

INFOWATCH

InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию

15/07/2024

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 5

2 Комплект документов 6

3 Аппаратные и программные требования 7

4 Установка InfoWatch Device Monitor 14

4.1 Схема развертывания InfoWatch Device Monitor 14

4.2 Установка серверной части InfoWatch Device Monitor 17

4.2.1 Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server 18

4.2.2 Рекомендации по развертыванию базы данных под управлением СУБД Oracle 18

Настройка параметров соединения InfoWatch Device Monitor с сервером СУБД Oracle 19

4.2.3 Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL 20

4.2.4 Рекомендации по установке Сервера InfoWatch Device Monitor 20

4.2.5 Порядок установки серверной части InfoWatch Device Monitor 21

4.3 Установка Агента InfoWatch Device Monitor 32

4.3.1 Локальная установка Агента 35

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью msi-пакета с последующим вводом параметров вручную: 36

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью cmd-пакета, уже содержащего параметры установки: 36

4.3.2 Установка Агента с помощью средств распространения программного обеспечения 38

5 Настройка Сервера InfoWatch Device Monitor 44

5.1 Раздел <applicationSettings> 45

5.2 Раздел <system.diagnostics> 52

5.3 Удаление временных файлов Device Monitor 54

5.4 Настройка защиты от подбора паролей Device Monitor 55

5.5 Настройка проверки сертификатов удаленных серверов 56

5.5.1 Чтобы настроить проверку сертификатов удаленных серверов при установлении SSL-сессии: 56

5.5.2 Чтобы установить сертификат службы XAPI Traffic Monitor: 57

5.5.3 Чтобы установить сертификат веб-сервера Traffic Monitor: 58

5.5.4 Чтобы установить сертификат службы EPEVENTS Платформы: 58

5.5.5 Просмотр логов 59

6 Обновление InfoWatch Device Monitor 60

6.1 Обновление серверной части InfoWatch Device Monitor 60

6.2 Обновление Агента InfoWatch Device Monitor 62

7 Удаление InfoWatch Device Monitor 65

7.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения 67

8 Приложение А. Рекомендации по составлению имен и паролей 68

9 Настройка сетевых правил доступа 70

В настоящем руководстве вы сможете найти сведения по установке, обновлению, удалению и настройке компонентов модуля InfoWatch Device Monitor.
InfoWatch Device Monitor (далее Модуль/Система или Device Monitor) - программный продукт, позволяющий осуществлять перехват данных в информационных потоках компании.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных объектов и т. п.).

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Windows, РЕД ОС и СУБД PostgreSQL.

2 Комплект документов

В комплект документации по InfoWatch Device Monitor входят:

- «InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию». Содержит описание установки, обновления, удаления и настройки модуля.
- «InfoWatch Device Monitor Руководство пользователя». Содержит описание порядка работы с модулем.

Сопутствующая документация по продукту InfoWatch Traffic Monitor включает в себя:

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

Сопутствующая документация по продукту InfoWatch Activity Monitor включает в себя:

- «InfoWatch Activity Monitor. Руководство по установке». Содержит описание процесса установки, обновления и удаления Activity Monitor.
- «InfoWatch Activity Monitor. Руководство администратора». Содержит информацию по настройке и подготовке к работе Activity Monitor.
- «InfoWatch Activity Monitor. Руководство пользователя». Содержит описание работы в Activity Monitor.

3 Аппаратные и 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				
Не менее 3 GB свободного пространства для установки. Также понадобится свободное пространство для анализа данных, объем зависит от нагрузки на сервер.	От 2-х ядер	От 2 GB	ОС (поддерживаются платформы x86 и x64): • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2. • Microsoft Windows Server 2016; • Microsoft Windows Server 2019. Платформа: • Microsoft .Net Framework 4.5.1. СУБД: • Oracle Database 19; • Microsoft SQL Server 2005, 2008, 2012, 2014, 2016, 2017, 2019 (Standard, Enterprise);	• На сервере TM 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

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• PostgreSQL 11 и более поздние версии.	
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-х 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 Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16); • Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 6 (20210611SE16).	• Наличие локального DNS для перевода доменных имен в адреса • Должен поддерживаться протокол TLS 1.2 Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 6 поддерживается только для первичной установки Агента Device Monitor. **Поддерживаемые версии ядра Astra Linux Special Edition "Смоленск" версии 1.6 (все пакеты безопасности)** • 4.15.3-1-generic • 4.15.3-1-hardened • 4.15.3-2-generic • 4.15.3-2-hardened • 4.15.3-154-generic • 4.15.3-154-hardened • 4.15.3-177-generic • 4.15.3-177-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.10.142-1-generic • 5.15.0-33-generic

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 6 (20200722SE16); • Astra Linux Special Edition "Смоленск" (x64) версии 1.6 с установленным обновлением безопасности Update 12; • Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"; • Astra Linux Common Edition "Орел" (x64) версии 2.12; • РЕД ОС 7.3; • Альт Рабочая станция 10.	**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 • 5.10.0-1045-generic • 5.10.0-1045-hardened • 5.10.142-1-generic • 5.15.0-33-generic • 5.15.0-70-generic • 6.1.50-1-generic (начиная с версии 7.11.2) **Поддерживаемые версии ядра Astra Linux Common Edition "Орел" версии 2.12** • 4.9.135-1-generic • 4.15.3-1-generic • 4.15.3-1-hardened • 4.15.3-2-generic • 4.15.3-2-hardened • 4.15.3-3-generic • 4.15.3-3-hardened • 4.15.3-141-generic • 4.15.3-141-hardened • 4.19.0-1-generic • 5.2.13-050213-generic • 5.4.0-54-generic • 5.4.0-54-hardened • 5.4.0-71-generic • 5.4.0-71-hardened • 5.4.0-110-generic

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 5.4.0-110-hardened • 5.10.0-1038.40-generic • 5.10.0-1038.40-hardened • 5.10.0-1057-generic • 5.10.142-1-generic • 5.10.142-1-hardened • 5.15.0-33-generic • 5.15.0-33-hardened • 5.15.0-70-generic • 5.15.0-70-hardened **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 • 5.15.125 • 5.15.131 • 6.1.20-2 • 6.1.44 • 6.1.52 (начиная с версии 7.11.4)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				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 • 5.10.179-std-def-alt1 • 5.10.182-std-def-alt1 • 5.10.185-std-def-alt1 • 5.10.186-std-def-alt1 • 5.10.198-std-def-alt1 (начиная с версии 7.11.2) • 5.10.199-std-def-alt2 (начиная с версии 7.11.2) • 5.15.94-un-def-alt1 • 5.15.109-un-def-alt1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 6.1.29-un-def-alt1 (начиная с версии 7.11.2) • 6.1.32-un-def-alt1 • 6.1.42-un-def-alt1
Консоль управления Device Monitor				
Не менее 35 MB	Как у используемой ОС	Как у используемой ОС	ОС: • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 и 8.1; • Microsoft Windows 10.	

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.

4 Установка InfoWatch Device Monitor

Процесс установки выполняется в следующей последовательности:

1. Установка серверной части InfoWatch Device Monitor.
   В состав серверной части входят следующие компоненты:
   - база данных,
   - сервер InfoWatch Device Monitor,
   - консоль управления InfoWatch Device Monitor,
   - сервис распространения дистрибутивов.
2. Установка агента InfoWatch Device Monitor.
   Агент устанавливается на каждый компьютер, который необходимо контролировать с помощью InfoWatch Device Monitor.

До начала установки убедитесь, что среда, в которой будет развернут InfoWatch Device Monitor, удовлетворяет аппаратным и программным требованиям (см. "Аппаратные и программные требования").

Важно!

Для корректной работы и доступа ко всей функциональности версии Traffic Monitor и Device Monitor должны быть совместимы. Подробнее о совместимости Device Monitor см. в статье Базы знаний InfoWatch "Особенности совместимости разных версий TM, DM и Агентов".

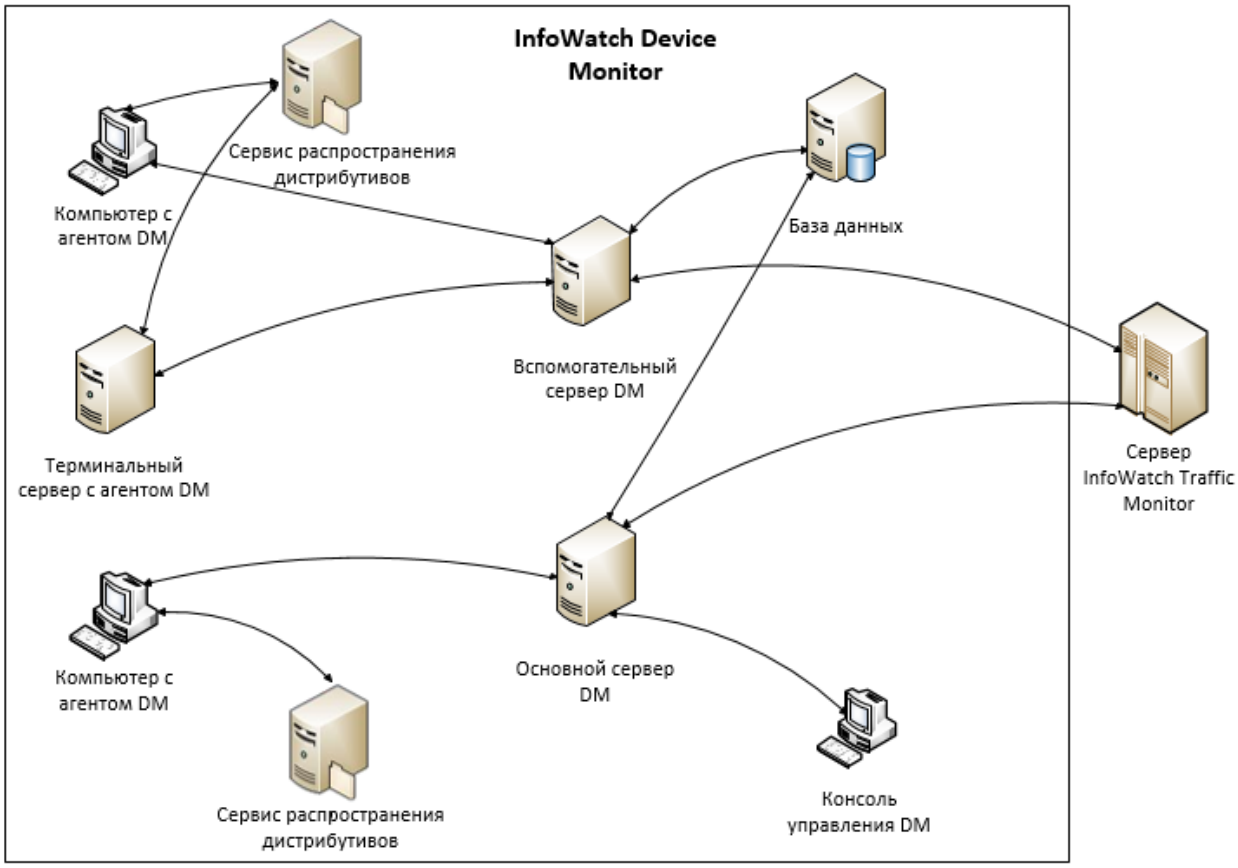
4.1 Схема развертывания InfoWatch Device Monitor

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
InfoWatch Device Monitor Database (база данных)	Хранение информации, необходимой для работы Device Monitor
Консоль управления InfoWatch Device Monitor (Консоль управления)	Управление модулем Device Monitor
Сервис распространения дистрибутивов (Сервис распространения)	Получение и хранение новой версии дистрибутива агента Device Monitor

Компонент	Назначение
Менеджер управления серверами	Изменение ролей и других атрибутов серверов 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. Первым устанавливают **основной сервер** (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Работа с Менеджером управления серверами").
2. При установке основного сервера определяют используемый сервер **базы данных**: СУБД может располагаться как отдельно, так и на том же компьютере, что и основной сервер.
3. При установке основного сервера 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. **Консоль управления** может устанавливаться на любую рабочую станцию. Консоль управления подключается к основному серверу. Из Консоли управления выполняется настройка схемы безопасности в соответствии с требованиями корпоративной политики безопасности.
6. **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**.
7. 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.
8. 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.
9. 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.

4.2 Установка серверной части InfoWatch Device Monitor

Серверная часть InfoWatch Device Monitor устанавливается при помощи универсальной программы установки.
Универсальная программа установки находится на диске с дистрибутивом Device Monitor (каталог `Setup.Unified`). При помощи данной программы можно установить все компоненты, за исключением Агента: базу данных, Сервер Device Monitor и Консоль управления.
Для управления базой данных может использоваться СУБД Microsoft SQL Server, Oracle или PostgreSQL.
Консоль управления может подключаться к основному Серверу.
Подробнее об установке читайте в следующих разделах:

- Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server;
- Рекомендации по развертыванию базы данных под управлением СУБД Oracle;
- Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL;
- Рекомендации по установке Сервера InfoWatch Device Monitor;
- Порядок установки серверной части InfoWatch Device Monitor.

