-2 • 6.1.44-1 • 6.1.52-1 • 6.1.85-1 (начиная с версии 7.13.4) • 6.1.94-1 (начиная с версии 7.14.1) • 6.1.110-1 (начиная с версии 7.14.5) • 6.1.128-2 (начиная с версии 7.16.4) **Поддерживаемые версии ядра РЕД ОС 8.0** • 6.6.6-1 (начиная с версии 7.17.0) • 6.6.26-1 (начиная с версии 7.17.0) • 6.6.34-1 (начиная с версии 7.17.0) • 6.6.51-1 (начиная с версии 7.17.0) • 6.6.76-1 (начиная с версии 7.17.0) **Поддерживаемые версии ядра Альт Рабочая станция 10** • 5.10.133-std-def-alt1 • 5.10.135-std-def-alt1 • 5.10.136-std-def-alt1 • 5.10.163-std-def-alt1 • 5.10.164-std-def-alt1 • 5.10.165-std-def-alt1 • 5.10.168-std-def-alt1 • 5.10.170-std-def-alt1 • 5.10.172-std-def-alt1 • 5.10.174-std-def-alt1 • 5.10.176-std-def-alt1 • 5.10.177-std-def-alt1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• Mac OS Sequoia 15.1; • Mac OS Sequoia 15.2; • Mac OS Sequoia 15.3.	• 5.10.179-std-def-alt1 • 5.10.182-std-def-alt1 • 5.10.185-std-def-alt1 • 5.10.186-std-def-alt1 • 5.10.191-std-def-alt1 • 5.10.194-std-def-alt1 • 5.10.195-std-def-alt1 • 5.10.197-std-def-alt1 • 5.10.198-std-def-alt1 • 5.10.199-std-def-alt2 • 5.10.200-std-def-alt1 • 5.10.203-std-def-alt1 • 5.10.204-std-def-alt1 • 5.10.205-std-def-alt1 • 5.10.206-std-def-alt1 • 5.10.207-std-def-alt1 (начиная с версии 7.12.1) • 5.10.208-std-def-alt1 (начиная с версии 7.12.1) • 5.10.209-std-def-alt2 (начиная с версии 7.12.2) • 5.10.211-std-def-alt1 • 5.10.212-std-def-alt1 • 5.10.213-std-def-alt1 (начиная с версии 7.13.1) • 5.10.216-std-def-alt1 (начиная с версии 7.13.6) • 5.10.217-std-def-alt1 (начиная с версии 7.13.9) • 5.10.218-std-def-alt1 (начиная с версии 7.13.10) • 5.10.219-std-def-alt1 (начиная с версии 7.14.1)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 5.10.220-std-def-alt2 (начиная с версии 7.14.1) • 5.10.221-std-def-alt1 (начиная с версии 7.14.2) • 5.10.227-std-def-alt1 (начиная с версии 7.15.1) • 5.10.228-std-def-alt1 (начиная с версии 7.15.2) • 5.10.231-std-def-alt1 (начиная с версии 7.16.1) • 5.10.233-std-def-alt1 (начиная с версии 7.16.2) • 5.10.234-std-def-alt1 (начиная с версии 7.16.3) • 5.10.235-std-def-alt1 (начиная с версии 7.17.1) • 5.15.94-un-def-alt1 • 5.15.109-un-def-alt1 • 6.1.29-un-def-alt1 • 6.1.32-un-def-alt1 • 6.1.42-un-def-alt1 • 6.1.49-un-def-alt1 (начиная с версии 7.13.2) • 6.1.67-un-def-alt0.c10f.1 (начиная с версии 7.12.4) • 6.1.75-un-def-alt1 (начиная с версии 7.12.2) • 6.1.77-un-def-alt1 (начиная с версии 7.12.2)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 6.1.78-un-def-alt1 (начиная с версии 7.12.4) • 6.1.79-un-def-alt1 (начиная с версии 7.12.5) • 6.1.80-un-def-alt1 • 6.1.81-un-def-alt1 • 6.1.82-un-def-alt1 (начиная с версии 7.13.1) • 6.1.83-un-def-alt1 (начиная с версии 7.13.2) • 6.1.84-un-def-alt1 (начиная с версии 7.13.4) • 6.1.85-un-def-alt1 (начиная с версии 7.13.4) • 6.1.90-un-def-alt1 (начиная с версии 7.13.8) • 6.1.94-un-def-alt1 (начиная с версии 7.14.1) • 6.1.96-un-def-alt1 (начиная с версии 7.14.1) • 6.1.99-un-def-alt1 (начиная с версии 7.14.2) • 6.1.112-un-def-alt1 (начиная с версии 7.15.0) • 6.1.113-un-def-alt1 (начиная с версии 7.15.1) • 6.1.115-un-def-alt1 (начиная с версии 7.15.2)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 6.1.119-un-def-alt1 (начиная с версии 7.16) • 6.1.121-un-def-alt1 (начиная с версии 7.16.1) • 6.1.123-un-def-alt1 (начиная с версии 7.16.1) • 6.1.124-un-def-alt1 (начиная с версии 7.16.2) • 6.1.127-un-def-alt1 (начиная с версии 7.16.3) • 6.1.128-un-def-alt1 (начиная с версии 7.16.3) • 6.1.129-un-def-alt1 (начиная с версии 7.16.4) • 6.1.130-un-def-alt1 (начиная с версии 7.17.1) • 6.1.131-un-def-alt1 (начиная с версии 7.17.1)
Веб-консоль Device Monitor				
	Дополнительно 1 ядро	1 GB на каждую вкладку браузера	Браузеры: • Google Chrome • Яндекс.Браузер	В браузере должна быть реализована аппаратная поддержка WebGL/WebGL2 Платформа версии 1.7 и выше

Примечание:

[1] - для указанных ОС требуется установка следующих исправлений от компании Microsoft: KB4474419, KB4490628. Проверка на наличие данных исправлений на компьютере проводится Системой перед установкой и/или обновлением продукта.

Примечание:

Допустима установка в виртуальную среду: VMware, MS Hyper-V или других систем виртуализации.

Работа агентов Device Monitor поддержана в средах виртуализации Microsoft RDS, Citrix XenApp 6.0, 7.6, 7.13, 7.14 и 7.15 LTSR.

1.5 Установка Device Monitor

Рекомендуется соблюдать следующий порядок установки:

1. Подготовка окружения.
2. Установка Платформы с Центром расследований.
3. Установка Сервера Device Monitor.
4. Настройка проверки сертификатов удаленных серверов.
5. Получение открытого ключа Платформы.
6. Установка Агентов Device Monitor.

1.5.1 Состав дистрибутива

В состав дистрибутива Device Monitor входят следующие компоненты:

- `data/iwdms` – содержит архив с исполняемыми файлами Сервера Device Monitor и скрипт для его установки с поддержкой установки через параметры командной строки.
- `data/scripts/include` – содержит вспомогательные скрипты, необходимые для корректной работы `setup.sh` и `install_iwdms.sh`;
- `data/ui` – дистрибутив Платформы с веб-интерфейсом Центра расследований.
- `setup.sh` – скрипт, запускающий установщик Сервера Device Monitor в терминале Linux.

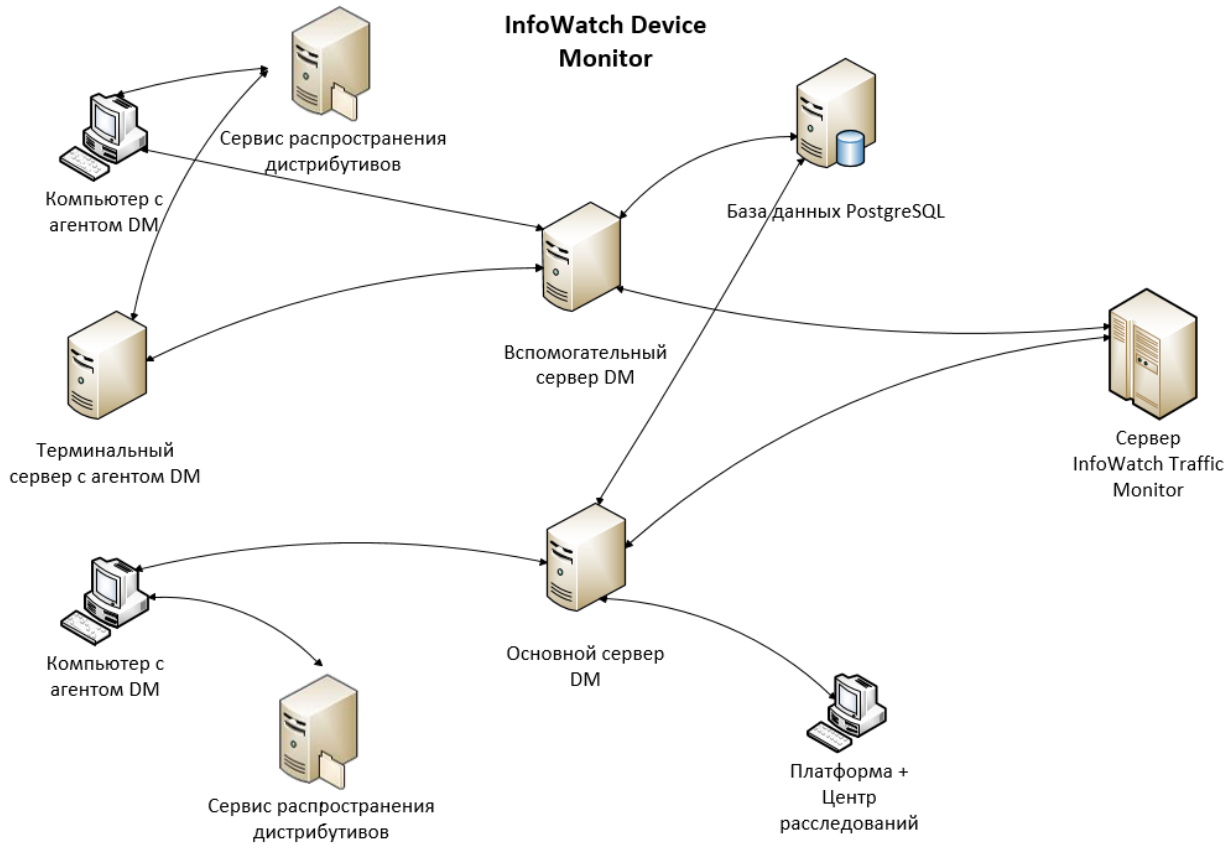
1.5.2 Схема развертывания Device Monitor

Компоненты, входящие в состав InfoWatch Device Monitor, перечислены в следующей таблице:

Компонент	Назначение
InfoWatch Device Monitor Client (клиентское приложение InfoWatch Device Monitor, Агент)	Перехват действий сотрудников на контролируемых рабочих станциях
InfoWatch Device Monitor Server (сервер InfoWatch Device Monitor, Сервер)	Конфигурирование клиентских приложений, сбор данных от клиентских приложений и передача этих данных системе InfoWatch Traffic Monitor, распространение deploy-агентов на рабочие станции

Компонент	Назначение
InfoWatch Device Monitor Database (база данных)	Хранение информации, необходимой для работы Device Monitor
Центр расследований	Управление модулями Device Monitor и Device Control
Сервис распространения дистрибутивов (Сервис распространения)	Получение и хранение новой версии дистрибутива агента Device Monitor

Взаимодействие компонентов Device Monitor показано на рисунке:



Для повышения производительности Device Monitor, можно использовать кластеризацию. При этом одна схема базы данных будет использоваться несколькими серверами для хранения и распространения общей схемы безопасности.

Сервер и база данных могут находиться на одном компьютере. Однако для увеличения производительности рекомендуется размещать базу данных и сервер на разных компьютерах.

Консоль управления может подключаться только к основному серверу. Используя Консоль управления можно управлять всеми серверами в кластере.

Система разворачивается и работает следующим образом:

1. Первой устанавливается центральная нода **Платформы** с веб-интерфейсом **Центра расследований**, где выполняется настройка схемы безопасности в соответствии с требованиями корпоративной политики безопасности**.**

2. **На Платформу** устанавливается **основной сервер DM**.
3. При установке основного сервера определяют используемый сервер **базы данных**: СУБД может располагаться как отдельно, так и на том же компьютере, что и основной сервер, а также создается **схема базы данных**, где будет храниться **схема безопасности** и другие параметры Device Monitor.
4. При необходимости, можно установить **вспомогательные серверы**, которые будут обеспечивать балансировку нагрузки.
5. **Сервис распространения дистрибутивов** устанавливается вместе с **основным сервером Device Monitor** по умолчанию, имеет хранилище с дистрибутивами Агентов для используемых ОС и платформы. Сервис может быть установлен и со **вспомогательными серверами Device Monitor**.
6. С **основного сервера** на **рабочие станции** распространяются deploy-агенты (агентом распространения) Device Monitor, которые затем скачивают дистрибутивы Агентов с ближайшего **сервиса распространения** из указанных точек публикации дистрибутивов. Скачивание Агентов может происходить параллельно несколькими рабочими станциями одновременно.
7. Агенты выполняют подключение к серверу Device Monitor по зашифрованному каналу, с привязкой к серверу на основании ключа, используемого для шифрования трафика. Агенты Device Monitor обеспечивают реализацию схемы безопасности, а также получение теневых копий и их отправку на сервер Device Monitor.
8. Серверы Device Monitor получают из базы данных обновленные версии схемы безопасности и распространяют их на контролируемые рабочие станции. С контролируемых рабочих станций на сервер передается информация о событиях, подпадающих под действие правила схемы безопасности, а также теневые копии файлов. Информация о событиях передается в базу данных. Теневые копии передаются в систему InfoWatch Traffic Monitor.

Пример 1

1. Сотрудник, работающий на контролируемой рабочей станции, обращается к контролируемому периферийному устройству (например, дает команду распечатать документ через USB принтер).
2. Агент проверяет, имеет ли сотрудник право на работу с периферийным устройством. Если такого разрешения нет, то сотруднику будет отказано в доступе к устройству (в рассматриваемом случае документ не будет отправлен на печать).

Печать документов на локальных и сетевых принтерах отслеживается перехватчиком Print Monitor. Копия задания на печать передается в InfoWatch Traffic Monitor для анализа. Отправка документов на печать возможна при условии, что сотруднику разрешен доступ к принтеру (проверяется перехватчиком Device Monitor).

Пример 2

В Device Monitor задано правило, отслеживающее запись в PDF-файл на съемном устройстве. В правиле указано, что при выполнении этой операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к записи в файл на съемном устройстве (например, копирует файл на USB Flash Drive).
2. Если операция записи в файл на съемном устройстве успешно завершена, то Агент InfoWatch Device Monitor генерирует событие и создает теневую копию файла.
3. Если создать теневую копию файла невозможно (например, при отсутствии свободного места на жестком диске), операция записи в файл на съемном устройстве будет

произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию файла) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемом компьютере. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются в базе данных. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

Попытки записи в файлы на съемных устройствах отслеживаются перехватчиком File Monitor. Полученные сведения передаются затем в InfoWatch Traffic Monitor для анализа. В то же время доступ к съемному устройству контролируется перехватчиком Device Monitor. Поэтому сотрудник может выполнять операцию записи в файл только на тех съемных устройствах, к которым у него есть доступ.

Пример 3

В Device Monitor задано правило, отслеживающее печать DOC-файлов. В правиле указано, что при выполнении подобной операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к отправке документа на печать.
2. Если задание на печать сформировано успешно, то Агент InfoWatch Device Monitor генерирует событие и создает теневую копию документа, отправленного на печать.
3. В случае если создать теневую копию документа невозможно (например, при отсутствии свободного места на жестком диске), операция печати будет произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию документа) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемом компьютере. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются в базе данных. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

1.5.3 Подготовка окружения

Для функционирования Сервера Device Monitor необходимо подготовить окружение:

1. Ввести в домен компьютер, на который будет установлен Сервер Device Monitor.
2. Удостовериться, что для сервера задано FQDN имя хоста. Для этого выполните команду:

   ```
   echo $HOSTNAME
   ```

   В результате должно быть выведено полное имя, например, `dmserv.company.ru` . Если выведено короткое имя, например, `dmserv` , то:
   a. Задайте полное имя хоста:
      - На компьютере под управлением ОС Astra Linux или Альт используйте команду:

```
hostnamectl set-hostname <FQDN>
```

- На компьютере под управлением РЕД ОС:
  i. Запустите утилиту `nmtui`:

```
nmtui
```

  ii. В текстовом интерфейсе выберите `Set system hostname`.
  iii. В окне `Set Hostname` введите новое имя хоста и нажмите `OK`.
  iv. В окне `Set hostname to '<новое_имя>'` нажмите `OK`.
  v. Нажмите `Quit`.

b. Перезагрузите сервер.
c. Повторно выполните команду:

```
echo $HOSTNAME
```

3. Установить Microsoft .NET 6 (https://dotnet.microsoft.com/) на этом компьютере.
4. Установить пакеты `conntrack` (или `conntrack-tools`) и `socat`.
5. Настроить антивирус для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для Device Monitor Server на ОС Linux").
6. Настроить правила POD сети или отключить межсетевой экран (см. статьи Базы знаний "Конфликты при взаимодействии firewalld и Kubernetes", "Полное отключение межсетевого экрана").
7. Установить интерпретатор языка Python версии 2.7. Пакет с интерпретатором не входит в состав дистрибутива продукта.
8. Если установка проводится на ОС Альт:
   - Установить утилиту `unzip` аналогично установке `conntrack` и `socat`;
   - Установить пакет с интерпретатором языка Python версии 2.7, а также следующие пакеты:
     - `python-modules-json`
     - `python-modules-distutils`
     - `python-modules-sqlite3`

> **Примечание:**
>
> Пакеты не входят в состав дистрибутива продукта и могут отсутствовать в репозиториях. В этом случае загрузите и установите требуемые пакеты вручную

   - Настроить соответствие алгоритмов шифрования Сервера Device Monitor и Сервера Traffic Monitor. Для этого измените файл `/etc/openssl/openssl.cnf` следующим образом:
     - Найдите в файле строки:

```
# Extra OBJECT IDENTIFIER info:
#oid_file       = $ENV::HOME/.oid
oid_section     = new_oids
```

- После них добавьте строки:

```
# System default
openssl_conf = default_conf
```

- В конец файла добавьте следующие строки:

```
[default_conf]
ssl_conf = ssl_sect

[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = TLSv1.2
CipherString =  DEFAULT:@SECLEVEL=1
```

9. Установить СУБД PostgreSQL на другом компьютере. Вы можете установить СУБД PostgreSQL совместно с сервером Device Monitor, если необходимо получать события от небольшого количества Агентов.

> **Примечание:**
>
> Для обеспечения корректной и бесперебойной работы Сервера необходимо хранение файлов СУБД и теневых копий событий на разных физических дисках.
>
> Для работы с СУБД необходима роль с правами на создание базы данных.

10. Подготовить СУБД:
    a. Откройте конфигурационный файл `postgresql.conf` и присвойте параметру `"max_connections"` значение 250.
    b. Настройте файл доступа `pg_hba.conf`. Для более точного подбора параметров используйте калькулятор PGTune.

> **Важно!**
>
> Для успешного соединения Сервера Device Monitor с Сервером Traffic Monitor необходимо до или после установки настроить проверку сертификата удаленного сервера (подробнее см. "Настройка проверки сертификатов удаленных серверов") .

11. Убедитесь, что на сервере установлены актуальные дата и время.

Установка .NET на примере операционной системы Альт

1. Убедитесь, что репозитории Альт доступны, выполнив команду: `apt-repo list`
2. Если репозитории недоступны (закомментированы), необходимо отредактировать файл **/etc/apt/sources.list** , раскомментировав в нем строки с адресами репозиториев

3. Отредактируйте файл **/etc/apt/apt.conf** :
    a. Раскомментируйте все строки
    b. Укажите корректные имя пользователя и пароль доменной учетной записи.
4. Установите среду выполнения NET 6 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:
   `apt-get install dotnet-aspnetcore-runtime-6.0`
   В результате будет установлена среда выполнения .NET 6 с поддержкой ASP.NET Core.
5. Проверьте установленный NET 6, выполнив команду:
   `dotnet --info`

```
[root@dmalt ~]# dotnet --info

global.json file:
  Not found

Host:
  Version:      6.0.20
  Architecture: x64
  Commit:       6.0.20-alt

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 6.0.20 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 6.0.20 [/usr/lib64/dotnet/shared/Microsoft.NETCore.App]

Download .NET:
  https://aka.ms/dotnet-download

Learn about .NET Runtimes and SDKs:
  https://aka.ms/dotnet/runtimes-sdk-info
[root@dmalt ~]#
```

Установка .NET на примере операционной системы Astra Linux

1. Убедитесь, что репозитории Astra Linux доступны, выполнив команду:
   `apt-get update`
2. Если репозитории недоступны (закомментированы), необходимо отредактировать файл **/etc/apt/sources.list** , раскомментировав в нем строки с адресами репозиториев
3. Отредактируйте файл **/etc/apt/apt.conf** :
    a. Раскомментируйте все строки
    b. Укажите корректные имя пользователя и пароль доменной учетной записи.
4. Установите среду выполнения NET 6 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:
   `apt install dotnet-aspnetcore-runtime-6.0`
   В результате будет установлена среда выполнения .NET 6 с поддержкой ASP.NET Core.
5. Проверьте установленный NET 6, выполнив команду:
   `dotnet --info`

```
root@dmAstra:~# dotnet --info

global.json file:
  Not found

Host:
  Version:      6.0.10
  Architecture: x64
  Commit:       5a400c212a

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 6.0.10 [/usr/lib/dotnet/dotnet6-6.0.110/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 6.0.10 [/usr/lib/dotnet/dotnet6-6.0.110/shared/Microsoft.NETCore.App]

Download .NET:
  https://aka.ms/dotnet-download

Learn about .NET Runtimes and SDKs:
  https://aka.ms/dotnet/runtimes-sdk-info
root@dmAstra:~#
```

Установка .NET на примере операционной системы РЕД ОС

1. Убедитесь, что репозитории РЕД ОС доступны, выполнив команду:
   `dnf repoinfo`
2. Установите среду выполнения NET 6 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:
   `sudo yum install aspnetcore-runtime-6.0`
   В некоторых дистрибутивах Linux имя пакета может быть `dotnet-aspnetcore-runtime-6.0`
   В результате будет установлена среда выполнения .NET 6 с поддержкой ASP.NET Core.
3. Проверьте установленный NET 6, выполнив команду:
   `dotnet --info`

```
[root@aspredos731dm yum.repos.d]# dotnet --info

Host (useful for support):
  Version: 6.0.5
  Commit:  70ae3df4a6

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 6.0.5 [/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 6.0.5 [/usr/share/dotnet/shared/Microsoft.NETCore.App]

To install additional .NET runtimes or SDKs:
  https://aka.ms/dotnet-download
```

В процессе установки .NET могут возникнуть ошибки. В этом случае:

1. Удалите из операционной системы все пакеты, связанные с .NET, выполните команду:
   `sudo dnf remove 'dotnet*' 'aspnet*' 'netstandard*'`
2. Установите заново конкретную версию .NET, например:
   `sudo dnf install aspnetcore-runtime-6.0-6.0.5-1.el7`

3. Чтобы посмотреть список доступных версий, выполните:
   `dnf --showduplicates list aspnetcore-runtime-6.0`

Установка conntrack и socat на примере операционной системы РЕД ОС

Для корректной поддержки Kubernetes проверьте наличие установленных пакетов `conntrack` и `socat`.
Для этого:

1. Введите в командной строке:
   `conntrack`

   В ответ будут выведены сведения о работе и актуальная версия этого пакета.
2. Если `conntrack` не установлен, следует установить его с помощью команды:
   `sudo yum install conntrack`
3. Если пакет недоступен в репозитории, скачайте его, перейдите в директорию с пакетом и установите вручную с помощью команды вида:
   `rpm -Uhv ./<имя_пакета>`
4. Повторите описанные выше действия для установки пакета `socat`.

1.5.4 Новая установка

Основой для установки Device Monitor является Платформа. Инсталлятор каждого продукта содержит и Платформу, и продуктовые компоненты. Обе части обязательны к установке при развертывании продуктов.
И продуктовые компоненты, и Платформа поддерживают установку в двух режимах:

- **`central`**;
- **`office`**.

Режимы установки продукта и Платформы вы указываете при запуске инсталлятора. Если оба режима не указаны пользователем, инсталлятор по умолчанию использует значение **`central`** для обоих компонентов.

Центр расследований поддерживает **распределенную установку**: центральная (**`central`**) и офисные (**`office`**) ноды Платформы объединены в кластер.
Вы можете установить компоненты продуктов и на центральную, и на офисные ноды Платформы. Это позволяет создать кластер Платформы с несколькими продуктами с учетом инфраструктуры, требований к безопасности и доступных мощностей компании.

> **Важно!**
>
> При распределенной установке примите во внимание следующие ключевые аспекты:
>
> - Продукты в кластере должны быть установлены на одной версии Платформы. Если вы установите в кластер продукт на новой версии Платформы, для корректной работы вам будет необходимо обновить все продукты.
> - В одном кластере можно развернуть только одну центральную ноду Платформы и каждый продукт в режиме `central` только в единственном экземпляре.

- Если в кластере уже установлен продукт в режиме `central`, еще одна установка этого продукта в режиме `central` в том же кластере будет прервана ошибкой.
- Device Monitor поддерживает установку только в режиме `central`. При этом он поддерживает установку как на центральную, так и на офисные ноды Платформы.

Продукты в одном кластере имеют:

- доступ ко всей функциональности в одной консоли управления;
- общие настройки;
- общую ролевую модель;
- общий доступ к данным независимо от того, на каком из них выполнена интеграция с источником, а также доступ к обработанным данным.

Важно!

Для подключения к веб-интерфейсу Центра расследований **всегда** используйте адрес или имя сервера, на котором установлена **Платформа в режиме `central`**.

Если в распределенной установке продукт в режиме `central` установлен на офисной ноде Платформы, для работы все равно используйте центральную ноду Платформы (`central`).

Возможные режимы установки Device Monitor:

- Установка "**Все-в-одном**" предполагает размещение Платформы с веб-интерфейсом Центра расследований и Сервера Device Monitor на одном физическом сервере.

  Важно!

  Если вы переходите на Device Monitor for Linux с ОС Windows и вам необходима миграция данных:

  - Убедитесь, что база данных готова к миграции; в противном случае подготовьте ее. Подробнее см. статью "Подготовка Сервера Device Monitor к миграции с ОС Windows на ОС семейства Linux".
  - На шаге 25 инструкции выберите **Update an existing database**.
  - После установки убедитесь, что для базы данных установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

- **Распределенная** установка Сервера Device Monitor на офисную ноду Платформы на отдельном сервере.

Шаги установки в режиме "Все-в-одном":

Режим подходит для новой чистой установки Device Monitor, а также при переходе на Device Monitor for Linux с ОС Windows.

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям ("Аппаратно-программные требования").

   > **Примечание:**
   >
   > В ходе установки инсталлятор проверит наличие:
   > - не менее 100 ГБайт на диске для директорий, которые будут указаны далее в пп. 15-18. Если директории для хранения данных находятся на разных дисках, то проверятся наличие 100 Гбайт свободного места на каждом из них;
   > - не менее 20 ГБайт на диске для директорий с образами;
   > - не менее 16 ГБайт ОЗУ;
   > - не менее 4 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета `conntrack`.

2. Выполните шаги по подготовке сервера к установке Device Monitor (см. "Подготовка окружения").
3. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск.
4. Создайте директорию и распакуйте в нее содержимое архива. В примере архив будет распакован в директорию `/dmsl_distr`:

   ```
   mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.17.0.310.tar.gz -C /dmsl_distr
   ```

5. Перейдите в созданную директорию.
6. Добавьте файлу **setup.sh** атрибут "*исполняемый*":

   ```
   chmod +x ./setup.sh
   ```

7. Запустите скрипт **setup.sh**, который входит в состав дистрибутива:

   ```
   ./setup.sh
   ```

   После этого будут доступны действия:
   - **Install** – новая установка Платформы и Центра администрирования
   - **Update** – обновление установленных компонентов
   - **Utilities** – переход в меню утилит
   - **Exit** – выход из программы
8. Выберите тип установки **Install**. Будет доступен список компонентов:
   - **DM Server Service, FrontEnd** – установка "все-в-одном" при отсутствии установленной Платформы либо другого Сервера Device Monitor
   - **Only FrontEnd** – установка только Платформы и веб-интерфейса Центра администрирования
   - **Only DM Server Service** – установка только Сервера Device Monitor
9. Выберите **DM Server Service, FrontEnd**. В этом случае будут автоматически:
   - получен и записан в Device Monitor открытый ключ службы **guard** Платформы, необходимый для корректного взаимодействия веб-интерфейса с Сервером
   - исправлен файл n.yaml

> **Важно!**
>
> Любой продукт, который будет установлен в Центре расследований после Device Monitor, сгенерирует новый файл n.yaml, и из него будет удалена секция, которая необходима для корректного взаимодействия веб-интерфейса с Сервером. Чтобы восстановить n.yaml, выполните шаги 37-39.

Будут предложены режимы установки Платформы с веб-интерфейсом Центра расследований:

- **Central** – предназначен для установки на основную ноду или в случае отсутствия уже установленного Центра расследований.
- **Office** – предназначен для распределенной установки.

10. Выберите режим **Central**. Начнется процесс установки Платформы
11. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
12. Введите **y**, чтобы принять лицензионное соглашение, и нажмите **Enter**.
13. Введите IP-адрес сервера в формате IPv4: `"xxx.xxx.xxx.xxx"` и нажмите **Enter**.
14. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию 80%) и нажмите **Enter**.
15. Укажите путь для размещения данных Clickhouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
16. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
17. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
18. Укажите путь для хранения данных (по умолчанию `/opt/dsdata`) и нажмите **Enter**.
19. Укажите порт подключения к веб-интерфейсу (по умолчанию `443`) и нажмите **Enter**.
20. Дождитесь окончания процесса установки Платформы. Далее будет произведена установка Сервера Device Monitor. При этом:
    a. Будут созданы каталоги:
       - /var/log/iwdms - каталог логов выполнения сервера DM
       - /opt/iw/dmserver/bin - каталог с файлами сервера DM
       - /opt/iw/dmserver/queue - каталог файловой очереди
       - /opt/iw/dmserver/log - символическая ссылка на каталог /var/log/iwdms
    b. Добавлен пользователь **iwdms** с ключом `--system`, что позволяет запустить под этим пользователем службу, но не дает авторизоваться под этим пользователем в Центре администрирования
    c. Распакован zip-файл из `data/iwdms` инсталляционного пакета в требуемые каталоги. Для вышеуказанных папок в качестве владельца буден назначен пользователь **iwdms**
    d. В каталоге systemd служб `/etc/systemd/system` будет добавлен файл манифеста службы Сервера Device Monitor **iwdms.service**, а также службы синхронизации с Active Directory - **iwdms_ldap.service**
21. Выберите язык устанавливаемого сервера и нажмите **Enter**. Это определит названия предустановленных групп, политик и правил.
22. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Выберите **Accept and continue** и нажмите **Enter**
23. Далее можно выбрать, какой тип сервера необходимо установить: **Primary** (основной) или **Secondary** (второстепенный).

24. Если вы устанавливаете Систему впервые или переходите с Device Monitor, установленном на ОС Windows, выберите **Primary**. Для установки второстепенного сервера выполните шаги 27-31 и далее начиная с шага 35.
25. Настройте взаимодействие с Базой данных:
    - **Create new database** – чтобы создать новую Базу данных. Используйте этот вариант **для чистой установки**;
    - **Update an existing database** – чтобы настроить существующую Базу данных. Используйте этот вариант **для установки с миграцией данных**.
26. Укажите имя или IP-адрес сервера, на котором располагается СУБД PostgreSQL. Если вы устанавливаете Device Monitor с миграцией данных, используйте СУБД Postgresql, ранее используемую для установки Сервера Device Monitor на ОС Windows.
27. Укажите порт для настройки взаимодействия. Если порт не указан, будет использован порт по умолчанию – `5432`.
28. Введите имя базы данных. По умолчанию – `iwdm`.
29. Введите имя пользователя СУБД. По умолчанию – `postgres`.
30. Введите пароль.
31. Если на шаге 24 вы выбрали **основной** сервер, то укажите путь до PFX-файла ключа шифрования канала между Сервером DM и агентами. Если путь не указывать, то будет использован путь, предложенный по умолчанию, – `/opt/iw/dmserver/ssl.pfx`
32. Введите адрес InfoWatch Traffic Monitor (IWTM). Для этого используйте имя сервера или его IP-адрес.
    Если взаимодействие с Traffic Monitor не планируется, то введите любое не существующее в вашей сети имя сервера.

    Важно!

    Имя сервера может содержать латинские буквы от «a» до «z» (без учета регистра), цифры от «0» до «9» и знак дефиса "-". Оно не должно состоять только из цифр. Рекомендуется использовать имя сервера, начинающееся с буквы.

    Примечание:

    Если после установки необходимо изменить адрес InfoWatch Traffic Monitor, вы можете сделать это в базе данных сервера Device Monitor:

    - поле `TRAFFIC_MONITOR_POLICY_SERVER_ADDRESS` таблицы Settings - содержит адрес сервера Traffic Monitor, который используется всеми серверами пула DM - основным и вспомогательными - для получения политики Traffic Monitor и ее распространения на агенты;
    - поле `TmAddress` таблицы ServerOption - содержит адрес сервера Traffic Monitor, на который отправляются события из DM. В этой таблице поле `TmAddress` может присутствовать несколько раз (по количеству серверов в пуле).

33. Введите токен доступа к IWTM. Для успешного соединения Сервера Device Monitor с Сервером Traffic Monitor необходимо настроить проверку сертификата удаленного сервера (подробнее см. далее в разделе "Настройка проверки сертификатов удаленных серверов").
    Если взаимодействие с Traffic Monitor не планируется, то введите любое значение токена.