4.2.1 Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server

На компьютере, с которого будет запущен процесс создания базы данных, предварительно должен быть установлен пакет Microsoft .NET Framework 2.0 Service Pack 1, Microsoft .NET Framework 4.0 или выше. Учетная запись, от имени которой будет создаваться база данных, должна быть подготовлена заранее. Выбор типа учетной записи зависит от того, какой способ аутентификации вы планируете использовать для подключения к серверу базы данных. В СУБД Microsoft SQL Server поддерживаются два способа аутентификации:

- **Аутентификация Windows**. Аутентификация выполняется с использованием учетных записей, принадлежащих к домену Windows. Данные аутентификации обрабатываются системой безопасности Microsoft Windows.
- **Встроенная в SQL Server**. Используются учетные записи СУБД Microsoft SQL Server. Аутентификация выполняется средствами СУБД.

Важно!

Для обеспечения приемлемого уровня безопасности настоятельно рекомендуется использовать способ **Аутентификация Windows**.

Если вы планируете использовать способ Аутентификация Windows:

1. Убедитесь, что в домене Windows существует учетная запись, от имени которой будет создаваться база данных. Эта учетная запись должна иметь права локального администратора на том компьютере, с которого будет запущен процесс создания базы данных. При необходимости создайте новую учетную запись.
2. Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server, выбрав при этом **Аутентификация Windows**.
3. Назначьте учетной записи роль **dbcreator**.

Если вы планируете использовать способ Встроенная в SQL Server:

1. Создайте новую учетную запись Microsoft SQL Server. При настройке параметров записи: выберите **Встроенная в SQL Server**, задайте имя и пароль.
2. Назначьте учетной записи роль **dbcreator**.

Примечание:

Имя и пароль встроенной учетной записи указывают при настройке параметров базы данных (см. "Порядок установки серверной части InfoWatch Device Monitor", шаг 7).

4.2.2 Рекомендации по развертыванию базы данных под управлением СУБД Oracle

На компьютере, с которого будет запущен процесс создания схемы базы данных, предварительно должны быть установлены:

- пакет Microsoft .NET Framework 4.5
- клиент СУБД Oracle (только после установки пакета Microsoft .NET Framework 4.5)

- провайдер Oracle Database Provider for .NET (ODP.NET)

Важно!

Выбор данного компонента рекомендуется производить путем отметки соответствующего поля при пользовательском типе установки (Custom). Проводить установку необходимо от имени администратора.

Перед тем как начать создание схемы базы данных, убедитесь, что идентификатор соединения с сервером базы данных прописан в файле **tnsnames.ora** (см. "Настройка параметров соединения с сервером СУБД ORACLE").

Настройка параметров соединения InfoWatch Device Monitor с сервером СУБД Oracle

Для корректного соединения с сервером СУБД Oracle на каждом компьютере, на котором установлен клиент СУБД Oracle, необходимо указать параметры подключения. Выберите один из двух вариантов, представленных ниже.

Вариант 1. Настроить файл tnsnames.ora ([ORACLE_HOME]\network\admin)

Укажите параметры подключения к серверу СУБД Oracle. Для этого добавьте в файл tnsnames.ora запись следующего вида:

```
tns_name =
 (DESCRIPTION =
 (ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
 (CONNECT_DATA =
 (SERVER = DEDICATED)
 (SERVICE_NAME = service_name)
 )
 )
```

Здесь нужно подставить действительные значения для следующих параметров:

- `tns_name` – псевдоним сервера СУБД Oracle;
- `host_name` – доменное имя или IP-адрес сервера СУБД Oracle;
- `port_number` – порт сервера, на котором запущен процесс прослушивания клиентских подключений;
- `service_name` – имя сервиса базы данных.

Пример записи в файле tnsnames.ora

```
IWDM =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

Важно!

Файл **tnsnames.ora** чувствителен к форматированию. Поэтому, если вы редактируете его, копируя приведенный пример, обратите внимание: в скопированном фрагменте не должно быть пустых строк.

Вариант 2. Указать в качестве сервера БД строковое представление TNS из файла tnsnames.ora.

Пример строкового представления

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=iwdm.infowatch.ru)(PORT=1521))
(CONNECT_DATA=(SERVER=dedicated)(SERVICE_NAME=iwtm)))
```

4.2.3 Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL

На компьютере, с которого будет запущен процесс создания базы данных, предварительно должны быть установлены:

- ОС Microsoft Windows Server 2008 R2/2012/2012 R2/2016/2019;
- пакет Microsoft .NET Framework 4.5.2.

Скачайте на официальном сайте PostgreSQL 13 и установите с параметрами по умолчанию.

При установке будет создан супер-пользователь postgres, для которого нужно прописать пароль. Информация о нем будет доступна во входящей в комплект установки утилите pgAdmin III в секции "Роли входа".

После установки PostgreSQL откройте конфигурационный файл `postgresql.conf` и присвойте параметру `"max_connections"` значение 250.

Примечание:

Для увеличения быстродействия системы рекомендуется устанавливать ОС, серверную часть InfoWatch Device Monitor и СУБД PostgreSQL на разные физические жесткие диски.

4.2.4 Рекомендации по установке Сервера InfoWatch Device Monitor

Для повышения производительности InfoWatch Device Monitor рекомендуется развертывать Сервер и базу данных на отдельных компьютерах.

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

Важно!

При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одинаковая версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

В процессе настройки параметров Сервера (см. "Порядок установки серверной части InfoWatch Device Monitor") необходимо указать учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor. Возможны следующие варианты:

- **Пользователь**. Запуск службы от имени учетной записи домена Windows,
- **Network Service**. Запуск службы от имени учетной записи, не имеющей административных привилегий на рабочей станции.

Для базы данных под управлением СУБД Microsoft SQL Server. Если для аутентификации пользователя, создающего базу данных, выбран способ Аутентификация Windows (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server"), а база данных и Сервер будут находиться на разных компьютерах, то выберите вариант Пользователь.

Важно!

Не рекомендуется выбирать вариант Local System. В этом случае пользователь может получить неограниченные права, что противоречит принципам создания политики безопасности.

Создайте сервисную учетную запись и предоставьте ей права записи в каталог установки сервера DM: `\Program Files\InfoWatch\Device Monitor\Server`

Учетная запись домена Windows (вариант **Пользователь**) должна быть подготовлена заранее. Для этого выполните следующие действия:

1. Разрешите учетной записи запускать процесс как службу. Для этого:

- В **Панели управления** откройте компонент **Администрирование > Локальная политика безопасности**.
- В открывшемся диалоговом окне выберите узел **Локальные политики > Назначение прав пользователя**.
- Справа в области сведений дважды щелкните право **Вход в качестве службы**.
- На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.

- Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server.
По окончании установки предоставьте учетной записи доступ к созданной базе данных. При выборе разрешения на доступ к базе данных укажите роль **db_owner**.

4.2.5 Порядок установки серверной части InfoWatch Device Monitor

Важно!

Перед началом установки ознакомьтесь с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor".

Важно!

При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одна и та же версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

1. **Запуск мастера установки**
   Откройте папку с дистрибутивом Device Monitor. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите **Далее**.
2. **Принятие лицензионного соглашения**
   Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.
3. **Выбор устанавливаемого компонента**
   На шаге **Выборочная установка** по умолчанию выбраны все компоненты:
   - Сервер
   - Консоль управления
   - Сервис распространения дистрибутивов

   Если необходимо, измените состав устанавливаемых компонентов. По умолчанию все компоненты устанавливаются на одну рабочую станцию. Если вы рассчитываете использовать Консоль управления или Сервис распространения на другой рабочей станции, то вам не нужно устанавливать этот компонент: нажмите **Консоль управления** или **Сервис распространения дистрибутивов** и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**.
   Вы также можете изменить папку, куда будет установлен тот или иной компонент: выберите компонент в списке, нажмите и укажите другое местоположение. При установке Сервиса распространения новый дистрибутив Агентов будет автоматически размещен в директорию с дистрибутивами.
   Нажмите **Далее**.
4. **Определение параметров сервера**
   На шаге **Тип устанавливаемого сервера** выберите:
   - **Основной сервер** – должен быть установлен первым. К нему будут подключаться Агенты и Консоль управления.
   - **Вспомогательный сервер** – дополнительный сервер, обеспечивающий балансировку нагрузки от Агентов.

   > **Важно!**
   >
   > Изменение имени сервера Device Monitor после установки может привести к перебоям в работе Системы.

   > **Примечание:**
   >
   > Установка вспомогательного сервера возможна только после установки основного на отдельный компьютер. Установка вспомогательного сервера описана в пункте 14.

   Для обеспечения быстрой актуализации информации о серверах, рекомендуется отметить **Опубликовать сервер в Active Directory**.

> **Важно!**
>
> Актуализируя политики безопасности, компьютеры периодически взаимодействуют с сервером Device Monitor. Поэтому, чтобы вновь добавленный сервер мог сразу же приступить к обслуживанию компьютеров, а также для своевременного уведомления Агентов о возможных изменениях портов серверов, рекомендуется при установке сервера публиковать его данные в домене.
> Для публикации данных сервера Device Monitor в домене, учетной записи, от имени которой выполняется установка сервера, требуются права на создание и удаление точек подключения.

Если у вас есть СУБД со схемой БД Device Monitor того же номера версии, что устанавливается на сервер, снимите отметку **Установить новую базу данных** . Нажмите **Далее** .

5. **Файл для импорта элементов конфигурации**

   Если установка новой базы данных не производится, этот шаг будет пропущен. Чтобы использовать ранее экспортированный файл конфигурации сервера (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Импорт/экспорт настроек и схемы безопасности"), нажмите **Выбрать** и укажите место расположения файла конфигурации.

   > **Важно!**
   >
   > Файл конфигурации должен быть расположен на локальном диске или внешнем носителе. Расположение в сетевой папке программой установки не поддерживается.

   Нажмите **Далее**. В этом случае все существующие настройки и элементы конфигурации будут заменены на импортированные.

6. **Выбор сервера базы данных**
   Укажите СУБД, под управлением которой будет находиться база данных Device Monitor, выбрав один из следующих вариантов:
   - Microsoft SQL Server
   - Oracle
   - PostgreSQL

   Если на Шаге 4 вы решили использовать уже существующую базу данных (опция **Установить новую базу данных** не была выбрана), то вам будет необходимо дополнительно указать параметры соединения с существующей базой данных Device Monitor.
   Нажмите **Далее**.
7. **Настройка базы данных**
   Этот шаг будет пропущен, если на Шаге 4 вы решили использовать уже существующую базу данных.
   Принцип настройки базы данных зависит от типа используемой СУБД.
   При использовании СУБД Microsoft SQL Server укажите следующие параметры:
   - **Сервер БД**. NetBIOS имя сервера СУБД Microsoft SQL Server, на котором будет создана база данных.

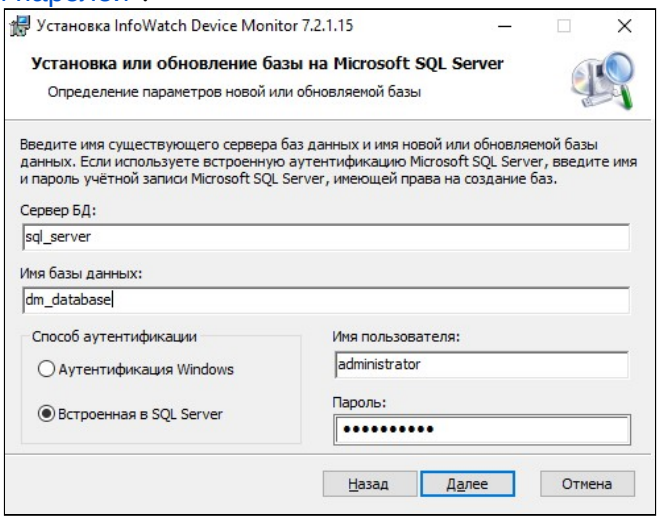
Не задавайте в поле **Сервер БД** IP-адрес, так как в этом случае вы не сможете подключиться к серверу базы данных.
Если на сервере базы данных есть именованные экземпляры, то имя сервера нужно указывать в следующем виде: `<имя_сервера>\<имя_экземпляра>`.

- **Имя базы данных**. Имя создаваемой базы данных.

Может содержать буквы латинского алфавита, цифры и прочие символы, за исключением пробелов и специальных символов: «*», «?», «/», «\», «|», «^», «:», «"». Должно начинаться с латинской буквы.
Длина имени может составлять от 1 до 123 символов.

- **Способ аутентификации**. Способ аутентификации пользователя, от имени которого создается база данных и который будет использоваться для работы с БД. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**. В этом случае процесс создания БД будет выполняться от имени доменного пользователя, выполняющего установку.
Если учетной записи назначена встроенная в SQL Server аутентификация, выберите значение Встроенная в SQL Server. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно. При составлении пароля ознакомьтесь с рекомендациями в статье "Приложение А. Рекомендации по составлению имен и паролей".