34. Укажите **Yes**, чтобы установить сервис распространения дистрибутивов. В этом случае точка распространения сможет распространять дистрибутивы агентов на рабочие станции;
35. Если вы выбрали **Update an existing database**, то запускается проверка на наличие неподдерживаемых для настройки правил в новой версии Device Monitor. В случае, если обнаружено неподдерживаемые правила, то миграция завершится с ошибкой. В этом случае рекомендуем обратиться в службу технической поддержки InfoWatch.
36. Если вы выбрали **Update an existing database** и планируете использовать модуль Device Control, правила и белые списки, выберите **Using Device Control is required, migrate rules and white lists**. Подождите, пока правила Device Control и белые списки будут мигрированы на новую версию. Если использование Device Control не планируется, выберите **Using Device Control is not required, delete rules and white lists**
37. Если вы далее будете устанавливать другой продукт InfoWatch, то необходимо прописать в файл **n.yaml** настройки, получить открытый ключ службы **nguard** Платформы и сохранить его в каталог Сервера. Введите IP-адрес Сервера Device Monitor, а затем запустите скрипт установки:

```
./setup.sh
```

38. Выберите в меню пункт **Utilities**. Раздел содержит утилиты:
    a. **Fix n.yaml file** – если на текущем компьютере установлен Device Monitor в роли основного сервера, а также Платформа (в любом из режимов central или office), то с помощью запуска этой утилиты можно автоматически прописать в **n.yaml** необходимые настройки. Это действие следует производить после установки любого продукта в Центр расследований;
    b. **Save platform guard public key to IWDM Service** - если на текущем компьютере установлен Device Monitor в роли основного сервера, а также Платформа (в любом из режимов central или office), то с помощью запуска этой утилиты можно автоматически получить открытый ключ службы **guard** Платформы и сохранить его в каталог сервера;
    c. **Show IWDM Service version** - утилита показывает версию установленного сервера;
    d. **Export ssl key** – утилита позволяет экспортировать ключ защиты канала "агент-сервер".
39. Выберите **Fix n.yaml file**. Дождитесь окончания процесса.
40. Запустите скрипт установки:

```
./setup.sh
```

41. Выберите в меню пункт Utilities и далее **Save platform guard public key to IWDM Service**. Дождитесь окончания процесса.
42. Перезапустите службу iwdms :

```
systemctl restart iwdms
```

Распределенная установка используется в случаях, если в организация использует также и другие продукты Infowatch или имеет филиальную структуру с центральным офисом и филиалами. В этом случае необходимо дополнительно установить один или несколько Серверов Device Monitor на другие компьютеры с офисными ноды Платформы с другими установленными продуктами InfoWatch.

Шаги распределенной установки Device Monitor:

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям ("Аппаратно-программные требования").

   > **Примечание:**
   >
   > В ходе установки инсталлятор проверит наличие:
   > - не менее 100 ГБайт на диске для директорий, которые будут указаны далее на шаге 16. Если директории для хранения данных находятся на разных дисках, то проверятся наличие 100 Гбайт свободного места на каждом из них;
   > - не менее 20 ГБайт на диске для директорий с образами;
   > - не менее 16 ГБайт ОЗУ;
   > - не менее 4 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета **`conntrack`**.

2. Выполните шаги по подготовке сервера к установке Device Monitor (см. "Подготовка окружения").
3. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск другого компьютера.
4. Создайте директорию и распакуйте в нее содержимое архива. В примере архив будет распакован в директорию `/dmsl_distr`:

   ```
   mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.17.0.310.tar.gz -C /dmsl_distr
   ```

5. Перейдите в созданную директорию.
6. Добавьте файлу **setup.sh** атрибут "*исполняемый*":

   ```
   chmod +x ./setup.sh
   ```

7. Запустите скрипт **setup.sh**, который входит в состав дистрибутива:

   ```
   ./setup.sh
   ```

8. Выберите тип установки **Install**. Будет доступен список компонентов:
9. Выберите **DM Server Service, FrontEnd**. В этом случае будут автоматически:
   - получен и записан в Device Monitor открытый ключ службы **guard** Платформы, необходимый для корректного взаимодействия веб-интерфейса с Сервером
   - исправлен файл n.yaml

   > **Важно!**

Любой продукт, который будет установлен в Центре расследований после Device Monitor, сгенерирует новый файл **n.yaml**, и из него будет удалена секция, которая необходима для корректного взаимодействия веб-интерфейса с Сервером. Чтобы восстановить **n.yaml**:

a. Запустите скрипт установки:

```
./setup.sh
```

b. Выберите в меню пункт **Utilities**.
c. Выберите **Fix n.yaml file**. Дождитесь окончания процесса.

Будут предложены режимы установки Платформы с веб-интерфейсом Центра расследований:

- **Central** – предназначен для установки на основную ноду или в случае отсутствия уже установленного Центра расследований.
- **Office** – предназначен для распределенной установки.

10. Выберите **Office**.
11. Введите IP-адрес центральной ноды Платформы, установленной ранее.
12. Получите токен центральной ноды. Для этого на сервере с центральной нодой выполните команду:

```
kubeadm token list
```

13. Скопируйте полученный токен. Начнется установка Платформы.
14. Введите полученный токен на ноде офисной Платформы.
15. Укажите лейбл для офисной ноды Платформы
16. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
17. Введите **y**, чтобы принять лицензионное соглашение, и нажмите **Enter**.
18. Введите IP-адрес сервера в формате IPv4: `"xxx.xxx.xxx.xxx"` и нажмите **Enter**.
19. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию 80%) и нажмите **Enter**.
20. Укажите путь для размещения данных Clickhouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
21. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
22. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
23. Укажите путь для хранения данных (по умолчанию `/opt/dsdata`) и нажмите **Enter**.
24. Укажите порт подключения к веб-интерфейсу (по умолчанию `443`) и нажмите **Enter**.
25. Дождитесь окончания процесса установки офисной ноды Платформы. Далее будет произведена установка Сервера Device Monitor. При этом:
    a. Будут созданы каталоги:
        - /var/log/iwdms - каталог логов выполнения сервера DM
        - /opt/iw/dmserver/bin - каталог с файлами сервера DM
        - /opt/iw/dmserver/queue - каталог файловой очереди
        - /opt/iw/dmserver/log - символическая ссылка на каталог /var/log/iwdms

b. Добавлен пользователь **iwdms** с ключом `--system`, что позволяет запустить под этим пользователем службу, но не дает авторизоваться под этим пользователем в Центре администрирования
c. Распакован zip-файл из `data/iwdms` инсталляционного пакета в требуемые каталоги. Для вышеуказанных папок в качестве владельца буден назначен пользователь **iwdms**
d. В каталоге systemd служб `/etc/systemd/system` будет добавлен файл манифеста службы Сервера Device Monitor **iwdms.service**, а также службы синхронизации с Active Directory - **iwdms_ldap.service**

26. Выберите язык устанавливаемого сервера и нажмите **Enter**. Это определит названия предустановленных групп, политик и правил.
27. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Выберите **Accept and continue** и нажмите **Enter**
28. Далее можно выбрать, какой тип сервера необходимо установить: Основной (**Primary**) или Второстепенный (**Secondary**).
29. Если вы выбрали основной сервер (**Primary**), то укажите путь до PFX-файла ключа шифрования канала между Сервером Device Monitor и Агентами. Если путь не указывать, то будет использован путь, предложенный по умолчанию, – `/opt/iw/dmserver/ssl.pfx`
30. Если вы устанавливаете Сервер на новую БД, то ключ шифрования необходимо создать. Выберите **Yes**.

В случае успешной установки будет запущена служба Сервера Device Monitor. Служба будет помечена как запускаемая автоматически. Чтобы проверить, запущена ли служба сервера DM, выполните команду:

```
systemctl status iwdms
```

Далее перейдите в Центр расследований, введя в браузере IP-адрес центральной ноды Платформы.

Подготовка Сервера Device Monitor к миграции с ОС Windows на ОС семейства Linux

Если при переходе с ОС Windows на Device Monitor for Linux вам необходима миграция данных, выполните шаги:

> **Важно!**
>
> Не удаляйте основной сервер Device Monitor до проверки поддержки миграции.

1. Обновите Device Monitor, установленный на ОС Windows, на версию 7.17 (подробнее см. "Документация для модуля InfoWatch Device Monitor, установленного на ОС MS Windows", статья "Обновление серверной части InfoWatch Device Monitor")
2. Убедитесь, что База данных поддерживает миграцию, т.е. не содержит правил, которые не поддерживаются в новой версии. Для этого:
   a. В дистрибутиве по пути `7.17.x\DM for Windows\Utils` скопируйте архив `CheckMigration_x64.zip`.
   b. Распакуйте архив.
   c. В файле `run.bat` укажите параметры доступа к Базе данных.

d. Запустите файл `run.bat` с компьютера, где установлен основной сервер DM.
e. Дождитесь сообщения о готовности к миграции: *The database is ready for migration*. Если утилита выведет список правил, которые не поддерживаются в новой версии, то необходимо:
   - удалить эти правила
     или
   - в текущей Консоли Офицера безопасности настроить параметры так, чтобы поддержка осуществлялась.

3. Проверьте, что и указанная в параметрах СУБД PostgreSQL для сервера Device Monitor на ОС Windows, и СУБД PostgreSQL сервера Device Monitor, установленного на ОС Linux, созданы и установлены **с поддержкой русской локали**. Это необходимо для корректной работы веб-интерфейса и поиска объектов с использованием кириллицы в нем. Чтобы проверить локаль, выполните команду:

   ```
   psql -l
   ```

   Локаль указана в столбцах `LC_COLLATE` и `LC_CTYPE` строки искомой базы данных, например:

   ```
                                Список баз данных
     Имя   | Владелец | Кодировка | LC_COLLATE  | LC_CTYPE   |    Права доступа
   ----------+----------+-----------+-------------+-------------+-----------------------
   iwdms    | postgres | UTF8      | ru_RU.UTF-8 | ru_RU.UTF-8 |
   ```

4. Если установлена английская локаль, то выполните действия, чтобы установить русскую:
   a. В файле `run.bat` укажите параметры доступа к Базе данных. При этом добавьте строку, если она отсутствует, и укажите актуальные значения IP, PORT, DB_NAME, USER_NAME, PASSWORD:

      ```
      "CheckMigration.exe" --Server <IP>:<PORT> --DBName <DB_NAME> --User <USER_NAME> --
      Password "<PASSWORD>" --Culture "ru-RU"
      ```

      Пример:

      ```
      "CheckMigration.exe" --Server 10.20.30.40:1234 --DBName iwdms --User postgres --
      Password "pass123" --Culture "ru-RU"
      ```

   b. Запустите файл `run.bat` с компьютера, где установлен основной Сервер Device Monitor.
5. Удалите все Серверы Device Monitor, оставив Базу данных и сохранив секретный ключ сервера. Для этого воспользуйтесь инструкцией для вашей версии продукта.

Неподдерживаемые в новой версии правила:

- Автоматическое создание снимков экрана для списков приложений и ресурсов
- Контроль ввода текста с клавиатуры для списка ресурсов
- Контроль активности сотрудника по сбору статистики действий: пользователя, с файлами, отправки на печать

- Контроль звукового окружения
- Контроль мессенджеров: MMP, Facebook
- Контроль копирования с/на CD/DVD
- Запрет создания снимков экрана для всех приложений или списков приложений
- Контроль файловых операций при теневом копировании файлов, передаваемых в приложениях
- Контроль приложений: запрет запуска, использования буфера обмена, печати
- Запись видео экрана рабочей станции по триггеру

Неподдерживаемые настройки:

- параметров AD и параметров серверов, подключение к которым разрешено
- автоматического обновление Агентов
- отправки событий с Агента в Activity Monitor
- ключа формирования кодов
- подключения для получения управляющих команд от Activity Monitor
- перехвата звукового окружения

1.5.5 Настройка проверки сертификатов удаленных серверов

На сервере Device Monitor для повышения безопасности реализована возможность проверки сертификатов удаленных серверов. Данная проверка позволяет установить подлинность удаленного сервера при подключении к нему.

Device Monitor осуществляет проверку следующих сертификатов:

- сертификата службы XAPI – при подключении к серверу Traffic Monitor для отправки событий
- сертификата веб-сервера Traffic Monitor (сертификат TMConfig) – при подключении к серверу Traffic Monitor для синхронизации политик защиты данных
- сертификата службы EPEVENTS – при подключении к серверу Платформы для отправки событий

Чтобы успешно подключиться к удаленному серверу для отправки событий:

1. Настройте проверку сертификатов на сервере Device Monitor;
2. На сервере Device Monitor установите корневой сертификат удаленного сервера в хранилище корневых сертификатов уровня "локальный компьютер".

Чтобы успешно подключиться к серверу Traffic Monitor для синхронизации политик защиты данных:

1. Настройте проверку сертификатов на сервере Device Monitor;
2. В центре сертификации вашей компании выпустите сертификат X.509 для веб-сервера Traffic Monitor;
3. Настройте работу веб-сервера Traffic Monitor с выпущенным сертификатом;
4. Установите корневой сертификат веб-сервера Traffic Monitor в хранилище корневых сертификатов уровня "локальный компьютер" на сервере Device Monitor.

Важно!

Если вы не выполните шаги 2-4, то необходимо отключить проверку сертификата веб-сервера Traffic Monitor. Соединение с сервером Traffic Monitor будет защищено протоколом TLS, но сервер Device Monitor не сможет удостовериться, что он подключился к нужному серверу Traffic Monitor.

Чтобы настроить проверку сертификатов удаленных серверов при установлении SSL-сессии:

Установите значение `True` или `False` для следующих полей таблицы Settings в базе данных сервера Device Monitor:

- `IGNORE_SSLERR_TMXAPI_CONNECTION` – игнорировать проверку сертификата службы XAPI Traffic Monitor;
- `IGNORE_SSLERR_TMCONFIG_CONNECTION` – игнорировать проверку сертификата TMConfig Traffic Monitor;
- `IGNORE_SSLERR_PLATFORM_CONNECTION` – игнорировать проверку сертификата службы EPEVENTS Платформы.

При значении `False` проверка сертификата будет выполняться.

Значение поля `IGNORE_SSLERR_TMXAPI_CONNECTION` по умолчанию:

- при первичной установке сервера Device Monitor – `False`, т.е. проверка сертификата службы XAPI Traffic Monitor включена;
- при обновлении сервера Device Monitor версии 7.9 и ниже – `True`, т.е. проверка выключена;
- при обновлении сервера Device Monitor версии 7.10 и выше – значение остается равным тому, что было до обновления.

Значение поля `IGNORE_SSLERR_TMCONFIG_CONNECTION` по умолчанию:

- при первичной установке сервера Device Monitor – `False`, т.е. проверка сертификата веб-сервера Traffic Monitor включена;
- при обновлении сервера Device Monitor – `True`, т.е. проверка выключена.

Значение поля `IGNORE_SSLERR_PLATFORM_CONNECTION` по умолчанию:

- при первичной установке сервера Device Monitor – `True`, т.е. проверка сертификата службы EPEVENTS Платформы выключена;
- при обновлении сервера Device Monitor версии 7.9 и ниже – `True`, т.е. проверка выключена;
- при обновлении сервера Device Monitor версии 7.10 и выше – значение остается равным тому, что было до обновления.

Если значения параметров `IGNORE_SSLERR_TMXAPI_CONNECTION`, `IGNORE_SSLERR_TMCONFIG_CONNECTION` и `IGNORE_SSLERR_PLATFORM_CONNECTION` были изменены, то чтобы правила проверки сертификатов удаленных серверов вступили в силу, перезапустите службу сервера Device Monitor.

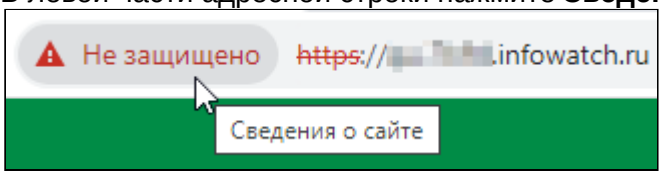
Чтобы установить сертификат службы XAPI Traffic Monitor:

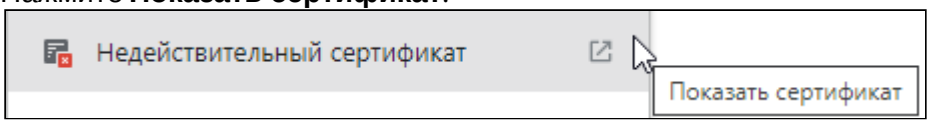
1. На сервере Traffic Monitor откройте файл `/opt/iw/tm5/etc/xapi.conf`.
2. В секции **ThriftServers** -> **xapi** найдите параметр `TrustedCertificatesPath`.
   В значении данного параметра указаны путь к файлу корневого сертификата и его имя. Если указан относительный путь, то его необходимо рассматривать от каталога `/opt/`

`iw/tm5`.
Значение параметра `TrustedCertificatesPath` по умолчанию: `/opt/iw/tm5/etc/cert/trusted_certificates`.

3. Скопируйте корневой сертификат на компьютер, где установлен или будет установлен сервер Device Monitor.
4. Перейдите в директорию, куда был скопирован корневой сертификат.
5. Переименуйте корневой сертификат в `tmca.crt`.
6. Введите команды в зависимости от операционной системы, в среде которой производится установка корневого сертификата:
   - Для операционной системы РЕД ОС:
     ```
     sudo cp tmca.crt /etc/pki/ca-trust/source/anchors/
     sudo update-ca-trust force-enable
     sudo update-ca-trust extract
     ```
   - Для операционной системы Альт:
     ```
     su -
     cp tmca.crt /etc/pki/ca-trust/source/anchors/
     update-ca-trust
     ```
   - Для операционной системы Astra Linux:
     ```
     sudo cp tmca.crt /usr/local/share/ca-certificates/tmca.crt
     sudo update-ca-certificates
     ```
     Выполнение команд может занять некоторое время.

Чтобы установить сертификат веб-сервера Traffic Monitor Traffic Monitor:

1. Откройте Консоль управления Traffic Monitor в браузере.
2. Экспортируйте сертификат веб-сервера Traffic Monitor из браузера, в нашем примере Google Chrome. Для этого:
   a. В левой части адресной строки нажмите **Сведения о сайте**.
   

   b. Нажмите **Показать сертификат**.
   

   c. В Инструменте просмотра сертификатов откройте вкладку *Подробнее*.
   d. Нажмите **Экспорт**.
   e. Нажмите **Сохранить**.
3. Скопируйте корневой сертификат на компьютер, где установлен или будет установлен сервер Device Monitor.
4. Перейдите в директорию, куда был скопирован корневой сертификат.
5. Выполните шаг 6 инструкции по установке сертификата службы XAPI Traffic Monitor, описанной выше, используя вместо `tmca.crt` имя скопированного ранее корневого сертификата веб-сервера Traffic Monitor.

Чтобы установить сертификат службы EPEVENTS Платформы:

1. На сервере Платформы получите корневой сертификат `plca.crt` с помощью команды:
   `kubectl get secret -n infowatch epeventskeys-central -o 'go-template={{index .data "tls.crt"}}' | base64 -d > plca.crt`
   Если сервер Платформы не является центральным в кластере, то команда будет иметь вид:
   `kubectl get secret -n infowatch epeventskeys-<node label> -o 'go-template={{index .data "tls.crt"}}' | base64 -d > plca.crt`
   где `<node label>` – это имя серверной ноды.
2. Скопируйте корневой сертификат на компьютер, где установлен или будет установлен сервер Device Monitor.
3. Перейдите в директорию, куда был скопирован корневой сертификат.
4. Выполните шаг 6 инструкции по установке сертификата службы XAPI Traffic Monitor, описанной выше, используя вместо `tmca.crt` имя скопированного ранее корневого сертификата Платформы.

Выполнение команд может занять некоторое время.

Просмотр логов

Если сервер Device Monitor не сможет проверить сертификат, в логах появится ошибка с указанием сертификата и его статуса:

`Can't validate TmXapi certificate. Chain error: Certificate thumbprint: <thumbprint> Subject: CN=XAPI, OU=TD, O=InfoWatch, S=Moscow, C=RU`

> `UntrustedRoot Цепочка сертификатов обработана, но обработка прервана на корневом сертификате, у которого отсутствует отношение доверия с поставщиком доверия.`

`Certificate thumbprint: <thumbprint> Subject: CN=XAPI, OU=TD, O=InfoWatch, L=Moscow, S=Moscow, C=RU`

> `UntrustedRoot Цепочка сертификатов обработана, но обработка прервана на корневом сертификате, у которого отсутствует отношение доверия с поставщиком доверия.`

Интервал между отправкой сообщений об ошибках в лог определяется значениями полей `WRITE_SSLVERIFY_TMXAPI_LOG_INTERVAL`, `WRITE_SSLVERIFY_TMCONFIG_LOG_INTERVAL` и `WRITE_SSLVERIFY_PLATFORM_LOG_INTERVAL` таблицы Settings базы данных сервера Device Monitor. По умолчанию эти значения равны 3600 секунд. Если сертификат удаленного сервера повторно не пройдет проверку и с момента последней отправки сообщения об ошибке прошло меньше указанного времени, то новое сообщение об ошибке отправлено не будет.

Чтобы просмотреть логи:

1. Перейдите в каталог `/opt/iw/dmserver/log`.
2. Откройте файл `iwdms-<date>.txt`, где `<date>` – это дата в формате YYYYMMDD.

1.5.6 Установка Агентов Device Monitor

Агент Device Monitor и Сервер Device Monitor необходимо устанавливать в одном часовом поясе. Это обеспечит отображение корректного времени перехвата события.

Важно!

Не допускается установка Агента InfoWatch Device Monitor и сервера Device Monitor на один компьютер, это может привести к неработоспособности сервера.

Агенты InfoWatch Device Monitor могут быть установлены на рабочие станции одним из следующих способов:

- Локальная установка. Выполняется при помощи универсальной программы установки непосредственно на каждом компьютере:
  - Локальная установка Агента на рабочей станции под управлением ОС Windows
  - Локальная установка Агента на рабочей станции под управлением ОС семейства Linux
  - Локальная установка Агента на рабочей станции под управлением Mac OS
- Установка с помощью задачи распространения. Выполняется в веб-консоли InfoWatch Device Monitor.

Чтобы успешно установить или обновить Агент InfoWatch Device Monitor, следуйте рекомендациям:

1. Исключите параллельное использование сторонних DLP-систем;
2. Добавьте в исключения антивируса процессы Агента InfoWatch Device Monitor (список файлов см. в статье "Список файлов Агента InfoWatch для добавления в исключения антивирусов");
3. Отключите самозащиту антивируса;
4. По возможности отключите или удалите антивирус на время установки, обновления и удаления Агента InfoWatch Device Monitor;
5. Если на рабочих станциях используется VMWare Horizon VDI 8.0.0-16530, то необходимо отключить компонент ftapihook654.dll версии 3.2.4.1. (подробнее см. "Проблема совместимости с VmWare Horizon VDI")
6. **На рабочих станциях под управлением ОС Astra Linux на время удаленной установки Агентов Device Monitor отключите часть настроек ОС.**

   Для этого:

   a. Отключите блокировку интерпретаторов, кроме bash, с помощью команды: `sudo astra-interpreters-lock disable`
   b. Отключите блокировку интерпретатора bash с помощью команды: `sudo astra-bash-lock disable`
   c. Отключите запрет установки бита исполнения с помощью команды: `sudo astra-nochmodx-lock disable`

   Примечание:

   После установки Агентов Device Monitor, вы можете вернуть измененные настройки к исходным значениям, для этого выполните те же команды, заменив в них `disable` на `enable`.

   Подробнее о настройках безопасности ОС Astra Linux см. документацию на официальном сайте.

7. Обеспечьте доступ к портам, необходимым для работы Агента InfoWatch Device Monitor (список портов см. в "*Infowatch Traffic Monitor. Руководство администратора*", раздел "Настройка Сервера InfoWatch Device Monitor");
8. **Для быстрого получения FQDN имени рабочей станции под управлением ОС семейства Linux, перед установкой Агента убедитесь, что следующие параметры настроены:**
    a. Файл `/etc/hostname` содержит:
        - имя хоста, например, `computer-20`;
        или
        - FQDN имя, например, `computer-20.corp.ad`
    b. В файле `/etc/hosts` определено соответствие между именем хоста, FQDN именем и IP-адресом:
        - если на рабочей станции определено имя хоста и у рабочей станции есть FQDN имя, то файл должен содержать следующую строку:
        `127.0.1.1 <FQDN name> <hostname>`

        где `<FQDN name>` – FQDN имя;
        `<hostname>` – имя хоста.
        Например, для имени хоста `computer-20` и FQDN имени `computer-20.corp.ad` строка будет выглядеть следующим образом:
        `127.0.1.1 computer-20.corp.ad computer-20`
        - если у рабочей станции нет FQDN имени, то файл должен содержать следующую строку:
        `127.0.1.1 <hostname>`
        - если в файле `/etc/hostname` указано FQDN имя, то файл должен содержать следующую строку:
        `127.0.1.1 computer-20.corp.ad`

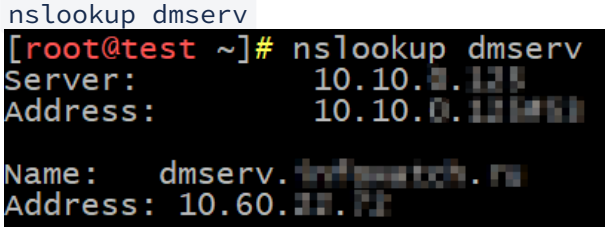
        > **Примечание:**
        >
        > Значение IP-адреса в строке может быть равно 127.0.1.1 или 127.0.0.1.

        > **Примечание:**
        >
        > Перечисленные параметры также могут быть настроены с помощью стороннего ПО, например, программы "Ввод в домен".

        Для исключения ошибок при добавлении хоста в Active Directory к имени хоста предъявляются следующие требования:
        - разрешены символы латинского алфавита (A-Z,a-z), цифры (0-9) и дефис;
        - длина имени должна быть не более 15 символов.
9. Для соединения между сервером InfoWatch Device Monitor и рабочей станцией, на которую устанавливается Агент InfoWatch Device Monitor, необходимо, чтобы их доменные имена корректно преобразовывались (резолвились) DNS-сервером в IP-адреса. Убедитесь в этом с помощью команды:
`nslookup <имя_хоста>`
В результате будет выведено сообщение, содержащее адрес DNS-сервера, FQDN имя рабочей станции и ее адрес.

Пример:

`nslookup dmserv`



Если в результате выполнения данной команды для сервера InfoWatch Device Monitor выведена ошибка `server can't find dmserv: SERVFAIL`, то соединение не будет установлено.

> **Примечание:**
>
> Также для установления соединения Агента InfoWatch Device Monitor с сервером InfoWatch Device Monitor вы можете добавить следующую строку в файл `/etc/hosts` на рабочей станции, на которую устанавливается Агент:
> `<IP_адрес_сервера_Device_Monitor> <имя_сервера_Device_Monitor>`

При возникновении трудностей с настройкой сетевых параметров обратитесь к системному администратору.

10. Если не требуется использовать компонент контроля сетевых соединений, отключите его при создании дистрибутива Агента InfoWatch Device Monitor;
11. Установите Агенты InfoWatch Device Monitor сначала на тестовые машины или небольшую группу рабочих станций;
    Если на тестовой группе в течение 2-3 дней не возникало ошибок, снижения производительности, зависания приложений, продолжайте установку на рабочие станции.

> **Важно!**
>
> Обратите внимание, что в процессе установки Агента:
>
> - Выключение питания компьютера может привести к ошибкам, ведущим к нестабильной работе операционной системы. Особенность также относится к процессу удаления Агента.
> - Выполняется кратковременный разрыв всех сетевых соединений. Это связано с установкой компонентов контроля сетевого трафика, используемых в Device Monitor (IWPROXY и IWNBG). Кроме того, разрыв связан как с технологическими особенностями ОС при установке модулей, так и с принудительным перезапуском сетевых карт при установке модуля «прозрачная прокси». Особенность также относится к процессам удаления и обновления Агента.
> - Будут закрыты (если они были запущены) программы Mozilla Firefox и Mozilla Thunderbird.

> **Примечание:**

Если вы устанавливаете Агента на рабочую станцию под управлением ОС Windows 7 Service Pack 1 или Windows 2008 R2 Server:

- Установите пакеты исправлений Windows для указанных ОС. См. в статье "Аппаратные и программные требования".
- Учтите, что если Агент устанавливается впервые, компонент *Контроль сетевых соединений* не будет установлен. При необходимости, данный компонент возможно установить вручную, используя командную строку.

Примечание:

Запуск Агента InfoWatch Device Monitor осуществляется автоматически сразу после установки. До перезагрузки компьютера функционал Агента ограничен только:

- перехватом трафика, проходящего через proxy-сервер,
- сетевым перехватом (при установке Агента на ОС Windows 8 и более поздние),
- перехватом копирования на внешние носители.

Чтобы ограничить доступ к данным Device Monitor, при установке Агента на ОС семейства Linux создаются следующие учетные записи в операционной системе:

- *iwdm* – используется основной службой Device Monitor;
- *iwdeployagent* – используется службой распространения агентов Device Monitor;
- *iwregistry* – в настоящий момент не используется.

При удалении Агента InfoWatch Device Monitor указанные учетные записи будут удалены автоматически.

Важно!

Не допускается самостоятельное удаление или изменение перечисленных выше учетных записей, так как это приведет к неработоспособности Агента InfoWatch Device Monitor.

Локальная установка Агента на рабочей станции под управлением ОС Windows

Важно!

Настоятельно не рекомендуется устанавливать Агенты InfoWatch Device Monitor на компьютеры с одинаковыми именами. Такие компьютеры будут зарегистрированы как один компьютер и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

Получите и запишите на внешний носитель актуальный пакет для установки Агента. Установку на компьютере может выполнять пользователь, имеющий на нем права локального администратора.

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета с последующим вводом параметров вручную:

1. **Запуск мастера установки**
   Вставьте внешний носитель с дистрибутивом Агента в компьютер. Затем откройте

каталог `Client`. В данном каталоге найдите и запустите пакет установки для требуемой платформы для развертывания в соответствии с заданными при формировании пакетов параметрами, например, `InfoWatch.DeviceMonitor.Client.7.17.0.x64.msi`.
В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor Client. Нажмите на кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

2. **Выбор каталога для установки**
Укажите путь к каталогу, в который будет установлен **Агент**.

> **Важно!**
>
> Путь к каталогу может содержать следующие символы:
>
> `0-9`, `a-z`, `A-Z`, `" "`, `":"`, `"."`, `"_"`, `"-"`, `"\"`, `"("`, `")"`
>
> При наличии в пути других символов, установка Агента будет некорректной.

Нажмите кнопку **Далее**.

3. **Настройка параметров**
Укажите параметры соединения с Сервером InfoWatch Device Monitor:
   - **Сервер**. Имя сервера InfoWatch Device Monitor.
   - **Порт**. Номер порта, используемого для соединения между Агентом и Сервером InfoWatch Device Monitor (по умолчанию задан порт 15101).

Нажмите кнопку **Далее**.

4. **Завершение установки**
После перехода к окну **Подтверждение установки**, нажмите кнопку **Далее**, чтобы начать установку Агента. Следуйте дальнейшим указаниям мастера для завершения установки. По окончании установки перезагрузите компьютер.

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета в тихом режиме:

Для минимизации участия в процессе установки вы можете установить Агента в тихом режиме.

Перед запуском инсталлятора:

1. Вставьте внешний носитель с дистрибутивом Агента в компьютер.
2. Запустите командную строку (`cmd.exe`) от имени Администратора.
3. Перейдите в каталог, где находится дистрибутив Агента, выполнив команду:

```
cd <путь_до_дистрибутива>
```

Ознакомьтесь со списком ключей в таблице ниже, с их помощью вы можете указать инсталлятору параметры установки продукта.

Ключ	Описание
`/quiet`	Запуск установки без отображения пользовательского интерфейса

Ключ	Описание
`/i <имя_пакета_установки>`	Запуск установки продукта с помощью указанного файла

`PREDEFINED_CLIENTDIR`	Директория для установки продукта
	Значение по умолчанию:
	`"%ProgramFiles%\Infowatch\DeviceMonitor\Client"`
	Важно!
	Путь к каталогу может содержать следующие символы:
	`0-9` , `a-z` , `A-Z` ,`":"`,`"."`,`"_"`,`"-"`,`"\"`,`" "`
	При наличии в пути других символов, установка Агента будет некорректной.

`UNINSTALL_PASSWORD_SHA1_HASH`	Хеш-значение пароля деинсталляции в шестнадцатеричном формате, вычисленное по алгоритму SHA-1. Если задать данный параметр, то удалить Агента Device Monitor можно будет только введя правильный пароль. **Важно!** Хеш-значение пароля необходимо вычислять для кодировки Юникод UTF-16LE. Указывайте хеш-значение, используя только заглавные буквы и цифры.
`IWPROXYDN`	Строка с доменным именем корневого сертификата proxy-сервера на рабочей станции, который используется для выпуска сертификатов при перехвате защищенного трафика. Имя должно соответствовать стандарту X.509 и содержать поле CN (Common Name). Поля внутри имени должны быть разделены запятой Значение по умолчанию: `"CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow"`
`SHOW_USER_NOTIFICATION`	Показывать пользователю уведомление о необходимости перезагрузить компьютер. Возможные значения: • `"#x01000000"` (по умолчанию) – показывать • `"#x00000000"` – не показывать
`WAITING_REBOOT_PERIOD`	Время ожидания перезагрузки рабочей станции до момента, когда Агент начнет показывать пользователю уведомление о необходимости перезагрузить компьютер.

Ключ	Описание
	Указывается в часах Значение по умолчанию: `"0"`
`REBOOT_NOTIFICATION_PERIOD`	Время до принудительной перезагрузки, в течении которого Агент показывает пользователю уведомление о необходимости перезагрузить компьютер. Указывается в часах. Возможные значения: • целые числа от 0 до 1000; • `"-1"` (по умолчанию), чтобы показывать уведомление бесконечно и не перезагружать компьютер принудительно.
`REBOOT_NOTIFICATION_RATE`	Частота, с которой Агент показывает пользователю уведомление о необходимости перезагрузить компьютер. Указывается в минутах. **Примечание:** Если параметр не задан, уведомление показывается каждые 10 минут
`REBOOT_NOTIFY_MESSAGE`	Текст уведомления о необходимости перезагрузить компьютер. Сообщение может содержать не более 255 символов Текст по умолчанию: `"Необходимо как можно скорее перезагрузить компьютер"`
`FORCE_REBOOT`	Отправить финальное уведомление перед принудительной перезагрузкой. Возможные значения: • `"0"` (по умолчанию) – показывать финальное уведомление • `"1"` – не показывать финальное уведомление **Важно!** После финального уведомления у сотрудника будет 5 минут на завершение своих операций. Если для параметра задано значение `"1"`, то принудительная перезагрузка (если она предусмотрена параметром `REBOOT_NOTIFICATION_PERIOD`) будет осуществлена неожиданно для сотрудника
`HIDE_CLIENT`	Скрывать присутствие Агента Device Monitor от пользователя рабочей станции. Возможные значения: • `"#x01000000"` – скрывать Агента • `"#x00000000"` (по умолчанию) – не скрывать Агента **Важно!**

Ключ	Описание
	Неуведомление об использовании перехватчиков может входить в конфликт с действующим законодательством вашей страны. **Важно!** Уведомление о необходимости перезагрузить компьютер не будет показано, если для данного параметра задано значение `"#x01000000"` – скрывать Агента.
`NOIWPROXY`	Не устанавливать компонент перехвата сетевого трафика. Возможные значения: • `"0"` (по умолчанию) – установить компонент • `"1"` – не устанавливать компонент
`NOIWNBG`	Не устанавливать компонент контроля периметра сети. Возможные значения: • `"0"` (по умолчанию) – установить компонент • `"1"` – не устанавливать компонент
`SRVPOOL`	Список серверов Device Monitor, с которыми может соединяться Агент. Список задается в следующем виде: `<Сервер>[;<Сервер>[;<Сервер>[...]]]` где `<Сервер>` = `<DNS имя сервера>:<номер порта>` Пример значения параметра: `"dmserver:15101;"` Если Агент не сможет соединиться с первым по списку сервером, то он будет пытаться соединиться со следующим по списку и так далее. После соединения с сервером Агент будет привязан к нему.
`/lvp <имя_лог_файла>`	Записывать данные в указанный лог-файл

Чтобы установить Агента InfoWatch Device Monitor:

1. В командной строке запустите программу установки Агента с указанием параметров.
   Пример команды установки:

   ```
   %windir%\system32\msiexec.exe /quiet /i
   InfoWatch.DeviceMonitor.Client.x64.ru.7.17.0.192.msi
   PREDEFINED_CLIENTDIR="%ProgramFiles%\Infowatch\DeviceMonitor\Client"
   IWPROXYDN="CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO
   InfoWatch,OU=TechDep,ST=Moscow" SHOW_USER_NOTIFICATION="#x01000000"
   WAITING_REBOOT_PERIOD="48" REBOOT_NOTIFICATION_PERIOD="10"
   REBOOT_NOTIFICATION_RATE="1" HIDE_CLIENT="#x00000000" FORCE_REBOOT="0"
   NOIWPROXY="0" NOIWNBG="0" SRVPOOL="dmserver:15101;" /lvp
   InfoWatch.DeviceMonitor.Client.x64.ru.7.17.0.192.log
   ```
2. Дождитесь завершения установки.
3. Перезагрузите компьютер.