Настройка базы данных Microsoft SQL Server

При использовании СУБД Oracle настройте следующие параметры:

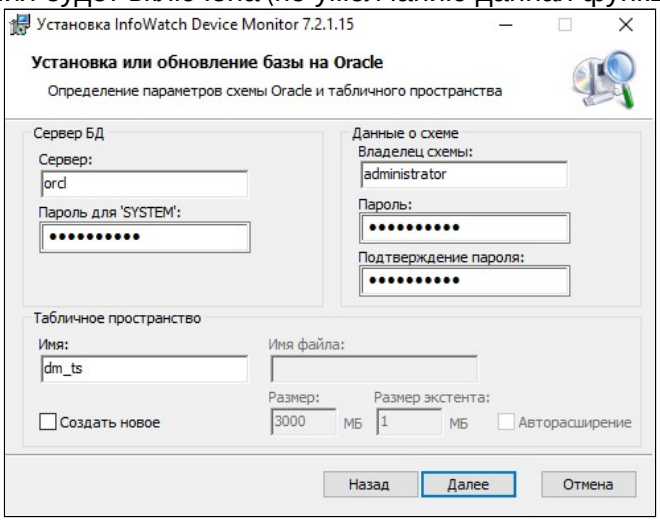
a. В области **Сервер БД** задайте параметры соединения с сервером базы данных:
   - **Сервер**. Имя сервера базы данных. В качестве значения данного параметра укажите псевдоним сервера `tns_name из файла` **tnsnames.ora** или строковое представление TNS.
   - **Пароль для 'SYSTEM'**. Пароль учетной записи пользователя SYSTEM.
b. В области **Данные о схеме** укажите параметры учетной записи владельца создаваемой схемы базы данных:

> **Важно!**

Не рекомендуется указывать параметры существующей схемы базы данных.

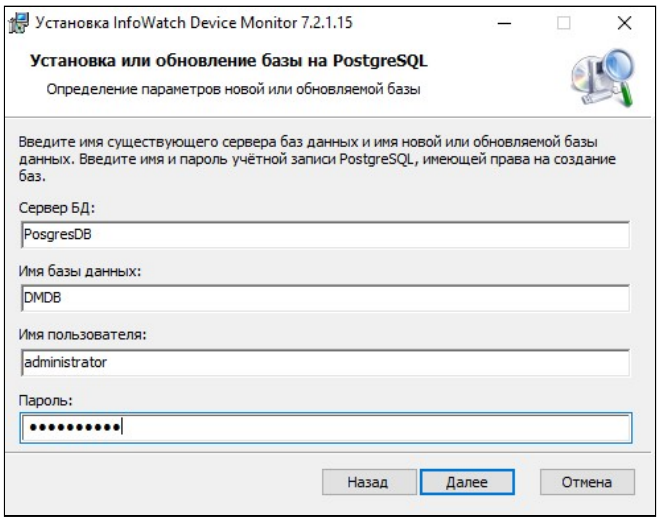
- **Владелец схемы**. Имя учетной записи владельца схемы базы данных.
- **Пароль, Подтверждение пароля**. Пароль учетной записи владельца схемы базы данных.
Назначение пароля выполняется в соответствии с требованиями, указанными в документации к СУБД Oracle.

c. Настройте параметры табличного пространства в области **Табличное пространство**.
Вы можете использовать существующее табличное пространство или создать новое. При использовании существующего табличного пространства, укажите имя табличного пространства в поле **Имя**.
Чтобы создать новое табличное пространство, отметьте поле **Создать новое**. Затем укажите параметры табличного пространства:
- **Имя**. Имя нового табличного пространства.
- **Имя файла**. Имя файла данных, в котором будет храниться новое табличное пространство.
- **Размер**. Максимальный размер (в МБ) файла данных (значение по умолчанию - 3000 МБ).
- **Размер экстента**. Максимальный размер (в МБ) непрерывного фрагмента пространства в файле данных (значение по умолчанию - 1 МБ).
- **Авторасширение**. Возможность автоматического расширения файла данных средствами СУБД Oracle. Если отмечено поле **Авторасширение**, то функция авторасширения будет включена (по умолчанию данная функция отключена).



При использовании СУБД PostgreSQL укажите следующие параметры:
- **Сервер БД**. Имя сервера СУБД PostgreSQL, на котором будет создана база данных. Порт по умолчанию - 5432. Если будет использовать другой порт, необходимо его задать в формате `host:port`.
- **Имя базы данных**. Имя создаваемой базы данных.Может содержать буквы латинского алфавита, цифры и прочие символы, за исключением пробелов и специальных символов: «*», «?», «/», «\», «|», «^», «:», «". Должно начинаться с латинской буквы.Длина имени может составлять от 1 до 123 символов.
- **Имя пользователя** - имя учетной записи, имеющей права на создание БД на PostgreSQL сервере.
- **Пароль** - пароль учетной записи, имеющей права на создание БД на PostgreSQL

сервере.



После того как все необходимые параметры будут заданы, нажмите **Далее**.

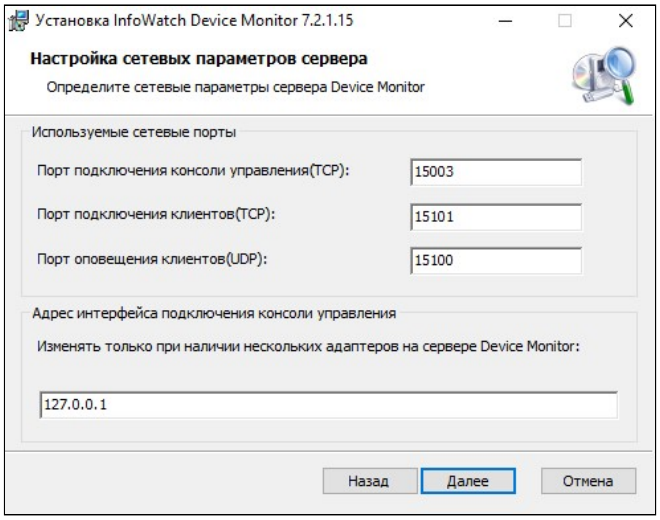
8. **Настройка сетевых параметров сервера**

   Настройте параметры Сервера:

   a. В области **Используемые сетевые порты** задайте номера TCP и UDP портов, используемые для:
      - **подключения Консоли управления**;
      - **подключения Агентов** для передачи схем безопасности на контролируемые компьютеры, отправки информации о событиях и теневых копий на сервер;
      - **оповещения Агентов** об изменениях схем безопасности.

   b. В области **Адрес интерфейса подключения консоли управления** укажите IP-адрес, через который будет осуществляться взаимодействие между Сервером и Консолью управления.

> **Важно!**
>
> Изменять значение данного параметра следует, только если Сервер будет установлен на компьютер с несколькими сетевыми адаптерами, подключенными к разным сетям. При наличии одного сетевого адаптера не допускается изменение данного параметра, иначе подключение Консоли управления к Серверу будет невозможно.
> Если в процессе работы на компьютер с установленным Сервером будут добавлены дополнительные сетевые адаптеры, то изменить настройку данного параметра можно в конфигурационном файле Сервера.



После того как все необходимые параметры будут указаны, нажмите **Далее**.

9. **Настройка защищенного канала**
   Укажите порт, по которому будут передаваться трафик между Агентом и Сервером InfoWatch Device Monitor.
   Если на Шаге 4 вы выбрали **Установить новую базу данных**, то в области **Ключ защищенного канала** выберите:
   - если установка выполняется впервые - оставьте настройку **Создать новый ключ**;
   - если вы использовали сервер версии 6.0 и выше и удалили его, а затем хотите опять установить, то для того, чтобы Агенты Device Monitor смогли подключиться и привязаться к новому серверу, необходимо указать ключ шифрования, который использовался на старом сервере. Рекомендации о сохранении ключа шифрования даны в разделе "Удаление InfoWatch Device Monitor". Выберите **Использовать существующий ключ** и укажите путь к файлу с имеющимся ключом шифрования.

   Нажмите **Далее**.
   Если была выбрана настройка **Создать новый ключ**, укажите путь, куда Система сохранит файл со сгенерированным ключом.
10. **Настройка учетной записи сервера**

    Выберите учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor, в соответствии с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor". При выборе варианта **Пользователь** укажите имя и пароль подготовленной учетной записи домена Windows. Имя задается в формате `DOMAIN\USERNAME`.
    Нажмите **Далее**.
11. **Настройка учетной записи администратора сервера**

    Укажите данные (имя и пароль) учетной записи администратора сервера. Данной учетной записи будет присвоена роль **Суперпользователь** (подробнее см. " *Infowatch Traffic Monitor. Руководство пользователя* ", статья "Управление учетными записями Консоли управления"): она используется при первом подключении к Серверу с помощью Консоли управления.
    Нажмите **Далее**.

12. **Настройка параметров соединения с сервером InfoWatch Traffic Monitor**

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

Если на Шаге 4 вы решили использовать уже существующую базу данных (опция **Установить новую базу данных** не была выбрана), то этот шаг будет пропущен. Укажите параметры для взаимодействия с сервером InfoWatch Traffic Monitor:

- Адрес сервера TM. Адрес сервера InfoWatch Traffic Monitor. Запись адреса должна иметь следующий формат:
  `host:port`
  Параметр host должен содержать доменное имя или IP-адрес сервера InfoWatch Traffic Monitor. Адрес сервера является стандартным URI-адресом (Uniform Resource Identifier), формальный синтаксис которого описан в RFC 3986 http://tools.ietf.org/html/rfc3986.
  В качестве параметра *port* указывается порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor – 9100.

  > **Важно!**
  >
  > Если планируется интеграция с Traffic Monitor версии 5.5 или ниже, используйте формат `host:port`, где `port` - 4101.

- Количество соединений. Количество соединений с сервером InfoWatch Traffic Monitor. Вы можете задать значение от 1 до 32 соединений.
  - **Токен авторизации**. Токен для подключения к API. Необходимо указывать при работе с Traffic Monitor версии 6.0 и выше. Получите актуальный токен от администратора Traffic Monitor.
  - если в схеме развертывания Device Monitor не планируется интеграция с InfoWatch Traffic Monitor, отметьте поле **Работать в автономном режиме**. В этом случае вы можете, отметив поле **Сохранять теневые копии**, сохранять перехваченные теневые копии файлов в директорию установки сервера.

Нажмите **Далее**.

13. **Завершение установки**

Нажмите **Установить**, чтобы начать установку Сервера. Следуйте указаниям для завершения установки.

> **Важно!**
>
> При установке на Microsoft Windows Server 2012 и Microsoft Windows Server 2012 R2, на экран будет выведено диалоговое окно **Windows Security**, которое устанавливает виртуальный принтер InfoWatch, необходимый для обработки печати из metro-приложений. Для установки виртуального принтера нажмите **Install**.

> **Примечание:**
>
> Этап установки сигнатур может занимать существенное время (до получаса).

14. **Установка вспомогательного сервера**

Работа вспомогательного сервера связана с основным, и настройки основного распространяются на вспомогательный сервер, что гарантирует принцип соединения серверов Device Monitor.

a. Запуск мастера установки
Откройте папку с дистрибутивом Device Monitor. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы. В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите **Далее**.

b. Принятие лицензионного соглашения
Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.

c. Выбор устанавливаемого компонента
На шаге **Выборочная установка** по умолчанию выбраны все компоненты:
   - Сервер
   - Консоль управления
   - Сервис распространения дистрибутивов

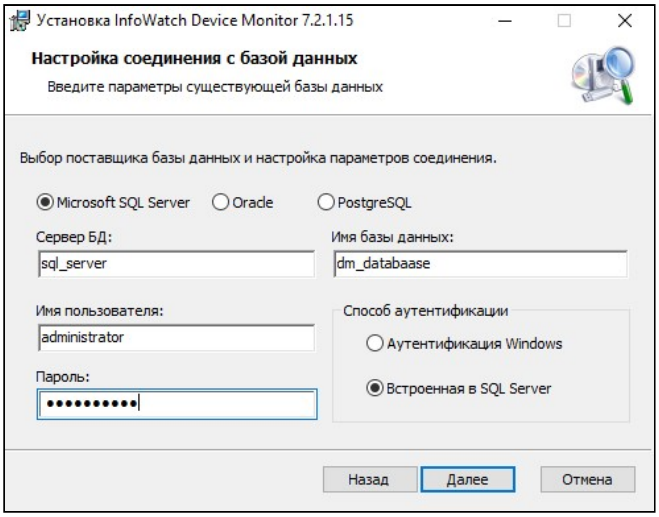
Если необходимо, измените состав устанавливаемых компонентов. По умолчанию все компоненты устанавливаются на одну рабочую станцию. Если вы рассчитываете использовать Консоль управления или Сервис распространения на другой рабочей станции, то вам не нужно устанавливать этот компонент: нажмите **Консоль управления** или **Сервис распространения дистрибутивов** и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**.
Вы также можете изменить папку, куда будет установлен тот или иной компонент: выберите компонент в списке, нажмите и укажите другое местоположение. При установке Сервиса распространения новый дистрибутив Агентов будет автоматически размещен в директорию с дистрибутивами.
Нажмите **Далее**.

d. Определение параметров сервера
На шаге **Тип устанавливаемого сервера** выберите **Вспомогательный сервер**.