Локальная установка Агента на рабочей станции под управлением ОС семейства Linux

> **Важно!**
>
> Настоятельно не рекомендуется устанавливать Агенты InfoWatch Device Monitor на компьютеры с одинаковыми именами. Такие компьютеры будут зарегистрированы как один компьютер и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

> **Примечание:**
>
> Если на компьютере установлена кастомизированная версия системы SeLinux, корректная установка Агента не гарантируется.

1. **Подготовка к установке:**
   a. Убедитесь, что пользователь, от имени которого будет произведена установка, имеет необходимые права:
      - на компьютере под управлением ОС Альт Рабочая Станция 10 - права на исполнение su;
      - на компьютере под управлением других ОС семейства Linux - привилегии sudoers.

   b. Скопируйте на компьютер архив, в котором содержатся пакет и скрипты для установки и удаления Агента Device Monitor. Архив поставляется в составе дистрибутива. Название архива может отличаться в зависимости от используемой ОС:
      - `Setup.AstraLinux-1.7-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.7;
      - `Setup.AstraLinux-1.8-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.8;
      - `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 7.3.1;
      - `Setup.RedOS-8.0-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 8.0;
      - `Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz` - для Альт Рабочая станция 10.

      где `x.x.x.xx` - номер сборки.
      Далее мы рассмотрим пример установки Агента на РЕД ОС 7.3. Установка на других поддерживаемых ОС аналогична. Примеры команд для них приведены ниже.

   c. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:
      ```
      sudo tar -xvzf Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz
      ```
      В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrade.sh`, `iwdm_<версия_агента>.deb`.
2. **Установка Агента InfoWatch Device Monitor:**

a. Перейдите в директорию, в которую распаковано содержимое архива `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` .
b. Для установки Агента запустите скрипт, выполнив команду:
   - Для обычной установки (при этом будет установлен компонент перехвата сетевого трафика):
     `sudo ./install.sh <сервер>:<порт>`
     где `<сервер>` - ip-адрес или доменное имя Сервера InfoWatch Device Monitor, `<порт>` - порт подключения к Серверу InfoWatch Device Monitor.
     В нашем примере команда будет следующей:
     `sudo ./install.sh dm-server:15101`

     Продукт будет установлен в директорию `/opt/iw/dmagent` .
   - Для установки без компонента перехвата сетевого трафика:
     `sudo IWDM_NO_PROXY=1 ./install.sh <сервер>:<порт>`
c. Проверить статус сервисов можно командой:
   `sudo systemctl status "iwdm*"`

   > **Примечание:**
   >
   > Если вы выбрали не устанавливать компонент перехвата сетевого трафика, то:
   >
   > - Сервис `iwdmproxy` не будет запущен.
   > - В директории `/opt/iw/dmagent/etc/iwdmproxy` будет создан файл `no_proxy` .
   > - При обновлении Агента компонент перехвата сетевого трафика также не будет установлен.

d. Перезагрузите рабочую станцию с помощью команды:
   `reboot`

Примеры команд для других ОС:

1. **ОС Astra Linux:**
   a. Распаковка архива:
      `sudo tar -xvzf Setup.AstraLinux-1.7-iwdm.x64.x.x.x.xx.tar.gz`
   b. Запуск установки:
      `sudo ./install.sh dm-server:15101`
      В случае установки без компонента перехвата сетевого трафика:
      `sudo IWDM_NO_PROXY=1 ./install.sh dm-server:15101`
   c. Проверка статуса сервисов:
      `sudo systemctl status "iwdm*"`
2. **ОС Альт:**
   a. Распаковка архива:

      `tar -xvzf Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz`
   b. Запуск установки:

```
su -c "./install.sh dm-server:15101"
```

В случае установки без компонента перехвата сетевого трафика:

```
su -c "IWDM_NO_PROXY=1 ./install.sh dm-server:15101"
```

c. Проверка статуса сервисов:
`su - -c 'systemctl status "iwdm*"'`

Локальная установка Агента на рабочей станции под управлением Mac OS

Важно!

Настоятельно не рекомендуется устанавливать Агенты InfoWatch Device Monitor на компьютеры с одинаковыми именами. Такие компьютеры будут зарегистрированы как один компьютер и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

Важно!

Не допускается установка через SSH-подключение.

1. **Подготовка к установке:**
   a. Убедитесь, что пользователь, от имени которого будет произведена установка, имеет привилегии `sudoers`.
   b. Скопируйте на компьютер архив, в котором содержатся пакет и скрипты для установки и удаления Агента Device Monitor.
   В нашем примере – `Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`, где `x.x.x.xx` – номер сборки.
   c. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:

   ```
   sudo tar -xvzf Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz
   ```

   В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<версия_агента>.pkg`.
2. **Установка Агента InfoWatch Device Monitor:**
   a. Перейдите в директорию, в которую распаковано содержимое архива **`Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`**.
   b. Для установки Агента запустите скрипт, выполнив команду:

   ```
   sudo ./install.sh <сервер>:<порт>
   ```

   В команде выше:

`<сервер>` – IP-адрес или доменное имя Сервера InfoWatch Device Monitor,
`<порт>` – порт подключения к Серверу InfoWatch Device Monitor.
В нашем примере команда будет следующей:

```
sudo ./install.sh dm-server:15101
```

c. При установке скрипт вносит изменения в настройки доверительных сертификатов системы. После запуска скрипта операционная система запросит разрешение на это действие в отдельном окне. Для подтверждения введите пароль вашей учетной записи.
Дождитесь окончания установки. Продукт будет установлен в директорию `/opt/iw/dmagent`.
d. Проверьте статусы сервисов с помощью команд:

```
sudo launchctl print system/com.infowatch.iwdmproxy | grep state
```

```
sudo launchctl print system/com.infowatch.iwdmc | grep state
```

e. Перезагрузите рабочую станцию с помощью команды:

```
reboot
```

Установка Агентов с помощью задачи распространения

> **Примечание:**
>
> Установка Агента с помощью задачи распространения возможна только на рабочих станциях под управлением ОС Windows или ОС семейства Linux.

Для установки Агентов Device Monitor на рабочие станции с помощью задачи распространения в веб-консоли Device Monitor необходимо наличие установленного сервиса распространения (подробнее см. "Установка "Все-в-одном"", Шаг 34).

Перед установкой Агентов:

- Рекомендуется добавить файлы Агента в исключения антивируса. Список файлов см. в статье "Список файлов Агента InfoWatch для добавления в исключения антивирусов".
- Для распространения Агентов на рабочие станции под управлением:
  - ОС **Windows**:
    Установите Samba-клиент на сервер.
  - ОС **Astra Linux Special Edition** версий **1.7** и **1.8:**
    Для пользователя, от имени которого будет произведена установка Агента, настройте максимальный уровень мандатного доступа. Например, чтобы повысить уровень доступа для пользователя `root`, используйте команду:

```
sudo pdpl-user -i 63 root
```

- ОС **Альт Рабочая станция 10**:
  Для пользователя, от имени которого будет выполняться запуск задачи:
  1. Вручную включите доступ на рабочую станцию по SSH, выполнив команду:

     ```
     service sshd start
     ```

  2. В файле `/etc/openssh/sshd_config` раскомментируйте строку `PermitRootLogin`.
  3. Добавите пользователя в группу `/etc/sudoers`.

Для установки Агентов:

1. В разделе **Задачи** веб-консоли создайте задачу первичного распространения. См. "Задача первичного распространения и обновления".
2. Сформируйте список рабочих станций для установки Агентов.
3. Запустите задачу, нажав .
4. Введите учетные данные пользователя, от имени которого запускается задача, и нажмите **Запустить**.
5. Дождитесь окончания выполнения задачи. В области **Выполнение задачи** будет отображен список рабочих станций с информацией об Агентах.
6. Для корректной работы функциональности на рабочей станции под управлением ОС семейства Linux перезагрузите компьютер после установки Агента.

Важно!

Учтите, что:

- Не допускается установка Агента InfoWatch Device Monitor и сервера Device Monitor на один компьютер, т.к. это может привести к неработоспособности сервера.
- При установке, обновлении и удалении Агента выполняется кратковременный разрыв всех сетевых соединений. Это связано с установкой компонентов контроля сетевого трафика, используемых в Device Monitor (`IWPROXY` и `IWNBG`). Кроме того, разрыв связан как с технологическими особенностями ОС при установке модулей, так и с принудительным перезапуском сетевых карт при установке модуля *прозрачная прокси*.
- Если на компьютере установлена кастомизированная версия системы SELinux, корректная установка Агента не гарантируется.

1.6 Настройка сетевых правил доступа

Для корректной работы Системы должны быть разрешены соединения:

Компонент Системы, для работы которого	Взаимодействие между компонентами	Порт	Назначение порта

необходимо соединение	**Источник**	**Получатель**		
Сервер Device Monitor (DM)	Платформа	Сервер DM	TCP 15007	Взаимодействие Платформы с Сервером DM
	Сервер DM	Сервер БД	TCP 5432	Взаимодействие Сервера DM с базой данных
	Агент DM	Сервер DM	TCP 15004	Защищенное соединение Сервера DM с Агентами: Передача теневых копий (шифрованный канал)
	Агент DM	Сервер DM	UDP 15100	Защищенное соединение Сервера DM с Агентами: Уведомление Агентов
	Сервер DM	Агент DM		
	Агент DM	Сервер DM	TCP 15101	Защищенное соединение Сервера DM с Агентами: Передача теневых копий
	Агент DM	Сервер DM	TCP 15200	Инициация загрузки дистрибутива Агента с Сервера DM на рабочую станцию
	Сервер DM	Агент DM	TCP 15505	Установка и удаление Агента
	Рабочая станция Офицера безопасности	Платформа	TCP 443	Взаимодействие Офицера безопасности с Веб-консолью Сервера DM
Агент DM на ОС семейства Linux	Сервер DM	Рабочая станция сотрудника	TCP 22	Установка Агента

Примечание:

Если в процессе установки были назначены порты, отличные от указанных в таблице:

- используйте те порты, что были назначены, вместо указанных в таблице;

или

- измените их на порты из таблицы:
  a. Остановите службу Сервера DM с помощью команды:
  `systemctl stop iwdms`

b. Чтобы изменить порты соединения Сервера DM с Агентами, в таблице `ServerOption` базы данных Сервера DM отредактируйте параметры:
   - `NotificationPort` (UDP 15100);
   - `ClientFacadePort` (TCP 15101);
   - `SSLPort` (TCP 15004).

c. Включите службу Сервера DM с помощью команды:
`systemctl start iwdms`

1.7 Обновление Device Monitor

Обновление Device Monitor выполняется в том же порядке, что и установка:

1. Обновление Сервера Device Monitor
2. Обновление Агентов Device Monitor

1.7.1 Обновление Сервера Device Monitor

Важно!

Поддерживается обновление с версий **7.15** и **7.16**, и только **со сбросом** установки компонента **FrontEnd**.

Для обновления кластера из нескольких серверов сначала обновите по инструкции основной (**Primary**) сервер Device Monitor, а затем второстепенные (**Secondary**) серверы.

Убедитесь, что для базы данных, с которой взаимодействует сервер Device Monitor, установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

В статье представлены:

- Обновление с версии
- Обновление при распределенной установке

Обновление Сервера Device Monitor

Чтобы обновить Сервер Device Monitor:

1. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск.
2. Создайте каталог и распакуйте в него содержимое архива. В примере архив будет распакован в каталог `/tmp/dmsl_distr` :

```
mkdir -p /tmp/dmsl_distr && tar xvf dmsl_setup_7.17.0.296.tar.gz -C /tmp/dmsl_distr
```

3. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.17. В примере файл будет извлечен в каталог `/tmp/iwdm` :

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.17.0.296.tar.xz -C /tmp/iwdm
```

4. Перейдите в каталог `/tmp/iwdm` и выполните сброс установки Платформы. Если у вас установлены несколько продуктов InfoWatch на разных серверах, то выполните команду сначала на **офисной** ноде Платформы, затем на **центральной** ноде:

   ```
   ./setup.py reset
   ```

   Дождитесь окончания процесса.
5. Перезагрузите сервер с помощью команды:

   ```
   reboot
   ```

   Если у вас были установлены несколько продуктов InfoWatch, перезагрузите все серверы.
6. Чтобы освободить место на диске, вы можете удалить папку `/tmp/iwdm`.
7. Если вы обновляетесь с переходом на другой сервер или на новую ОС:
   a. Скопируйте на другой раздел или на новый сервер каталоги с данными, которые были указаны при установке.

      > **Примечание:**
      >
      > В **Device Monitor 7.15 и более ранних** каталоги по умолчанию расположены по пути **`/mnt`**.
      > В **Device Monitor 7.16** – по умолчанию по пути **`/opt`**.
      > Обязательно копируйте каталоги с сохранением прав и владельцев. Для копирования используйте стандартные средства, например, утилиту **`rsync`**.

   b. После сброса текущей установки скопируйте со старого сервера на новый файл с паролями базы данных `/var/lib/iwplatform/` **`dbadmin.yaml`**.
8. Вы можете удалить старые образы контейнеров с помощью команды:

   ```
   rm -rf /var/lib/containerd/
   ```

9. Перейдите в каталог `/tmp/dmsl_distr.`
10. Добавьте файлу **setup.sh** атрибут "*исполняемый* ":

    ```
    chmod +x ./setup.sh
    ```

11. Установите Платформу с Центром администрирования в режиме **Central** (или **Office** при распределенной установке):
    a. Запустите скрипт **setup.sh** :

```
./setup.sh
```

b. Выберите **Install**.
c. Выберите компонент **Only FrontEnd**.
d. Выберите режим **Central** (или **Office** при распределенной установке) и далее следуйте шагам 8-16, описанным в инструкции по установке "Новая установка". Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»

12. Обновите Сервер Device Monitor:
    a. Запустите скрипт **setup.sh**:

```
./setup.sh
```

    b. Выберите **Update**. Будет определена версия установленного Сервера Device Monitor.
    c. Для начала обновления выберите **Yes** и дождитесь окончания процесса.
13. Далее необходимо прописать в файл **n.yaml** настройки. Запустите скрипт установки:

```
./setup.sh
```

    a. Выберите **Utilities** и выполните пункт **Fix n.yaml file**.
    b. Укажите IP-адрес компьютера, на котором был установлен Сервер Device Monitor. Если он был установлен на текущем компьютере, нажмите **Enter** . Дождитесь окончания процесса.
    c. Затем необходимо получить открытый ключ службы **nguard** Платформы и сохранить его в каталог Сервера. Запустите скрипт установки:

```
./setup.sh
```

    d. Выберите **Utilities** и выполните пункт **Save platform guard public key to IWDM Service**. Дождитесь окончания процесса.

14. Перезапустите службу Сервера Device Monitor :

```
systemctl restart iwdms
```

15. Обновите все установленные второстепенные (**Secondary**) Серверы Device Monitor, выполнив шаг 8 инструкции.

Чтобы проверить корректность обновления, перейдите в веб-интерфейс Центра расследований и проверьте доступность раздела **Настройки > Сервер DM**.

Обновление при распределенной установке

> **Примечание:**

В инструкции для примера указаны версии продуктов, совместимые с Device Monitor 7.15, однако действия актуальны и для Device Monitor 7.16, и для совместимых с ним версий продуктов.

Исходные условия:

- Device Control версии 1.0 и Activity Monitor версии 3.1 установлены на центральной ноде Платформы.
- Сервер Device Monitor версии 7.15 установлен (в режиме `central`) на офисной ноде Платформы.

1. Скопируйте на офисную ноду архив с дистрибутивом Сервера Device Monitor.
2. Создайте каталог и распакуйте в него содержимое архива. В примере архив будет распакован в каталог `/tmp/dmsl_distr`:

   ```
   mkdir -p /tmp/dmsl_distr && tar xvf dmsl_setup_7.17.0.296.tar.gz -C /tmp/dmsl_distr
   ```

3. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.17. В примере файл будет извлечен в каталог `/tmp/iwdm`:

   ```
   mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.17.0.296.tar.xz -C /tmp/iwdm
   ```

4. Перейдите в каталог `/tmp/iwdm` и выполните сброс установки Платформы:

   ```
   ./setup.py reset
   ```

5. Перезагрузите текущий сервер с помощью команды:

   ```
   reboot
   ```

6. Чтобы освободить место на диске, вы можете удалить папку `/tmp/iwdm`.
7. Если вы обновляетесь с переходом на другой сервер или на новую ОС:
   a. Скопируйте на другой раздел или на новый сервер каталоги с данными, которые были указаны при установке.

      Примечание:

      В **Device Monitor 7.15 и более ранних** каталоги по умолчанию расположены по пути `/mnt`.
      В **Device Monitor 7.16** – по умолчанию по пути `/opt`.
      Обязательно копируйте каталоги с сохранением прав и владельцев. Для копирования используйте стандартные средства, например, утилиту `rsync`.

   b. После сброса текущей установки скопируйте со старого сервера на новый файл с паролями базы данных

/var/lib/iwplatform/
dbadmin.yaml .

8. На центральной ноде Платформы распакуйте архив с дистрибутивом Device Control версии 1.1 и выполните команду:

```
./setup.py reset
```

> **Важно!**
>
> Так как на сервере установлен также и Activity Monitor, то его установка будет сброшена в результате сброса установки Платформы. При сбросе установки на центральной ноде продукты на офисных нодах перестанут функционировать.

9. Перезагрузите текущий сервер с помощью команды:

```
reboot
```

10. На центральной ноде Платформы установите Activity Monitor версии 3.2 из его же установочного файла с помощью команды:

```
./setup.py install
```

Выполните шаги по установке из инструкции из руководства "Activity Monitor. Руководство по установке", статья "Установка Activity Monitor". Когда инсталлятор потребует указать каталоги для размещения данных, указывайте каталоги с данными прошлой версии и выбирайте « **n** » при ответе на вопрос «Очищать ли папки перед установкой?»

11. Затем на центральной ноде Платформы установите Device Control версии 1.1 из его же установочного файла с помощью команды:

```
./setup.py install
```

Выполните шаги по установке из инструкции из руководства "Device Control. Руководство по установке", статья "Установка Device Control".

12. На офисной ноде Платформы перейдите в каталог, где находится скрипт **setup.sh**, и добавьте ему атрибут " *исполняемый* ":

```
chmod +x ./setup.sh
```

13. Выберите **Install**, а затем **Only FrontEnd**, и выполните шаги из инструкции по установке в статье "Новая установка".
Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»

14. На офисной ноде Платформы запустите обновление Сервера Device Monitor, выполнив команду:

```
/setup.sh
```

15. Выберите **Update**.
16. Выберите компонент **Only IWDM Service** и выполните шаги из инструкции по установке в статье "Новая установка".
    Если вы обновляетесь **с версии 7.15**, учитывайте, что с версии **7.16** пути установки по умолчанию изменились. Если ранее вы использовали пути по умолчанию, при установке Device Monitor 7.16 и более новых по умолчанию установщик не обнаружит данные прошлой версии и создаст каталоги по пути `/opt`. Поэтому переместите данные в `/opt` или укажите старые каталоги при установке новой версии.
17. Далее необходимо прописать в файл **n.yaml** настройки . Запустите скрипт установки:

```
/setup.sh
```

18. Выберите **Utilities** и выполните пункты **Fix n.yaml file**.
19. Затем необходимо получить открытый ключ службы **nguard** Платформы и сохранить его в каталог Сервера. Запустите скрипт установки:

```
./setup.sh
```

20. Выберите **Utilities** и выполните пункт **Save platform guard public key to IWDM Service**.
21. Перезапустите службу Сервера Device Monitor:

```
systemctl restart iwdms
```

22. Чтобы вывести на экран информацию о Платформе и продуктах в кластере, выполните команду:

```
./setup.py showproducts
```

1.7.2 Обновление Агентов Device Monitor

Обновление Агентов Device Monitor может быть выполнено:

- на рабочих станциях под управлением **ОС Windows**:
  - локально на каждой контролируемой рабочей станции.
- на рабочих станциях под управлением **ОС семейства Linux**:
  - с помощью задачи распространения в веб-консоли Device Monitor (см. "Задача первичного распространения и обновления");
  - локально на каждой контролируемой рабочей станции.

Обновление Агентов Device Monitor на рабочих станциях под управлением **Mac OS** не поддерживается. Чтобы перейти на новую версию, необходимо удалить Агент текущей версии и выполнить установку более поздней версии.

При обновлении Агентов Device Monitor до новой версии следует действовать следующим образом:

1. Произвести обновление на группе не более 10 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
2. Произвести обновление на группе не более 50 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
3. Произвести обновление на группе не более 500 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
4. Произвести обновление на группе не более 1000 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
5. Произвести обновление на оставшихся компьютерах до полного завершения процесса обновления.

Чтобы локально обновить Агенты на рабочей станции под управлением ОС Windows до новой версии:

1. Удалите Агента старой версии (см. "Удаление Агентов Device Monitor");
2. Установите Агента новой версии (см. "Локальная установка Агента на рабочей станции под управлением ОС Windows").

Чтобы локально обновить Агенты на рабочей станции под управлением ОС семейства Linux до новой версии:

1. Выполните *Шаг 1* инструкции по локальной установке (см. "Локальная установка Агента на рабочей станции под управлением ОС семейства Linux").
2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт обновления, выполнив команду:

```
sudo ./upgrade.sh
```

4. Дождитесь окончания обновления. Проверить статус выполнения можно, выполнив команду:

```
sudo systemctl status "iwdm*"
```

Примечание:

При обновлении Агента на ОС Windows 7 и Windows 2008 R2 Server следует учесть, что если компонент **Контроль сетевых соединений** был установлен ранее, то при обновлении Агента он будет удален. При необходимости данный компонент можно установить вручную, используя командную строку.

Важно!

Если остановленный Агент был обновлен, то после завершения обновления он будет запущен.

После обновления Агента обязательно перезагрузите рабочую станцию, чтобы использовать новый механизм перехвата для приложений, запущенных до обновления.

Важно!

Агенты версии 7.13 и более ранних, не поддерживающие новые политики, не будут функционировать до обновления на версию 7.14 и выше. На агенты старых версий не приходят обновления конфигурации.

1.8 Удаление Device Monitor

В этом разделе:

1. Удаление Платформы и Сервера Device Monitor
2. Удаление Агентов Device Monitor

1.8.1 Удаление Платформы и Сервера Device Monitor

Чтобы удалить Платформу:

1. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом при установке.
2. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.17:

```
tar xvf data/ui/iw_devicemonitor_setup_7.17.0.310.tar.xz
```

3. Выполните команду:

```
./setup.py remove
```

4. Дождитесь завершения удаления. Программа удалит компоненты Платформы и веб-интерфейса Центра расследований.

Удаление Сервера Device Monitor осуществляется с помощью скрипта **remove.sh**, который располагается в каталоге `/opt/iw/dmserver/bin/`.

Чтобы удалить Сервер Device Monitor:

1. По умолчанию файл скрипта не помечен как исполняемый. Чтобы сделать его исполняемым, перейдите в указанный каталог и добавьте ему атрибут "*исполняемый*", используя команды:

```
cd /opt/iw/dmserver/bin/
sudo chmod +x ./remove.sh
```

2. Скрипт должен выполняться от имени суперпользователя **root**. Запустите скрипт удаления:

```
sudo ./remove.sh
```

3. Подтвердите запрос на удаление, нажав **Y**. При этом можно выбрать:
4. Дождитесь остановки службы сервера и определения его типа.
   ```
   Stopping the service iwdms...
   Service iwdms stopped
   Server role: primary
   ```
5. Если сервер основной, то подтвердите последующее удаление БД. Нажмите **Y** и введите пароль пользователя БД для подтверждения удаления.
6. Если требуется удалить каталог с файлами журнала (логами), нажмите **Y**.
7. Если требуется удалить каталог файловой очереди, нажмите **Y**. Если ввести **N**, то каталог с теневыми копиями событий будет сохранен, так как в нем могут быть еще не отправленные в Traffic Monitor или Activity Monitor события.
8. Дождитесь окончания процесса удаления, который включает в себя:
   - удаление СУБД. Если на шаге 5 вы ввели **N**, то сервер будет помечен как "устаревший".
   - удаление каталогов сервера;
   - удаление службы сервера;
   - удаление пользователя *iwdms;*
   - удаление сервиса распространения, если он был установлен.
9. В процессе удаления возможно появление ошибок. Например, в случаях, когда сервер был не полностью сконфигурирован, БД оказалась недоступной на момент удаления или возникли ошибки при определении типа сервера. В этом случае в консоли вы увидите текст ошибки и вопрос, нужно ли продолжить удаление только файлов сервера Device Monitor.

1.8.2 Удаление Агентов Device Monitor

В настоящей статье перечислены возможные способы удаления Агента InfoWatch Device Monitor. Удаление Агентов производится локально на рабочих станциях:

- Локальное удаление Агента на рабочей станции под управлением ОС Windows
- Локальное удаление Агента на рабочей станции под управлением ОС семейства Linux
- Локальное удаление Агента на рабочей станции под управлением Mac OS

Важно!

Выключение питания компьютера в процессе установки/удаления Агента может привести к ошибкам, ведущим к нестабильной работе операционной системы.

В случае возникновения трудностей при удалении Агента рекомендуем обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.
Вы также можете посетить раздел технической поддержки на нашем сайте: http://www.infowatch.ru/services/support.

Локальное удаление Агента на рабочей станции под управлением ОС Windows

В данном подразделе описаны способы локального удаления Агентов InfoWatch Device Monitor на рабочих станциях под управлением ОС Windows:

- Удаление Агента с помощью инструмента "Программы и компоненты"
- Удаление Агента с помощью Microsoft Program Install and Uninstall troubleshooter
- Удаление Агента с помощью Windows Management Instrumentation (WMI)
- Удаление Агента с помощью Windows Management Instrumentation (WMI) и утилиты PsExec

Удаление Агента с помощью инструмента "Программы и компоненты"

Если Агент установлен не в скрытом режиме, то вы можете удалить его следующим способом:

1. Введите **панель управления** в поле поиска на панели задач, а затем в списке результатов выберите **Панель управления**.
2. Выберите **Программы** > **Программы и компоненты**.
3. Выберите в списке **InfoWatch Device Monitor Client**.
4. Щелкните по выбранной строке правой кнопкой и выберите **Удалить**. Затем следуйте инструкциям на экране.

Удаление Агента с помощью Microsoft Program Install and Uninstall troubleshooter

Вы можете использовать данный способ вне зависимости от того, находится Агент в скрытом режиме или нет, но только если не установлен пароль деинсталляции (пароль защиты от удаления). Рекомендуется использовать способ, когда:

- Не удается удалить Агент с помощью перечисленных ранее способов;
- Агент и его части могли остаться в реестре и/или на диске;
- Не получается повторно установить Агент на рабочую станцию.

Чтобы удалить Агент:

1. Скачайте утилиту **Microsoft Program Install and Uninstall troubleshooter** с официального сайта.
2. Запустите утилиту на рабочей станции, где необходимо удалить Агент.
3. Выберите **Удаление** – **InfoWatch Device Monitor Client**.
4. Дождитесь окончания удаления и перезагрузите компьютер.

Удаление Агента с помощью Windows Management Instrumentation (WMI)

Вы можете удалить Агент с помощью Windows Management Instrumentation (WMI). Для этого:

1. Запустите командную строку (cmd.exe) от имени администратора.
2. Запустите удаление Агента одним из следующих способов в зависимости от наличия пароля деинсталляции:
   - Если пароль не установлен, выполните команду:
     `wmic product where "Name like '%%Device Monitor client%%'" call uninstall`

     Примечание:

Чтобы запустить процесс удаления в тихом режиме, добавьте к команде параметр `/nointeractive`.

Если пароль все же установлен, то будет предложено ввести его.

- Если пароль установлен:
  a. Узнайте идентификатор Агента с помощью команды:
  `wmic product where "Name like '%%Device Monitor client%%'" get IdentifyingNumber`
  b. Выполните команду удаления Агента:
  `msiexec /x {<IdentifyingNumber>} /qn /lvp c:\Windows\dm.log UNINSTALL_PASSWORD=<пароль>`
  где `<IdentifyingNumber>` – идентификатор Агента;
  " `/qn` " – параметр, скрывающий графический интерфейс msiexec. Если вы хотите наблюдать за процессом удаления, вместо этого используйте параметр " `/q` ";
  " `/lvp c:\Windows\dm.log` " – необязательный параметр ведения журнала удаления Агента. Файл " `c:\Windows\dm.log` " приведен в качестве примера, вы можете указать любой другой.
3. Дождитесь окончания удаления, после чего будет сформирован лог-файл с подробной информацией. В случае успешного удаления Агента в лог-файле появится запись вида: «Удаление завершено с состоянием: 0».
4. Перезагрузите рабочую станцию.

Удаление Агента с помощью Windows Management Instrumentation (WMI) и утилиты PsExec

Данный способ повторяет предыдущий (см. "Удаление Агента с помощью Windows Management Instrumentation (WMI)"), но использует утилиту **PsExec** и позволяет удалить Агент в случае, когда пароль деинсталляции утерян:

1. Скачайте утилиту PsExec с официального сайта.
2. Поместите скачанный файл в директорию `C:\Windows\`.
3. Запустите командную строку (cmd.exe) от имени администратора.
4. Узнайте идентификатор Агента с помощью команды:
`wmic product where "Name like '%%Device Monitor client%%'" get IdentifyingNumber`
5. Выполните команду удаления Агента:
`PsExec.exe -i -s msiexec.exe /X {<IdentifyingNumber>} /q /lvp c:\Windows\dm.log`
где `<IdentifyingNumber>` – идентификатор Агента;
" `/q` " – параметр, запускающий команду в тихом режиме, без взаимодействия с пользователем;
" `/lvp c:\Windows\dm.log` " – необязательный параметр ведения журнала удаления Агента. Файл " `c:\Windows\dm.log` " приведен в качестве примера, вы можете указать любой другой.
6. Дождитесь окончания удаления, после чего будет сформирован лог-файл с подробной информацией. В случае успешного удаления Агента в лог-файле появится запись вида: «Удаление завершено с состоянием: 0».
7. Перезагрузите рабочую станцию.

Локальное удаление Агента на рабочей станции под управлением ОС семейства Linux

Вы можете локально удалить Агент на рабочей станции под управлением ОС семейства Linux следующими способами:

- Удаление с помощью скрипта
- Удаление средствами ОС

Удаление с помощью скрипта

Чтобы удалить Агент:

1. Убедитесь, что на рабочей станции есть архив, в котором содержатся пакет и скрипты для установки и удаления Агента. Архив поставляется в составе дистрибутива. Название архива может отличаться в зависимости от используемой ОС, подробнее см. "Локальная установка Агента на рабочей станции под управлением ОС семейства Linux".
   При необходимости скопируйте архив на рабочую станцию и распакуйте его содержимое.

   > **Примечание:**
   >
   > На рабочей станции архив может находится в директории `/tmp/iwdmupload/` . Также его можно найти на сервере Device Monitor в директории `/opt/iw/iwdistribution/bin/SetupPackages` .

2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт:
   `sudo ./remove.sh`
   Пример команды для Агента на Alt Linux:
   `su -c "./remove.sh"`
   В результате будут удалены и Агент Device Moinitor, и Агент распространения.

Удаление средствами ОС

Если не удается удалить Агент с помощью скрипта, вы можете удалить его, выполнив следующие команды:

- На ОС Astra Linux:
  `dpkg --purge iwdm`
  `dpkg --purge iwdeployagent`
- На РЕД ОС и Альт Рабочая станция:
  `rpm -e iwdm`
  `rpm -e iwdeployagent`

Локальное удаление Агента на рабочей станции под управлением Mac OS

Вы можете локально удалить Агент на рабочей станции под управлением Mac OS с помощью скрипта. Для этого:

1. Убедитесь, что на рабочей станции есть архив, в котором содержатся пакет и скрипты для установки и удаления Агента.
   При необходимости скопируйте архив на рабочую станцию и распакуйте его содержимое.
   В нашем примере – `Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`, где `x.x.x.xx` – номер сборки.
2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт:

   ```
   sudo ./remove.sh
   ```

4. Перезагрузите рабочую станцию с помощью команды:

   ```
   reboot
   ```

2 InfoWatch Device Monitor for Linux. Руководство пользователя

В настоящем документе содержится инструкция по работе в Веб-консоли InfoWatch Device Monitor for Linux (далее Система или Device Monitor).

2.1 Аудитория

Данное руководство предназначено для инженеров внедрения и офицеров безопасности, которые будут работать с Системой и заниматься ее администрированием. Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Windows и Linux.

2.2 Комплект документов

В документацию входят:

- «InfoWatch Device Monitor for Linux. Руководство по установке». Документ содержит описание установки Сервера, Веб-консоли и Агентов, входящих в Систему.
- «InfoWatch Device Monitor for Linux. Руководство пользователя». Содержит описание работы в Веб-консоли для решения задач.

Сопутствующая документация по системе InfoWatch Traffic Monitor (далее Traffic Monitor) включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию системы InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

2.3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера;
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Часы работы службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

2.4 Обзор

InfoWatch Device Monitor – это модуль системы InfoWatch Traffic Monitor, позволяющий контролировать обмен данными на рабочих станциях сотрудников. Собранные данные передаются для анализа в систему InfoWatch Traffic Monitor и продукты на Платформе.

Основные функции InfoWatch Device Monitor:

Название функции	Соответствующее правило политик безопасности
Контроль буфера обмена	Правило контроля буфера обмена
Контроль облачных хранилищ	Правило контроля облачных хранилищ
Контроль доступа к внешним устройствам	Правило контроля внешних устройств
Контроль файлов, копируемых с/на съемные устройства	Правило контроля съемных носителей
Контроль файлов, копируемых с/на сетевые ресурсы	Правило контроля сетевых ресурсов
Контроль трафика, передаваемого по протоколам FTP и FTPS	Правило контроля FTP
Контроль трафика, передаваемого по протоколам HTTP и HTTPS	Правило контроля HTTP(S)
Контроль систем мгновенного обмена сообщениями: VK (ВКонтакте), Telegram, Яндекс Мессенджер, WhatsApp, Skype, протокол XMPP	Правило контроля мессенджера VK, Правило контроля мессенджера Telegram, Правило контроля Яндекс Мессенджера, Правило контроля мессенджера WhatsApp, Правило контроля мессенджера Skype Правило контроля протокола XMPP
Контроль ввода текста с клавиатуры	Правило контроля ввода текста с клавиатуры
Контроль систем передачи почтовых сообщений по протоколам SMTP, POP3, IMAP и HTTPS	Правило контроля почты

Название функции	Соответствующее правило политик безопасности
Мониторинг печати на контролируемых компьютерах	Правило контроля печати
Контроль экрана компьютера	Правило контроля экрана
Контроль активности сотрудника и сбор статистики	Правило контроля активности сотрудника

2.5 Настройки пользователей

Раздел содержит справочник пользователей – Офицеров безопасности, которые могут работать в Системе, и описание ролей, которые определяют компетенции пользователя в Системе.

Для каждого пользователя, в задачи которого входит управление схемой безопасности, создается учетная запись в веб-консоли. Данные учетной записи используются при авторизации в Системе, на их основании определяются права на выполнение тех или иных действий.

В веб-консоли используется один предустановленный пользователь – **Суперпользователь,** обладающий всеми правами при работе в ней. Для разграничения полномочий пользователей используются роли. Есть возможность для одного пользователя задать разные роли на разные группы. Для каждой роли определен набор полномочий. Пользователь не может выполнять действия, которые выходят за рамки назначенной ему роли.

В веб-консоли используются следующие предустановленные роли:

- **Главный офицер безопасности** – роль администратора, позволяющая управлять другими учетными записями;
- **Офицер безопасности** – роль пользователя, позволяющая управлять схемой безопасности и настройками Сервера.

2.5.1 Пользователи

При установке Системы создается предустановленный пользователь – Главный офицер. Чтобы войти в Систему, выберите **InfoWatch Device Monitor** в списке установленных продуктов и введите логин и пароль по умолчанию:

Логин	Пароль
officer	xxXX1234

При первом входе в Систему вы должны будете сменить пароль на постоянный (см. "Смена пароля пользователя").

Главная страница раздела **Пользователи** содержит список пользователей, допущенных к работе в Системе:

- Главный Офицер безопасности;
- Офицер безопасности (ОБ), подчиненный ему.

Целевые действия:

- Создание нового пользователя
- Просмотр профиля пользователя

- Редактирование учетной записи
- Смена пароля пользователя
- Активация и деактивация пользователя
- Удаление пользователя

Создание нового пользователя

Главный офицер может добавить новых пользователей, которые также могут выполнять функции Офицеров безопасности. Для этого:

1. Перейдите в раздел **Настройки -> Пользователи**.
2. Нажмите **+Создать**.
3. Введите параметры согласно таблице:

Параметр	Обязательный параметр	Описание
Фотография	Нет	Фотография пользователя
Имя пользователя	Да	Имя нового пользователя (правила составления имени см. "Управление безопасностью")
Логин	Да	Имя учетной записи пользователя (правила см. "Управление безопасностью"). Логин не зависит от верхнего или нижнего регистра
Пароль	Да	Пароль учетной записи (правила см. "Управление безопасностью")
Подтверждение пароля	Да	Пароль учетной записи
Роли	Нет	Роль пользователя в Системе. Пользователю может быть назначена только одна роль
Язык консоли	Нет	Язык интерфейса для нового пользователя: *Русский* или *Английский*
Контакты	Нет	Номер мобильного телефона или email-адрес. Можно добавить одно или несколько значений

4. Нажмите **Создать**. Новый пользователь будет добавлен в Систему. При первом входе в Систему он должен поменять пароль своей учетной записи (см. "Смена пароля пользователя").

Просмотр профиля пользователя

На странице профиля представлены:

1. Вкладка **Персональная информация**. Содержит данные, указанные при создании:
   - фото пользователя;
   - имя пользователя;
   - логин пользователя в Системе;
   - язык, используемый пользователем в Системе;
   - статус пользователя: – активный, – деактивирован;
   - контактные данные: номера телефонов, адреса электронной почты;
   - журнал последних активностей с учетной записью .
2. Вкладка **Права доступа**. Содержит информацию о правах пользователя в Системе:
   - роль, назначенная пользователю;
   - доступные для выполнения функции:
     - доступ, который имеет данный пользователь к настройкам и продуктам;
     - совокупность данных, к которым пользователь имеет доступ.

Чтобы снять или назначить новую роль, перейдите в окно редактирования учетной записи (см. "Редактирование учетной записи").

Действия пользователя:

- Редактирование учетной записи
- Смена пароля пользователя
- Активация и деактивация пользователя

Редактирование учетной записи

Для внесения изменений в учетную запись пользователя:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Нажмите напротив нужного пользователя (или на странице профиля пользователя).
3. Выберите **Редактировать**.
4. В открывшемся окне измените одну или несколько настроек. Доступны настройки, заданные при создании пользователя (см. "Создание нового пользователя").
5. Нажмите **Сохранить**. Новые настройки вступят в силу.

Смена пароля пользователя

Чтобы сменить пароль, выданный при первом входе в Систему, или скомпрометированный пароль:

1. Выполните одно из следующих действий:
   - в разделе **Настройки** -> **Пользователи** нажмите напротив нужного пользователя;
   - в профиле пользователя нажмите ;
   - войдите в главное меню пользователя.
2. Выберите **Сменить пароль**.
3. Заполните поля:

Поле	Описание
Старый пароль	Введите действующий пароль
Новый пароль	Введите новый пароль. Новый пароль должен удовлетворять настройкам безопасности (см. "Управление безопасностью")
Подтверждение пароля	Введите новый пароль еще раз

4. Нажмите **Сохранить**.

Активация и деактивация пользователя

Главный офицер может запретить выбранному пользователю выполнять любые действия в Системе. Для этого:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Напротив требуемого пользователя нажмите  (или  в профиле пользователя).
3. Выберите **Деактивировать**. Учетная запись пользователя будет заблокирована.

Чтобы разблокировать ранее заблокированную учетную запись:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Напротив заблокированного пользователя нажмите  (или  в профиле пользователя).
3. Выберите **Активировать**. Разблокированный пользователь может снова работать в Системе.

Учетная запись Главного офицера деактивации не подлежит.

Удаление пользователя

Главный офицер может удалять учетные записи пользователей. Для этого:

1. Перейдите в раздел **Настройки** -> **Пользователи**.
2. Нажмите  напротив нужного пользователя (или  на странице профиля пользователя).
3. Выберите **Удалить**.
4. В открывшемся окне нажмите **ОК**. Учетная запись пользователя со всеми данными будет удалена без возможности восстановления.

Учетная запись Главного офицера удалению не подлежит.

2.5.2 Роли

Пользователи Системы могут иметь разные роли, которые определяют их права в Системе. Один пользователь может иметь только одну роль. В случае если пользователю не назначена ни одна роль, его доступ в Систему невозможен.

В Системе есть две предустановленные роли:

1. **Главный офицер безопасности** – имеет полный доступ ко всем данным Системы и ее настройкам и управлению ролями, включая создание новых пользователей.
2. **Офицер безопасности** – имеет полный доступ к данным Системы, кроме раздела **Настройки**.

В данной версии Системы не поддерживается создание новых ролей.

2.6 Общие настройки

Раздел содержит общие настройки, распространяющиеся на установленные продукты InfoWatch, и включает в себя:

- Управление безопасностью
- Мониторинг состояния
- Интеграции

2.6.1 Управление безопасностью

Чтобы предотвратить несанкционированный вход в Систему и максимально обезопасить пользователя от компрометации его учетных данных, вы можете устанавливать правила формирования паролей учетных записей и их сроки действия. Для этого:

1. Перейдите в раздел **Настройки** -> **Настройки пароля**.
2. В открывшемся окне установлены настройки по умолчанию. Чтобы ввести новые требования к паролю учетной записи, измените параметры:

Параметр	Описание
Буквы	Заглавные и строчные буквы русского и латинского алфавитов, которые используются для составления пароля. Можно установить: - обязательно для ввода (☑) – обязательно присутствие букв в пароле - опционально (☐) – допускается пароль без букв
Цифры	Арабские цифры, которые используются для составления пароля. Можно установить: - обязательно для ввода (☑) – обязательно присутствие цифр в пароле - опционально (☐) – допускается пароль без цифр
Специальные символы	Перечень спецсимволов, которые могут быть в пароле. Можно установить: - обязательно (☑) – обязательно присутствие спецсимволов в пароле - опционально (☐) – допускается пароль без спецсимволов

Параметр	Описание
Минимальная длина	Минимально допустимая длина пароля в символах
Нельзя использовать последние N паролей	Чтобы избежать компрометации, запрещено использовать пароли за предыдущие периоды
Время действия пароля	Количество дней действия пароля. До истечения указанного срока пароль необходимо сменить
Период неудачных попыток авторизации	Период (в минутах), в течение которого пользователь может вводить неверный пароль
Количество неудачных попыток ввода	Количество неуспешных попыток ввода пароля, после которого учетная запись будет заблокирована
Период блокировки пользователя	Период блокировки учетной записи (в минутах)

3. Нажмите **Сохранить**, чтобы новые параметры вступили в силу. Если нужно вернуться к прежним настройкам, нажмите **Сбросить настройки до значений умолчанию**.

> **Пример**
>
> `Период неудачных попыток авторизации – 5.`
>
> `Количество неудачных попыток ввода – 4.`
>
> `Период блокировки пользователя – 15.`
>
> Если установлены указанные параметры, то после 4 неудачных попыток ввода пароля в течение 5 минут учетная запись пользователя будет заблокирована на 15 минут. После этого можно повторить ввод пароля.

Требования к имени пользователя и учетной записи

Имя пользователя должно содержать не менее четырех символов.

Логин пользователя:

- должен начинаться с буквы и не заканчиваться точкой;
- может состоять из букв латинского алфавита, арабских цифр и содержать спецсимволы: "_", "-", "–", ".".

2.6.2 Мониторинг состояния Системы

Подсистема мониторинга выполняет проверку работы всех узлов распределенной сети, входящих в состав Системы. При этом анализируется доступность узла, информация от его основных аппаратных компонентов, а также информация о состоянии всех служб Системы.

Раздел **Настройки** -> **Состояние системы** содержит панели, отражающие состояние узлов сети – филиалов. Каждая панель содержит следующую информацию:

Поле	Описание
Адрес	IP-адрес ноды InfoWatch Device Monitor
Последнее обновление статуса	Дата и время получения информации о статусе узла: • *Ready* – доступен и готов к работе; • *Not Ready* – не готов к работе; • *Unknown* – зарегистрирован, но не отвечает на запросы.
Версия ядра	Версия ядра ОС
Операционная система	ОС ноды InfoWatch Device Monitor
Память	Общий объем оперативной памяти сервера и сколько памяти занято
ЦПУ	Загрузка центрального процессора сервера InfoWatch Device Monitor
Дисковое пространство (Root)	Общее выделенное и занятое место, отведенное для системных данных в корневой директории
Дисковое пространство (DataStorage)	Общее выделенное и занятое место на диске для DataStorage
Дисковое пространство (Tarantool)	Общее выделенное и занятое место на диске для хранения данных БД Tarantool
Дисковое пространство (Clickhouse)	Общее выделенное и занятое место на диске для хранения данных БД Clickhouse
Дисковое пространство (PostgreSQL)	Общее выделенное и занятое место на диске для хранения данных БД PostgreSQL
Список всех служб узла InfoWatch Vision	
Статус	Служба может иметь один из следующих статусов: • *Запущена* – работает; • *Недоступна* – невозможно получить статус; • *Не инициализирована* – находится в процессе запуска; • *Не найдена* – должна быть на узле, но отсутствует; • *Ошибка* – завершена с ошибкой.

Поле	Описание
Имя	Имя службы в Системе
Версия	Версия сборки службы
Просмотреть детали	Вывод информации о состоянии, событиях и внутренних сообщениях службы

Все события мониторинга в Системе записываются в журнал.

Чтобы скачать весь журнал:

1. Сформируйте лог-файлы по всем службам. Для этого нажмите **Экспорт диагностических данных**. После формирования начнется загрузка.
2. Скачайте zip-архив, содержащий txt-файлы с логами.

Чтобы скачать диагностические данные отдельной службы:

1. Нажмите напротив нужной службы. Начнется формирование лог-файла, а затем загрузка.
2. Скачайте zip-архив, содержащий txt-файлы с логами службы.

2.6.3 Интеграции

Для настройки доменной авторизации в веб-интерфейс сервера DM и получения информации для распространения агентов необходимо настроить синхронизацию с Active Directory.

В этом разделе:

- Интеграция с Active Directory
- Редактирование и удаление интеграции

Интеграция с Active Directory

Чтобы добавить новую интеграцию с Active Directory и запустить ее:

1. Перейдите в раздел **Настройки** -> **Интеграции**.
2. Нажмите **+Добавить**.
3. Выберите **Active Directory** и введите параметры:

Параметр	Описание
Имя интеграции	Название интеграции
Филиал	Нода для подключения: головное отделение или филиал
Адрес источника	Сетевой адрес сервера, с LDAP-каталогами которого производится синхронизация
Тип соединения	Выбор типа соединения, которое будет установлено:

Параметр	Описание
	• Незащищенное соединение (LDAP); • Защищенное соединение по протоколу LDAP + StartTLS; • Защищенное соединение по протоколу LDAPS (SSL). **Важно!** Соединение без сертификатов небезопасно.
Сертификат	Загрузка файла сертификата в формате .pem для защищенных соединений
Глобальный порт	Порт для подключения глобального LDAP-каталога. В зависимости от типа соединения или при нажатии  будут использованы значения по умолчанию: • 3268 для незащищенного соединения и защищенного соединения по протоколу LDAP + StartTLS; • 3269 для защищенного соединения по протоколу LDAPS.
Порт	Порт для подключения локального каталога домена. В зависимости от типа соединения или при нажатии  будут использованы порты по умолчанию: • 389 для незащищенного соединения и защищенного соединения по протоколу LDAP + StartTLS; • 636 для защищенного соединения по протоколу LDAPS.

LDAP запрос	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. При этом может быть указан только один каталог в организационной структуре Active Directory. Для оптимизации поиска вы можете использовать отдельные уровни иерархии базы:
	`C-countryName`
	`O-organizationName`
	`OU-organizationalUnitName`
	`DC-domainComponent`
	`CN-commonName`
	
	Пример: Чтобы использовать в качестве базы поиска ветку `Users`, расположенную в домене компании, необходимо ввести: `cn=users,dc=company,dc=com`

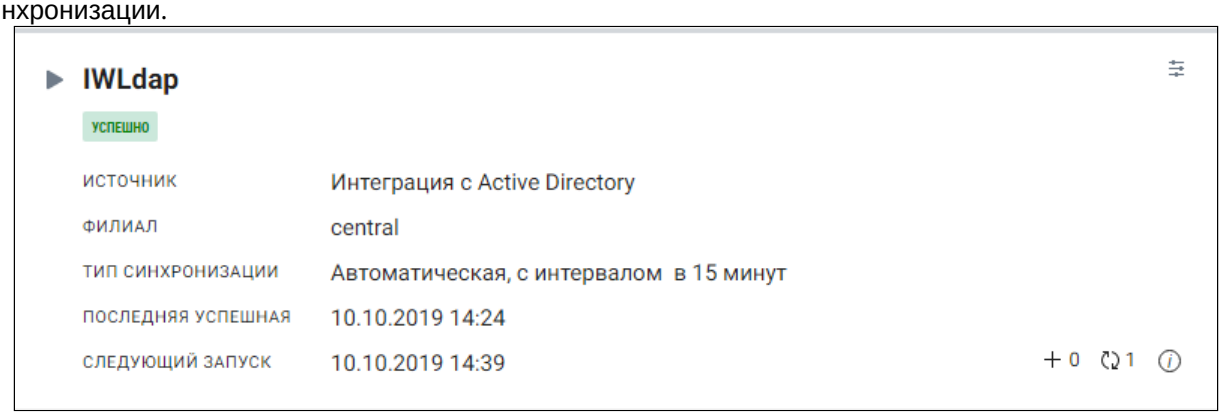
Логин	Логин для доступа к серверу Active Directory
Пароль	Пароль для доступа к серверу Active Directory

Параметр	Описание
Синхронизация	*Ручная* или *Автоматическая*. Во втором варианте необходимо указать *Периодичность* и *Повторение*
Периодичность	Как часто необходимо запускать синхронизацию: *Ежеминутно*, *Ежечасно*, *Ежедневно*, *Еженедельно*
Повторение	День недели и время следующей синхронизации

4. Нажмите **Проверить соединение**, чтобы проверить полноту и корректность введенных параметров, и дождитесь сообщения "*Соединение успешно установлено*".
5. Нажмите:
   - **Сохранить** – при этом новая синхронизация будет ожидать запуска позднее в статусе ***Не синхронизировалось***
     или
   - **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации.

> **Примечание:**
>
> Синхронизация осуществляется с организационными подразделениями (Organizational units) и с группами безопасности (Security groups) Active Directory.

Возможна последовательная синхронизация с несколькими различными LDAP-каталогами. Список серверов, синхронизация с LDAP-каталогами которых настроена, отображается в центральной области. В нижней строке указано количество добавленных персон при последней синхронизации (+) и количество персон, данные которых обновились в ходе последней синхронизации ( ). Детальная информация ( ) показывает, сколько персон было добавлено или обновлено в ходе последней синхронизации.



Если необходимо провести ручную синхронизацию с теми же параметрами (например, при изменении в дереве каталогов компании):

1. Нажмите .
2. Дождитесь изменения статуса выполнения ***Синхронизируется*** > ***Успешно***. Данный процесс может занять длительное время (например, при низкой скорости передачи данных по сети или при большом объеме передаваемых данных).

3. В случае получения статуса ***Ошибка*** проверьте, доступен ли сервер и введены ли корректные учетные данные.

> **Важно!**
>
> Настоятельно рекомендуется проводить первую синхронизацию с Active Directory в ночное время. Это связано с большой нагрузкой на AD и сеть в процессе синхронизации.

Редактирование и удаление интеграции

Чтобы внести изменения в уже созданную интеграцию:

1. Дождитесь, пока данные синхронизируются или нажмите  в левом углу, чтобы остановить процесс синхронизации.
2. Нажмите  в правом углу и выберите **Редактировать**.
3. Внесите нужные изменения.
4. Нажмите **Сохранить**.

Чтобы удалить устаревшую интеграцию:

1. Нажмите  в правом углу.
2. Выберите **Удалить**, а затем нажмите **ОК**.

2.7 Настройка Device Monitor

В этом разделе:

- Серверы DM
- Синхронизации DM
- Агенты
- Каналы перехвата
- Настройка отправки данных в продукты
- Диагностика событий
- Корпоративные сети
- Уведомления

2.7.1 Серверы DM

Чтобы отправлять события на анализ в InfoWatch Traffic Monitor и/или продукты на Платформе, необходимо настроить:

- общие параметры для всех серверов Device Monitor;
- параметры хранения и удаления событий;
- параметры синхронизации политик Traffic Monitor;
- параметры соединения с сервером Traffic Monitor и/или сервером Платформы.

Чтобы задать общие настройки, которые распространяются на основной и все вспомогательные сервера Device Monitor:

1. Перейдите в раздел **Настройки** > **Серверы DM**.
2. В области **Общие** задайте следующие настройки:

- **Количество теневых копий, получаемых сервером одновременно** – определяет количество копий, которые могут поступить на сервер в один момент времени;
- **Количество агентов, одновременно обрабатывающих уведомления от сервера** – определяет количество агентов, которые могут получать уведомления (например, политику безопасности) от сервера в один момент времени;
- **Версия агента DM для установки и обновления** – определяет версию для задач распространения агентов Device Monitor. Эта же версия задана по умолчанию для задач первичного распространения и обновления, если они создаются вручную (см. "Задача первичного распространения и обновления").

> **Примечание:**
>
> Все доступные версии расположены в директории `/opt/iw/iwdistribution/bin/SetupPackages/`.

Чтобы настроить параметры хранения и удаления событий:

1. Перейдите в раздел **Настройки** > **Серверы DM**.
2. В области **Хранение событий** укажите:
   - **Удалять события в статусе "Отправлено в Traffic Monitor"** – чтобы удалять события, отправленные на сервер Traffic Monitor для последующего анализа. При этом события со статусами **Обработано** и **Отправлено в TM** будут удаляться раз в сутки либо при старте сервера;
   - **Хранить события** – чтобы определить время, в течение которого событие будет находиться в базе данных и отображаться в консоли управления, в том числе для событий со статусом **Ошибка отправки в TM** или **Нет лицензии**. По умолчанию срок хранения событий – 1 неделя. При этом будут удалены все события, сформированные ранее указанного периода;
   - **Разделять по периодам** – чтобы разделить события на блоки по времени создания для ускорения процессов обращения.

Если параметры для удаления не отмечены, события со статусами **Обработано** и **Отправлено в TM** должны храниться в соответствии с параметрами хранения, после чего должно быть произведено удаление.

Чтобы настроить синхронизацию с Traffic Monitor для получения политик:

1. Перейдите в раздел **Настройки** > **Серверы DM**.
2. В области **Синхронизация политик защиты данных на агенте** укажите:
   a. **Адрес сервера Traffic Monitor** – IP-адрес или имя сервера InfoWatch Traffic Monitor, с которого Device Monitor будет получать версию конфигурации. Полученная конфигурация распространяется на агенты Device Monitor.
   b. **Токен Traffic Monitor** – токен для подключения к API, который указывается на этапе установки InfoWatch Device Monitor. Вы можете получить актуальный токен от администратора Traffic Monitor или сформировать токен самостоятельно в Консоли управления.
3. Нажмите **Применить**.

> **Примечание:**

Конфигурация, полученная из Traffic Monitor, распространяется с серверов Device Monitor под управлением РЕД ОС, ОС Альт или ОС Astra Linux 1.7 на агенты Device Monitor под управлением РЕД ОС, ОС Альт, ОС Astra Linux 1.7 или ОС семейства Windows.

Примечание:

Версия конфигурации, используемой в Traffic Monitor, отображается в Консоли управления ТМ (подробнее см. "InfoWatch Traffic Monitor. Руководство пользователя", статья "Работа с конфигурацией Системы"). При необходимости вы можете сравнить номера версий в Traffic Monitor и Device Monitor и убедиться, что в Device Monitor используется актуальная версия.

Чтобы увидеть актуальную версию конфигурации, используемой в Device Monitor, обновите страницу.

Чтобы просмотреть или настроить параметры соединения с сервером InfoWatch Traffic Monitor и/или Платформы:

1. Перейдите в раздел **Настройки** > **Серверы DM**.
2. По умолчанию установлен только основной сервер Device Monitor. Выберите его в области **Серверы Device Monitor**, чтобы перейти в настройки.

   Примечание:

   Чтобы установить вспомогательный сервер Device Monitor, пройдите шаги "InfoWatch Traffic Monitor. Руководство по установки", инструкции "Новая установка".

3. На странице настроек сервера подключения отображается информация по следующим параметрам соединения:
   - **Роль сервера** – роль сервера (*основной* или *вспомогательный*), назначенная при его установке;
   - **Номер порта для протокола уведомлений**. По умолчанию – 15100;
   - **Номер порта для основного протокола**. По умолчанию – 15101;
4. На вкладке **Подключение к Traffic Monitor** укажите:
   - **Адрес сервера Traffic Monitor** – IP-адрес или имя сервера InfoWatch Traffic Monitor, на который будут доставляться события. Возможные форматы записи: `host:port.` Адрес указывается на этапе установки InfoWatch Device Monitor. В качестве параметра `port` указывается порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor – 9100;
   - **Токен Traffic Monitor** – токен для подключения к API, который указывается на этапе установки InfoWatch Device Monitor. Вы можете получить актуальный токен от администратора Traffic Monitor или сформировать токен самостоятельно в Консоли управления.
5. На вкладке **Подключение к Платформе** укажите:
   - **Адрес сервера Платформы** – IP-адрес или имя сервера Платформы, на который будут доставляться события. Возможные форматы записи: `host:port.` В качестве параметра `port` указывается порт сервера Платформы, через который будет осуществляться доставка событий. По умолчанию, порт сервера Платформы – 17104. Если не указать порт, будет использовано значение по умолчанию;

- **Токен Платформы** – токен для подключения к API Платформы. Вы можете получить актуальный токен в консоли управления продукта на Платформе, в разделе **Основные настройки** в поле **Токен для Device Monitor Server**.

6. Если требуется установить соединение с другим сервером Traffic Monitor или Платформы, перейдите на нужную вкладку и измените адрес сервера и токен.
7. Нажмите **Применить**.

При соединении сервера Device Monitor с сервером Traffic Monitor или с сервером Платформы осуществляется проверка сертификата удаленного сервера. Для успешного соединения с удаленным сервером выполните настройку данной проверки. Подробнее см. "InfoWatch Device Monitor for Linux. Руководство по установке", статья "Настройка проверки сертификатов удаленных серверов".

2.7.2 Синхронизации DM

Чтобы получать информацию о компьютерах или сотрудниках из службы каталогов, в разделе **Настройки** > **Синхронизации DM** создайте и выполните синхронизацию с LDAP-сервером.