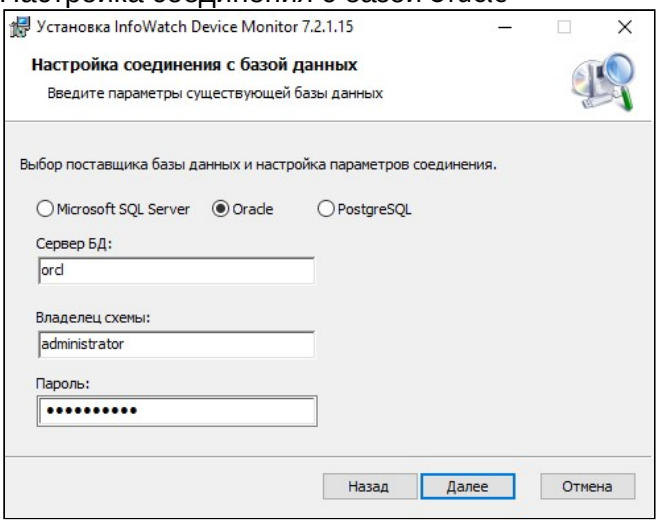
> **Важно!**
>
> Установка вспомогательного сервера не позволяет установить новую базу данных, поэтому следует указать параметры существующей базы данных.

e. Настройка соединения с базой данных
Укажите СУБД, под управлением которой находится база данных Device Monitor и введите оставшиеся параметры соединения такими же, которые были использованы при установке основного сервера:
Настройка соединения с базой Microsoft SQL Server
Если учетной записи назначена аутентификация Windows, и база данных была создана от имени доменного пользователя, то выберите

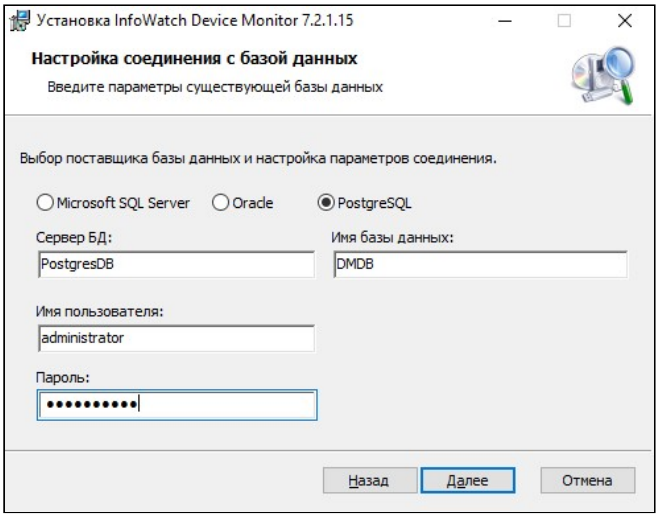
значение **Аутентификация Windows.** Если учетной записи назначена встроенная в SQL Server аутентификация, выберите значение **Встроенная в SQL Server** :



Настройка соединения с базой Oracle

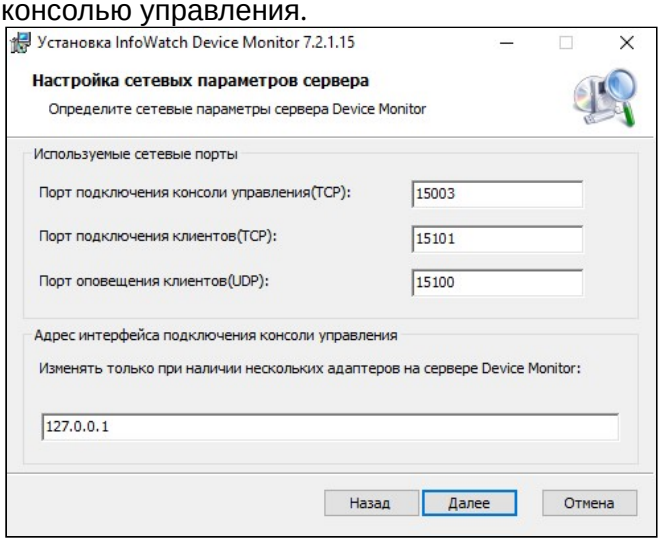


Настройка соединения с базой PostgreSQL



После того как все необходимые параметры будут указаны, нажмите **Далее**.

f. Настройка сетевых параметров сервера
Настройте параметры сервера:
В области **Используемые сетевые порты** задайте номера TCP и UDP портов, используемых для:
- подключения Консоли управления;
- подключения Агентов для передачи схем безопасности а контролируемые компьютеры, отправки информации о событиях и теневых копий на сервер;
- оповещения Агентов об изменениях схем безопасности.
В области **Адрес интерфейса подключения консоли управления** укажите IP-адрес, через который будет осуществляться взаимодействие между сервером и консолью управления.



После того как все необходимые параметры будут указаны, нажмите **Далее**.

g. Настройка учетной записи сервера
Выберите учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor, в соответствии с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor". При выборе варианта **Пользователь** укажите имя и пароль подготовленной учетной записи домена Windows. Имя задается в формате `DOMAIN\USERNAME`.
Нажмите **Далее**.

h. Завершение установки
Нажмите **Установить**, чтобы начать установку сервера. Следуйте указаниям для завершения установки. Этап установки сигнатур может занять некоторое время.

4.3 Установка Агента InfoWatch 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.

Агент InfoWatch Device Monitor может быть установлен на рабочие станции одним из следующих способов:

- Локальная установка. Выполняется при помощи универсальной программы установки непосредственно на каждом компьютере.
- Удаленная установка с помощью стороннего ПО. Осуществляется с использованием средств распространения программного обеспечения: например, посредством механизма групповых политик Microsoft Active Directory.
- Установка через задачи распространения. Выполняется в Консоли управления InfoWatch Device Monitor (подробнее см. "Удаленная установка, обновление и удаление Агентов").
- Автоматическая установка. Выполняется в Консоли управления InfoWatch Device Monitor (подробнее см. "Соединение и синхронизация со службами каталогов").

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. 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");
7. 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>`

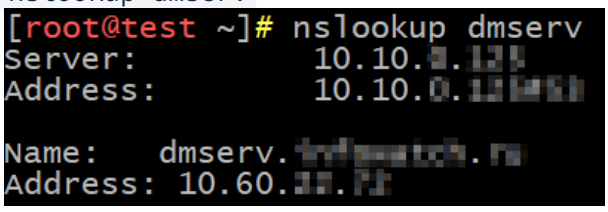
     где `<FQDN name>` – FQDN имя;
     `<hostname>` – имя хоста.
     Например, для имени хоста `computer-20` и FQDN имени `computer-20.corp.ad` строка будет выглядеть следующим образом:
     `127.0.1.1 computer-20.corp.ad computer-20`
   - если у рабочей станции нет FQDN имени, то файл должен содержать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

8. Для установления 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.

9. Если не требуется использовать компонент контроля сетевых соединений, отключите его при создании дистрибутива Агента InfoWatch Device Monitor;
10. 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!**
>
> Выключение питания компьютера в процессе установки/удаления Агента может привести к ошибкам, ведущим к нестабильной работе операционной системы.

> **Важно!**
>
> 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».

> **Важно!**
>
> В процессе установки Агента будут закрыты (если они были запущены) программы Mozilla Firefox и Mozilla Thunderbird.

> **Примечание:**
>
> Перед установкой Агента на рабочей станции с ОС Windows 7 Service Pack 1 или Windows Server 2008 R2 следует установить пакеты исправлений Windows для указанных ОС (подробнее см. в статье "Аппаратные и программные требования").

> **Примечание:**

Перед установкой Агента Device Monitor на рабочую станцию под управлением ОС Astra Linux версий 1.6 или 2.12 проверьте наличие установленной библиотеки `libxcb-res0`:

```
dpkg -s libxcb-res0
```

При необходимости установите ее:

```
sudo apt-get install libxcb-res0
```

Примечание:

При установке Агента на ОС Windows 7 и Windows 2008 R2 Server следует учесть, 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.

4.3.1 Локальная установка Агента

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 развёртывания в соответствии с заданными при формировании пакетов параметрами, например, `InfoWatch.DeviceMonitor.Client.7.11.0.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 cmd-пакета, уже содержащего параметры установки:

1. **Создание пакета установки**
   Создайте актуальный cmd-пакет установки Агента (см. документ "*InfoWatch Device Monitor. Руководство пользователя. Создания пакета установки*") и запишите его на внешний носитель.
2. **Вход в командную строку Windows**
   Запустите командную строку (cmd.exe) от имени Администратора.
3. **Запуск скрипта**
   a. Перейдите в каталог, где находится скрипт установки:
   `cd <путь_до_скрипта>`

b. Запустите скрипт, полностью указав его имя, например:
`InfoWatch.DeviceMonitor.Client.7.11.0.x64.msi.cmd`
c. Будет запущена установка без графического интерфейса в тихом режиме и без оповещений. Дождитесь окончания установки, после чего будет сформирован лог-файл с подробной информацией.

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС семейства Linux:

> **Важно!**
>
> Если на компьютере под управлением ОС Astra Linux 1.6 установлен Агент InfoWatch Device Monitor версии ниже 7.0, для установки Агента новой версии **обязательно** выполните следующие действия:
>
> 1. Удалите Агент InfoWatch Device Monitor;
> 2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 6 (20200722SE16) (см. официальную инструкцию);
> 3. Установите новую версию Агента InfoWatch Device Monitor.

> **Важно!**
>
> Для установки Агента на компьютерах под управлением ОС семейства Linux необходимы привилегии sudoers.

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

1. **Подготовка к установке:**
   a. Если на компьютере под управлением ОС Astra Linux 1.6 ранее было установлено обновление безопасности (например, Update 5):
      i. Узнайте номер установленного обновления безопасности Astra Linux:
      `cat /etc/astra?update?version`
      ii. Узнайте текущую версию ядра Astra Linux (например, **4.15.3-2-generic**):
      `uname -r`
      iii. Проверьте, что директория */boot* не содержит старых пакетов ядра с более ранней версией, чем в предыдущем шаге (например, **initrd.img-4.15.3-1-generic** или **initrd.img-4.15.3-1-hardened.**
      iv. Удалите такие пакеты при наличии:
      `apt-get purge linux-image-4.15.3-1`
      v. Удалите неиспользуемые Системой пакеты:
      `apt-get autoremove`
      `apt-get autoclean`
   b. Скопируйте на целевой компьютер архив, в котором содержаться 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.AstraLinuxSE-1.6-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.6;
- `Setup.AstraLinuxCE-2.12-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Common Edition 2.12;
- `Setup.AstraLinux-1.7-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.7;
- `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 7.3;
- `Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz` - для Альт Рабочая станция 10.

x.x.x.xx - номер сборки.

Далее будет рассмотрен пример установки и удаления Агента на РЕД ОС 7.3. Установка и удаление на других поддерживаемых ОС аналогичны.

В нашем примере:

`Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`

c. На целевом компьютере 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`

Пример команды для Агента на Alt Linux:

`tar -xvzf Setup.AltLinux-10.0-iwdm.x64.7.11.0.126.tar.gz`

В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrage.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:

`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`

Пример команды для Агента на Alt Linux:

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

Продукт будет установлен в директорию `/opt/iw/dmagent`.

   c. Проверить статус сервисов можно командой:

`sudo systemctl status iwdm*`

Пример команды для Агента на Alt Linux:

`su - -c "systemctl status iwdm*"`

   d. По окончании установки перезагрузите компьютер.

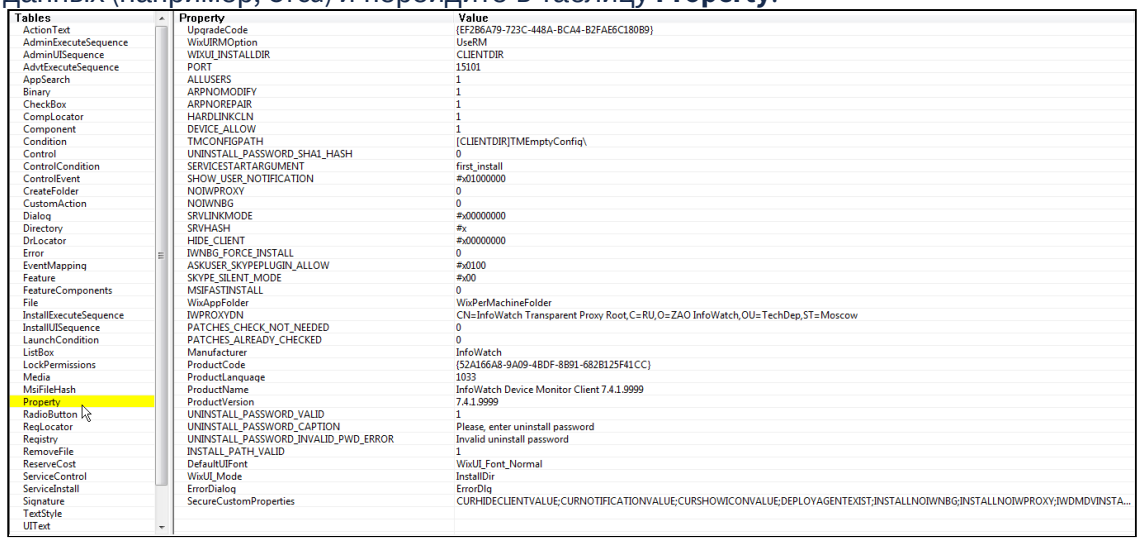
4.3.2 Установка Агента с помощью средств распространения программного обеспечения

Установка Агента на компьютеры может выполняться администратором корпоративной сети централизованно, с помощью средств распространения программного обеспечения. В настоящем разделе описывается пример такой установки посредством Microsoft Active Directory.