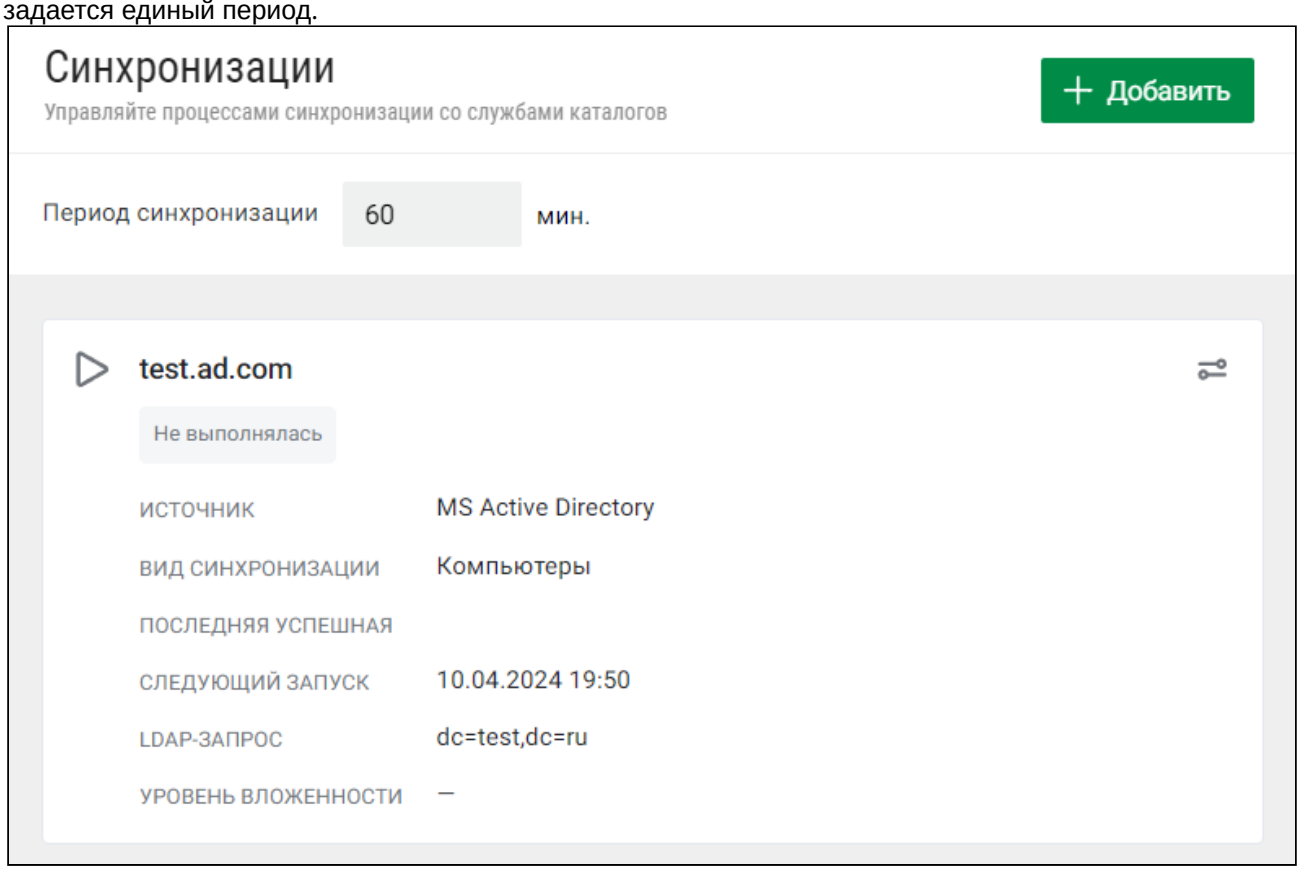
В центральной части рабочей области данного раздела отображаются все созданные синхронизации, их параметры и статусы.

Если вы выполните синхронизацию с компьютерами, то в разделе **Компьютеры** Веб-консоли Device Monitor в группе **Импортированные** появится новая подгруппа. Она будет содержать данные о компьютерах из службы каталогов, сохранив при этом иерархическую структуру источника. Аналогично вы можете выполнить синхронизацию с сотрудниками.

Далее синхронизация происходит автоматически с периодом, указанным в поле **Период синхронизации**.

Чтобы изменить период синхронизации, введите в поле требуемое значение и нажмите в любом месте рабочей области. Вы можете указать значение от 1 до 999 минут. Для всех синхронизаций

задается единый период.



Чтобы создать новую синхронизацию:

1. Перейдите в раздел **Настройки** > **Синхронизации DM**.
2. В верхней правой части рабочей области нажмите **Добавить**.
3. В открывшемся окне укажите параметры для нового подключения:

Параметр	Описание
Адрес источника	Доменное имя или IP-адрес LDAP-сервера, с которым производится синхронизация
Тип источника	Тип службы каталогов. Имеет неизменяемое значение *MS Active Directory*
Порт	Порт для подключения к серверу синхронизации. Имеет неизменяемое значение *389*
LDAP-запрос	Атрибуты фильтрации, являющиеся полным путем к указанному каталогу. При этом может быть указан только один каталог в организационной структуре Active Directory. **Примечание.** Синхронизация осуществляется с организационными подразделениями (Organizational units) и с группами безопасности (Security groups) Active Directory.

	Примечание. Также вы можете синхронизировать объект типа Container, явно указав в запросе полный путь к нему, например: `cn=container_example,ou=ou_example,dc=company,dc=com` Если же объект типа Container находится внутри указанного в запросе каталога, то синхронизации данных с этим объектом не будет. **Примечание.** В атрибуте DC можно использовать следующие символы: • Цифры • Буквы (кириллица и латиница без учета регистра) • Символ "-" (не может быть в начале или конце значения атрибута) • Символ "_" В атрибутах OU и CN можно использовать следующие символы: • Цифры • Буквы (кириллица и латиница без учета регистра) • Символы * ( ) . & - _ [ ] ` ~ | @ $ % ^ ? : { } ! ' • Пробел, если он стоит не в начале или конце значения атрибута • Зарезервированные символы, экранированные с помощью обратного слеша "\" : • \ # + < > , ; " = • Пробелы в начале и в конце значения атрибута (например, " `OU=\ test` ") Длина значений атрибутов DC, OU, CN должна быть от 1 до 64 символов
Логин	Логин для доступа к серверу синхронизации
Пароль	Пароль учетной записи для доступа к серверу синхронизации
Вид синхронизации	Синхронизируемые объекты. Выберите значение *Компьютеры* или *Сотрудники*
Политика по умолчанию	Политика, которая будет назначена на синхронизируемые группы после первой синхронизации
Уровень вложенности	Уровень вложенности, до которого осуществляется синхронизация узлов дерева из службы каталогов. Группы данного уровня включают в себя все компьютеры или всех сотрудников входящих подгрупп. По умолчанию уровень вложенности не задан. В таком случае происходит синхронизация **всех** узлов дерева из службы каталогов.

4. Нажмите **Применить**.

Чтобы запустить синхронизацию:

1. На плитке синхронизации нажмите  **Запустить синхронизацию**.
2. Дождитесь окончания синхронизации. Статус синхронизации примет значение **Успешно**.

Чтобы редактировать синхронизацию:

1. На плитке синхронизации нажмите .
2. Из выпадающего списка выберите **Редактировать**.
3. Внесите требуемые изменения в синхронизацию.

> **Примечание:**
>
> Если изменить **Политику по умолчанию**, то новая политика будет применена только для новых групп, созданных в рамках синхронизации.

4. Нажмите **Сохранить**.

Чтобы удалить синхронизацию:

1. На плитке синхронизации нажмите .
2. Из выпадающего списка выберите **Удалить**.
3. В появившемся окне нажмите **Подтвердить**.

> **Важно!**
>
> При удалении синхронизации будут удалены все связанные с ней синхронизированные данные кроме:
>
> - компьютеров, на которых установлен Агент Device Monitor;
> - компьютеров и сотрудников, входящих не только в импортированные группы, но и в группы Device Monitor.
>
> Если компьютер, на котором установлен Агент Device Monitor, входит только в группы, импортированные из служб каталогов, то при удалении синхронизации он будет добавлен в группу компьютеров по умолчанию.

2.7.3 Агенты

Для эффективной работы агентских приложений Device Monitor необходимо задать ряд общих параметров.

Чтобы указать общие настройки работы агентов Device Monitor:

1. В главном меню выберите **Настройки** > **Агенты**.
2. Измените необходимые параметры:

Параметр	Описание
Соединение	
Отправлять на сервер уведомления о работе агента каждые	Периодичность, с которой агент отправляет на сервер уведомления о своей работе, в секундах. Значение по умолчанию – 600 сек.

Проверять работоспособность сервера каждые	Периодичность, с которой агент выполняет проверку доступности сервера, в секундах. Значение по умолчанию – 2400 сек.
Проверять изменения схемы безопасности каждые	Если агент работает в активном режиме (т.е. сам опрашивает Сервер об изменениях схемы безопасности), то проверка будет выполняться с указанной периодичностью, в секундах. Значение по умолчанию – 600 сек.
Контроль дискового пространства на Агентах	
Минимальное свободное дисковое пространство на агенте	Минимальный размер свободного пространства (в процентах) на контролируемом компьютере, при достижении которого, теневые копии не будут создаваться. Значение по умолчанию – 10%. Т.е. если при создании теневой копии свободного пространства на Агенте останется меньше чем указано, то копия создаваться не будет; частичной копии также не будет.
Если превышено максимальное количество событий на агенте	На том диске контролируемого компьютера, куда выполняется установка Агента Device Monitor, выделяется место, достаточное для хранения информации о 30000 событий. Если Агент Device Monitor настолько долго не имел связи с сервером Device Monitor, что накопилось более 30000 событий, контролируемых правилами, определенными для сотрудника/компьютера, то любые действия, контролируемые текущей политикой безопасности, могут быть запрещены. Чтобы запретить, выберите **Запрещать операции**. Чтобы все действия могли неконтролируемо выполняться, выберите **Разрешать операции**.
Скорость отправки данных с Агента	
Ограничивать скорость отправки данных	При узком канале связи, во избежание его чрезмерной загрузки, вы можете регулировать скорость отправки теневых копий на сервер. Для этого отметьте настройку и укажите верхнюю границу скорости, Кбит/с.
Логирование событий	
Логировать события от перехватчика устройств и облачных хранилищ	Степень детализации при сохранении сведений о работе с внешними устройствами и облачными хранилищами. Подробнее см. "Правило контроля внешних устройств" и "Правило контроля облачных хранилищ". Возможен один из следующих вариантов:

	• **Не логировать** – события не сохраняются; • **При отказе в доступе** (является значением по умолчанию) – события создаются только при попытках нарушения политик безопасности Device Monitor, то есть при блокировании использования устройства или облачного хранилища, включая блокирование попыток превышения уровня доступа. Использование внешних устройств и облачных хранилищ, не запрещенных политиками, не фиксируется. • **Логировать всегда** – события создаются всегда и содержат сведения обо всех действиях, в том числе о подключении/использовании устройств, занесенных в белые списки.
Уведомления сотруднику	
Показывать уведомления сотруднику	Если флажок установлен, то сотрудник будет получать уведомление, когда пытается выполнить действие, запрещенное политикой безопасности. Отображение отдельных типов уведомлений вы можете настроить в разделе Уведомления.

3. Чтобы внесенные изменения вступили в действие, нажмите **Применить**.

> **Примечание:**
>
> Для Агентов под управлением ОС Astra Linux 1.7, РЕД ОС и ОС Альт поддерживается отправка событий о подключении/использовании внешних устройств через USB. При этом:
>
> - может не определяться имя учетной записи пользователя, которым было подключено устройство;
> - может отсутствовать идентификатор устройства, если он не задан в этом устройстве производителем.
>
> Для отправки таких событий необходимо для параметра **Логировать события от перехватчика устройств и облачных хранилищ** указать значение **Логировать всегда**.

2.7.4 Каналы перехвата

Задайте параметры перехвата:

Чтобы настроить периодичность получения событий с теневыми копиями чата для правила "Контроль мессенджеров":

1. В главном меню Консоли управления выберите **Настройки** > **Каналы перехвата**.
2. Укажите, через сколько минут после начала общения в чате необходимо создать теневую копию.

3. Укажите количество сообщений в чате, при достижении которого необходимо создать теневую копию.

Создание каждой последующей теневой копии по установленным настройкам осуществляется в зависимости от того, какая из настроек сработала первой.

Чтобы настроить условия для правила "Контроль ввода текста с клавиатуры", укажите:

1. Через сколько секунд после остановки ввода с клавиатуры пользователем необходимо создать событие.
2. Минимальное количество символов, введенное пользователем и достаточное для создания события;
3. Реакцию на нажатие Enter / Ctrl+Enter / Shift+Enter.

Событие перехвата будет сформировано при соблюдении хотя бы одного условия, а также при смене пользователем активного окна.

После установки нужных значений и выбора условий нажмите **Применить**. Настройки будут действовать всегда.

Чтобы настроить параметры для снимков экрана, укажите:

1. Какого качества снимки необходимо создавать.
2. На сколько изменять размер снимка (в %, значение по умолчанию – 80%).
3. Период от 120 до 1200 секунд, по истечении которого не требуется создавать снимок экрана (значение по умолчанию – 120 секунд).
4. Если нужно создавать снимок только активного окна.

> **Примечание:**
>
> Если при выбранной настройке **Создавать снимок экрана только активного окна** и при активном окне какого-либо приложения пользователь совершает действия не в данном приложении (например, открывает контекстное меню в системном трее на рабочей станции), то на снимке экрана может отображаться часть активного окна приложения.

2.7.5 Настройка отправки данных в продукты

Вы можете указать, в какие продукты InfoWatch необходимо отправлять данные.

Для этого:

1. В главном меню Консоли управления выберите **Настройки** > **Настройка отправки данных в продукты**.

2. В области **Настройка отправки в Traffic Monitor** снимите флаг, если вы не хотите:
   - **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры);
   - **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (активна, если включена настройка "Отправлять события с текстом по правилу контроля ввода текста с клавиатуры"). Настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры).
3. В области **Настройка отправки в Платформу** снимите флаг, если вы не хотите:

- **Отправлять события с текстом по правилу контроля ввода текста с клавиатуры** (настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры);
- **Отправлять события со снимками экрана по правилу контроля ввода текста с клавиатуры** (активна, если включена настройка "Отправлять события с текстом по правилу контроля ввода текста с клавиатуры"). Настройка контроля событий производится в Правиле контроля ввода текста с клавиатуры.

По умолчанию включена отправка событий в Traffic Monitor и Платформу.

> **Важно!**
>
> Для того, чтобы события отправлялись в Платформу и снимки экрана отображались в InfoWatch Activity Monitor, настройте правило сбора статистики (подробную информацию см. "Правило контроля активности сотрудника").

2.7.6 Диагностика событий

В данном разделе вы можете выгрузить отчет с событиями Агентов согласно заданным фильтрам. Для этого:

1. Перейдите в **Настройки** > **Диагностика событий**.
2. В фильтре *Дата событий* выберите период, за который необходимо выгрузить отчет. Если выбран период длиной в один день, вы также можете выбрать отрезок времени, за который необходимо сформировать отчет. По умолчанию в отчет включаются события с 00:00 до 23:59.
3. Нажмите **Выгрузить отчет**.

В папке Загрузки вашего компьютера будет выгружен отчет в формате CSV, содержащий поля:

- *Дата и время события*;
- *Компьютер*;
- *Сотрудник* (поле может быть пустым);
- *Приложение* (поле может быть пустым);
- *Правило* – название правила, в соответствии с которым создано событие (поле может быть пустым);
- *Операция* – действие, заданное в правиле;
- *Тип операции* – выполненная операция;
- *Статус события* с возможными значениями:
  - не определено,
  - ожидает обработки,
  - обработано,
  - ожидает отправки,
  - отправлено,
  - нет лицензии,
  - ожидает отправки в Traffic Monitor,
  - отправлено в Traffic Monitor;
- *Версия схемы безопасности*;
- *Вердикт операции* (поле может быть пустым);
- *Идентификатор события*.

Для событий с использованием устройств отчет также имеет дополнительные поля:

- *Тип устройства*;
- *Идентификатор экземпляра или модели устройства*;
- *Описание устройства*.

Данные в отчете отсортированы по дате и времени событий по убыванию.

2.7.7 Корпоративные сети

Чтобы не создавать события для запросов на внутренние ресурсы при работе правила контроля HTTP(S)-трафика, вы можете исключить сегменты корпоративной сети. Для этого:

1. Перейдите в раздел **Настройки** > **Корпоративные сети**.
2. В верхней правой части рабочей области нажмите **Добавить**.
3. В открывшемся окне укажите:
   - Название сети;
   - Адрес подсети в формате CIDR, например:
     - `182.0.7.1/21` (протокол IPv4)
     - `2001:4f8:3:ba::/64` (протокол IPv6).
4. Нажмите **Добавить**.

> **Примечание:**
>
> Если задать сегменты, в параметрах агентов под управлением ОС Windows будет некорректно отображаться информация о нахождении адаптеров в корпоративной сети.

2.7.8 Уведомления

Если на контролируемом компьютере сотрудник пытается выполнить действие, запрещенное политикой безопасности, ему отображается уведомление о запрете.

В зависимости от ОС на компьютере, где установлен Агент Device Monitor, отображаются следующие уведомления:

Тип уведомления	Причина отправки уведомления	ОС Windows	ОС Linux
Запрет доступа к устройству	Сработало правило, запрещающее чтение и запись на устройство (см. "Правило контроля съемных носителей").	+	+
Запрет записи на устройство	Сработало правило, запрещающее запись на устройство (см. "Правило контроля съемных носителей").	+	+
Запрет записи в открытую область	Сработало правило, запрещающее запись на незашифрованные флоппи-дисководы и съемные устройства (см. "Правило контроля съемных носителей").	+	-

Тип уведомления	Причина отправки уведомления	ОС Windows	ОС Linux
Запрет копирования/печати файла, если места для событий недостаточно	Если Агент Device Monitor настолько долго не имел связи с сервером, что закончилось место, выделенное для хранения информации о событиях, контролируемых правилами (30000 событий), а в общих настройках работы агентов для такого случая выбрано **Запрещать операции** (подробнее см. "Агенты"), то запрещаются любые операции, контролируемые текущей политикой безопасности.	+	-
Запрет вставки из буфера обмена при нехватке места для событий		+	-
Запрет передачи данных по сетевым протоколам, если места для событий недостаточно		+	-
Запрет передачи данных по сетевым протоколам	Сработало правило, запрещающее обмен данными по сетевому протоколу FTP/FTPS/SMTP/POP3/IMAP/Outlook/XMPP/MMP/Telegram/WhatsApp/Skype (см. "Правило контроля FTP", "Правило контроля почты", "Правило контроля протокола XMPP", "Правило контроля мессенджера VK", "Правило контроля мессенджера Telegram", "Правило контроля Яндекс Мессенджера", "Правило контроля мессенджера WhatsApp" и "Правило контроля мессенджера Skype").	+	+
Запрет передачи данных по сетевым протоколам при срабатывании политики защиты данных	Отображается при блокировании передачи данных по почтовым протоколам, FTP, HTTP(S) в результате применения политики защиты данных Traffic Monitor.	+	+
Запрет использования буфера обмена при срабатывании	Отображается при блокировании копирования текста в результате применения политики защиты данных Traffic Monitor.	+	-

Тип уведомления	Причина отправки уведомления	ОС Windows	ОС Linux
политики защиты данных			
Запрет печати при срабатывании политики защиты данных	Отображается при блокировании копирования файла на принтер в виде задания на печать в результате применения политики защиты данных Traffic Monitor.	+	-
Запрет копирования файла при срабатывании политики защиты данных	Отображается при блокировании копирования файла в результате применения политики защиты данных Traffic Monitor.	+	+
Запрет доступа к облачному хранилищу	Сработало правило, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило контроля облачных хранилищ", настройка **Запретить доступ**).	+	+
Запрет записи в облачное хранилище	Сработало правило, контролирующее использование веб-клиентов облачных хранилищ (см. "Правило контроля облачных хранилищ", настройка **Разрешить только скачивание**).	+	+
Запрет вставки данных	Сработало правило, контролирующее вставку данных из буфера обмена (см. "Правило контроля буфера обмена").	+	-

Чтобы полностью отключить отображение уведомлений сотрудникам или включить его обратно:

1. В Центре Администрирования перейдите в раздел **Настройки** → **Настройки продуктов** → **Агенты**.
2. Снимите флажок с поля **Показывать уведомления сотруднику** – чтобы отключить отображение уведомлений сотрудникам, или установите его – чтобы включить уведомления.
3. Справа вверху нажмите **Применить.**

Вы можете изменить текст уведомлений, а также отключить отображение любого типа уведомлений, или включить отображение обратно.

Важно!

Если вы отключили уведомления способом, описанным выше, то уведомления, включенные способом, описанным далее, отображаться не будут.

Чтобы изменить текст уведомлений или включить/отключить отдельные уведомления:

1. В Центре Администрирования, перейдите в раздел **Настройки** → **Настройки продуктов** → **Уведомления**.
2. Из раскрывающегося списка **Тип уведомления** выберите тот, который вы хотите настроить.
3. Чтобы включить/отключить отображение выбранного типа уведомлений, установите/снимите флажок **Показывать сотруднику уведомление системы**.
4. В поле **Текст уведомления** задайте текст уведомления.
   В сообщении вы можете использовать переменные, которые при выводе сотруднику будут преобразовываться в актуальные данные: например, тип заблокированного устройства или протокол, по которому сотрудник пытался передать данные. Для этого установите курсор в необходимое место текста уведомления, нажмите + Добавить и в раскрывшемся списке выберите необходимую переменную.

   Чтобы отменить внесенные изменения, нажмите .

   Чтобы вернуть системный текст уведомления, нажмите .

   > **Примечание:**
   >
   > По умолчанию текст уведомлений - на том языке, который был выбран при установке сервера Device Monitor. При смене языка веб-интерфейса язык текста уведомлений не изменяется.

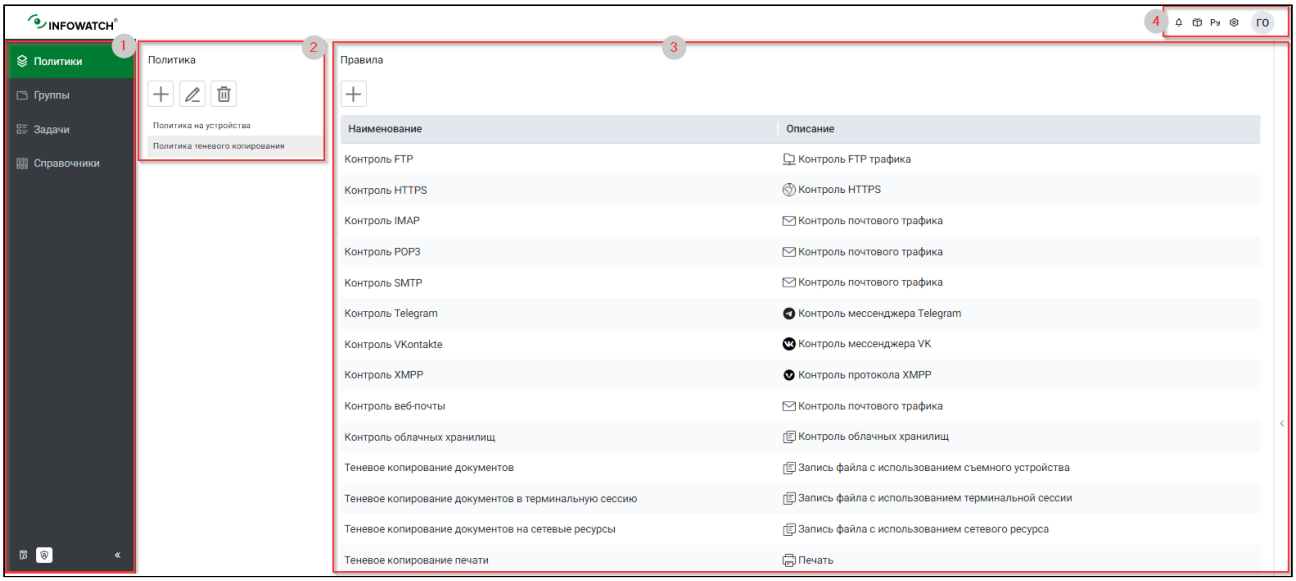
5. После того, как изменения для выбранного типа уведомления внесены, справа вверху нажмите **Сохранить**.
6. При необходимости, измените настройки для других типов уведомлений, повторяя шаги 2-5.

2.8 Интерфейс Центра Администрирования (Device Monitor)

Веб-консоль Центра администрирования (Device Monitor) предназначена для решения следующих задач:

- управление доступом к системе InfoWatch Device Monitor;
- централизованная установка и обновление Агентов Device Monitor на рабочих станциях;
- настройка системы мониторинга компьютеров, сотрудников и устройств;
- контроль доступа к компьютерам и устройствам.

Интерфейс Центра администрирования содержит несколько областей с настройками и данными (на примере раздела **Политики**).



Элементы интерфейса:

Номер на схеме	Элемент окна	Назначение элемента
1	Панель навигации	Переключение между режимами веб-интерфейса: • – Центр расследований; • – Центр администрирования (Device Monitor) Рабочие разделы Центра администрирования (Device Monitor): • **Политики** – управление политиками Device Monitor: создание политик, настройка правил для каждой политики • **Группы** – управление учетными записями сотрудников и группами сотрудников (вкладка **Сотрудники**), управление контролируемыми компьютерами: создание групп компьютеров, добавление распределение контролируемых компьютеров по группам (вкладка **Компьютеры**) • **Задачи** – централизованная установка, обновление и удаление Агентов InfoWatch Device Monitor на компьютеры • **Справочники** – управление списками приложений для использования в правилах и просмотр протокола приложений

Номер на схеме	Элемент окна	Назначение элемента
2-3	Рабочие области	Отображение элементов выбранного раздела Центра администрирования (Device Monitor) и работа с ними
4	Меню пользователя	Пользовательское меню, в котором вы можете: • ознакомиться с полученными уведомлениями; • открыть справочник Центра расследований; • выбрать язык интерфейса: *Русский* или *Английский*; • открыть раздел **Настройки**, содержащий вкладки: Серверы DM, Синхронизации DM, Агенты, Каналы перехвата, Настройка отправки данных, Диагностика событий. • открыть меню пользователя: вход в профиль пользователя, изменение пароля, контакты технической поддержки, информация о версии и используемых горячих клавишах

2.8.1 Политики

Раздел **Политики** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  слева внизу на Панели навигации.

Политика – это совокупность правил, в соответствии с которыми проводятся анализ и обработка объектов перехвата.

Назначение политики группе компьютеров происходит в соответствии со следующими принципами:

- Каждой группе компьютеров обязательно должна быть назначена политика. Добавление новой группы компьютеров невозможно, если для данной группы не определена политика. Поэтому сначала нужно создать политику, после чего создать группу и выбрать для нее политику.
- Группе компьютеров не может быть назначено более одной политики.
- Одна и та же политика безопасности может быть назначена нескольким группам компьютеров, однако рекомендуется, чтобы каждой группе компьютеров была назначена своя политика безопасности.

Важно!

В случае многопользовательского доступа к рабочей станции и при невозможности определения инициатора процесса (события) правила перехвата для сотрудников учитываться не будут. Будут работать правила перехвата только для данной рабочей станции. В связи с этим необходима настройка правил перехвата не только для сотрудников, но и для рабочей станции, к которой возможен многопользовательский доступ.

Правила – это набор ограничений и условий, в соответствии с которыми осуществляется мониторинг операций, связанных с переносом файлов на съемные устройства и сетевые ресурсы, сетевой активностью и отправкой документов на печать. Для каждой политики создается свой набор правил.

В Device Monitor существуют следующие типы правил:

- **Контроль съемных устройств**. Позволяет отслеживать действия с файлами на съемных устройствах:
  - создание файла непосредственно на съемном устройстве;
  - копирование/перемещение файла на съемное устройство. В данном случае отслеживаются операции копирования/перемещения файла с контролируемого компьютера, другого съемного устройства или сетевых ресурсов.
- **Контроль сетевых ресурсов**. Позволяет отслеживать действия с сетевыми ресурсами:
  - копирование файла на сетевые ресурсы с использованием UNC (например, *Server**SharedFolder**Folder**File*);
  - перехват копирования файлов с сетевых ресурсов;
  - запрет копирование файлов на сетевые ресурсы.
- **Контроль терминальной сессии**. Позволяет отслеживать операции копирования файлов в приложение терминальной сессии и копирования файлов на ресурсы, подключенные через терминальную сессию.
- **Контроль печати**. Позволяет отслеживать действия, связанные с печатью документов на локальных и сетевых принтерах. Также возможно создавать теневую копию задания на печать.
- **Контроль внешних устройств**. Позволяет разрешать, ограничивать доступ и запрещать использование съемных устройств хранения.
- **Контроль FTP**. Позволяет контролировать обмен данными по протоколу FTP/FTPS. Система позволяет ограничивать или полностью запрещать использование FTP/FTPS протокола, а также создавать теневые копии передаваемых файлов.
- **Контроль HTTP(S)**. Позволяет контролировать обмен данными по протоколам HTTP и HTTPS. Система позволяет создавать теневые копии передаваемых файлов.
- **Контроль почты**. Позволяет контролировать отправку и получение электронной почты. Система позволяет полностью запрещать или разрешать использование почты, либо разрешать только получение почты, а также создавать теневые копии передаваемых файлов.
- **Контроль облачных хранилищ**. Позволяет контролировать получение и отправку любых данных на облачные хранилища и доступ к их веб-клиентам.
- **Контроль экрана**. Позволяет создавать снимки экрана компьютера.
- **Контроль буфера обмена**. Позволяет контролировать вставку данных с использованием буфера обмена через приложение терминальной сессии.
- **Контроль мессенджера VK**. Позволяет контролировать доступ сотрудников к сервису мгновенного обмена сообщениями VK. Система позволяет снимать копию чата и создавать теневые копии исходящих файлов.
- **Контроль мессенджера Telegram**. Позволяет контролировать доступ сотрудников к сервису мгновенного обмена сообщениями Telegram: обмен новыми, пересылаемыми

или исправленными сообщениями чата, в том числе группового, исходящими файлами и голосовыми сообщениями.
- **Контроль XMPP**. Позволяет контролировать обмен по протоколу **XMPP** входящими и исходящими текстовыми сообщениями, а также исходящими файлами.
- **Контроль ввода текста с клавиатуры**. Позволяет перехватывать ввод текста с клавиатуры в окне любого приложения на рабочих станциях и формировать события при смене активного окна.
- **Контроль активности сотрудника**. Позволяет собирать статистику активности сотрудника за контролируемым компьютером.

О настройке политик смотрите:

- Создание политик
- Создание правил

2.8.2 Задачи

Раздел **Задачи** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации. В этом разделе представлен список всех задач, созданных пользователем. Это могут быть задачи первичного распространения или обновления.

В рабочей области главного окна отображается список рабочих станций, для которых выполняется выбранная задача. На панели **Подробно** отображаются параметры, заданные при создании выбранной задачи. Чтобы скрыть панель, нажмите .

Чтобы создать и запустить задачу, смотрите статью "Задача первичного распространения и обновления".

2.8.3 Справочники

Раздел **Справочники** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации. Раздел **Справочники** содержит подразделы:

- **Приложения**
- **Протокол приложений**
- **Исключение приложений из перехвата**
- **Контроль сетевых приложений**.

Приложения

Подраздел **Приложения** содержит списки приложений, которые можно использовать в правилах для более точного контроля.

Вы можете использовать списки приложений в:

- Правиле контроля ввода текста с клавиатуры (подробнее см. "Правило контроля ввода текста с клавиатуры");
- Правиле контроля буфер обмена (подробнее см. "Правило контроля буфера обмена").

Чтобы создать список приложений:

1. Перейдите в раздел **Справочники** > **Приложения**.
2. В области **Список приложений** слева нажмите .
3. В открывшемся окне:
    - введите название приложения;

- выберите ОС: Windows или Linux.

4. Нажмите **Создать**.

Чтобы отредактировать список приложений:

1. Выберите список.
2. Нажмите  справа от него.
3. Выберите .
4. Внесите изменения и нажмите **Сохранить**.

Чтобы удалить список приложений:

1. Выберите список.
2. Нажмите  справа от него.
3. Нажмите .
4. Подтвердите действие.

Доступные действия с приложениями:

- создание
- редактирование
- перемещение между списками
- копирование в список
- удаление

Чтобы создать приложение:

1. Выберите список, в котором необходимо создать приложение.
2. Нажмите **Создать приложение**.
3. В открывшемся окне введите:
   - Описание приложения;
   - Имя приложения – имя исполняемого файла (с расширением);
   - Расположение исполняемого файла – папка на компьютере с Агентом Device Monitor, содержащая исполняемый файл приложения, либо папка верхнего уровня (возможно использование системных переменных).;
   - Издатель – Organization (O), Location (L), State (S), Country (C) из свойств, параметр доступен только для приложений на ОС Windows;
   - Название продукта – необязательный параметр. Доступен, только если заполнено поле **Издатель** и только для приложений на ОС Windows.
4. Нажмите **Создать**.

Чтобы редактировать приложение:

1. Выберите приложение.
2. Нажмите .
3. В открывшемся окне введите:
   - Описание;
   - Имя приложения;
   - Расположение исполняемого файла;
   - Издатель;
   - Название продукта.
4. Нажмите **Сохранить**.

Чтобы удалить приложение:

1. Выберите приложение.
2. Нажмите .
3. Подтвердите действие.

Чтобы переместить приложение в другой список:

1. Выберите приложение.
2. Нажмите .
3. Выберите .
4. Нажмите **Переместить**.

Чтобы скопировать приложение в другой список:

1. Выберите приложение.
2. Нажмите .
3. Выберите .
4. Нажмите **Скопировать в список**.

Список приложений содержит следующую информацию:

- Имя приложения
- Описание
- Расположение исполняемого файла
- Название продукта
- Издатель

Вы можете изменить ширину столбца в таблице и переместить столбец.

Протокол приложений

Подраздел **Протокол приложений** содержит таблицу с информацией о приложениях, которые запускались на контролируемых рабочих станциях под управлением ОС MS Windows.
После установки Агента InfoWatch Device Monitor на рабочие станции под управлением ОС MS Windows и их перезагрузки Система автоматически начинает получать информацию о запускаемых приложениях. Информация обо всех запусках и установках формирует *протокол приложений*.

Из протокола вы можете добавлять приложения в списки для ОС MS Windows. О создании списков и добавлении в них приложений см. "Создание и изменение списков приложений".

Примечание:

Для снижения нагрузки на CPU таблица базы данных, содержащая записи о запусках приложений, добавлена в очередь регулярной очистки. Подробнее см. в статье базы знаний "Удаление записей журнала приложений Device Monitor".

Важно!

Протокол приложений необходим для того, чтобы Офицер безопасности не мог запретить приложение, без которого компьютер перестанет функционировать в штатном режиме.

Список в протоколе приложения содержит следующую информацию:

- Дата добавления
- Компьютер
- Пользователь
- Описание
- Название продукта
- Издатель
- Расположение исполняемого файла

Вы можете переместить колонки в таблице и изменить их размер.

Вы также можете добавить одно или несколько приложений из протокола в список приложений.

Чтобы добавить приложение:

1. Выберите одно или несколько приложений .
2. На появившейся внизу экрана плашке нажмите **Добавить в список приложений**.
3. В открывшемся диалоговом окне выберите список, в который необходимо добавить приложение.
4. Нажмите **Сохранить**. В правом верхнем углу Система отобразит уведомление о том, что приложения были добавлены.

или

1. В списке приложений наведите курсор на строку приложения справа и нажмите **Добавить приложение в список**.
2. В открывшемся диалоговом окне выберите список, в который необходимо добавить приложение.
3. Нажмите **Сохранить**. В правом верхнем углу Система отобразит уведомление о том, что приложение были добавлено.

Исключение приложений из перехвата

Вы можете указать приложения, активность которых не будет перехватываться Системой.

Чтобы просмотреть и настроить параметры исключения приложений из перехвата:

1. Перейдите в раздел **Справочники** > **Исключение приложений из перехвата**.
2. В правой части рабочей области нажмите .
3. Исключение приложений в ОС семейств MS Windows и Linux настраиваются на разных вкладках.
    a. **Для поддерживаемых ОС семейства Linux**
        i. Откройте вкладку Linux.
        ii. В открывшемся окне введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.
        iii. Введите краткое описание. Поле обязательно для заполнения. Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути.
        iv. Укажите расположение файла – папку на компьютере с Агентом Device Monitor, содержащую исполняемый файл приложения, либо папку верхнего уровня (возможно использование системных переменных). Заданная строка должна быть в начале пути к файлу. Например, если исключение задано в

виде: `/opt/myapps`, то из перехвата будут исключены все приложения в папке `myapps`, а также в любой ее подпапке.

v. Укажите ОС, для которой настраивается исключение. Чтобы исключение работало на всех поддерживаемых ОС семейства Linux, выберите вариант **Любой дистрибутив Linux**.

b. **Для поддерживаемых ОС семейства Windows**

i. Откройте вкладку Windows.

ii. На панели инструментов нажмите ⊞.

iii. В открывшемся окне введите название исполняемого файла приложения. Исключение осуществляется по имени исполняемого файла. Поле обязательно для заполнения, регистр не учитывается.

iv. В поле **Описание** введите произвольное описание приложения. Вместо имени приложения можно ввести символ *. В этом случае из перехвата будут исключены все приложения, расположенные по указанному пути или имеющие указанную цифровую подпись (см. п. vi).

v. В поле **Тип перехвата** отметьте:

1. **Исключить из сетевого перехвата** – если требуется исключить сетевую активность приложения из перехвата.
2. **Исключить приложение из внедрения модулей** – если требуется не создавать события и теневые копии при печати из данного приложения.

> **Примечание**
>
> Должен быть выбран хотя бы один из типов перехвата.
> Программы со встроенной проверкой целостности (например, клиент SWIFT) или содержащие внутри себя антиотладочные методы необходимо добавлять в исключение приложений из внедрения модулей. В противном случае их запуск будет невозможен.

vi. В поле **Расположение файла** укажите папку на компьютере с Агентом Device Monitor, содержащую исполняемый файл приложения, либо папку верхнего уровня (возможно использование системных переменных). Заданная строка должна быть в начале пути к файлу. Например, если исключение задано в виде: `%ProgramFiles%\Citrix`, то из перехвата будут исключены все приложения в формате *.exe в папке Citrix, а также в любой ее подпапке.

vii. В поле **Исходное имя файла** укажите название приложения (в контекстном меню исполняемого файла приложения выберите **Свойства**, вкладка **Подробно**, атрибут **Исходное имя файла**).

viii. В поле **Имя оставившего цифровую подпись** укажите значение из свойств исполняемого файла (в контекстном меню файла выберите **Свойства**, вкладка **Цифровые подписи**, атрибут **Имя подписавшего**). Можно указать имя целиком или часть имени. Например, если исключение задано в виде: `*Kaspersky`, то из перехвата будут исключены все приложения, в цифровой подписи которых есть подстрока "Kaspersky".

4. Нажмите **Создать**. Чтобы применить исключение приложения из перехвата или отмену такого исключения, перезапустите приложение.

Контроль сетевых приложений

Для контроля сетевого трафика на Агенте Device Monitor реализован прозрачный прокси-сервер. На этот сервер перенаправляются все соединения, вне зависимости от используемого протокола. Далее Агент Device Monitor разбирает протокол и определяет, относится ли данный протокол к перехватываемым.

Перехватываются протоколы: FTP, FTPS, POP3, SMTP, S/MIME, HTTP, HTTPS, XMPP и MMP. Если поток данных защищен с использованием протокола TLS\SSL, то прокси-сервер раскрывает трафик и определяет, нужно ли контролировать данный поток.

Вы можете задать список адресов серверов, при соединении с которыми протоколы не контролируются (трафик на эти серверы не перенаправляется на внутренний прокси-сервер) либо принудительно контролируются (трафик перенаправляется на внутренний прокси-сервер).

При добавлении адреса сервера в исключения, требуется указать IP-адрес сервера или FQDN.

Чтобы задать список разрешенных или запрещенных серверов:

1. Перейдите в раздел **Справочники** > **Контроль сетевых приложений**.
2. Нажмите .
3. В диалоговом окне **Добавление сервера в список исключенных из анализа** введите описание сервера:
   - чтобы добавить отдельный порт сервера:
     a. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**;
     b. В поле **Тип адреса** выберите **Адрес и порт**;
     c. Укажите FQDN или IP-адрес (IPv4 или IPv6) сервера;
     d. В поле **Порт** укажите порт подключения (может быть пустым);
   - чтобы добавить диапазон адресов:
     a. Выберите нужное действие: **Исключить из перехвата** или **Включить в перехват**.
     b. В поле **Тип адреса** выберите **Диапазон адресов**;
     c. Укажите IP-адреса (IPv4 или IPv6) в полях "с" - "по".
   - чтобы добавить шаблон для исключения группы ресурсов из перехвата при SSL/TLS-соединении:
     a. Выберите действие **Исключить из перехвата**;
     b. В поле **Тип адреса** выберите **Домен из MITM перехватчика**;
     c. Укажите домен.
4. Нажмите **Добавить**, затем **Применить**.

В текстовом виде адрес IPv4 записывается как nnn.nnn.nnn.nnn, где nnn принимает значения от 0 до 255, а каждая буква n представляет десятичную цифру. Незначащие нули можно не указывать.
В текстовом виде адрес IPv6 записывается как xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, где каждая буква x – это шестнадцатеричная цифра, представляющая 4 бита. Незначащие нули можно не указывать.

Примечание:

Включение в перехват имеет более высокий приоритет, чем исключение.

Настройка с указанием конкретного адреса имеет более высокий приоритет, чем диапазон адресов.

Чтобы изменить параметры сервера, выберите его в списке и нажмите . После внесения изменений нажмите **Сохранить**, затем **Применить**.

Чтобы удалить сервер из списка разрешенных, выберите его, нажмите . Подтвердите удаление, затем нажмите **Применить**.

2.8.4 Группы

Раздел **Группы** находится в Центре администрирования Device Monitor. Чтобы перейти в него, нажмите  на панели навигации. Раздел **Группы** содержит подразделы:

- **Компьютеры**
- **Сотрудники**

Под компьютерами в системе Device Monitor понимаются контролируемые компьютеры, на которых установлены Агенты Device Monitor.

Действующие политики могут быть назначены только группе компьютеров. Определение политики для отдельного компьютера выполняется путем включения компьютера в ту или иную группу.

Компьютер, зарегистрированный в Device Monitor, должен входить как минимум в одну группу компьютеров (**Группу компьютеров по умолчанию**). Это связано с тем, что политика безопасности не может быть назначена отдельному компьютеру.

В **Группу компьютеров по умолчанию** входят все компьютеры, для которых не определены другие группы компьютеров:

- компьютеры, впервые зарегистрированные в Device Monitor;
- компьютеры, исключенные из всех прочих групп компьютеров.

После установки Системы на **Группу компьютеров по умолчанию** назначена **Политика на устройства**.

Исключить компьютер из **Группы компьютеров по умолчанию** можно при условии, что компьютер добавлен хотя бы в одну группу компьютеров, помимо нее.

Информация о работе с контролируемыми компьютерами содержится в подразделах:

- Создание и редактирование групп компьютеров
- Настройка состава групп компьютеров
- Просмотр сведений о компьютерах

Регистрация контролируемых пользователей (сотрудников) в Системе осуществляется в соответствии со следующими принципами:

- Каждый сотрудник должен входить как минимум в одну группу сотрудников (группу «по умолчанию»). Это связано с тем, что политика безопасности не может быть назначена отдельному сотруднику.
  В группу «по умолчанию» входят учетные записи всех сотрудников, для которых не определены другие группы сотрудников: сотрудники, впервые зарегистрированные в Device Monitor, сотрудники, исключенные из всех прочих групп сотрудников.
  Исключить сотрудника из группы «по умолчанию» можно при условии, что учетная запись сотрудника добавлена хотя бы в одну группу сотрудников, помимо группы «по умолчанию».
- После установки Системы группе сотрудников «по умолчанию» назначена **Политика теневого копирования**, содержащая следующие правила:

- Контроль FTP
- Контроль HTTPS
- Контроль IMAP
- Контроль POP3
- Контроль SMTP
- Контроль Telegram
- Контроль VKontakte
- Контроль XMPP
- Контроль веб-почты
- Контроль облачных хранилищ
- Теневое копирование документов
- Теневое копирование документов в терминальную сессию
- Теневое копирование документов на сетевые ресурсы
- Теневое копирование печати

Подробнее о правилах см. в разделе "Политики".

Информацию о работе с контролируемыми сотрудниками см. подразделах:

- Создание и редактирование групп сотрудников
- Настройка состава групп сотрудников

2.9 Настройка Системы после установки

В этом разделе:

- Создание и редактирование групп компьютеров
- Настройка состава групп компьютеров
- Просмотр сведений о компьютерах
- Задача первичного распространения и обновления

2.9.1 Создание и редактирование групп компьютеров

Важно!

При регистрации нового компьютера, информация о нем автоматически добавляется в схему безопасности (в группу компьютеров «по умолчанию»).

Примечание:

Чтобы получать информацию о компьютерах из службы каталогов, вы можете выполнить синхронизацию с LDAP-сервером. Подробнее см. "Синхронизации DM".

Чтобы добавить группу компьютеров:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Компьютеры** в разделе **Группы**.
3. В левой части рабочей области нажмите .
4. Укажите следующие параметры:

- **Наименование** группы;
- **Политика**. Выберите из раскрывающегося списка политику, которая будет назначена данной группе компьютеров.

5. Нажмите . Будет создана новая группа компьютеров, в которую необходимо добавить компьютеры.

Чтобы отредактировать группу компьютеров:

1. Выделите нужную группу.
2. Нажмите  и внесите изменения.
3. Нажмите .

Чтобы найти компьютер или группу компьютеров:

1. В верхней части рабочей области введите в строку поиска текст запроса, состоящий хотя бы из 3 символов.
   В раскрывшемся списке будут показаны первые 5 компьютеров и первые 5 групп компьютеров, параметры которых включают введенный текст.
2. Выберите результаты поиска для отображения:
   - Чтобы просмотреть все элементы, удовлетворяющие запросу, нажмите **Enter** или **Смотреть все результаты**. Результаты будут отображены в иерархическом списке в области слева, найденные группы при этом будут выделены синим цветом.
     Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.
   - Чтобы перейти к одному элементу, нажмите на группу или компьютер. В рабочей области откроется выбранная группа или группа, включающая выбранный компьютер.

> **Важно!**
>
> Если не осуществляется поиск объектов с использованием кириллицы, убедитесь, что для базы данных, с которой взаимодействует сервер Device Monitor, установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

Чтобы отменить фильтр, примененный с помощью поиска, нажмите  в строке поиска.

Чтобы удалить группу компьютеров:

1. Выделите группу для удаления.

   > **Примечание.**
   >
   > Группу компьютеров «по умолчанию» удалить нельзя.

2. Нажмите . В группе компьютеров, которую вы удаляете, могут быть компьютеры, не включенные в другие группы. В этом случае компьютеры будут автоматически добавлены в группу компьютеров «по умолчанию».

3. В открывшемся окне нажмите **Подтвердить**.

2.9.2 Настройка состава групп компьютеров

При установке Агента InfoWatch Device Monitor на компьютер в Системе автоматически создается запись о компьютере. Эта запись добавляется в группу «по умолчанию». На все компьютеры, входящие в эту группу, будет распространяться назначенная ей политика. В дальнейшем определение политик для компьютера происходит путем его включения в различные группы компьютеров.

Чтобы настроить состав группы компьютеров:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Компьютеры** в разделе **Группы**.
3. В левой части рабочей области выберите название необходимой группы. После этого в рабочей области главного окна будет выведен список всех компьютеров, уже входящих в группу.

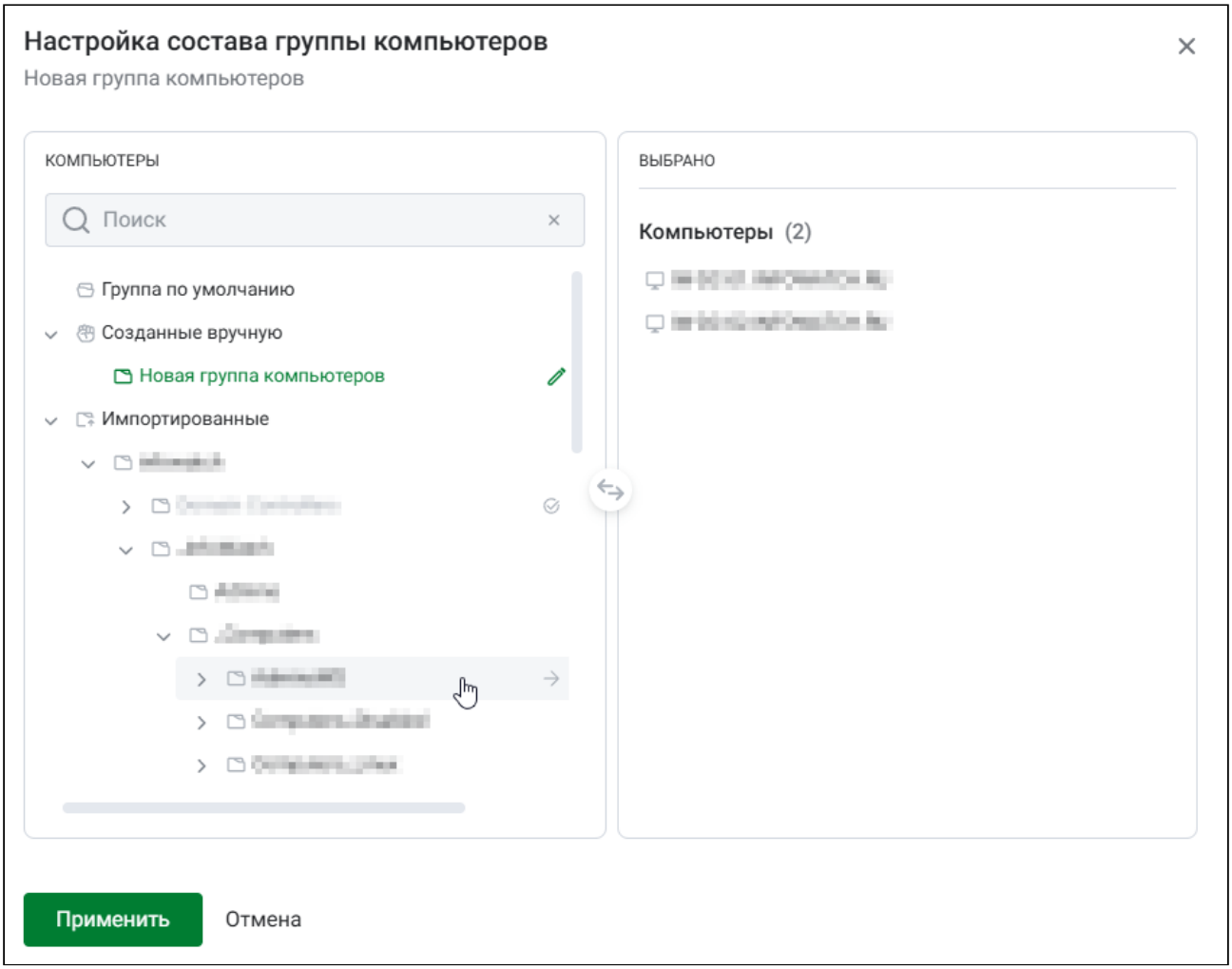
   > **Примечание:**
   >
   > Чтобы найти группу в списке, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп компьютеров".

4. В правом верхнем углу рабочей области нажмите 

   .
   В открывшемся диалоговом окне в области слева отобразится список компьютеров из числа ранее зарегистрированных в Системе, т.е. компьютеры, на которых установлен Агент, из группы «по умолчанию» и других групп.

   Чтобы развернуть или свернуть группу, используйте .
   Чтобы найти компьютер или группу, введите в строку поиска текст запроса, состоящий хотя бы из 3 символов. Результаты будут отображены в иерархическом списке в области слева и выделены синим цветом. Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.
5. Для добавления в группу, в области слева наведите курсор на компьютер или группу и нажмите  **Добавить компьютеры в "<Название группы компьютеров>"**.

   Напротив группы или компьютера, которые были добавлены, появится значок . В случае, если имя компьютера очень длинное, вы можете просмотреть его, используя полосу прокрутки внизу окна.
6. Для удаления из группы наведите курсор на удаляемую запись и нажмите  **Удалить из группы "<Название группы компьютеров>"**. Это можно сделать, как в области справа, так и в области слева.
7. Нажмите **Применить**.

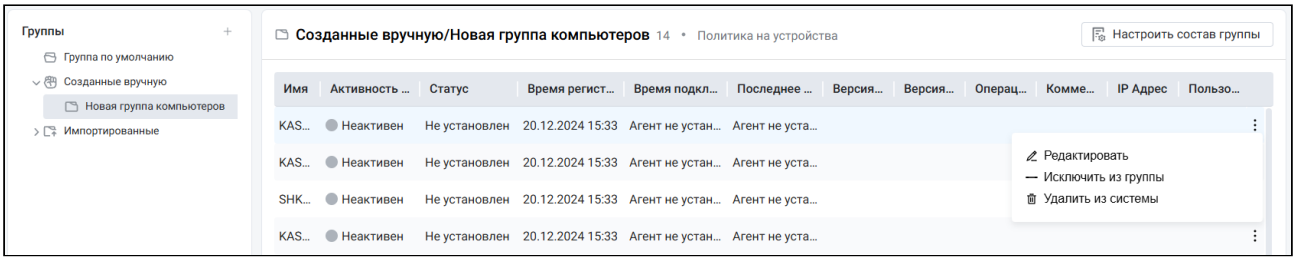


Примечание:

Если вы добавляете группу компьютеров, которая содержит подгруппы, то компьютеры из подгрупп не будут автоматически добавлены в выбранную группу. Вы можете добавить их отдельно.

Если компьютер включен в определенную группу компьютеров, ему будут назначены политики выбранной группы. Чтобы отменить действие какой-либо политики безопасности на компьютер, исключите его из группы, которой назначена эта политика.

Внутри группы компьютеров вы можете работать с их списком: редактировать, исключать, удалять компьютеры из системы.
Чтобы найти группу в списке, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп компьютеров".



Примечание:

Для импортированных групп компьютеров внутри группы доступно только редактирование.

Чтобы исключить компьютер из группы компьютеров:

1. В строке с именем компьютера нажмите ⋮.
2. Выберите — **Исключить из группы**.
3. Нажмите **Да**. Если компьютер входил только в одну группу, то при исключении он будет автоматически добавлен в группу компьютеров «по умолчанию».

Чтобы добавить комментарий компьютеру:

1. В строке с именем компьютера нажмите ⋮.
2. Выберите ✎ **Редактировать**.
3. В поле **Комментарий** добавьте комментарий и нажмите **Сохранить**.

При необходимости вы можете удалить компьютер из списка зарегистрированных (например, если эксплуатация рабочей станции прекращена).

Чтобы удалить компьютер из схемы безопасности:

1. В строке с именем компьютера нажмите ⋮.
2. Выберите 🗑 **Удалить из системы**.
3. В открывшемся диалоговом окне нажмите **Подтвердить**.

Важно!

Удаление компьютера из схемы безопасности повлечет за собой его удаление из всех групп и политик.

2.9.3 Просмотр сведений о компьютерах

В левой части рабочей области выводится перечень групп компьютеров. В правой части отображается перечень компьютеров, входящих в состав выделенной группы компьютеров.

Информация по компьютерам представлена в виде табличного списка. В столбцах выводятся основные свойства компьютеров. Вы можете менять порядок столбцов, а также скрывать столбцы, отображать которые не требуется.

Табличный список содержит следующие основные сведения:

- **Имя**. Доменное имя рабочей станции.
- **Статус**. Состояние Агента, установленного на компьютере. Данный параметр может принимать одно из следующих значений:
  - **Не установлен**. Агент никогда не устанавливали на рабочую станцию, либо она была добавлена в схему безопасности без агента;
  - **Установлен**. Агент установлен на рабочую станцию через задачу первичного распространения, или в схему безопасности была добавлена рабочая станция с установленным Агентом;
  - **Работает с ограничениями функциональности**. Агент установлен на рабочую станцию, но работает частично. Например, этот статус будет выставлен после старта Агента при проверке на загрузку и совместимость необходимых драйверов ядра ОС;
  - **Остановлен**. Агент установлен на рабочую станцию и остановлен через Консоль Device Monitor;

    > **Примечание:**
    >
    > Если остановленный агент был обновлен, то после завершения обновления он будет запущен.

  - **Работает в диагностическом режиме**. Агент установлен на рабочую станцию и переведен в диагностический режим работы через Консоль Device Monitor;
  - **Золотой образ**. Агент установлен на рабочую станцию, которой назначен статус «Золотой образ» – образ компьютера, из которого будут создаваться новые виртуальные машины (например, для создания однотипных серверов или рабочих станций для пользователей, решающих однотипные задачи);
  - **Удален**. Агент удален с рабочей станции через задачу удаления продукта или средствами самой рабочей станции.
- **Активность Агента**. Статус активности Агента, установленного на компьютере. Данный параметр может принимать одно из следующих значений:
  - **Активен**. Агент регулярно выходит на связь с сервером, передает события, данные;
  - **Не активен**. Агент регулярно не выходит на связь с сервером или отключен;
  - **Не активен более недели**. Агент не выходит на связь с сервером более недели;
  - **Не активен более месяца**. Агент не выходит на связь с сервером более месяца.

> **Примечание:**
>
> При удалении Device Monitor статус отправляется Агентом по протоколу UDP, не гарантирующему доставку. Кроме того, уведомление отправляется в случае, если с сервером Device Monitor уже была установлена сессия и сообщение отправляется тому серверу, с которым Агент взаимодействует в данный момент.

- **Время регистрации**. Дата и время регистрации рабочей станции (добавление в БД);
- **Время подключения**. Дата и время подключения к серверу Агента, установленного на компьютере. Подключение выполняется при старте клиента. Также, чтобы распределить нагрузку, периодически происходит переподключение к пулу серверов.

При каждом успешном подключении дата и время в поле **Время подключения** меняется. При запуске Агента после остановки будет установлено соединение с сервером и значение поля **Время подключения** обновится;

> **Примечание.**
>
> Для компьютера со статусом Агента **Не установлен** отображается значение **Неактивен**.

- **Последнее обращение**. Дата и время последнего обращения к серверу Агента, установленного на компьютере. Для компьютера со статусом Агента **Не установлен** отображается значение **Агент не установлен**;
- **Версия схемы**. Номер версии схемы безопасности, загруженной на Агент;
- **Версия Агента**. Номер версии Агента, установленного на компьютере;
- **Операционная система**. Версия операционной системы;
- **Комментарий**. Поле для ввода комментария;
- **IP-адрес**. IP-адрес рабочей станции;
- **Пользователь**. Имя пользователя, заходившего на рабочую станцию последним.

> **Примечание:**
>
> Пользователь не отображается для рабочих станций под управлением Linux.

Расширенная информация по свойствам компьютера выводится на панели **Подробно**. Чтобы просмотреть свойства отдельного компьютера, в рабочей области главного окна выберите строку с описанием нужного компьютера и нажмите .

На панели **Подробно** будет отображена таблица свойств, в которой содержатся дополнительные сведения по выбранному компьютеру:

- **Версия настроек**. Версия общих настроек политики безопасности (DM) (см. "Настройка Device Monitor");
- **Версия настроек сетевых приложений**. Версия настроек контроля сетевого трафика, передаваемого по протоколам XMPP, MMP, FTP, FTPS, SMTP/S/MIME/Outlook/POP3, HTTPS;
- **Версия настроек исключений**. Версия настроек исключения приложений из перехвата. В скобках указывается номер последней примененной версии.
- **Версия конфигурации ТМ**. Последняя версия конфигурации Traffic Monitor, доставленная на данную рабочую станцию.

> **Примечание:**
>
> Если Агент отправляет событие на сервер Device Monitor, Агент удаляет данные этого события с диска.

> **Важно!**

В некоторых случаях не поддерживается удаление данных на Агентах. Файл с метаданными события может остаться на диске Агента, даже если Агент отправил событие.

Информация, выводимая по некоторым свойствам, дублируется в рабочей области главного окна.

Каждый зарегистрированный компьютер автоматически добавляется в группу компьютеров «по умолчанию». При этом компьютеру назначается политика безопасности (DM), определенная для группы компьютеров «по умолчанию».

2.9.4 Задача первичного распространения и обновления

Соблюдайте последовательность действий:

1. Создайте задачу первичного распространения.
2. Сформируйте список рабочих станций для установки Агентов.
3. Запустите задачу.
4. При наличии ошибок ознакомьтесь со сведениями о них или выгрузите лог.

Чтобы создать задачу первичного распространения Агентов:

1. В левой части рабочей области нажмите .
2. Выберите ОС рабочих станций, на которые требуется распространить Агенты: *Windows*/*Linux*.
3. Введите имя новой задачи.
4. Снимите флаг **Устанавливать компонент перехвата сетевого трафика**, если не хотите, чтобы этот компонент был установлен.
5. Если необходимо, добавьте описание задачи.
6. Задайте количество запусков задачи и их периодичность в минутах.
7. Укажите точку распространения Агентов, установленную ранее на сервере Device Monitor (подробнее см. "Установка "Все-в-одном"", Шаг 30). Или установите флаг **Использовать все доступные точки распространения**, чтобы использовать все точки распространения.
8. Последняя доступная версия Агентов, дистрибутивы которых необходимо установить, отображается в поле **Версия** (см. "Серверы DM").

   Примечание:

   Все доступные версии расположены в директории `/opt/iw/iwdistribution/bin/SetupPackages/`.

9. Укажите количество попыток загрузки пакета. Количество попыток по умолчанию – 10.
10. Нажмите **Добавить**. Новая задача будет отображена в списке задач.

Чтобы обновить версию Агентов на рабочих станциях под управлением ОС семейства Linux:

1. Откройте на редактирование созданную задачу, нажав .
2. В поле **Версия** укажите новую версию Агента, директория с которой находится в точке распространения. Если в задаче указан компьютер с установленным Агентом более старой версии, то он будет обновлен после выполнения задачи.
3. Нажмите **Добавить**.

Важно!

Для корректной блокировки съемных устройств обязательно перезагрузите рабочую станцию после обновления Агента.

Чтобы сформировать список рабочих станций:

Добавьте компьютеры одним из способов:

1. Чтобы добавить компьютер вручную, в выбранной задаче нажмите .
2. В открывшемся окне введите IP-адрес или DNS-имя компьютера, разделенные точкой с запятой или переносом строки (имя компьютера в формате RFC 1123; вы можете использовать любые символы любых алфавитов, указанных в Unicode).
3. Нажмите **Добавить**.

или

1. Чтобы добавить компьютеры из списка, нажмите **Настроить состав задачи** :
2. В открывшемся окне будет отображен список компьютеров из доступной интеграции с Active Directory или ранее добавленных компьютеров Группы DM (подробнее см. "Настройка состава групп компьютеров") с указанием полного имени для установки Агентов. Выберите рабочие станции в области *Компьютеры* и нажмите . При добавлении группы добавляются компьютеры только из выбранной группы, не включая компьютеры в подгруппах. Вы можете воспользоваться полем поиск, чтобы быстро найти нужный компьютер и добавить его в задачу. Введите не менее 3 и не более 64 символов.
3. Нажмите **Применить**. В области с именем задачи будет отображен список компьютеров с указанием полного имени для установки Агентов. Если на указанных компьютерах не были ранее установлены Агенты или версии Агентов ниже версии, указанной в задаче, то после запуска задачи Агенты будут установлены или обновлены.
4. Чтобы удалить ошибочно добавленные адреса, выделите их и нажмите .

Чтобы запустить задачу:

1. Выберите задачу с добавленными адресами рабочих станций или нажмите  напротив нужной задачи в списке слева.
2. Нажмите **Запустить** .
3. В открывшемся окне введите учетные данные пользователя удаленной рабочей станции, от имени которого запускается задача.
4. Если вы запускаете задачу распространения агентов на рабочие станции под управлением ОС семейства Linux:
   a. Выберите механизм повышения привилегии *sudo*/*su*.
   b. Если вы выбрали механизм повышения привилегии su:
      - Введите учетные данные пользователя, от имени которого будет осуществлено распространение агентов.
        или
      - Отметьте **Использовать указанные учетные данные**, чтобы осуществить распространение агентов от имени пользователя, указанного на шаге 3.
5. Нажмите **Запустить**.
6. Дождитесь окончания работы задачи.

Для каждой рабочей станции, на которую распространяется задача, в рабочей области главного окна отображаются следующие параметры:

Параметр	Описание
Имя	IP-адрес или доменное имя рабочей станции
Статус выполнения задачи	Текущее состояние задачи для данной станции. Возможные значения: • ***Не выполняется*** • ***Подготовка*** • ***В процессе*** • ***Ожидание перезагрузки*** • ***Ошибка*** • ***Нет доступа*** • ***Выполнена***
Версия агента	Версия Агента, установленного на рабочей станции
Операционная система	Операционная система, установленная на рабочей станции
Разрядность операционной системы	Разрядность операционной системы на рабочей станции
Количество подключений	Количество сделанных попыток подключения к недоступной рабочей станции
Время последнего обращения	Дата и время последнего подключения к рабочей станции

Если в результате выполнения задачи выставлен статус ***Ошибка***, вы можете перейти в журнал ошибок и ознакомиться с расширенными сведениями.

Чтобы просмотреть сведения об ошибках при установке Агентов и выгрузить логи:

1. Выберите строку в таблице со статусом задачи ***Ошибка***.
2. Нажмите . Будут отображены общие сведения и описания ошибок.
3. Нажмите , чтобы выгрузить логи в формате TXT.

> **Примечание:**
>
> Если при установке Агента возникла ошибка, то вы можете выгрузить лог ошибок только последнего запуска задачи.

Чтобы вернуться к списку рабочих станций, нажмите .

2.10 Настройка схемы безопасности

Настройка схемы безопасности включает в себя:

- Создание политик
- Создание правил
- Создание и изменение списков приложений
- Создание и редактирование групп сотрудников
- Настройка состава групп сотрудников

2.10.1 Создание политик

> **Важно!**
>
> При обновлении сервера Device Monitor до версии 7.15 и выше подключенные к этому серверу агенты версии 7.13 и более ранних прекратят получать данные об изменении схемы безопасности. Поэтому для получения агентами правил, политик, компьютеров, сотрудников и т.д. необходимо также обновить агенты до версии 7.14 или более поздней.

На Агентах Device Monitor политики применяются в следующем порядке:

1. Запрещающие политики.
2. Политики защиты данных на агентах, созданные в TM.
3. Политика теневого копирования.

Каждая политика безопасности состоит из набора правил, при помощи которых осуществляется мониторинг операций, связанных с переносом файлов на съемные устройства и сетевые ресурсы, отправкой документов на печать и сетевой активностью, определяется уровень доступа к контролируемым периферийным устройствам.

Политики назначаются **группам сотрудников** и **группам компьютеров**. Политика, назначенная группе сотрудников, действует на всех сотрудников, включенных в эту группу. Политика безопасности, назначенная группе компьютеров, действует на всех сотрудников, работающих на контролируемых компьютерах, включенных в эту группу.

Работа с политиками безопасности ведется в разделе **Политики**. Чтобы перейти к этому разделу, воспользуйтесь кнопкой **Политики**, расположенной на панели навигации.

После установки Центра администрирования (Device Monitor) по умолчанию созданы две политики – **Политика теневого копирования** и **Политика на устройства**.

Политика теневого копирования содержит следующие правила:

- Контроль FTP;
- Контроль HTTPS;
- Контроль IMAP;
- Контроль Outlook;
- Контроль POP3;
- Контроль Skype;
- Контроль SMTP;
- Контроль Telegram;
- Контроль VKontakte;
- Контроль WhatsApp;
- Контроль XMPP;
- Контроль веб-почты;
- Контроль облачных хранилищ;
- Контроль Яндекс Мессенджера;
- Теневое копирование документов;
- Теневое копирование документов в терминальную сессию;
- Теневое копирование документов на сетевые ресурсы;
- Теневое копирование печати.

Политика на устройства по умолчанию не содержит правил.

Чтобы создать новую политику:

1. В левой части рабочей области нажмите  .
2. В поле **Наименование** укажите название политики.
3. Нажмите **Создать**.

После создания политики добавьте в нее одно или несколько правил. Подробнее об особенностях применения правил смотрите в подразделе "Создание правил".

Чтобы отредактировать политику:

1. В левой части рабочей области выберите политику.
2. Нажмите  напротив выбранной политики.
3. В раскрывшемся списке нажмите  **Редактировать политику**.
4. В поле **Наименование** укажите новое название политики.
5. Нажмите **Сохранить**.

Чтобы удалить политику:

1. В левой части рабочей области выберите политику.
2. Нажмите  напротив выбранной политики.
3. Нажмите  **Удалить политику**.
4. Подтвердите действие.

Примечание:

Если политика безопасности назначена хотя бы одной группе сотрудников или группе компьютеров, ее невозможно удалить из схемы безопасности.

2.10.2 Создание правил

Чтобы добавить в политику новое правило:

1. Перейдите в раздел **Политики** Центра администрирования.
2. В левой части рабочей области выберите политику безопасности, в которую вы хотите добавить правило.
3. Нажмите  напротив выбранной политики. Затем в раскрывшемся списке нажмите  **Создать правило**.
   или
   В правой верхней части рабочей области нажмите кнопку **Создать правило**.
4. В открывшемся окне укажите параметры правила. Доступные для создания правила:
   - Правило контроля съемных носителей;
   - Правило контроля сетевых ресурсов;
   - Правило контроля терминальной сессии;
   - Правило контроля печати;
   - Правило контроля внешних устройств;
   - Правило контроля FTP;
   - Правило контроля HTTP(S);
   - Правило контроля почты;
   - Правило контроля облачных хранилищ;
   - Правило контроля экрана;
   - Правило контроля буфера обмена;
   - Правило контроля мессенджера VK;
   - Правило контроля мессенджера Telegram;
   - Правило контроля Яндекс Мессенджера
   - Правило контроля мессенджера WhatsApp;
   - Правило контроля мессенджера Skype;
   - Правило контроля протокола XMPP;
   - Правило контроля ввода текста с клавиатуры;
   - Правило контроля активности сотрудника.
5. После того как вы указали все необходимые параметры, нажмите **Создать**. Правило будет добавлено в политику.

Чтобы просмотреть детальную информацию о правиле, выберите его. Справа откроется панель **Подробно** с информацией о выбранном правиле. Чтобы скрыть панель, нажмите  справа вверху или повторно нажмите на выбранное правило.

Чтобы отредактировать правило:

1. Перейдите в раздел **Политики** Центра администрирования.
2. Выберите правило, которое необходимо отредактировать.
3. Нажмите  напротив выбранного правила.
4. Нажмите **Редактировать**.
5. Внесите изменения.
6. Нажмите **Сохранить**.

Чтобы удалить правило:

1. Перейдите в раздел **Политики** Центра администрирования.
2. Выберите правило, которое необходимо удалить.
3. Нажмите  напротив выбранного правила.
4. Нажмите **Удалить**.
5. Подтвердите действие.

Правило контроля съемных носителей

Правило позволяет отслеживать операции:

- копирования файлов с/на съемные носители;
- создания новых файлов на съемных носителях;
- изменения и переименования файлов на съемных носителях;
- копирования файлов с/на медиа-устройства, использующие для подключения протокол MTP;
- копирования файлов на съемных носителях (например, из одной папки USB-устройства в другую).

К съемным носителям относятся:

- устройства, подключенные через порты USB и IEEE 1394 (FireWire, i-Link);
- накопители на гибких магнитных дисках (Floppy-disk, ZIP);
- оптические диски (CD, DVD, BD) в режиме Live File System;
- медиа-устройства.

Важно!

На компьютерах под управлением Astra Linux, РЕД ОС и ОС Альт не контролируются операции записи на CD/DVD-диски, в том числе подключенные через порты USB.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Съемные носители**.
3. Выберите направление перехвата копирования: *На устройство* или *С устройства*. Событие будет создано в результате копирования файла в выбранном направлении.
4. В **Действии** при срабатывании правила выберите реакцию Системы на копирование файла:
   - *Создавать событие* – при этом будет создано событие с теневой копией.
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Для создания правила заполните ниже хотя бы одно из полей: **Маска файла** или **Категория файла**.
5. Выберите **Формировать теневую копию**, если необходимо создавать теневую копию в событии (настройка доступна при выборе **Создать событие** в поле **Действие**).

Примечание:

В Traffic Monitor в событии без теневой копии отображается название и размер файла.

6. Укажите условия для формирования событий:
   a. Отметьте и укажите **Маску файлов**, чтобы исключить из перехвата подходящие под нее файлы. Вы можете использовать групповые символы:
      - ? – один неизвестный символ;
      - * – любое количество символов.
   b. Вы можете ограничить применение правила определенной категорией сигнатур, для этого отметьте и укажите **Категорию файла**. В выпадающем списке вы можете выбрать одну из следующих категорий:
      - CAD системы;
      - Архивы;
      - Аудио-видео;
      - Базы данных и таблицы;
      - Графические данные;
      - Документы (офисные файлы, PDF);
      - Другие файлы;
      - Защищенные данные (зашифрованные, элементы PKI, хранилища паролей);
      - Исполняемые файлы;
      - Образы (виртуальные машины, образы дисков, дампы памяти);
      - Форматы данных мобильных устройств.

      > **Примечание:**
      >
      > Вы можете ознакомиться со списком сигнатур файлов по категориям в статье базы знаний "Перехватываемые сигнатуры файлов в Device Monitor (для правил с выбором Категории файла)".
      >
      > Если вы указали и маску файлов, и категорию, для срабатывания правила должны выполниться оба указанных условия.
      >
      > На компьютерах под управлением Astra Linux, РЕД ОС и ОС Альт категории сигнатур не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов.

   c. Задайте **Размер файла**, чтобы ограничить размер файлов, подлежащих контролю. При этом укажите диапазон значений для минимального и максимального размера файла и единицы измерения. Если заполнены оба поля, то правило будет действовать только для файлов, размер которых находится внутри указанного диапазона.
      По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
      Если условия не отмечены, событие будет сформировано без их учета.
7. После того, как вы определите все необходимые параметры, нажмите **Создать**.
   Правило будет действовать всегда и разрешать копирование с созданием события с теневыми копиями. Далее такие события отправляются на анализ в Traffic Monitor.

> **Важно!**
>
> На рабочих станциях под управлением ОС семейства Linux при блокировке копирования:
>
> - Копируемые файлы удаляются (с возможностью восстановления при условии использования специального ПО).

- Если съемный носитель был извлечен принудительно, блокировка копирования файлов по результатам анализа может не произойти.
- При копировании файлов с рабочей станции на съемный носитель не определяется путь файла. Поэтому политики, настроенные на путь, как источник копирования, могут не сработать.
- Не осуществляется блокировка по результатам анализа при копировании файлов на медиа-устройства, подключённые по протоколу MTP.
- Если срабатывает блокировка файла по результатам анализа при его перемещении или осуществлении над ним операции *вырезать-вставить*, файл может быть удален из источника и отсутствовать в приемнике.

Система распаковывает архивы и применяет к ним политики Traffic Monitor, если:

- перехвачен архив формата 7Z, ZIP, TAR.GZ, AR, RAR или ISO на Агенте под управлением ОС Windows;
- перехвачен архив формата 7Z, ZIP, AR или TAR.GZ на Агенте под управлением ОС Альт, РЕД ОС или ОС Astra Linux 1.7.

Об особенностях работы правила см. статью Базы Знаний "Особенности и ограничения перехвата при копировании файлов с/на съемные устройства, сетевые ресурсы, FTP, перехвата исходящей почты. Особенности задания правил в политиках защиты данных на агентах".

Правило контроля сетевых ресурсов

Правило контролирует действия с сетевыми ресурсами и позволяет:

- перехватывать копирование файлов на сетевые ресурсы с использованием UNC (например, *\\Server\SharedFolder\Folder\File*);
- перехватывать копирование файлов с сетевых ресурсов;
- запрещать копирование файлов на сетевые ресурсы.

Важно!

Копирование файла с сетевых ресурсов на рабочую станцию под управлением ОС семейства Linux может быть заблокировано только при передаче по протоколу SMBv1/CIFS одним из способов:

- подключением к сетевым ресурсам с монтированием в файловую систему: `mount -t cifs`
- подключением к сетевым ресурсам с помощью стандартных проводников, встроенных и сторонних утилит

Система распаковывает архивы и применяет к ним политики Traffic Monitor, если:

- перехвачен архив формата 7Z, ZIP, TAR.GZ, AR, RAR или ISO на Агенте под управлением ОС Windows;
- перехвачен архив формата 7Z, ZIP, AR или TAR.GZ на Агенте под управлением ОС Альт, РЕД ОС или ОС Astra Linux 1.7.

Важно!

На компьютерах под управлением Astra Linux, РЕД ОС и ОС Альт:

- при копировании файлов на сетевые ресурсы известен только путь конечного назначения, а при копировании с сетевого ресурса, известен только путь источника;
- не перехватывается копирование файла на сетевой ресурс, если подключение осуществлялось вводом имени сервера в строке поиска файлового менеджера ОС.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Сетевые ресурсы**.
3. Выберите направление перехвата копирования: *На ресурс* или *С ресурса*. Событие будет создано в результате копирования файла в выбранном направлении.
4. Вы можете выбрать режим **Запретить копирование**. Запрет доступен только при направлении копирования *На ресурс*. При этом поле **Действие** примет значение Создавать событие и будет недоступно для редактирования. Также будут недоступны поля **Маска файла**, **Категория файла** и **Размер файла**.
5. В **Действии** при срабатывании правила выберите реакцию Системы на копирование файла:
   - *Создавать событие* – при этом будет создано событие с теневой копией;