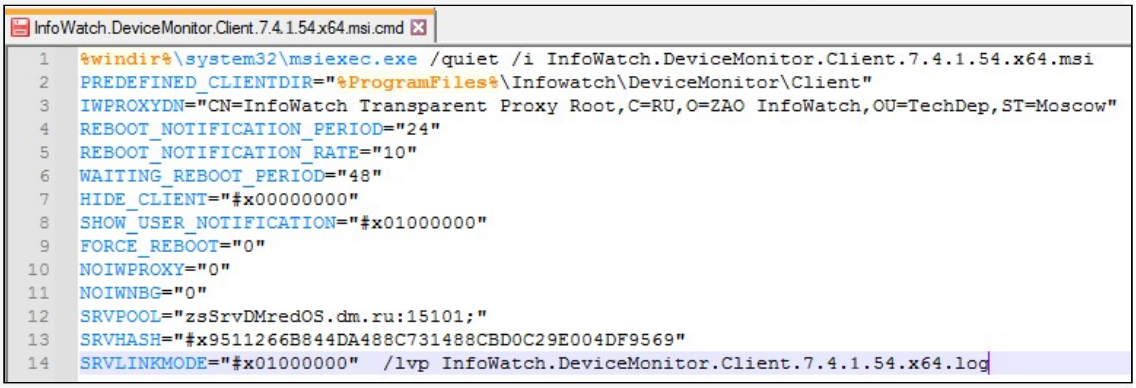
Установка Агента через Microsoft Active Directory осуществляется посредством механизма групповых политик. Для установки необходимо выбрать такую групповую политику, которая распространяется на все компьютеры, подлежащие контролю при помощи Агента. Это может быть политика, назначенная:

- контейнеру Active Directory, содержащему все компьютеры, на которые будет выполняться установка Агента;
- всему домену Active Directory, но не являющаяся доменной политикой по умолчанию (*Default Domain Policy*). Распространение этой политики должно быть назначено только той группе, которая включает в себя все компьютеры, подлежащие контролю при помощи Агента.

1. **Создание инсталляционного пакета**
   a. Создайте установочный cmd-пакет, например, `InfoWatch.DeviceMonitor.Client.7.11.0.x64.msi.cmd` (подробнее см. "*Infowatch Device Monitor. Руководство пользователя*", статья "Создание пакета установки").
   b. Разместите установочный пакет в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Агент.
2. **Создание файла трансформации**
   a. Откройте установочный файл `InfoWatch.DeviceMonitor.Client.7.11.0.x64.msi` в редакторе таблиц баз данных (например, Orca) и перейдите в таблицу **Property**:

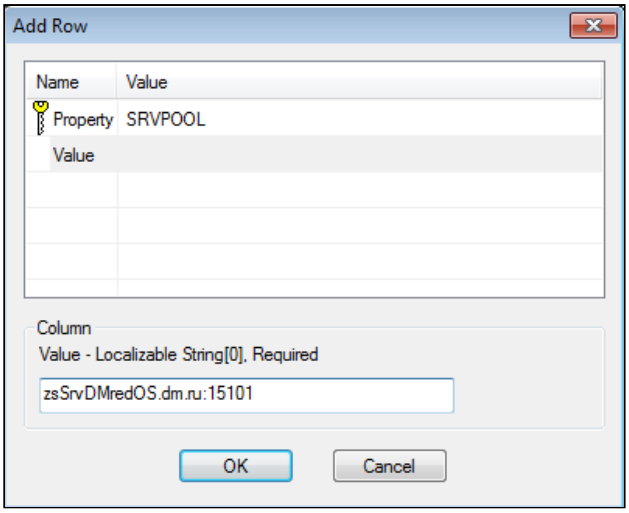


   b. Выберите в главном меню **Transform → New Transform**
   c. Откройте в текстовом редакторе ранее полученный cmd-пакет `InfoWatch.DeviceMonitor.Client.7.11.0.x64.msi.cmd`.



   d. В таблице **Property** добавьте отсутствующие свойства или замените старые значения новыми из cmd-пакета. Чтобы добавить новое свойство:
      i. Кликните на пустой строке таблицы.

ii. Введите пары значений <имя свойства>=<"новое значение"> и нажмите **OK**. И спользуйте ";" в качестве разделителя, чтобы ввести несколько значений в поле.



iii. Чтобы заменить значение свойства, выберите значение двойным кликом мыши, введите новое значение и нажмите **Enter**. Выполните эти операции для всех свойств из cmd-пакета.

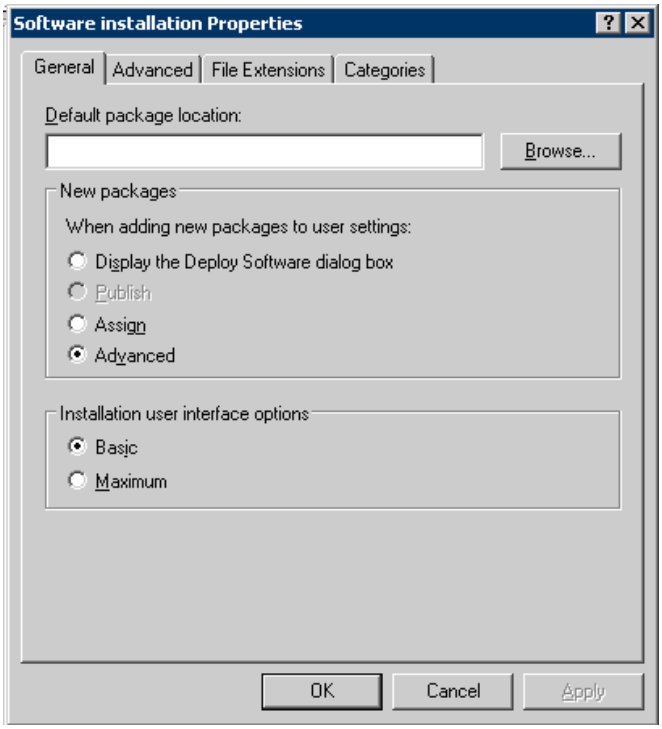
e. Перейдите в главном меню **Transform → Generate Transform**
f. Сохраните mst-файл трансформации.

3. **Редактирование групповой политики**

Перед установкой Агента средствами Active Directory необходимо отредактировать используемую групповую политику.

Чтобы отредактировать групповую политику:

a. Откройте оснастку **Active directory users and computers** (**Start** > **Settings** > **Control Panel** > **Administrative tools** > **Active directory users and computers**).
b. В дереве консоли выберите контейнер Active Directory, содержащий все компьютеры, на которые будет выполняться установка Агента.
c. Откройте оснастку **Group Policy**. Для этого в контекстном меню контейнера Active Directory выберите команду **Properties**. Затем в открывшемся диалоговом окне перейдите на вкладку **Group policy**. На данной вкладке выберите объект групповой политики и нажмите на кнопку **Edit**.
d. В дереве консоли выберите расширение **Software Installation** (**Computer Configuration** > **Software Settings**).
e. В контекстном меню расширения **Software Installation** выберите команду **Properties**. В открывшемся диалоговом окне на вкладке General выполните следующие настройки (см. рисунок):
- на панели **New packages** установите значение **Advanced**;
- на панели **Installation user interface options** установите значение **Basic**.



f. По окончании настройки нажмите на кнопку **OK**.

4. **Подготовка задания на установку Агента**

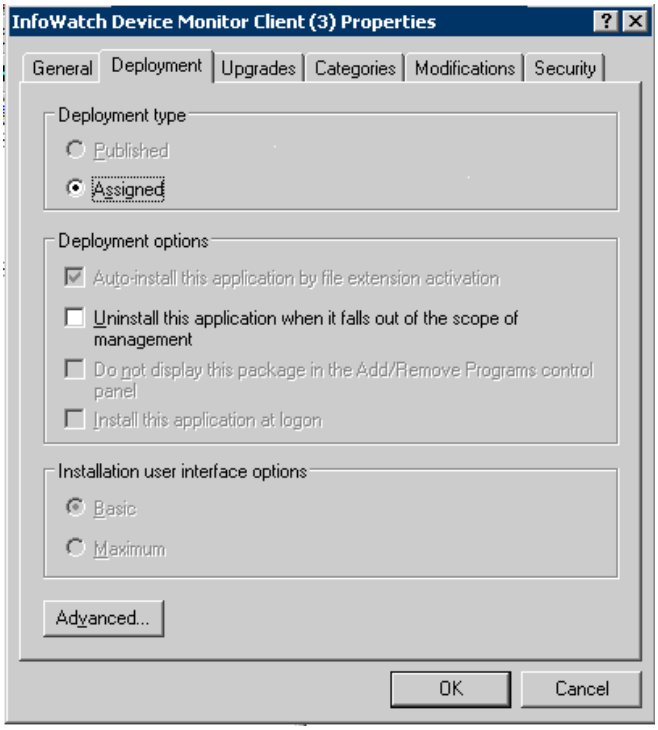
Создание и настройка задания на установку Агента выполняется в окне **Group Policy Object Editor**:

a. После того как окно **Group Policy Object Editor** будет открыто, в дереве консоли выберите расширение **Software Installation** (**Computer Configuration** > **Software Settings**). Щелкните правой кнопкой мыши по названию выделенного пункта и в раскрывшемся контекстном меню выберите пункт **New** > **Package**.

b. В открывшемся диалоговом окне **Open** укажите mst-файл трансформации (установочный пакет .msi должен быть предварительно размещен в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Агент).

> **Примечание:**
>
> Некоторые системы распространения поддерживают возможность указания параметров развёртывания. В этом случае можно использовать сам cmd-пакет клиентского модуля `InfoWatch.DeviceMonitor.Client.7.11.0.x64.msi.cmd` для передачи системе распространения.

c. Выполните настройку свойств нового пакета:
- Убедитесь, что настройки, заданные на вкладке **Deployment**, соответствуют показанным на следующем рисунке.



- После того как все необходимые настройки будут заданы, нажмите на кнопку **OK**.

d. В дереве консоли выберите каталог **Computer Configuration** > **Administrative templates** > **System** > **Scripts**. В области сведений выберите параметр **Run logon scripts synchronously**. Затем в окне свойств данного параметра установите значение **Enabled**.

5. **Выполнение установки**

Добавленное задание отображается в списке заданий оснастки **Software Installation**. Задание выполняется при первой перезагрузке компьютера, на который должен быть установлен Агент. Запуск службы InfoWatch Device Monitor Client осуществляется автоматически сразу после установки.
Способ установки отображается в столбце **Deployment state**. Состояние **assigned** означает, что установка осуществляется принудительно, т.е. без учета мнения пользователя, работающего за компьютером, на который выполняется установка Агента. Состояние **published** соответствует установке с запросом согласия от пользователя.

Важно!

В случае обновления Агента на ОС семейства Linux для корректной блокировки съемных устройств обязательно перезагрузите рабочую станцию.

Вы можете проверить успешность установки Агента в Консоли управления InfoWatch Device Monitor. Все компьютеры, на которые Агент был успешно установлен, должны отображаться в списке раздела **Группы компьютеров**. Чтобы просмотреть список всех контролируемых компьютеров, воспользуйтесь кнопкой **Показать все компьютеры**,

расположенной в верхней части Панели навигации. Чтобы получить актуальные сведения об установленных Агентах, воспользуйтесь кнопкой **Обновить**, расположенной на панели инструментов.

5 Настройка Сервера InfoWatch Device Monitor

В настоящем разделе описана низкоуровневая настройка Сервера InfoWatch Device Monitor. Выполнять описанные ниже действия без помощи инженеров InfoWatch не рекомендуется.

> **Примечание:**
>
> Для корректной работы InfoWatch Device Monitor на компьютерах, на которых установлены его компоненты, требуется настроить сетевые правила доступа. Подробнее см. "Настройка сетевых правил доступа".

Настройка Сервера осуществляется с помощью конфигурационного XML-файла `InfoWatch.DeviceMonitor.Server.exe.config`. Конфигурационный файл размещается в том же каталоге, что и исполняемый файл Сервера `InfoWatch.DeviceMonitor.Server.exe`.

По умолчанию после установки Сервер расположен в каталоге

```
C:\Program Files\InfoWatch\Device Monitor\Server
```

Конфигурационный файл можно просматривать при помощи любого текстового или XML-редактора. Кодировка файла UTF-8.

Корневым элементом конфигурационного файла является элемент `<configuration>`. Корневой элемент включает в себя дочерние элементы (конфигурационные разделы). Структура конфигурационного файла с описанием разделов приведена в следующей таблице. По ссылкам в названиях разделов содержится подробная информация об их настройке.

> **Важно!**
>
> Редактирование конфигурационного файла без помощи инженеров InfoWatch настоятельно не рекомендуется.
>
> По завершении редактирования необходимо перезапустить сервер Device Monitor.

Конфигурационный раздел	Описание
<configSections>	Служебный раздел. Содержит описание всех остальных разделов. Редактирование этого раздела не разрешается.
<runtime>	Содержит настройки для среды выполнения Microsoft .NET Framework. Эти настройки необходимы для корректной работы Сервера. В разделе `<runtime>` определен элемент `gcServer`, предназначенный для настройки сборщика мусора. Элемент имеет атрибут `enabled`, принимающий значение `true` (включен параллельный сбор мусора) или `false` (выключен параллельный сбор мусора). Изменение этого раздела крайне не рекомендуется.