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Для создания правила заполните ниже хотя бы одно из полей: **Маска файла** или **Категория файла**.
6. Выберите **Формировать теневую копию**, если необходимо создавать теневую копию в событии (настройка доступна при выборе *Создавать событие* в поле **Действие**).

> **Примечание:**
>
> В Traffic Monitor в событии без теневой копии отображается название и размер файла.

7. Если требуется, укажите **Ресурсы**, задав их адреса. Чтобы посмотреть правила заполнения, наведите курсор на .
8. При необходимости вы можете ограничить набор контролируемых файлов, задав маску файла. Для этого отметьте поле **Маска файла** и укажите маску. Можно использовать символы: **?** для замены одного символа или ***** для замены набора символов. Например, `*.doc`. Знак пробела интерпретируется как часть имени файла.

> **Важно!**
>
> Для одного правила может быть только одна маска. Если необходимо ввести несколько масок, следует создать по одному правилу на каждую из масок.

> **Примечание:**

На компьютерах под управлением ОС Astra Linux или РЕД ОС маски файлов не учитываются.

9. Вы можете ограничить применение правила определенной категорией сигнатур, для этого отметьте и укажите **Категорию файла**. В выпадающем списке вы можете выбрать одну из следующих категорий:
   - CAD системы;
   - Архивы;
   - Аудио-видео;
   - Базы данных и таблицы;
   - Графические данные;
   - Документы (офисные файлы, PDF);
   - Другие файлы;
   - Защищенные данные (зашифрованные, элементы PKI, хранилища паролей);
   - Исполняемые файлы;
   - Образы (виртуальные машины, образы дисков, дампы памяти);
   - Форматы данных мобильных устройств.

   Примечание:

   Вы можете ознакомиться со списком сигнатур файлов по категориям в статье базы знаний "Перехватываемые сигнатуры файлов в Device Monitor (для правил с выбором Категории файла)".

   Если вы указали и маску файлов, и категорию, для срабатывания правила должны выполниться оба указанных условия.

   На компьютерах под управлением Astra Linux, РЕД ОС и ОС Альт категории сигнатур не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов.

10. Чтобы ограничить размер файлов, подлежащих контролю, укажите диапазон значений для минимального и максимального размера файла и единицы измерения. Если заполнены оба поля, то правило будет действовать только для файлов, размер которых попадает в указанный диапазон.
    По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
11. После того, как вы определите все необходимые параметры, нажмите **Сохранить**. Правило будет действовать всегда.

Подробнее о работе правила см. "Особенности и ограничения перехвата при копировании файлов с/на съемные устройства, сетевые ресурсы, FTP".

Правило контроля терминальной сессии

Правило позволяет отслеживать операции:

- копирования файла в приложение терминальной сессии;

Важно!

При копировании файла через терминальную сессию с помощью буфера обмена будет известно только короткое имя файла, а не полный путь.

Чтобы в событии был известен IP-адрес узла, на который были скопированы данные, необходимо наличие Агента Device Monitor на удалённом компьютере, к которому открыта терминальная сессия.
Если Агент Device Monitor установлен только на компьютере, с которого идет подключение к терминальной сессии, то в событии будет известно только приложение, через которое осуществлялось копирование данных, без указания IP-адреса получателя.

Примечание:

Для передачи файлов при использовании средств обеспечения терминального доступа рекомендуется использовать механизм "проброса" дисков в удаленный сеанс вместо передачи при помощи буфера обмена.

- копирования файла на ресурсы, подключенные через терминальную сессию (поддерживается перенаправление для сетевых папок и виртуальных устройств).

Важно!

Не будут созданы события терминальной сессии при копировании файлов не через границу терминальной сессии, а внутри локального клиента удаленного подключения. Например, при копировании файлов пользователем в окне **Параметры подключения** -> **Открытие файла**.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Терминальная сессия**.
3. Выберите направление перехвата копирования: *В сессию* или *Из сессии*. Событие будет создано в результате копирования файла в выбранном направлении.
4. В **Действии** при срабатывании правила выберите реакцию Системы на копирование файла:
   - *Создавать событие* – при этом будет создано событие с теневой копией.
   - *Исключить из перехвата* – при этом копирование будет разрешено, событие создано не будет. Для создания правила заполните ниже хотя бы одно из полей: **Маска файла** или **Категория файла**.
5. Выберите **Формировать теневую копию**, если необходимо создавать теневую копию в событии (настройка доступна при выборе **Создать событие** в поле **Действие**).

Примечание:

В Traffic Monitor в событии без теневой копии отображается название и размер файла.

6. Укажите условия для формирования событий:
   a. Отметьте и укажите **Маску файлов**, чтобы исключить из перехвата подходящие под нее файлы. Вы можете использовать групповые символы:

- ? – один неизвестный символ;
- * – любое количество символов.

b. Вы можете ограничить применение правила определенной категорией сигнатур, для этого отметьте и укажите **Категорию файла**. В выпадающем списке вы можете выбрать одну из следующих категорий:
   - CAD системы;
   - Архивы;
   - Аудио-видео;
   - Базы данных и таблицы;
   - Графические данные;
   - Документы (офисные файлы, PDF);
   - Другие файлы;
   - Защищенные данные (зашифрованные, элементы PKI, хранилища паролей);
   - Исполняемые файлы;
   - Образы (виртуальные машины, образы дисков, дампы памяти);
   - Форматы данных мобильных устройств.

   > **Примечание:**
   >
   > Вы можете ознакомиться со списком сигнатур файлов по категориям в статье базы знаний "Перехватываемые сигнатуры файлов в Device Monitor (для правил с выбором Категории файла)".
   >
   > Если вы указали и маску файлов, и категорию, для срабатывания правила должны выполниться оба указанных условия.
   >
   > На компьютерах под управлением Astra Linux, РЕД ОС и ОС Альт категории сигнатур не учитываются – правило сработает на копирование любых файлов, вне зависимости от указанных категорий файлов.

c. Задайте **Размер файла**, чтобы ограничить размер файлов, подлежащих контролю. При этом укажите диапазон значений для минимального и максимальный размера файла и единицы измерения. Если заполнены оба поля, то правило будет действовать только для файлов, размер которых находится внутри указанного диапазона.
   По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
   Если условия не отмечены, событие будет сформировано без их учета.

7. После того, как вы определите все необходимые параметры, нажмите **Создать**.
   Правило будет действовать всегда и разрешать копирование с созданием события с теневыми копиями. Далее такие события отправляются на анализ в Traffic Monitor.

Правило контроля печати

Правило позволяет осуществлять мониторинг операций, связанных с печатью документов на локальных и сетевых принтерах, в том числе с запуском печати через терминальную сессию.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Печать**.

3. При необходимости отключите опцию **Формировать теневую копию**, сняв соответствующий флажок, – тогда событие будет сохранено без теневой копии. По умолчанию опция включена.
   Для Агентов на рабочих станциях под управлением ОС Windows есть возможность блокировки печати по результатам анализа. Для этого необходимо настроить политику защиты данных на агентах в Traffic Monitor.

   > **Важно!**
   >
   > Агент на ОС Astra Linux, РЕД ОС и MacOS при перехвате печати в некоторых случаях может создавать несколько событий. Такая ситуация может возникнуть, если задание печати было передано через несколько серверов печати и было на них перехвачено с большими временными интервалами.
   >
   > Если сервер печати и Агент Device Monitor установлены на ОС Astra Linux, РЕД ОС и ОС Альт:
   >
   > - не определяется пользователь, отправивший файл на печать;
   > - не определяется количество страниц в теневой копии;
   > - не осуществляется перехват документов, отправленных на печать через терминальную сессию;
   > - возможно изменение формата теневых копий перехваченных событий печати. При этом:
   >   - одностраничный EXCEL-документ разбивается на фрагменты, и каждый фрагмент конвертируется в формат JPEG;
   >   - многостраничный документ формата PDF разбивается постранично, и каждая страница конвертируется в формат JPEG;
   >   - документ WORD конвертируется в набор JPEG-файлов, где каждая страница является отдельным JPEG-файлом.
   >
   > Если Агент Device Monitor установлен на MacOS:
   >
   > - перехват печати может перестать осуществляться в случае, когда при работающем Агенте система печати CUPS была перенастроена так, чтобы копии печатаемых файлов не создавались;
   > - могут создаваться события в случае отмены печати.

   > **Важно!**
   >
   > События печати не будут сформированы при печати в файл на Агентах, установленных на ОС Astra Linux, РЕД ОС и ОС Альт, а также при печати на предустановленном принтере на Агентах, установленных на ОС Astra Linux.

4. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Правило контроля внешних устройств

> **Важно!**

Начиная с версии Device Monitor 7.15 работа с данным правилом доступна в системе Device Control (раздел "Устройства" Центра расследований) и недоступна в Device Monitor. См. подробнее "Обновление Сервера Device Monitor", "InfoWatch Device Control. Руководство пользователя".

Правило контроля FTP

Правило позволяет контролировать обмен данными по протоколу FTP/FTPS, в том числе:

- разрешать или запрещать передачу информации по протоколу FTP;
- перехватывать трафик по протоколу FTP с созданием теневых копий;
- ограничивать доступ к FTP-ресурсам.

Важно!

На компьютерах под управлением РЕД ОС и ОС Альт не перехватывается копирование файла на FTP-сервер, если подключение осуществлялось вводом имени сервера в строке поиска файлового менеджера ОС.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **FTP(S)**.
3. В **Действиях** при срабатывании правила выберите степень контроля при обмене данными:
   - *Разрешить скачивание и запись на FTP* – при этом будет создано событие с теневой копией в случае записи на FTP;
   - *Исключать файлы при скачивании и записи на FTP* – введите адреса FTP-серверов для исключения копирования файлов из перехвата;
   - *Запретить запись на FTP*;
   - *Запретить вход на FTP-адреса.*
4. Заполните поле **FTP-адреса**. Наведите указатель мыши на **?** (знак вопроса), чтобы узнать правила его заполнения. Если адреса не заданы, то правило будет применено ко всем адресам.

   Примечание:

   Следует иметь ввиду, что:

   - разрешающие правила на конкретные адреса имеют больший приоритет, чем запрещающие;
   - разрешающие правила без указания адресов менее приоритетны, чем любые запрещающие;
   - если в качестве адреса для запрета указать только адрес сервера, то будет запрещен доступ на все папки этого сервера;
   - если в качестве адреса для запрета указать адрес сервера и подпапки, то будут разрешены переходы между папками на этом сервере, но доступ к копированию файлов будет запрещен только для указанной папки.

5. Если требуется, укажите ограничение на размер файла:

a. Отметьте **Размер файла**.
b. Обозначьте диапазон значений и единицы измерения.
Если заполнены оба поля, то правило будет действовать только для файлов, размер которых находится внутри указанного диапазона.
По умолчанию условие отмечено и задан размер файлов от 0 до 10 МБ.
Этот параметр доступен только при создании событий с теневыми копиями отправляемых файлов и при создании события без теневых копий для случаев записи, если на компьютере осталось меньше свободного места, чем определено политикой.

6. После того, как вы определите все необходимые параметры, нажмите **Создать**.
Правило будет действовать всегда.

Подробнее о работе правила см. "Особенности и ограничения перехвата при копировании файлов с/на съемные устройства, сетевые ресурсы, FTP".

Правило контроля HTTP(S)

Правило позволяет контролировать обмен данными по протоколам HTTP и HTTPS.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **HTTP(S)**.
3. В **Действии** при срабатывании правила выберите:
   - *Создавать события для всех ресурсов;*
   - *Создавать события только для внешних ресурсов.*
   О том, как добавить сегменты корпоративной сети в исключения, см. "Корпоративные сети".
4. Определите размеры запросов, для которых будет создана теневая копия. Для этого:
   a. Активируйте **Минимальный**, укажите значение и единицы измерения. Если настройка задана, то теневое копирование будет выполняться только для запросов, размер которых больше либо равен указанному. Значение по умолчанию: 40 Байт.
   b. Активируйте **Максимальный**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для запросов, размер которых меньше либо равен указанному. Значение по умолчанию: 40 МБ.
5. После того, как вы определите все необходимые параметры, нажмите **Создать**.
Правило будет действовать всегда.

Важно!

На компьютерах под управлением ОС Astra Linux, РЕД ОС или ОС Альт:

- политика защиты данных на агентах применяется только к тексту запроса, анализ файлов не поддерживается;
- не перехватываются соединения по протоколу IPv6;
- запросы, относящиеся к веб-почте, перехватываются как обычные HTTP-запросы.

Важно!

Агент DM под управлением ОС Windows при работе с сервером DM на ОС семейства Linux будет передавать на сервер некорректную информацию о нахождении адаптеров в корпоративной сети. Причина в том, что для корректного определения нахождения в корпоративной сети необходимо верное указание сегментов сетей, включая адреса шлюзов.

Важно!

При миграции с сервера DM с ОС Windows на ОС семейства Linux

В случае, если на DM с ОС Windows было задано только одно правило HTTP, которое исключало перехват запросов на внутренние ресурсы, то после перехода на ОС семейства Linux это правило будет означать создание событий для всех ресурсов, кроме внутренних. Например: в DM с ОС Windows существовало правило "Не создавать события для запросов на внутренние ресурсы". После миграции на ОС семейства Linux правило будет означать "Создавать события только для внешних ресурсов".

В DM с ОС Windows существовало правило "Создавать события для запросов, передаваемых по какому-либо из каналов" с указанием размеров запросов. После миграции на ОС семейства Linux правило будет означать "Создавать события для всех ресурсов" с теми же размерами.

Правило контроля почты

Правило контроля почты позволяет перехватывать получение электронной почты по POP3, IMAP и отправку почты по SMTP, HTTPS, а также осуществлять запрет на отправку веб-почты по HTTPS.

Важно!

Перехват сообщений по протоколу HTTPS поддерживается только при использовании сервисов веб-почты: Gmail, Yandex, Mail.ru, Yahoo, Rambler, Outlook.com.

Не осуществляется перехват почты по протоколу HTTPS через Outlook Web App при использовании сервера MS Exchange.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Почта**.
3. Выберите, какие действия с почтой должны быть доступны пользователю:
   - *Запретить использование почты*;
   - *Разрешить использование почты.*
4. В поле **Протокол** выберите канал, который должен контролироваться правилом:
   - *Все протоколы*;
   - *SMTP* – только для исходящей почты;
   - *POP3* – только для входящей почты;
   - *IMAP* – только для входящей почты;
   - *HTTPS* – только для исходящей почты сервисов: Gmail, Yandex, Mail.ru, Yahoo, Rambler, Outlook.com;
   - MAPI/Outlook – для входящей и исходящей почты.
5. Выберите, если требуется создавать события с теневой копией для:
   - *Входящих*, если в поле **Протокол** выбрано *POP3* или *IMAP*;

- *Исходящих*, если в поле **Протокол** выбрано *SMTP* или *HTTPS*;
- обоих значений, если в поле **Протокол** выбрано *Все каналы* или *MAPI/Outlook*.

> **Важно!**
>
> Если в правиле установлено **Разрешить использование почты**, должно быть выбрано создание теневой копии хотя бы для одного из направлений почты: *Входящие* или *Исходящие*.

> **Важно!**
>
> В теневой копии события веб-почты будут только те данные, которые были в перехваченном в трафике. Например, события будут содержать все атрибуты письма, кроме вложений, в случаях если:
>
> - сотрудник отправляет письмо из черновиков после того, как событие было уже отправлено в Traffic Monitor по окончании таймаута с момента последней активности сотрудника с письмом;
> - сотрудник отправляет письмо из черновиков, созданных на другой рабочей станции;
> - сотрудник пересылает отправленное ранее письмо.

6. Если требуется, задайте **Максимальный размер письма**. Для этого введите его значение и единицы измерения. В этом случае теневое копирование будет выполняться только для писем, размер которых меньше либо равен указанному. По умолчанию условие отмечено и задан максимальный размер файлов 40 МБ. Чтобы создавать событие с теневой копией для писем любого размера, снимите флажок.
7. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

> **Важно!**
>
> На рабочих станциях под управлением ОС семейства Linux осуществляется блокировка только исходящего трафика (SMTP-протокол и веб-почта). При этом файлы, передаваемые по веб-почте, не анализируются.

> **Важно!**
>
> Система распаковывает архивы и применяет к ним политики Traffic Monitor, если:
>
> - перехвачен архив формата 7Z, ZIP, TAR.GZ, AR, RAR или ISO на Агенте под управлением ОС Windows;
> - перехвачен архив формата 7Z, ZIP, AR или TAR.GZ, передаваемый по протоколу SMTP как вложение к письму, на Агенте под управлением ОС Альт, РЕД ОС или ОС Astra Linux 1.7.

Правило контроля облачных хранилищ

Правило позволяет контролировать отправку и получение любых данных, доступ к веб-клиентам следующих облачных хранилищ:

- Dropbox;
- Evernote;
- Google Drive;
- OneDrive;
- SugarSync;
- Яндекс Диск.

> **Важно!**
>
> При запрете доступа к хранилищу Google Drive возможны некорректная работа и запрет использования других сервисов Google, которые используют хост docs.google.com. Например, Google Docs, Google Tabs, Google Slides и т.д.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Облачные хранилища**.
3. Выберите действие, которое будет применено. Для всех облачных хранилищ доступны следующие варианты:
   - **Запретить доступ**;
   - **Разрешить только скачивание**;
   - **Перехватывать загрузку файлов**.
4. Выберите одно или несколько файловых хранилищ для контроля.
5. При перехвате загрузки файлов будут создаваться теневые копии. В этом случае вы можете дополнительно указать:
   - **Минимальный размер файла для создания события**, установив значение и единицы измерения. Если поле заполнено, то правило будет создавать событие только для файлов, размер которых больше либо равен указанному;
     По умолчанию задано значение 1 КБ.
   - **Максимальный размер теневой копии**, установив значение и единицы измерения. Если поле заполнено, то теневая копия будет создана только для файлов, размер которых меньше либо равен указанному.
     По умолчанию задано значение 10 МБ.
6. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Правило контроля экрана

Правило позволяет создавать снимки экрана в формате PNG:

- при смене активного окна любых приложений;
- всех мониторов, подключенных к незаблокированному контролируемому компьютеру.

> **Примечание:**

Правило доступно для рабочих станций под управлением ОС Windows, РЕД ОС или ОС Альт.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Создание снимков экрана**.
3. Укажите, когда необходимо создавать снимки экрана, или выберите оба условия:
   - *При смене активного окна* – распространяется на любые приложения, но не учитывается смена вкладок браузера;
   - *Через каждые n секунд* – период времени между снимками экрана.
4. Нажмите **Создать**. Правило будет действовать всегда.

Важно!

Снимок всего экрана создается в течение 5 секунд после активации окна/вкладки. Если переключение активного окна/вкладки происходит чаще, чем один раз в 5 секунд, снимок экрана не будет создан.

Правило контроля буфера обмена

Правило позволяет контролировать доступ сотрудников к буферу обмена.

Важно!

Контроль буфера обмена работает на компьютерах под управлением ОС MS Windows, РЕД ОС и ОС Альт Рабочая станция.

По правилу контроля буфера обмена Device Monitor перехватывает только текстовые данные.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Буфер обмена**.
3. В блоке **Действие** доступно только **Перехватывать вставку**.
   Укажите, когда должно срабатывать привило. Для создания правила должна быть выбрана хотя бы одна из опций:
   - **Вставка в приложение терминальной сессии**. Если выбрана эта опция, правило будет срабатывать при вставке данных в приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.
   - **Копирование из приложения в терминальной сессии**. Если выбрана эта опция, правило будет срабатывать при вставке данных из приложения терминальной сессии. При вставке данных внутри терминальной сессии правило срабатывать не будет.

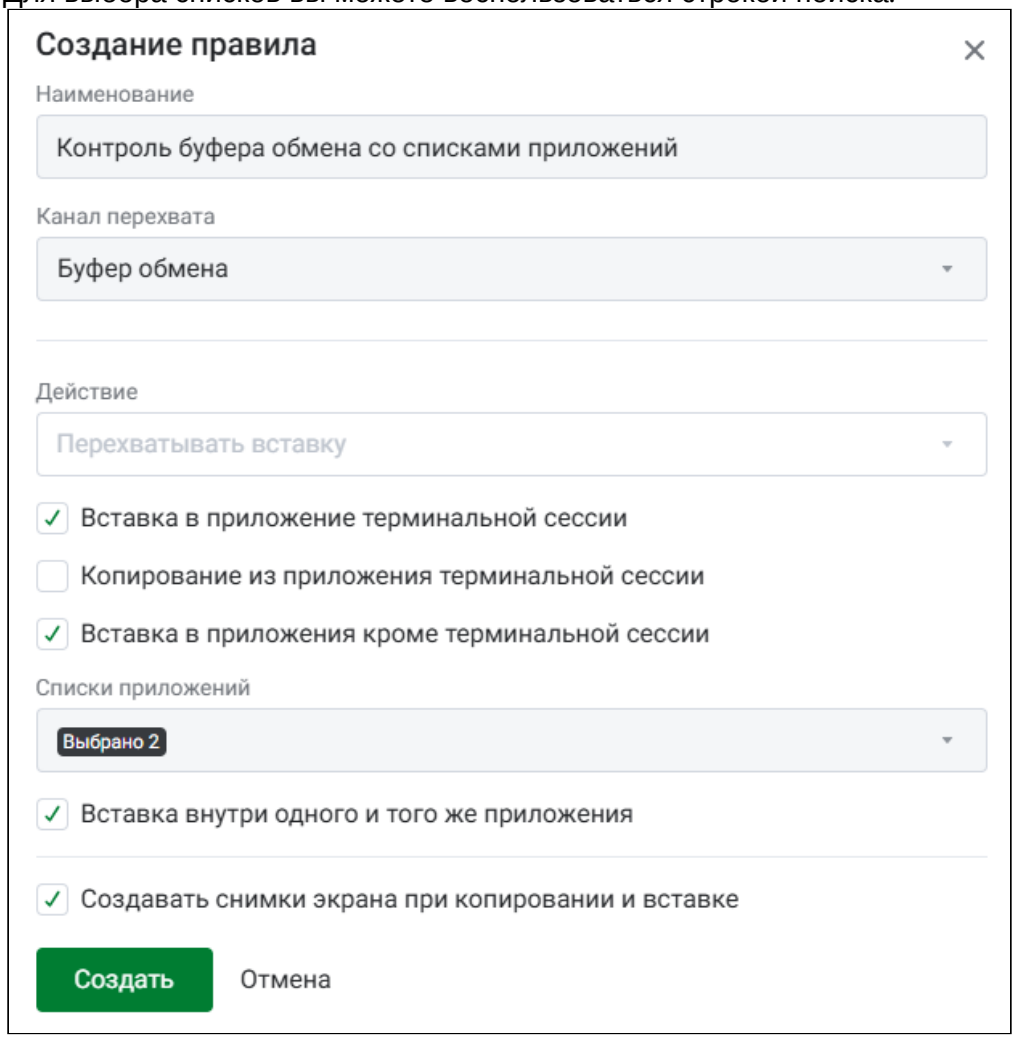
     Важно!

На рабочих станциях под управлением РЕД ОС и ОС Альт Рабочая станция не поддерживаются опции:

- **Вставка в приложение терминальной сессии**;
- **Копирование из приложения в терминальной сессии**.

Чтобы настроить правило для РЕД ОС и ОС Альт Рабочая станция, выберите опцию **Вставка в приложения кроме терминальной сессии** и выберите список приложений для Linux.
На рабочих станциях под управлением РЕД ОС и ОС Альт Рабочая станция не поддерживается использование опции **Вставка внутри одного и того же приложения**.

- **Вставка в приложения кроме терминальной сессии**. Выберите эту опцию, если правило должно действовать при вставке данных в указанные приложения. Правило также будет срабатывать при вставке в приложения данных, скопированных из терминальной сессии.
  Для использования опции выберите списки в поле **Списки приложений** (о создании списков приложений см. "Создание и изменение списков приложений"). Для выбора списков вы можете воспользоваться строкой поиска.



- Чтобы правило срабатывало также при вставке данных в приложение, из которого данные были скопированы, отметьте опцию **Вставка внутри одного и того же приложения**.

Перехват в пределах одного приложения поддерживается, только если приложение использует системные механизмы буфера обмена.

- Для создания снимков экрана при срабатывании правила отметьте опцию **Создавать снимки экрана при копировании и вставке**.

> **Важно!**
>
> Создание снимков экрана в этом правиле поддерживается только на рабочих станция под управление ОС MS Windows.

4. После того, как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Правило контроля мессенджера VK

Правило позволяет контролировать обмен сообщениями чата и любыми типами исходящих файлов в веб-версии системы мгновенного обмена сообщениями VK (ВКонтакте). При этом будет перехвачена вся история переписки на служебном компьютере, включая период до установки Агента Device Monitor.

> **Важно!**
>
> Не поддерживается перехват:
>
> - файлов, загруженных с компьютера без установленного Агента Device Monitor;
> - постов на стене;
> - сообщений, содержащих геопозицию;
> - истории отредактированных сообщений.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **VK**.
3. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии исходящих файлов, отметьте поле **Создавать теневую копию исходящих файлов**. Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте **Минимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   b. Отметьте **Максимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.
   Эти поля учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии.

> **Примечание:**

Чтобы задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

4. После того как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Правило контроля мессенджера Telegram

Правило позволяет контролировать обмен новыми, пересылаемыми или исправленными сообщениями чата, в том числе группового, исходящими файлами и голосовыми сообщениями на толстом клиенте и в веб-версии системы мгновенного обмена сообщениями Telegram. При этом будет перехвачена вся история переписки на служебном компьютере, включая период до установки Агента Device Monitor.

Важно!

Не поддерживается запрет использования.

Не поддерживается перехват:

- стикеров;
- gif-анимации;
- контактов;
- геоположения;
- каналов;
- аудиозвонков;
- опросов;
- текста, который был прикреплен в качестве ссылки.

Для Telegram на компьютерах под управлением **ОС семейства Linux**:

- поддерживается перехват только десктоп-версии Telegram;
- для перехвата должен быть включен системный вызов `ptrace()`;
- не поддерживается перехват Flatpak-приложения.

Для Telegram на компьютерах под управлением **MS Windows**:

- Правило позволяет перехватывать следующие версии Telegram:
  - десктоп-версию: приложение с официального сайта Telegram (desktop.telegram.org) или из Microsoft Store;
  - веб-версии: K, Z и устаревшую (Legacy).
- Перехват веб-версий имеет ряд особенностей:
  - разные веб-версии определяются Системой как разные приложения;
  - существует временная задержка начала перехвата - до 50 секунд с момента авторизации;
  - поддерживаются браузеры:
    - Google Chrome;
    - Microsoft Edge;
    - Mozilla Firefox;

- Opera;
- Яндекс Браузер.

При отправке сообщений в групповой чат Telegram, событие будет содержать идентификатор и название группового чата.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Telegram**.
3. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии исходящих файлов, отметьте поле **Создавать теневую копию исходящих файлов**.
   Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте **Минимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   b. Отметьте **Максимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.
   Эти поля учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии.

   Примечание:

   Чтобы задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

4. После того как вы определите все необходимые параметры, нажмите **Создать**.
   Правило будет действовать всегда.

Правило контроля Яндекс Мессенджера

Правило позволяет контролировать обмен сообщениями и исходящими файлами веб-версии системы мгновенного обмена сообщениями Яндекс Мессенджер. Правило позволяет перехватывать новые, пересылаемые и исправленные сообщения чатов, в том числе групповых. Система перехватывает историю переписки на служебном компьютере с момента установки на него Агента Device Monitor и создания данного правила.

Важно!

Перехват веб-версии Yandex поддерживается в следующих браузерах:

- Google Chrome;
- Microsoft Edge;
- Mozilla Firefox;
- Opera;
- Яндекс Браузер.

Не поддерживается запрет использования и перехват аудио сообщений.

В событиях группового звонка не содержится информация об участниках (получателях), которые не отправляли сообщения в групповой чат.
В случае, если одиночный звонок был переведен в групповой, не будет создано событие ни для одиночного, ни для группового звонка.

При перехвате исходящего файла в групповом чате в событии не будет наименования чата.

События для исправленных сообщений в групповом чате могут не содержать название чата.

При отправке сообщений в групповой чат, событие будет содержать идентификатор чата, а также может содержать название группового чата.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Яндекс Мессенджер**.
3. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии исходящих файлов, отметьте поле **Создавать теневую копию исходящих файлов**.
   Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте **Минимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   b. Отметьте **Максимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.
   Эти поля учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии.

   Примечание:

   Чтобы задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

4. После того как вы определите все необходимые параметры, нажмите **Создать**.
   Правило будет действовать всегда.

Правило контроля мессенджера WhatsApp

Правило позволяет контролировать обмен сообщениями и исходящими файлами десктоп- и веб-версии системы мгновенного обмена сообщениями WhatsApp. Правило позволяет перехватывать новые, пересылаемые и исправленные сообщения чатов, в том числе групповых. Система перехватывает историю переписки на служебном компьютере с момента установки на него Агента Device Monitor и создания данного правила.

Важно!

Перехват веб-версии WhatsApp поддерживается в следующих браузерах:

- Google Chrome;
- Microsoft Edge;
- Mozilla Firefox;

- Opera;
- Яндекс Браузер.

Не поддерживается запрет использования.

Не поддерживается перехват:

- аудио- и видеозвонков;
- метаинформации контакта (никнейма);
- файлов, пересылаемых из одного чата в другой;
- текста, который был прикреплен в качестве ссылки.

Перехват не будет осуществляться, если сотрудник вошел в веб-версию WhatsApp:

- когда Агент еще не был установлен;
- когда Агент был отключен.

В этих случаях после запуска новой версии Агента необходимо очистить кеш браузера.

Если Агент активируется при уже запущенном WhatsApp, он может завершить его процессы, чтобы при новом запуске WhatsApp встроить в него перехват. До тех пор пока WhatsApp не будет перезапущен, перехват осуществляться не будет.

При запуске сервера анализа (процесс IWProxy) все обнаруженные процессы WhatsApp могут быть принудительно завершены.

При перехвате фото- и видеофайлов, событие может содержать не оригинальный файл, а его превью. В этом случае имя файла будет иметь формат "Embedded <Тип содержимого: image/video> <Время отправки данных в миллисекундах>".

Если перехвачено несколько сообщений с одинаковым текстом и отправителем, отправленных с разницей порядка 3 секунд, то для них будет сформировано одно событие. Дублирующие события созданы не будут.

При отправке сообщений в групповой чат WhatsApp, событие будет содержать идентификатор чата и название группового чата.
События для исправленных сообщений в групповом чате могут не содержать название чата.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **WhatsApp**.
3. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии исходящих файлов, отметьте поле **Создавать теневую копию исходящих файлов**.
   Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте **Минимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   b. Отметьте **Максимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.
   Эти поля учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии.

> **Примечание:**
>
> Чтобы задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

4. После того как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Правило контроля мессенджера Skype

Правило позволяет контролировать обмен сообщениями и исходящими файлами в десктопной (версия 8) и веб-версии системы мгновенного обмена сообщениями Skype, а также осуществлять запрет или разрешение передачи данных по протоколу Skype.

Правило позволяет перехватывать:

- новые, цитируемые, исправленные и удаленные сообщения чатов, в том числе групповых;
- переданные файлы;

  > **Важно!**
  >
  > Если отправка файла была прервана, будет создано событие с той частью файла, которая была отправлена.

- SMS-сообщения;
- голосовой трафик:
  - аудиозвонки;
  - видеозвонки (только аудио-часть);
  - исходящие голосовые сообщения.

> **Важно!**
>
> По умолчанию создание теневой копии голосового трафика отключено.

Система перехватывает историю переписки на служебном компьютере с момента установки на него Агента Device Monitor и создания правила. История переписки, которая осуществлялась до момента установки Агента, не перехватывается.

> **Важно!**
>
> Не поддерживается перехват:
>
> - частных бесед (Private Conversation);
> - аудиозвонков в десктопной и metro-версии;
> - видео-части при видеозвонках;
> - контактов отправителей и получателей из цитируемых сообщений;

- истории группового чата до добавления в него пользователя, если в чате разрешен просмотр всей истории сообщений.

Особенности перехвата сообщений в групповых чатах:

- В первых событиях может отсутствовать список получателей.
- Если передача файла – это первое сообщение пользователя в групповой чат, то в качестве получателя для такого события будет указан идентификатор чата.
- В событиях в списке получателей помимо участников чата всегда будет присутствовать идентификатор чата.

Особенности перехвата истории переписки, которая осуществлялась вне служебного компьютера с установленным Агентом Device Monitor:

- История переписки перехватывается в том объеме, в котором она встречается в трафике, перехваченном Агентом. Это означает, что не всегда возможно перехватить полную историю переписки с момента ее последнего перехвата на компьютере с установленным Агентом.
- Переписка может быть не перехвачена или перехвачена не полностью.

Особенности перехвата аудиозвонков:

- Захват звука выполняется только через передние стерео-колонки. Если звук выводится только на задние колонки, он не будет записан.
- Если во время разговора по Skype пользователю поступит еще один звонок, перехватчик Device Monitor не сможет добавить в событие перехвата контакты нового собеседника, поэтому:
  - в событии будут указаны только изначальные участники беседы;
  - будет перехвачена запись всего разговора.
- Если на одном компьютере с установленным Агентом Device Monitor запущено два приложения Skype под разными учетными записями, перехватчик не сможет однозначно привязать звуковой поток к учетной записи.
- Если после аудиозвонка компьютер с Агентом был выключен, то в событии перехвата может отсутствовать теневая копия перехваченного разговора.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Skype**.
3. В поле **Действие** по умолчанию выбрано **Перехватывать сообщения**. Если вы хотите запретить использование Skype на компьютере с Агентом Device Monitor, выберите опцию **Запретить использование**.

> **Примечание:**
>
> Настройка работает следующим образом: перехватчик выполняет проверку того, запущено ли приложение, и, если приложение запущено, принудительно закрывает его. Проверка выполняется с частотой 1 раз в минуту.
>
> Если в настройках уведомлений включена настройка **Показывать сотруднику уведомления системы**, то в случае запуска приложения Skype при включенном запрете использования Агент Device Monitor отобразит сообщение в области уведомлений. Текст уведомления может быть задан в настройках в консоли.

> **Важно!**
>
> Если настроить запрет использования Skype, веб-версия Microsoft Teams будет недоступна.

4. Если вы хотите передавать в Traffic Monitor также теневые копии исходящих файлов, отметьте поле **Создавать теневую копию исходящих файлов**. Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте **Минимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше указанного либо равен ему.
   b. Отметьте **Максимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше указанного либо равен ему.
   Эти поля учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии.

   > **Примечание:**
   >
   > Чтобы задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

5. Если вы хотите передавать в Traffic Monitor также теневые копии голосового трафика, отметьте поле **Создавать теневую копию голосового трафика**. Запись голоса будет прикреплена к событию в формате `*.ogg`. Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте поле **Максимальная длительность**, укажите значение в минутах.

   > **Примечание:**
   >
   > Допустимые значения: от 10 до 1440 минут. Значение по умолчанию – 10 минут.
   >