Конфигурационный раздел	Описание
<applicationSettings>	Содержит настройки отдельных модулей Сервера, таких как порты, размеры буферов, таймауты и пр.
<system.diagnostics>	Содержит настройки протоколирования. Протоколирование может быть полезно при диагностике работы компонентов Сервера.

Если в процессе работы потребуется удалить временные файлы, генерируемые Device Monitor, вы можете это сделать с помощью специальной утилиты: подробнее см. "Удаление временных файлов".

5.1 Раздел <applicationSettings>

Раздел `<applicationSettings>` предназначен для настройки отдельных модулей Сервера. Всего таких модулей шесть. Все разделы имеют одинаковую структуру: в состав любого из этих разделов входит набор элементов, предназначенных для настройки параметров модуля. Каждый элемент `<setting>` имеет следующие атрибуты:

- `name` — имя настройки.
- `serializeAs` — способ сериализации данных. Данные всегда сериализуются в виде строки (используется тип данных string).

Настройки параметров модуля определяется дочерним элементом `<value>`. Например:

```
<setting name="RemotingPort" serializeAs="String">
<value>15003</value>
</setting>
```

Описание параметров для каждого модуля приводится в следующей таблице.

Параметр	Описание
`<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings>` Настройки ядра Сервера	
`RemotingPort`	Порт TCP, обслуживающий подключения Консоли управления. Значение по умолчанию - `15003` (крайне не рекомендуется изменять это значение)
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU` • `en-US`
`MachineName`	IP-адрес сетевого интерфейса, посредством которого Сервер принимает соединения с Консолью управления. Значение по умолчанию `127.0.0.1`. Изменять это значение нужно, только если Сервер имеет 2 или более сетевых интерфейсов. В этом случае для корректной работы необходимо явно задать адрес интерфейса,

Параметр	Описание
	посредством которого сервер принимает входящие соединения от различных экземпляров Консоли управления
`CheckServerSettingsInterval`	При наличии кластеризации – период (в секундах) синхронизации с базой данных. По истечении этого времени Сервер запрашивает базу данных об изменениях в схеме безопасности, произведенных с помощью основного Сервера, использующего ту же базу данных. Значение по умолчанию - 300.
`<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings>` Настройки модуля, взаимодействующего с базой данных	
`DatabaseType`	Тип базы данных. Возможные значения: • `Oracle` • `Microsoft` • `PostgreSql`
`ConnectionString`	Строка соединения с базой данных. Должна соответствовать правилам, установленным для строк соединения ADO.NET. Например: `Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security=True`
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU` • `en-US`
`ConnectionPoolSize`	Количество соединений к БД, которые будут открыты и которые будет использовать сервер в своей работе. Значение по умолчанию - `200`.
`CommunicationPort`	Номер порта, используемого при соединении сервера с Агентом распространения при установке Агента через механизм задач. Не рекомендуется менять в процессе работы. Значение по умолчанию - `15505`.
`UpdateStatusTimeOut`	Интервал времени, через который необходимо обновлять статус выполнения задачи на удаленном компьютере. С данным интервалом сервер опрашивает удаленные

Параметр	Описание
	компьютеры, где разворачивается Агент, о статусе установки продукта, для отображения информации на сервере. Значение по умолчанию - `60`.
`EventRelationStoredPeriod`	Интервал времени в днях. Параметр используется в формуле вычисления даты удаления при очистке мусорных событий. Значение по умолчанию - `7`.
`DeleteEventCount`	Максимальное количество удаляемых событий из БД за один проход Значение по умолчанию - `10000`.
`<InfoWatch.DeviceMonitor.Server.Gui.Properties.Settings>` Настройки модуля, предоставляющего интерфейс для Консоли управления	
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU` • `en-US`
`InitialLeaseTime`	Время (в минутах), в течение которого сеанс соединения с Консолью управления считается действительным. Значение по умолчанию - `5`.
`RenewOnCallTime`	Время (в минутах), на которое продлевается время жизни сеанса соединения Консоли с сервером. Значение по умолчанию - 2.
`<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings>` Настройки модуля, обслуживающего клиентские подключения (контролируемые компьютеры)	
`Backlog`	Длина очереди клиентских соединений, ожидающих подключения. Значение по умолчанию - `64`.
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU` • `en-US`
`ShadowCopyTempDir`	Полный путь к каталогу, в котором хранятся временные теневые копии, ожидающие отправки в InfoWatch Traffic Monitor.

Параметр	Описание
	Значение по умолчанию: `C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir\<0÷255>\`
`DmpV1Adress`	Список IP-адресов (разделитель в перечислении – «;»), на которых сервер должен прослушивать порты. Возможны следующие значения: • `AllAny` – порты на всех IP адресах, которые имеются на компьютере (значение по умолчанию); • `AllIp4` – порты на всех IP адресах версии 4; • `AllIp6` – порты на всех IP адресах версии 6.
`Dmpv1TraceLevel`	Уровень трассировки протокола взаимодействия клиента и сервера. Возможны следующие значения: • 1 – выключить трассировку; • 2 – выполнять трассировку только для информации о пакете (значение по умолчанию); • 3 – полная трассировка. Трассировка будет выведена в приемник диагностических сообщений (по умолчанию Журнал приложений Windows) только в случае значения параметра `3` и уровня протоколирования для фильтра модуля - `Verbose` (см. "Раздел <system.diagnostics>").
`Dmpv1TraceClients`	Список IP-адресов Агентов (разделитель в перечислении – «;»), взаимодействие с которыми необходимо трассировать. При значении `All` выполняется трассировка для всех Агентов.
`Dmpv1ConnectionsLimit`	Количество одновременно обрабатываемых соединений по протоколу TCP/IP с клиентами. Значение по умолчанию - `400`.
`Dmpv1ConnectionsQueueLimit`	Максимальное количество соединений, ожидающих обработку. Если значение превышено, то соединения "урезаются" до значения, указанного в параметре `Dmpv1ConnectionsQueueLengthAfterCut`. Значение по умолчанию - `700`.
`Dmpv1ConnectionsQueueLengthAfterCut`	Количество соединений после урезания очереди при превышении очередью максимального размера. Значение по умолчанию - `250`.

Параметр	Описание
`TimeoutPeriodSeconds`	Величина таймаута, по истечении которого зависшее соединение между Агентом и Сервером будет закрыто, частично созданные теневые копии будут удалены (отправка теневых копий будет повторяться при следующем установленном соединении). Значение по умолчанию - `120`.
`SSLPort`	Номер порта для шифрованных соединений. Значение по умолчанию - `15004`.
`CheckUpdateTmConfigPeriodMinutes`	Период опроса сервера TM на проверку изменений конфигурации в минутах. Значение по умолчанию - `30`.
`<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings>` Базовые настройки коннектора Traffic Monitor Server	
`DBPollTime`	Период (в миллисекундах) опроса базы данных, в процессе которого проверяется наличие событий в базе данных. Значение по умолчанию - `10 000`. Минимальное значение - `1000`, максимальное - `600000`
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU` • `en-US`
`NumberOfConnections`	Количество соединений с InfoWatch Traffic Monitor. Значение по умолчанию - `4`. Минимальное значение - `1`, максимальное - `32`.
`MaxSendEventCount`	Максимальное количество событий, вычитываемое за один раз из БД DM для отправки в TM Значение по умолчанию - `1000`. Минимальное значение - `1`, максимальное - `10000`
`ShadowCopyTrasferBlockSize`	Размер блока данных теневой копии, пересылаемой на сервер Traffic Monitor, в МБ. Значение по умолчанию - `16`. Минимальное значение - `1`, максимальное - `64`
`<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>` Настройки низкоуровневого драйвера базы данных	

Параметр	Описание
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU` • `en-US`
`MaxConnectionWaitingTime`	Время ожидания свободного соединения из пула в секундах. Значение по умолчанию - `300`
`CommandTimeoutSeconds`	Время выполнения операции или запроса в секундах. Значение по умолчанию - `30`. **Примечание:** Данный параметр не работает для СУБД Oracle.
`LongCommandTimeoutSeconds`	Время выполнения длительной операции или запроса в секундах. Применяется, когда время выполнения составляет значительный промежуток. Значение по умолчанию - `300` (0 - бесконечно). **Примечание:** Данный параметр не работает для СУБД Oracle.
`<InfoWatch.DeviceMonitor.EP.Sender.Properties.Settings>` Настройки модуля, взаимодействующего с Платформой	
`EPAddress`	Адрес сервера Платформы и токен Платформы. Система не использует значения этих параметров. Укажите адрес и токен Платформы в Консоли управления (см. "InfoWatch Device Monitor. Руководство пользователя", статья "Настройки сервера Device Monitor. Соединение с сервером Платформы").
`EPToken`	
`DBPollTime`	Частота опроса БД (в мс). Значение по умолчанию - `5000` Минимальное значение `- 5000,` максимальное `-` `600000`
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU`

Параметр	Описание
	• `en-US`
`NumberOfConnections`	Количество подключений сервера IW Device Monitor к серверу Платформы. Значение по умолчанию - `4` Минимальное значение `- 1,` максимальное `- 64`
`MaxSendEventCount`	Количество событий, которое единовременно может быть отправлено из базы данных. Значение по умолчанию - `5000` Минимальное значение `- 1,` максимальное `- 10000`
`RequestEventCount`	Количество событий статистики, допустимое для отправки в одном пакете. Значение по умолчанию - `100` Минимальное значение `- 1,` максимальное `- 10000`
`WriteDisconnectEventLogIntervalMinute`	Интервал записи лог-файла в случае отсутствия или обрыва связи (в мин). Значение по умолчанию - `60` Минимальное значение `- 10,` максимальное `- 240`
`WaitPlatformDiskErrInitialMinute`	Начальное время ожидания в минутах повторной отправки событий в Платформу в случае получения ошибки 507. Значение по умолчанию - `10` Минимальное значение `- 1,` максимальное `- 1440`
`WaitPlatformDiskErrMaxMinute`	Максимальное время ожидания в минутах повторной отправки событий в Платформу в случае получения ошибки 507. Значение по умолчанию - `60` Минимальное значение `- 1,` максимальное `- 1440`
`<InfoWatch.DeploymentSubSystem.Properties.Settings>` Настройка модуля распространения (установка/обновление/удаление) агентов и диагностики	
`NetworkLatency`	Технический параметр, изменять не рекомендуется.
`RunningInstallationsLimit`	Максимальное количество одновременных первичных инсталляций на компьютерах. Значение по умолчанию - `0` (вычисляется по формуле)
`BandwidthUsagePercentLimit`	Процент занимаемой данными задачами пропускной способности сети, чтобы его можно было контролировать. Значение по умолчанию при отсутствии параметра или ошибки – `0.5 (50%)`

5.2 Раздел <system.diagnostics>

Раздел предназначен для диагностики работы Сервера. Включает в себя следующие элементы:

- `<trace>`. Общие настройки модуля диагностики.
- `<sources>`. Настройки, необходимые для диагностики отдельных компонентов Сервера.
- `<switches>`. Управление уровнем детализации диагностической системы в целом. Включает в себя определения детализаторов. Как правило, существует один детализатор. Если для разных модулей требуются разные настройки детализации, то необходимо использовать фильтры. При этом общий детализатор, должен иметь значение, соответствующее максимальной детализации одного из модулей.

Элемент *<trace>*

Используется для описания глобальных настроек модуля диагностики. В данном элементе можно задавать величину отступов в сообщениях, параметры сохранения данных из потока диагностики на жесткий диск.

Элемент *<sources>*

Используется для настройки отдельных модулей приложения. Включает в себя дочерние элементы `<source>` – по одному на каждый модуль приложения (список модулей Сервера см. "Раздел <applicationSettings>").

Также в списке модулей присутствуют вспомогательные, которые необходимы для вывода отладочной информации для основных компонентов:

- `InfoWatch.DeviceMonitor.Server.FileIdentification.Core` - модуль который описывает объектную модель сигнатур;
- `InfoWatch.DeploymentSubSystem` - модуль подсистемы отвечающей за развертывание на компьютеры;
- `InfoWatch.DeviceMonitor.EventPostProcessorManager` - модуль пост-обработки событий печати;
- `InfoWatch.DeviceMonitor.ScreenShotStorage` - модуль для сохранения скриншотов в файловую систему;
- `InfoWatch.DeviceMonitor.Server.Remote.Install` - модуль для запуска удаленной установки\обновления\удаления агента на компьютер.

Элемент `<source>` имеет следующие атрибуты:

- `name`. Имя модуля сервера.
- `switchName`. Имя модуля, определяющего детализацию диагностики (детализатора).
- `switchType`. Тип модуля, определяющего детализацию диагностики. Всегда имеет значение `System.Diagnostics.SourceSwitch`.

В каждом элементе `<source>` также содержится определение приемника диагностических сообщений (`<listeners>`). Приемником диагностических сообщений может быть:

- журнал приложений Windows (Application log);
- системный отладочный вывод (можно просматривать с помощью специальных инструментов, например, DebugView);
- текстовый файл.

Элемент `<source>` имеет дочерний элемент `<listeners>`. В данном элементе содержатся параметры приемника диагностических сообщений. Элемент `<listeners>` может включать в себя следующие дочерние элементы:

- `<add>`. Добавление нового приемника диагностических сообщений.
- `<remove>`. Удаление приемника диагностических сообщений. Применяется только для удаления приемника сообщений по умолчанию (таковым является журнал приложений Windows). С этой целью нужно установить имя элемента равным `Default`: `<remove name="Default" />`

Элемент *<add>*

Данный элемент добавляет приемник диагностических сообщений к модулю Сервера. Элемент содержит следующие атрибуты:

- `name`. Имя приемника диагностических сообщений.
- `type`. Тип приемника диагностических сообщений.
- `initializeData`. Идентификатор модуля Сервера. Как правило, это значение совпадает с именем соответствующего модуля Сервера. Если в качестве приемника используется журнал приложений Windows, то это информация, которая заносится в столбец `source`.

Тип приемника — это полное имя типа приемника из библиотеки классов .NET Framework или собственного типа, реализующего требуемый интерфейс приемника диагностических сообщений.

В библиотеке классов .NET Framework определены следующие типы приемников диагностических сообщений:

- `System.Diagnostics.EventLogTraceListener`. Журнал приложений Windows (Application log).
- `System.Diagnostics.ConsoleTraceListener`. Вывод сообщений в консольном приложении.
- `System.Diagnostics.TextWriterTraceListener`. Вывод в текстовый файл.
- `System.Diagnostics.DefaultTraceListener`. Отладочный вывод Windows (по умолчанию включен).

Также элемент `<add>` содержит фильтр диагностических сообщений. Данный фильтр выводит только те сообщения, которым назначен уровень детализации, превышающий уровень, заданный в настройках фильтра. Определены следующие уровни детализации (приводятся в порядке убывания важности уровня):

- `Verbose`. Отладочный уровень. В журнале регистрируются все события. Этот уровень нужно применять только для отладки Device Monitor. Не разрешается устанавливать данный уровень, если Device Monitor работает в нормальном режиме, так как это приводит к значительному снижению производительности.
- `Information`. Информационный уровень. Регистрируются события не связанные с ошибками, такие как, например, информация об изменении параметров Сервера.
- `Warning`. Уровень предупреждения. Регистрируются некритичные ошибки в работе Device Monitor, такие как неожиданное прекращение соединения с Сервером, истекший таймаут соединения и пр.
- `Error`. Уровень ошибок. Регистрируются ошибки, мешающие корректной работе Device Monitor (т.е. ошибки, требующие исправления).
- `Critical`. Критический уровень. Регистрируются серьезные нарушения в работе, которые могут привести к неработоспособности Device Monitor.

Пример 1

Для детализатора установлен уровень протоколирования *Verbose*, а для фильтра какого-либо модуля – *Warning*. Тогда детализатор пропускает события с уровнем *Warning*, *Error* и *Critical*, но отфильтровывает события с уровнем *Information* и *Verbose*.

Пример 2

Для детализатора установлен уровень протоколирования *Error*, а для фильтра какого-либо модуля – *Warning*. В этом случае детализатор пропускает события с уровнем *Error* и *Critical*, но отфильтровывает события с уровнем *Warning*, *Information* и *Verbose*. Это происходит потому, что общий уровень детализации - *Error*, т.е. вне зависимости от того, как настроены фильтры, регистрируются только сообщения с уровнем *Error* и выше.

Элемент *<remove>*

Удаление приемника сообщений. Как правило, применяется для удаления приемника по умолчанию, выводящего диагностические сообщения в отладочный вывод Windows:

```
<remove name="Default" />
```

Элемент *<switches>*

Определяет детализаторы Сервера. Как правило, определен только один детализатор, который устанавливает глобальный (для всего Сервера) уровень детализации диагностической системы. Если отдельным модулям Сервера требуется более низкий уровень детализации, то в этом случае можно воспользоваться фильтрами.

По умолчанию элемент `<switches>` содержит только один дочерний элемент:

```
<add name="applicationLogger" value="Information"/>
```

Уровень детализации задается как значение атрибута `value`.

5.3 Удаление временных файлов Device Monitor

InfoWatch Device Monitor предоставляет возможность удалять временные файлы, генерируемые Device Monitor, а именно:

- все файлы из директории временных файлов операционной системы (%Temp%);
- данные из файловой очереди обработки событий Device Monitor (по умолчанию - `C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir`; о настройке см. "Раздел <applicationSettings>").

Удаление производится с помощью утилиты `RemShadowCopyFiles`, расположенной в папке установки сервера (по умолчанию - `C:\Program Files\InfoWatch\DeviceMonitor\Server`).

Запуск утилиты должен производиться от имени учетной записи администратора, имеющего права на чтение и запись в директориях с удаляемыми файлами.

> **Важно!**
>
> На время выполнения процедуры обработка событий, поступающих в Device Monitor, будет приостановлена.
>
> Данные обо всех событиях, не обработанных на момент начала удаления, будут удалены.

Чтобы удалить временные файлы:

1. Авторизуйтесь на том сервере InfoWatch Device Monitor, где требуется произвести удаление временных файлов.
2. Запустите утилиту `RemShadowCopyFiles`.
3. Подтвердите удаление временных файлов, нажав **Y**.

Утилита выполнит остановку служб Device Monitor, выполнит удаление временных файлов, а затем вновь запустит службы Device Monitor.

> **Важно!**
>
> При удалении временных файлов из системной папки `%Temp%` может возникать отказ в доступе: некоторые файлы могут быть созданы и использоваться другими процессами, не относящимися к Device Monitor.

5.4 Настройка защиты от подбора паролей Device Monitor

Для защиты Системы реализована блокировка авторизации пользователя при повторяющихся неудачных попытках входа. Защита от подбора паролей настраивается в базе данных. По умолчанию защита отключена.

Чтобы включить защиту для сервера Device Monitor:

1. Подключитесь напрямую к базе данных, которую использует сервер Device Monitor.
2. Найдите таблицу `PasswordProtection`.
3. Найдите 3 параметра, которые отвечают за настройку защиты:
   - **`MaxAuthFailCount`** – количество допустимых неудачных попыток авторизации;
   - **`MaxBlockingTimeInSeconds`** – время, на которое будет заблокирована возможность авторизации для пользователя, в секундах;
   - **`MaxFailAuthPeriodInSeconds`** – период неудачных попыток авторизации, в секундах.
4. Задайте значения всех трех параметров в соответствии с требованиями безопасности.

   > **Важно!**
   >
   > Если любому из параметров задано некорректное значение или 0, защита будет отключена.

5. Сохраните изменения в базе данных.

   > **Важно!**
   >
   > Защита от подбора пароля будет работать только для пользователей Device Monitor. Учетным записям домена AD, которым назначаются права на вход в Device Monitor, необходимо будет настраивать защиту средствами AD. При перезапуске сервиса DM попытка авторизации будет считаться первой. Если пользователь совершил 3 неудачных попытки подряд, его четвертая попытка после перезапуска будет считаться первой.

При блокировании авторизации в журнале аудита (кнопка **Журнал** на Панели навигации консоли управления Device Monitor) будет создано событие, в котором будет указано время разблокировки. При очередной неуспешной попытке авторизации заблокированный пользователь будет уведомлен о превышении числа неудачных попыток входа.

Пример настроек защиты:

- MaxAuthFailCount – 5

- `MaxBlockingTimeInSeconds` – 300
- `MaxFailAuthPeriodInSeconds` – 120

При данных настройках, если в течение 2 минут (120 секунд) от имени пользователя будут выполнены 5 неудачных попыток авторизации, для данного пользователя будет заблокирована возможность авторизации на 5 минут (300 секунд). Отсчет периода неудачных попыток начинается с первой. Если за 120 секунд пользователь совершит только 4 неудачные попытки, следующая попытка будет первой в новом периоде.

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. Если вы хотите использовать встроенный сертификат веб-сервера Traffic Monitor, то перейдите к шагу 5.
3. В центре сертификации вашей компании выпустите сертификат X.509 для веб-сервера Traffic Monitor.
4. Настройте работу веб-сервера Traffic Monitor с выпущенным сертификатом.
5. На сервере Device Monitor установите корневой сертификат веб-сервера Traffic Monitor в хранилище корневых сертификатов уровня "локальный компьютер".

5.5.1 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 TMConfig 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.

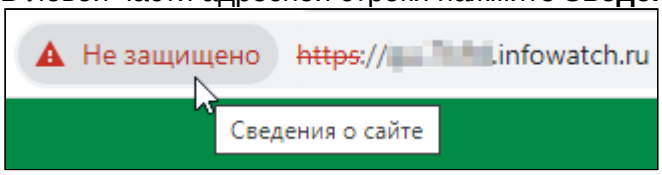
Если значения параметров `IGNORE_SSLERR_TMXAPI_CONNECTION`, `IGNORE_SSLERR_TMCONFIG_CONNECTION` и `IGNORE_SSLERR_PLATFORM_CONNECTION` были изменены, то чтобы правила проверки сертификатов вступили в силу, перезапустите службу сервера Device Monitor.

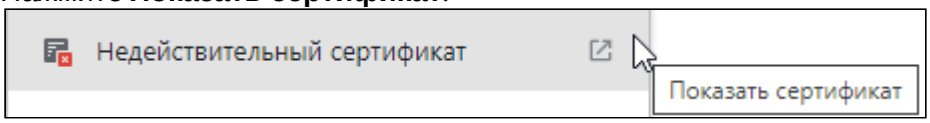
5.5.2 Чтобы установить сертификат службы XAPI Traffic Monitor:

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. Переименуйте корневой сертификат в `tmca.crt`.
5. Откройте оснастку управления сертификатами компьютера. Для этого:
   a. В меню **Пуск** выберите **Выполнить**.
   b. Введите `mmc`. Откроется Консоль Управления.
   c. В меню **Файл** выберите **Добавить или удалить оснастку**.
   d. В открывшемся окне в списке **Доступные оснастки** выберите **Сертификаты**, а затем нажмите **Добавить**.
   e. В окне **Оснастка диспетчера сертификатов** выберите **Учетная запись компьютера**, а затем нажмите **Далее**.
   f. В окне **Выбор компьютера** убедитесь, что выставлен флажок **Локальный компьютер,** и нажмите **Готово**.
   g. В окне **Добавление или удаление оснастки** нажмите **ОК**.
6. Перейдите в раздел **Доверенные корневые центры сертификации** -> **Сертификаты**.
7. В меню **Действие** выберите **Все задачи** -> **Импорт**.

8. В открывшемся окне нажмите **Далее**.
9. Укажите путь к скопированному ранее корневому сертификату и нажмите **Далее**.
10. Убедитесь, что выставлен флажок **Поместить все сертификаты в следующее хранилище** и в качестве хранилища сертификатов выбрано **Доверенные корневые центры сертификации**, и нажмите **Далее**.
11. Нажмите **Готово**.

5.5.3 Чтобы установить сертификат веб-сервера 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. Выполните шаги 5-11 инструкции по установке сертификата службы XAPI Traffic Monitor, описанной выше.

5.5.4 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. Выполните шаги 5-11 инструкции по установке сертификата службы XAPI Traffic Monitor, описанной выше.

5.5.5 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. Запустите приложение Windows **Просмотр событий**.
2. Откройте раздел **Журналы Windows** -> **Приложение**.

6 Обновление InfoWatch Device Monitor

Если у вас установлен InfoWatch Device Monitor, то вы можете обновить его до более поздней версии.

> **Важно!**
>
> Для корректной работы и доступа ко всей функциональности версии Traffic Monitor и Device Monitor должны быть совместимы. Подробнее о совместимости Device Monitor см. в статье Базы знаний InfoWatch "Особенности совместимости разных версий TM, DM и Агентов".

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

1. Обновление серверной части InfoWatch Device Monitor (база данных, сервер, сервис распространения дистрибутивов и консоль управления).

   > **Важно!**
   >
   > При обновлении Системы с ранних версий:
   >
   > 1. Соблюдайте следующий порядок: в первую очередь обновите Сервер Device Monitor, затем Сервер Traffic Monitor, затем Агенты DM на рабочих станциях.
   >
   > 2. Если требуется обновить Device Monitor версии 3.4, удалите старую версию сервера (не удаляя базу данных) и установите сервер заново, указав при этом параметры соединения с существующей базой данных.
   >
   > 3. Если требуется обновить Device Monitor, начиная с версии 4.0, то выполните обновление без удаления предыдущей версии.
   >
   > 4. Чтобы при обновлении Device Monitor версии 6.0 (путем удаления и повторной установки Сервера) Агенты Device Monitor смогли подключиться и привязаться к новому серверу:
   >
   > - при удалении: сохраните ключ шифрования, хранящийся в папке установки сервера DM, файл `SSLServerKey.pfx`.
   >
   > - при установке: укажите путь к сохраненному ключу шифрования, который использовался на старом сервере.

2. Обновление Агента InfoWatch Device Monitor.

   > **Важно!**
   >
   > Обновление Агентов Device Monitor следует проводить после обновления Сервера Device Monitor и Сервера Traffic Monitor.

6.1 Обновление серверной части InfoWatch Device Monitor

> **Важно!**

Если вы используете основной и вспомогательные серверы Device Monitor, в процессе обновления они не должны взаимодействовать с базой данных.
Для обновления Системы из нескольких серверов:

1. Остановите работу всех обновляемых серверов Device Monitor.
   Для прекращения работы вы можете вручную остановить службу InfoWatch Device Monitor Server в Диспетчере задач (Task manager) на вкладке Службы.
2. Обновите по инструкции основной сервер Device Monitor.
   После обновления инсталлятор сам запускает работу сервера.
3. Обновите второстепенные серверы Device Monitor.

Шаг 1. Начало обновления

Откройте папку с дистрибутивом Device Monitor и запустите файл установки для требуемой платформы.

В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

Шаг 2. Принятие лицензионного соглашения

Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.

Шаг 3. Настройка базы данных

При обновлении база данных сохраняется, и в окне **Установка или обновление базы** по умолчанию указываются параметры ранее использовавшейся базы данных. Однако вам потребуется указать некоторые параметры, в зависимости от используемой СУБД.

Обновление базы данных под управлением СУБД Microsoft SQL Server

На панели **Способ аутентификации** выберите способ аутентификации, назначенный пользователю, от имени которого обновляется база данных. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**.

Если учетной записи назначена встроенная аутентификация SQL Server, выберите значение **Встроенная в SQL Server**. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно.

Примечание:

В процессе обновления вы можете указать прежние параметры аутентификации или задать новые. Рекомендации по выбору способа аутентификации и подготовке необходимой учетной записи приведены в статье "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server".

Обновление базы данных под управлением СУБД Oracle

В поле **Сервер БД** укажите сервер, используемый для работы с обновляемой базой данных.

В полях **Владелец схемы** и **Пароль** укажите учетную запись владельца схемы базы данных и введите пароль от нее.

Обновление базы данных под управлением PostgreSQL

Укажите имя пользователя и пароль учетной записи, используемой для работы с обновляемой базой данных. Имя по умолчанию - `postgres`.

После того как необходимые параметры будут настроены, нажмите кнопку **Далее**.

Шаг 4. Завершение обновления

После перехода к следующему окну, нажмите на кнопку **Установить**, чтобы запустить процесс обновления серверной части Device Monitor.

Следуйте дальнейшим указаниям мастера установки, чтобы завершить обновление серверной части.

Важно!

После обновления сервера Device Monitor обязательно введите повторно или обновите пароли для синхронизации со службами каталогов и для задач первичного распространения (см. документ "*InfoWatch Device Monitor. Руководство пользователя*" статьи "*Соединение и синхронизация со службами каталогов*" и "*Создание задачи первичного распространения*").

Примечание:

При обновлении сервера Device Monitor не гарантируется работа фильтров отображения данных в консоли (фильтры событий, логов журнала аудита и т.д.), которые были настроены в предыдущей версии.

Примечание:

При обновлении сервера в поле **Статус** возможны следующие значения:

- **Не установлен** - если не было ни одного обращения Агента к серверу;
- **Установлен** - если Агент хотя бы один раз обращался к серверу.

Для поля **Активность агента** актуальный статус будет установлен в соответствии со значениями, указанными в настройках.

При обновлении на новую версию переименование рабочих станций, которые уже находятся в схеме безопасности, не производится. Новый механизм проверки и регистрации распространяется на компьютеры, которые обращаются к серверу после обновления. Он подразумевает проверку только идентификатора: если он совпадает, у рабочей станции меняется имя, а прежнее имя будет только отображаться в Консоли до тех пор, пока Пользователь не удалит ее.

Прежний механизм также включал проверку имени, что приводило к возникновению в Консоли DM двух записей для одной рабочей станции, с новым и старым именем.

6.2 Обновление Агента InfoWatch Device Monitor

Device Monitor поддерживает совместимость с Агентами версий 7.2 и более поздними. Таким образом, обновленные компоненты Device Monitor могут работать со старыми версиями Агента. Однако вы можете обновить Агент до более поздней версии.

Важно!

Если на компьютере под управлением ОС Astra Linux 1.6 установлен Агент InfoWatch Device Monitor версии ниже 7.0, для обновления Агента **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;
2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 6 (20200722SE16) (см. официальную инструкцию);
3. Установите новую версию Агента InfoWatch Device Monitor.

Для успешного обновления Агента InfoWatch Device Monitor следуйте рекомендациям на странице "Установка Агента InfoWatch Device Monitor". Обновление может быть выполнено одним из способов:

- автоматическое обновление;
- централизованное обновление через Консоль управления;
- удаленное обновление с помощью средств распространения программного обеспечения;
- локальное обновление с использованием мастера установки;
- локальное обновление Агентов на компьютере под управлением ОС семейства Linux с помощь скрипта (см. ниже).

Чтобы локально обновить Агента на компьютере под управлением ОС семейства Linux на новую версию:

1. Выполните Шаг 1 инструкции по локальной установке (см. "Установка Агентов Device Monitor").
2. Перейдите в директорию, в которую 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*`

Важно!

Для корректной блокировки съемных устройств после обновления Агента на ОС семейства Linux обязательно перезагрузите рабочую станцию.

При обновлении Агента 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.

Примечание:

При обновлении Агента на ОС Windows 7 и Windows 2008 R2 Server следует учесть, что:

Если компонент Контроль сетевых соединений был установлен ранее, при обновлении Агента он будет удален. При необходимости, данный компонент возможно 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.

7 Удаление InfoWatch Device Monitor

> **Важно!**
>
> Если вы планируете вновь устанавливать сервер Device Monitor, то для обеспечения Агентам Device Monitor возможности подключаться и привязываться к новому серверу, начиная с версии 6.0, рекомендуется сохранить ключ шифрования старого сервера.
>
> Ключ шифрования хранится в папке установки сервера InfoWatch Device Monitor, файл `SSLServerKey.pfx`.

Чтобы удалить серверную часть InfoWatch Device Monitor вместе с Консолью управления и Сервисом распространения дистрибутивов:

1. Выполните одно из следующих действий:
   - На диске с дистрибутивом системы откройте каталог `Setup\Unified`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   - В оснастке **Добавить или удалить программы** (**Add or remove programs**), входящей в состав операционной системы Windows, выберите **InfoWatch Device Monitor Server** и нажмите на кнопку **Изменить** (**Change**).
2. В окне **Изменение, восстановление или удаление...** выберите команду **Удалить**.
3. Если вы хотите удалить систему вместе с базой данных, в окне **Удаление базы данных...** отметьте поле **Удалить базу**. В этом случае вам потребуется задать параметры удаления; параметры зависят от вида используемой СУБД:
   - **Microsoft SQL Server** – укажите используемый способ аутентификации, выбрав нужный вариант на панели **Способ аутентификации** (см. также "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server"). Если аутентификация выполнялась средствами SQL-сервера (**Встроенная в SQL Server**), то на панели **Администратор базы данных**, в полях **Имя пользователя** и **Пароль** укажите параметры той учетной записи, при помощи которой осуществлялось подключение к базе данных.
   - **Oracle** – в поле **Пароль учетной записи SYSTEM** укажите необходимый пароль. В результате будет удалена учетная запись владельца схемы базы данных, а также все объекты, за исключением табличного пространства.
   - **PostgreSQL** – в полях **Имя пользователя** и **Пароль** укажите имя и пароль учетной записи, от имени которой была создана эта БД при установке сервера (см. "Порядок установки серверной части InfoWatch Device Monitor").

     > **Важно!**
     >
     > Если БД не функционирует или ограниченно функционирует, то для удаления InfoWatch Device Monitor рекомендуется снять отметку с поля **Удалить базу**, иначе удаление может произойти не полностью.

4. После того как необходимые параметры будут заданы, нажмите **Далее**, а затем – **Удалить**, чтобы запустить процесс удаления.

Чтобы удалить серверную часть InfoWatch Device Monitor, или Консоль управления, или Сервис распространения дистрибутивов отдельно:

1. В оснастке **Добавить или удалить программы** (**Add or remove programs**) воспользуйтесь кнопкой **Изменить** (**Change**).
2. В окне **Выборочная установка** нажмите  слева от компонента, который вы намерены удалить, и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**. Нажмите **Далее**.
3. Если на предыдущем шаге вы выбрали для удаления сервер, то в окне **Удаление базы данных...** определите необходимость удаления базы данных и при необходимости задайте параметры учетной записи, имеющей на это права (подробнее см. выше).
4. Нажмите **Изменить**, чтобы запустить процесс удаления.

Важно!

В результате удаления Сервиса распространения дистрибутивов будет удалена зарегистрированная в Системе точка распространения и директория со всеми размещенными в ней дистрибутивами.

Чтобы удалить Агент InfoWatch Device Monitor на компьютере, где он установлен, в оснастке **Добавить или удалить программы** (**Add or remove programs**) выберите **InfoWatch Device Monitor Client** и воспользуйтесь кнопкой **Удалить** (**Remove**).

Чтобы удалить Агент InfoWatch Device Monitor на ОС Astra Linux, РЕД ОС и Альт Рабочая станция:

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

Удаление Агентов можно также выполнять централизованно:

- с помощью средств Active Directory (если Агенты были установлены при помощи средств распространения программного обеспечения), как описано в статье "Удаление Агента, установленного с помощью средств распространения программного обеспечения".
- с помощью задач распространения в Консоли управления (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Удаленная установка, обновление и удаление Агентов").

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.

7.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения

Агенты, установленные с помощью средств распространения программного обеспечения, могут быть удалены тем же способом.

Например, если установка Агентов была выполнена через Microsoft Active Directory, то администратор корпоративной сети может удалить назначенное задание на установку из соответствующей групповой политики. Порядок редактирования групповой политики описывается в статье "Установка Агента с помощью средств распространения программного обеспечения", шаг 3.

Чтобы удалить Агент со всех контролируемых компьютеров:

1. Выделите задание на установку, которое нужно удалить. Затем щелкните правой кнопкой мыши по выделенной строке и в раскрывшемся контекстном меню выберите пункт **All tasks** > **Remove**.
2. В открывшемся диалоговом окне **Remove software** выберите **Immediately uninstall thesoftware from users and computers**.

   > **Примечание.**
   >
   > Если будет выбрано другое действие, то задание на установку будет удалено, но все ранее установленные Агенты останутся. Удаление этих Агентов средствами Microsoft Active Directory в дальнейшем будет невозможно.

3. Нажмите **OK**. Агент будет удален со всех компьютеров, на которые распространяется выбранная групповая политика.

Удалить Агент InfoWatch Device Monitor, установленный на ОС Astra Linux, РЕД ОС или Альт Рабочая станция, можно несколькими способами:

- Локально, при это также необходимо отдельно удалить средство распространения. Для этого выполните команды:
  - На ОС Astra Linux:
    ```
    dpkg --purge iwdm
    dpkg --purge iwdeployagent
    ```
  - На РЕД ОС и Альт Рабочая станция:
    ```
    rpm -e iwdm
    rpm -e iwdeployagent
    ```
- Предварительно обновить Агент через задачу первичного распространения и после этого запустить задачу на удаление продукта.

8 Приложение А. Рекомендации по составлению имен и паролей

Требования к именам пользователей

- Длина имени пользователя может составлять от 1 до 20 символов.
- Имя пользователя может состоять из букв латинского алфавита, цифр и символа подчеркивания «_». Должно начинаться с буквы.

Требования к паролям пользователей

- Длина пароля может составлять от 8 до 128 символов.
- Пароль пользователя может состоять из символов, соответствующих трем из следующих четырех категорий:

1. Прописные буквы латинского алфавита (A-Z)
2. Строчные буквы латинского алфавита (a-z)
3. Арабские цифры (0-9)
4. Символы: «#», «$», «!» или «%»

- Пароль не должен содержать имя пользователя или его часть.
- Пароль чувствителен к регистру символов.

Требование к паролям пользователей БД

- Пароль не должен содержать символы «"» и «'».

Рекомендации по составлению надежных паролей

- Рекомендуемая длина пароля: от 10 до 30 символов.
- Пароль должен представлять собой смешанный набор букв верхнего и нижнего регистров, цифр и символов.
- Не рекомендуется:
    - включать в состав пароля слова и словосочетания;
    - включать в состав пароля несколько идущих подряд одинаковых символов;
    - начинать и заканчивать пароль одним и тем же символом;
    - создавать новый пароль путем добавления символов к текущему паролю.

Общие рекомендации
Не рекомендуется начинать имена и пароли пользователей с последовательностей: SYS_ и ORA_.
В составе имени и пароля пользователя не рекомендуется использовать зарезервированные слова СУБД Oracle:

ACCESS	EXCLUSIVE	MODE	SELECT
ADD	EXISTS	MODIFY	SESSION
ALL	FILE	NOAUDIT	SET
ALTER	FLOAT	NOCOMPRESS	SHARE
AND	FOR	NOT	SIZE
ANY	FROM	NOWAIT	SMALLINT

AS	GRANT	NULL	START
ASC	GROUP	NUMBER	SUCCESSFUL
AUDITBETWEEN	HAVING	OF	SYNONYM
BY	IDENTIFIED	OFFLINE	SYSDATE
CHAR	IMMEDIATE	ON	TABLE
CHECK	IN	ONLINE	THEN
CLUSTER	INCREMENT	OPTION	TO
COLUMN	INDEX	OR	TRIGGER
COMMENT	INITIAL	ORDER	UID
COMPRESS	INSERT	PCTFREE	UNION
CONNECT	INTEGER	PRIOR	UNIQUE
CREATE