   > Если параметр **Максимальная длительность** не указан, будет сформировано одно событие с полной записью перехваченного разговора. В противном случае при перехвате разговора, длительность которого превышает заданное значение параметра **Максимальная длительность**, запись будет разделена на несколько теневых копий. С каждой теневой копией будет сформировано отдельное событие. Таким образом, на один разговор может быть создано несколько событий.

6. После того как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Правило контроля протокола XMPP

Правило позволяет контролировать обмен по протоколу **XMPP** входящими и исходящими текстовыми сообщениями, а также исходящими файлами.

Чтобы создать и настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **XMPP**.
3. В поле **Действие** по умолчанию выбрано **Перехватывать сообщения**. Если вы хотите запретить обмен сообщениями по протоколу XMPP на компьютере с Агентом Device Monitor, выберите опцию **Запретить использование**.
4. Если вы хотите передавать в Traffic Monitor, помимо события, и теневые копии исходящих файлов, отметьте поле **Создавать теневую копию исходящих файлов**. Если вы хотите определить дополнительные параметры теневых копий:
   a. Отметьте **Минимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых больше либо равен указанному.
   b. Отметьте **Максимальный размер файла**, укажите значение и единицы измерения. Если поле отмечено, то теневое копирование будет выполняться только для файлов, размер которых меньше либо равен указанному.
   Эти поля учитываются только при создании теневой копии: если размер файла попадает в указанный диапазон, то событие будет содержать теневую копию; в противном случае событие будет сформировано без теневой копии.

   > **Примечание:**
   >
   > Чтобы задать условия для формирования событий, перейдите в раздел **Настройки > Каналы перехвата** (подробнее см. "Каналы перехвата").

5. После того как вы определите все необходимые параметры, нажмите **Создать**. Правило будет действовать всегда.

Правило контроля ввода текста с клавиатуры

Правило позволяет перехватывать ввод текста с клавиатуры в окне любого приложения на рабочих станциях и формировать события при смене активного окна. Далее события, содержащие теневые копии введенных с клавиатуры данных, будут отправлены в Traffic Monitor для обработки и анализа.

> **Примечание:**
>
> Правило применяется на рабочих станциях под управлением ОС MS Windows, ОС Альт и РЕД ОС.

По умолчанию перехватывается ввод текста с клавиатуры на рабочих станциях:

- при смене активного окна;
- по истечении 20 секунд с момента окончания ввода;
- при накоплении 100 символов в одном слове или 200 символов, введенных с клавиатуры;
- при нажатии Enter / Ctrl+Enter / Shift+Enter.

Чтобы создать правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Ввод текста с клавиатуры**.

3. Выберите одно из действий правила:
   - **Перехватывать ввод текста во всех приложениях**
   - **Перехватывать ввод текста для приложений из списка** - Device Monitor будет создавать событие при вводе текста в активном окне приложений из списка.

     > **Примечание:**
     >
     > Поддерживается использование только списков для ОС MS Windows.

   - **Не перехватывать ввод текста для приложений из списка** - Device Monitor **не** будет создавать событие при вводе текста в активном окне приложений из списка.
4. Если выбрано действие, учитывающее списки приложений, в появившемся поле укажите их.
   Подробнее о создании списков приложений см. "Создание и изменение списков приложений".
5. Если требуется, включите опцию **Создавать снимок экрана при создании события**.

   > **Примечание:**
   >
   > Создание снимка экрана при создании события поддерживается только на рабочих станциях под управлением ОС MS Windows.

   > **Примечание:**
   >
   > Настройка и применение правила контроля ввода текста с клавиатуры и правила контроля экрана осуществляются независимо друг от друга.

6. Нажмите **Создать**.

Чтобы задать условия для формирования событий, перейдите в раздел **Настройки> Каналы перехвата** (подробнее см. "Каналы перехвата").

> **Важно!**
>
> Для Агента на ОС Альт или РЕД ОС смена вкладки в браузере игнорируется.
>
> **Пример:** открыто приложение, с которого ведется перехват ввода текста с клавиатуры. Сотрудник переключается между вкладками и вводит в них текст. Такое поведение сгенерирует одно событие на ввод текста в приложении, а не на каждую вкладку.

> **Важно!**
>
> Перехват текста с клавиатуры корректно работает для русского и английского языков. При добавлении других языков требуется перезагрузка рабочей станции.

Правило контроля активности сотрудника

Правило позволяет собирать статистику активности сотрудника за контролируемым компьютером, формировать события и отправлять их в Activity Monitor.

> **Примечание:**
>
> Правило доступно для рабочих станций под управлением ОС Windows, РЕД ОС или ОС Альт.

Чтобы настроить правило:

1. Откройте окно создания правила и в поле **Наименование** укажите название правила.
2. В поле **Канал перехвата** выберите **Активность сотрудника**.
3. Выберите действие:
   - **Собирать статистику активности**, чтобы контролировать активность и собирать данные по действиям сотрудника:
     - Локальный вход в сессию;
     - Локальный выход из сессии;
     - Удаленный вход в сессию;
     - Удаленный выход из сессии;
     - Локальная блокировка сессии;
     - Локальная разблокировка сессии;
     - Удаленная блокировка сессии;
     - Удаленная разблокировка сессии;
     - Запуск приложения;
     - Остановка приложения;
     - Переключение между приложениями;
     - Переключение между вкладками в браузере;
     - Выполнение поисковых запросов;
     - Получение и потеря фокуса активного окна;
     - Использование клавиатуры.
   - **Не собирать статистику активности**, чтобы контролировать активность без сбора данных.
4. Нажмите **Создать**. Правило будет действовать всегда.

Чтобы данные статистики успешно отправлялись в Activity Monitor, убедитесь, что установлено подключение к Платформе (подробнее см. "Серверы – Подключение к Платформе").

> **Важно!**
>
> Для операционной системы РЕД ОС контролируются следующие действия пользователя в Системе:
>
> - Локальный вход в сессию;
> - Локальный выход из сессии;
> - Локальная разблокировка сессии;
> - Локальная блокировка сессии;
> - Получение фокуса активного окна приложения;
> - Потеря фокуса активного окна приложения;
> - Использование клавиатуры;

- Получение фокуса вкладкой браузера (для браузера Edge (Chromium).

Для операционной системы ОС Альт контролируются такие же действия пользователя, как для системы РЕД ОС, за исключением *Получения фокуса вкладкой браузера*.

Примечание:

Если выбрано действие **Не собирать статистику активности**, то события, сформированные в Device Monitor, не отправляются в Платформу.

Если вы хотите, чтобы какие-либо события (например, события создания снимков экрана по Правилу контроля экрана) отправлялись в Платформу, даже если выбрано действие **Не собирать статистику активности**, задайте значение `False` полю `SEND_EVENT_TO_PLATFORM_WITH_CHECK` таблицы Settings Базы Данных. По умолчанию данное поле имеет значение `True`.

2.10.3 Создание и изменение списков приложений

Для более точной работы Агентов на контролируемых рабочих станциях вы можете использовать списки приложений.

Создание списка приложения

Чтобы создать список приложений:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. В разделе **Справочники** откройте вкладку **Приложения**.
3. Слева в секции **Списки приложений** нажмите .
4. В окне **Создание списка приложений**:
   a. В поле **Название** укажите название списка.
   b. В поле **Операционная система** выберите одно из семейств ОС:
      - **Windows** – список будет отмечен значком 
      - **Linux** – список будет отмечен значком 
5. Нажмите **Создать**.

Добавление приложений в список

Чтобы наполнить список, вы можете:

- Добавить приложение вручную;
- Добавить приложение из подраздела **Протокол приложений** (только в списки **для ОС MS Windows**);
- Переместить или скопировать приложение из другого списка.

Добавление приложения в список вручную

Чтобы добавить приложение в список:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. В разделе **Справочники** откройте вкладку **Приложения**.
3. Слева в секции **Списки приложений** кликните список, в который вы хотите добавить приложение.
4. Нажмите **Создать приложение**:
   - в правом верхнем углу;
   - в окне списка, если список пустой.
5. В окне **Создание приложения** укажите:
   a. **Описание**;
   b. **Имя приложения** – имя исполняемого файла с расширением;
   c. **Расположение исполняемого файла** – абсолютный (полный) путь к папке, содержащей исполняемый файл. При указании пути вы можете использовать переменные окружения;
   d. **Издатель** – только для списков приложений ОС MS Windows;
   e. **Название продукта** – поле доступно, если указан **Издатель**.

   > **Примечание:**
   >
   > Для добавления приложения в список обязательно должны быть заполнены поле **Описание** и одно из полей: **Имя приложения**, **Расположение исполняемого файла** или **Издатель**.
   >
   > Чтобы определить, соответствует ли запускаемое приложение приложению из списка, сравниваются значения атрибутов:
   >
   > - **Имя приложения**;
   > - **Расположение исполняемого файла**;
   > - **Издатель**.
   >
   > Проверка отличается в зависимости от ОС контролируемой рабочей станции:
   >
   > - ОС MS Windows – регистр **не** учитывается;
   > - ОС семейства Linux – регистр учитывается.
   >
   > Обратите на это внимание при указании атрибутов приложений.
   >
   > Если в списке приложений поле атрибута не заполнено, оно проходит проверку.
   >
   > **Пример**: Если добавить в список приложение, в котором будут заполнены только **Описание** и **Издатель**, ему будут соответствовать все приложения этого издателя, независимо от имени и расположения исполняемого файла.

6. После заполнения полей нажмите **Добавить**.

Добавление в список из Протокола приложений

Вы можете добавлять приложения из протокола только в списки **для ОС MS Windows**.

Чтобы добавить приложение из протокола приложений:

1. В консоли управления Device Monitor перейдите в раздел **Справочники** -> **Протокол приложений**.
2. Выберите одно или несколько приложений, которые необходимо добавить в списки приложений.
3. Справа вверху нажмите 

4. В открывшемся окне в поле **Списки** выберите список, в который необходимо добавить приложения.
5. Нажмите **Сохранить**.

Если необходимо добавить приложения в новый список:

1. Выполните шаги 1-3 из инструкции выше.
2. В открывшемся окне нажмите **Новый список**.
3. В открывшемся окне в поле **Название** введите название списка.
4. Нажмите .

> **Примечание:**
>
> Если из протокола приложений добавляется приложение, у которого нет описания, то в поле **Описание** у данного приложения будет отображаться его имя

Копирование и перемещение приложений

Приложения можно копировать и перемещать из одного списка в другой.

> **Примечание:**
>
> Не поддерживается перемещение или копирование приложения в список для ОС другого семейства. То есть вы не можете скопировать или переместить в список для Linux приложение из списка для Windows, и наоборот.

Чтобы скопировать или переместить приложение:

1. Выделите приложение.
2. Нажмите:
   -  – для перемещения приложения;
   -  – для копирования приложения.
3. В окне **Копирование** / **Перемещение приложения** выберите список, в который планируете переместить или скопировать приложение.
4. Нажмите **Скопировать в список** / **Переместить**.

Редактирование и удаление списка приложений

Чтобы отредактировать список или приложение:

1. Выберите необходимый элемент.
2. Нажмите , затем  **Редактировать**.
3. В окне редактирования внесите правки и нажмите **Сохранить**.

Чтобы удалить список или приложение:

1. Выберите необходимый элемент.
2. Нажмите , затем  **Удалить**.

3. В окне подтвердите действие, нажав **Удалить**.

> **Примечание:**
>
> Список приложений нельзя удалить, если он используется в правиле политики.

2.10.4 Создание и редактирование групп сотрудников

Управление учетными записями сотрудников и их мониторинг ведется в разделе **Сотрудники**.

> **Важно!**
>
> Когда регистрируется новый сотрудник, информация о нем автоматически добавляется в схему безопасности (в группу сотрудников «по умолчанию»).

> **Примечание:**
>
> Чтобы получать информацию о сотрудниках из службы каталогов, вы можете выполнить синхронизацию с LDAP-сервером. Подробнее см. "Синхронизации DM".

Чтобы добавить группу сотрудников:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Сотрудники** в разделе **Группы**.
3. В левой части рабочей области нажмите .
4. Укажите следующие параметры:
   - **Наименование** группы;
   - **Политика**. Выберите из раскрывающегося списка политику, которая будет назначена данной группе сотрудников.
5. Нажмите **Добавить**. Будет создана новая группа сотрудников, в которую необходимо добавить сотрудников.

Чтобы отредактировать группу сотрудников:

1. Напротив нужной группы нажмите .
2. Выберите  **Редактировать** и внесите изменения.
3. Нажмите **Сохранить**.

Чтобы найти сотрудника или группу сотрудников:

1. В верхней части рабочей области введите в строку поиска текст запроса, состоящий хотя бы из 3 символов.
   В раскрывшемся списке будут показаны первые 5 сотрудников и первые 5 групп сотрудников, параметры которых включают введенный текст.
2. Выберите результаты поиска для отображения:
   - Чтобы просмотреть все элементы, удовлетворяющие запросу, нажмите **Enter** или **Смотреть все результаты**. Результаты будут отображены в иерархическом списке в области слева, найденные группы при этом будут выделены синим

цветом.
Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.

- Чтобы перейти к одному элементу, нажмите на группу или сотрудника. В рабочей области откроется выбранная группа или группа, включающая выбранного сотрудника.

Важно!

Если не осуществляется поиск объектов с использованием кириллицы, убедитесь, что для базы данных, с которой взаимодействует сервер Device Monitor, установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

Чтобы отменить фильтр, примененный с помощью поиска, нажмите  в строке поиска.

Чтобы удалить группу сотрудников:

Примечание

Группу сотрудников «по умолчанию» удалить нельзя.

1. Напротив нужной группы нажмите .
2. Нажмите  **Удалить**. В группе сотрудников, которую вы удаляете, могут быть сотрудники, не включенные в другие группы. В этом случае сотрудники будут автоматически добавлены в группу сотрудников «по умолчанию».
3. В открывшемся окне подтвердите действие, нажав **Удалить**.

2.10.5 Настройка состава групп сотрудников

При установке Агента InfoWatch Device Monitor на рабочую станцию, в Системе автоматически создаются записи о пользователях этой рабочей станции. Эти записи добавляются в "Группу сотрудников по умолчанию". На всех сотрудников, входящих в эту группу, будет распространяться назначенная ей политика. В дальнейшем определение политик для сотрудника происходит путем его включения в различные группы сотрудников.

Чтобы настроить состав группы сотрудников:

1. Перейдите в Центр администрирования, нажав  на панели навигации.
2. Откройте вкладку **Сотрудники** в разделе **Группы**.
3. В левой части рабочей области выберите группу. В центральной части рабочей области будет выведен список всех сотрудников, уже входящих в группу.

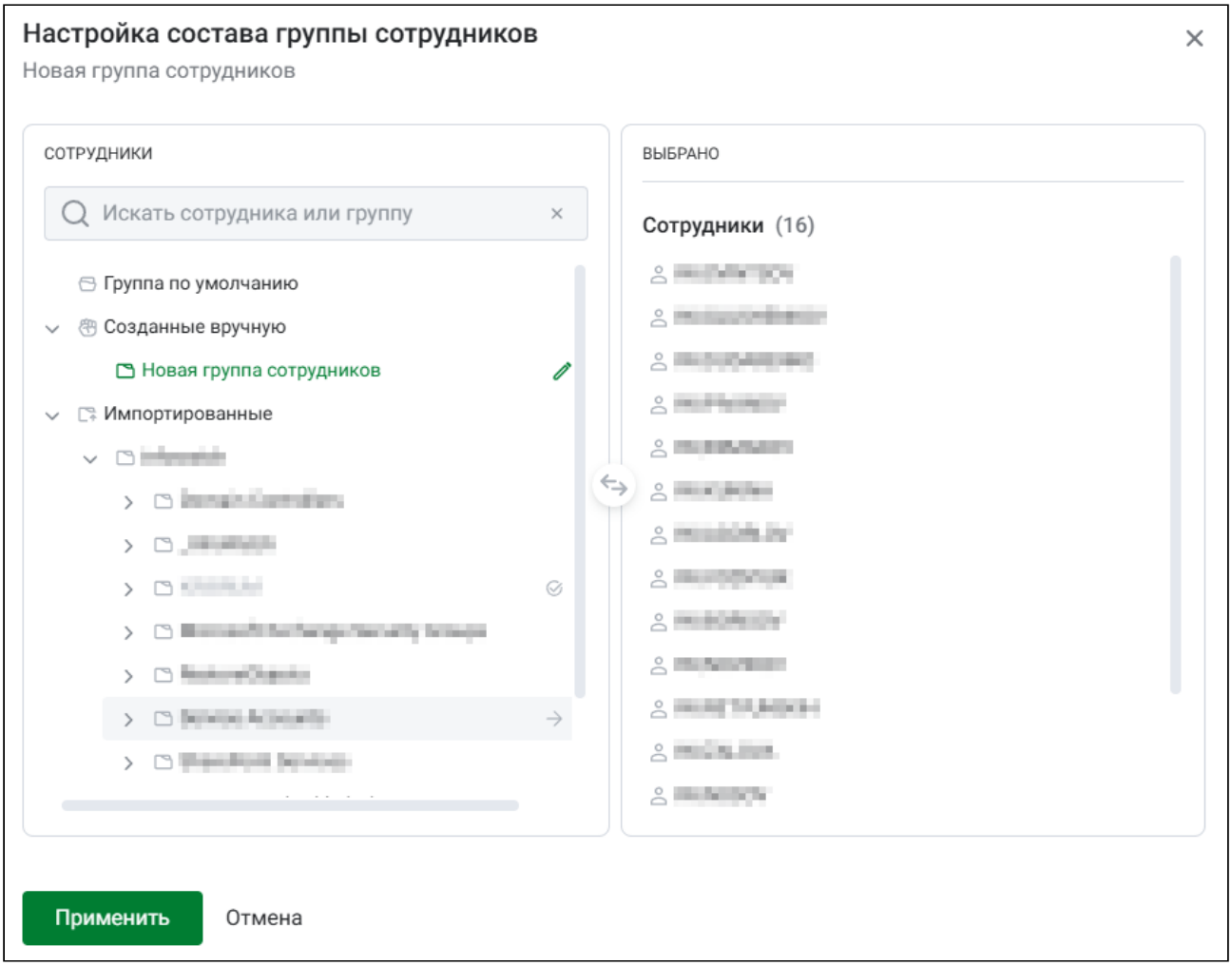
Примечание:

Чтобы найти группу в списке, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп сотрудников".

4. Напротив группы нажмите , затем выберите 

, или выберите группу и в правом верхнем углу рабочей области нажмите 

.
Откроется диалоговое окно. В его левой части отобразится список ранее зарегистрированных в Системе сотрудников.
Чтобы развернуть или свернуть какую-либо группу сотрудников в списке, используйте .
Чтобы найти сотрудника или группу, введите в строку поиска текст запроса, состоящий хотя бы из 3 символов. Результаты будут отображены в иерархическом списке в области слева и выделены синим цветом. Если одним из результатов поиска является группа, то будут показаны все входящие в нее элементы, в том числе не подходящие под условие поиска.
5. Для добавления в группу, в области слева наведите курсор на сотрудника или группу и нажмите  **Добавить сотрудников в "<Название группы сотрудников>"**.
Напротив группы или сотрудника, которые были добавлены, появится значок .
6. Для удаления из группы наведите курсор на удаляемого сотрудника или группу и нажмите  **Удалить из группы "<Название группы сотрудников>"**. Это можно сделать, как в области справа, так и в области слева.
7. Нажмите **Применить**.



Примечание:

Если вы добавляете группу сотрудников, которая содержит подгруппы, то сотрудники из подгрупп не будут автоматически добавлены в выбранную группу. Вы можете добавить их отдельно.

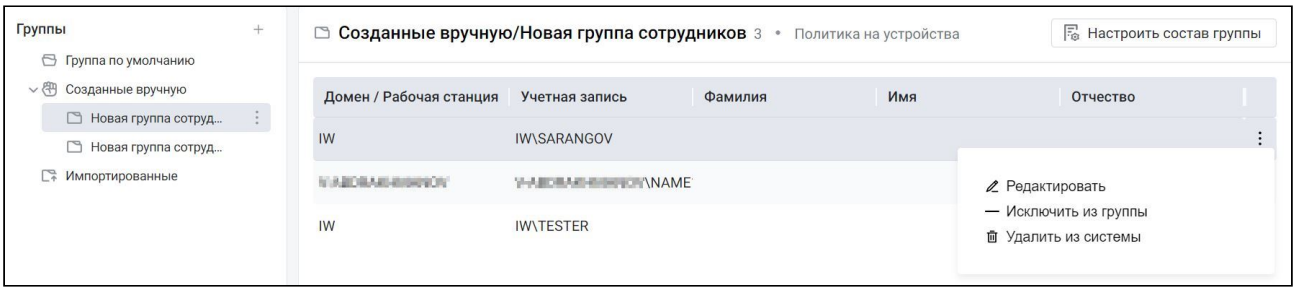
Если сотрудник включен в определенную группу сотрудников, ему будут назначены политики выбранной группы. Чтобы отменить действие какой-либо политики безопасности на сотрудника, исключите его из группы, которой назначена эта политика.

Важно!

Если сотрудник никогда не выполнял вход на рабочую станцию с Агентом (например, подключался по SSH), то назначенная ему политика не сработает. В этом случае перехват производится в соответствии с правилами в политике по умолчанию. Если правил в политике по умолчанию нет, то перехват не будет осуществлен.

Внутри группы сотрудников вы можете работать с их списком: редактировать, исключать из группы, удалять сотрудников из системы.

Чтобы найти сотрудника в списке групп, вы можете воспользоваться поиском. Подробнее см. "Создание и редактирование групп сотрудников".



Примечание:

Для импортированных групп сотрудников внутри группы доступно только редактирование.

Чтобы отредактировать запись сотрудника:

1. В строке с именем сотрудника нажмите ⋮.
2. Выберите ✎ **Редактировать**.
3. Если запись сотрудника создана при синхронизации со службой каталогов, нажмите **Получить имя**, чтобы получить актуальные данные этого сотрудника.
4. Также вы можете вручную изменить **Фамилию**, **Имя** и **Отчество** сотрудника.
5. После внесения необходимых изменений нажмите **Сохранить**.

Чтобы исключить сотрудника из группы:

1. В строке с именем сотрудника нажмите ⋮.
2. Выберите — **Исключить из группы**.
3. В открывшемся диалоговом окне подтвердите действие, нажав **Исключить**. Если сотрудник входил только в одну группу, то при исключении он будет автоматически добавлен в группу сотрудников "по умолчанию".

При необходимости вы можете удалить сотрудника из списка зарегистрированных.

Чтобы удалить сотрудника из схемы безопасности:

1. В строке с именем сотрудника нажмите ⋮.
2. Выберите 🗑 **Удалить из системы**.
3. В открывшемся диалоговом окне нажмите **Удалить**.

Важно!

Удаление сотрудника из схемы безопасности повлечет за собой его удаление из всех групп и политик.

2.11 ПОЛЬЗОВАТЕЛЬСКОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями настоящего Лицензионного соглашения с конечным пользователем (далее – «Соглашение») перед началом работы с программным обеспечением. Установка и/или использование программного обеспечения означает ваше полное и безоговорочное согласие со всеми условиями настоящего Соглашения.

Если вы не согласны с условиями настоящего Соглашения, или если вы заключаете настоящее Соглашение от имени юридического лица, но у вас нет таких полномочий, вы должны прервать установку и/или прекратить использование программного обеспечения и удалить его копии.

1. Предоставление лицензии

1.1. Настоящее Лицензионное соглашение с конечным пользователем является договором присоединения, заключаемым между вами и ООО «Лаборатория ИнфоВотч», ИНН 7734583888 (далее – «Правообладатель»).

1.2. По настоящему Соглашению вам на условиях личной, не подлежащей передаче неисключительной лицензии предоставляются права на использование программного обеспечения Правообладателя (далее — «ПО»), а именно права загрузки, установки, резервного копирования и использования программного обеспечения по функциональному назначению в соответствии с условиями, указанными в Документации к ПО (Руководстве Пользователя, Руководстве Администратора, Руководстве по установке), настоящем Соглашении и Договоре, заключенном между вами и вашим лицензиаром. Документация к ПО признается частью настоящего Соглашения.

1.3. ПО предназначено только для использования в вашей текущей операционной деятельности. В случае если вы получили, загрузили и/или установили ПО, предназначенное для ознакомительных целей, вы имеете право использовать ПО только в целях ознакомления и только в течение ознакомительного периода. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

1.4. Если вы используете ПО разных версий или версии ПО для разных языков, если вы получили ПО на нескольких носителях, если вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее число используемых вами лицензий не должно превышать их количества, определенного Договором между вами и вашим лицензиаром.

1.5. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

1.6. Вы самостоятельно несете ответственность и обеспечиваете соблюдение применимого экспортного и импортного законодательства, а также применимых торговых санкций и эмбарго в отношении передачи прав и использования ПО.

2. Условия использования

2.1. Программное обеспечение предназначено исключительно для использования в целях анализа и контроля информационных потоков в корпоративной среде, в том числе, для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

2.2. Вы обязаны использовать ПО исключительно в соответствии с применимыми к вам требованиями законодательства Российской Федерации и иных стран, которые, не ограничиваясь, могут включать:

- законодательство о персональных данных;
- законодательство о коммерческой тайне;
- законодательство о противодействии неправомерному использованию инсайдерской информации;
- законодательство о противодействии коррупции;

- законодательство о критической информационной инфраструктуре;
- законодательство о государственных информационных системах;
- законодательство о защите данных в Национальной платежной системе;
- нормы Трудового кодекса РФ;
- а также иные применимые источники права.

2.3. Вы не вправе использовать ПО для любых целей или любым способом, нарушающим применимое законодательство, настоящее Соглашение и/или права третьих лиц. Правообладатель не несет ответственность за нарушение вами условий настоящего пункта.

2.4. Если вы не являетесь резидентом РФ, вы обязаны использовать ПО в соответствии с применимым правом, включая законы и нормативные акты, регламентирующие защиту персональных данных и коммерческой тайны.

2.5. Во избежание нарушения вами статей 138, 138.1 УК РФ, статьи 23 Конституции РФ и иных правовых норм перед началом использования программного обеспечения вам рекомендовано письменно проинформировать сотрудников о том, что:

- на рабочей станции используется данное ПО, о функциональности данного ПО и о данных, которые могут быть получены в результате применения данного ПО;
- рабочая станция и используемые каналы связи (электронная почта, локальная корпоративная сеть, телефония и IP-телефония и прочее) являются вашей собственностью и передаются им во временное пользование для выполнения служебных обязанностей;
- вся информация, созданная на рабочей станции, является вашей собственностью и подлежит контролю и логированию на законных основаниях.

2.6. Обращаем ваше внимание, что вам необходимо получить согласие лиц, данные которых будут обрабатываться при использовании ПО, на соответствующий сбор, хранение, использование, обработку, распространение и иную обработку указанных данных.

2.7. Напоминаем, что установка программы на компьютере другого лица без его ведома, получение личной информации третьих лиц без их ведома, нарушение неприкосновенности частной жизни, нарушение тайны переписки, телефонных переговоров, телеграфных и иных видов сообщений является уголовно наказуемым деянием и преследуется в соответствии с действующим законодательством Российской Федерации.

2.8. Правообладатель не имеет доступа к данным, созданным и/или полученным в рамках использования вами ПО. Вы имеете исключительный доступ к указанным данным. С учетом этого Правообладатель не осуществляет сбор, хранение, использование и распространение указанных данных.

2.9. Вы самостоятельно несете риск того, что данные, созданные и/или полученные в рамках использования вами ПО, могут содержать данные неэтического и/или противоправного характера, компьютерные вирусы или программы (или ссылки на них), способные прервать или нарушить нормальную функциональность компьютерного оборудования, программного обеспечения или средств телекоммуникации любых лиц.

2.10. Вам не разрешается:

- целиком или частично редактировать, изменять, адаптировать, переводить, декомпилировать, дизассемблировать, осуществлять инженерный анализ, создавать или воссоздавать исходный код, модернизировать, исправлять явные ошибки, модифицировать ПО и/или его компоненты, осуществлять попытки предпринять аналогичные действия в отношении ПО и/или его компонентов, а также создавать производные работы, основанные на ПО и/или Документации;
- использовать ПО сверх лицензируемого количества учетных записей, предусмотренных договором с вашим непосредственным лицензиаром;

- осуществлять интеграцию ПО в сторонние сайты и программные продукты, за исключением случаев, когда такая интеграция прямо разрешена Правообладателем и правообладателем сторонних сайтов и программных продуктов. Допускается интеграция ПО в сторонние программные продукты посредством встроенного модуля API в рамках функциональных возможностей указанного модуля;
- удалять или изменять уведомления об авторских правах, правах собственности на ПО и/или его элементы;
- использовать ПО с целью извлечения прибыли, сдавать ПО в аренду, прокат или во временное пользование, предоставлять подписку на ПО, предоставлять услуги аутсорсинга с использованием ПО, сублицензировать, распространять или иным образом предоставлять любому физическому или юридическому лицу любые права в отношении ПО и/или Документации, разглашать результаты стендовых испытаний ПО, за исключением случаев, прямо разрешенных настоящим Соглашением либо письменным согласием Правообладателя;
- передавать и предоставлять ссылку на дистрибутив и/или доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между вами и вашим лицензиаром;
- использовать ПО с целью создания данных или кода, предназначенных для использования другими программными продуктами;
- самостоятельно устанавливать дополнительные приложения к ПО, заменять компоненты ПО;
- осуществлять незаконный сбор, систематизацию, хранение и распространение конфиденциальной и/или персональной информации;
- использовать ПО для несанкционированного удаленного доступа к компьютерам третьих лиц, а также изменения конфигурации компьютера так, чтобы такие возможности могли появиться у стороннего ПО;
- собирать, хранить, использовать, обрабатывать и распространять с помощью ПО любые информационные данные, которые нарушают применимое законодательство, права и законные интересы третьих лиц.

2.11. Лицензионный ключ является конфиденциальной информацией, его несанкционированная передача третьим лицам запрещена. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у вас лицензионного ключа.

3. Ограничение гарантий и ответственности Правообладателя

3.1. Программное обеспечение предоставляется «КАК ЕСТЬ» («AS IS») в соответствии с общепринятым в международной практике обычаем делового оборота. За проблемы, возникающие в процессе эксплуатации ПО, в том числе: проблемы совместимости с другими программными продуктами (пакетами, драйверами и др.), проблемы, возникающие из-за неоднозначного толкования Документации в отношении ПО, несоответствия результатов использования ПО вашим ожиданиям и т.п.) и иные, Правообладатель ответственности не несет.

3.2. Вы подтверждаете, что вам известны функциональные свойства ПО, в отношении которых предоставляется право использования, и самостоятельно несете риск соответствия ПО своим индивидуальным пожеланиям и потребностям, а также за результаты, полученные с его помощью.

3.3. Правообладатель не предоставляет никаких гарантий, выраженных или подразумеваемых, и настоящим отказывается от всех гарантий.

Правообладатель не гарантирует, что ПО не содержит ошибок, будет работать непрерывно, быстро, без неточностей, и не несет никакой ответственности за прямые или косвенные последствия использования ПО, в том числе возникшие из-за возможных ошибок в ПО или опечаток в ПО и/или прилагаемой или переданной позднее Документации.

Правообладатель не дает никаких гарантий и не несет никакой ответственности перед вами в случае любых изменений в программном обеспечении третьих лиц, произошедшее после установки/ внедрения ПО и повлекшее потерю функциональности ПО (включая, но не ограничиваясь, изменением протокола передачи данных, формата хранения данных, логике работы стороннего программного обеспечения, обновлением программного обеспечения, которое перестает поддерживать работу с ПО). Правообладатель не дает никаких гарантий, условий, представлений или положений (выражаемых в явной или в подразумеваемой форме) на все, включая без ограничений нарушения прав третьих лиц, коммерческое качество, интеграцию или пригодность для определенных целей.

3.4. Данные, которые становятся доступными при использовании ПО, включая файлы, ссылки, изображения и текст, являются исключительной ответственностью физического или юридического лица, от которого они были получены, и являются собственностью соответствующего лица. Настоящее Соглашение не дает никаких прав на такие данные. Вы принимаете на себя ответственность за возможные последствия, риски безопасности и любые убытки, вызванные такими данными, просмотренными или полученными Вами с помощью ПО.

3.5. Правообладатель не несет ответственности за какие-либо убытки, ущерб, независимо от причин его возникновения (включая, но не ограничиваясь прямым или косвенным ущербом, убытками связанными с недополученной прибылью, прерыванием коммерческой или производственной деятельности, утратой деловой информации, небрежностью, или какими-либо иными убытками), возникшие вследствие использования или невозможности использования ПО, даже если Правообладатель был уведомлен о возможных убытках. При любых обстоятельствах ответственность Правообладателя ограничена возмещением документально подтвержденного реального ущерба, ограниченного 3 000 (тремя тысячами) рублей, и возлагается на него при наличии в его действиях вины.

4. Права на объекты интеллектуальной собственности

4.1. Вы соглашаетесь с тем, что исключительные права на любые объекты интеллектуальной собственности, воплощенные в ПО и /или любой предоставленной вам документации, принадлежат Правообладателю. По настоящему Соглашению ПО не передается в собственность, не продается, а предоставляются права его использования на условиях ограниченной неисключительной лицензии. Ничто в данном Соглашении не предоставляет вам никаких прав на указанные объекты интеллектуальной собственности иные, чем предоставленные вам по Договору, заключенному между вами и вашим лицензиаром.

4.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются собственностью Правообладателя.

5. Права на информацию, доступ к которой получен вами в рамках осуществления настоящего Соглашения

5.1. Вы соглашаетесь с тем, что вам не принадлежат никакие права на любую информацию, не являющуюся объектом интеллектуальной собственности в соответствии с разделом 4, доступ к которой получен вами в рамках осуществления настоящего Соглашения.

5.2. К указанной информации, включая, но не ограничиваясь, относятся системы, методы работы, иная информация.

5.3. Указанная выше информация будет использоваться Вами только в целях осуществления прав на ПО, предоставленных вам по настоящему Соглашению и Договору с лицензиаром, без права использования указанной информации в собственных интересах и за пределами Соглашения и Договора, заключенного между вами и вашим лицензиаром.

6. Открытое программное обеспечение

Вы проинформированы **о том, что ПО содержит открытое программное обеспечение, распространяемое под определенными лицензиями, с которыми вы можете ознакомиться в файле licenses.inf (license.info), распространяемом с ПО в составе дистрибутива.**

Вы соглашаетесь с тем, что входящие в состав ПО программные компоненты внешних поставщиков предоставляются без гарантий доступа к обновленным версиям компонент и к иным программам, оборудованию, сертификатам на обучение или услугам внешних поставщиков.

7. Заключительные положения

7.1. Настоящее Соглашение вступает в силу с начала установки ПО и действует на протяжении всего периода использования.

7.2. В случае нарушения вами какого-либо из условий Соглашения и/или Договора, заключенного между вами и вашим лицензиаром, или в случае, если исполнение Соглашения или Договора, заключенного между вами и вашим лицензиаром будет нарушать или нарушает применимое право, Правообладатель вправе отказаться от исполнения Соглашения и расторгнуть его (включая, но не ограничиваясь, путем блокировки лицензионного ключа, прекращения предоставления прав) в любое время без уведомления вас. В указанном в настоящем пункте случае стоимость ПО/размер вознаграждения за права на ПО, а также возможные убытки по настоящему Соглашению и/или Договору, заключенному между вами и вашим лицензиаром, вам не возмещаются.

7.3. При расторжении или прекращении Соглашения Пользователь обязан уничтожить все копии установленного ПО.

7.4. Вы настоящим уведомляетесь о том, что при включении в ПО функции сбора статистики использования, ПО может осуществлять сбор и запись информации в обезличенном виде:

а) об аппаратном обеспечении, об операционной системе устройства, на котором установлено и эксплуатируется ПО, а также иная техническая информация, содержащая сведения об использовании аппаратных средств, нагрузке на аппаратные средства и быстродействии ПО;

б) данные о действиях конечного пользователя в пользовательском интерфейсе ПО.

Правообладатель вправе использовать указанные данные для принятия решений о развитии функциональности и улучшении эксплуатационных характеристик ПО.

Правообладатель обязуется обеспечить конфиденциальность полученных данных, не разглашать и не передавать их третьим лицам.

7.5. Настоящее Соглашение, а также любые споры, возникающие из или в связи с настоящим Соглашением, регулируются и истолковываются в соответствии с законодательством Российской Федерации.

7.6. Все споры и разногласия, возникающие в процессе исполнения Соглашения, будут по возможности разрешаться путем переговоров. В случае недостижения согласия, споры будут рассматриваться в судебном порядке в Арбитражном суде г. Москвы.

7.7. Настоящее Соглашение может быть изменено Правообладателем в любой момент без какого-либо уведомления. Новая редакция Соглашения вступает в силу с момента ее размещения по указанному в настоящем пункте адресу. С условиями действующей редакции Соглашения вы всегда можете ознакомиться по адресу https://kb.infowatch.com/display/EULA/. При этом продолжение использования ПО после внесения изменений и/или дополнений в настоящее Соглашение означает согласие с такими изменениями и/или дополнениями. В случае несогласия с условиями такого измененного Соглашения, вы обязаны немедленно отказаться от дальнейшего использования ПО.

8. Контактная информация Правообладателя

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru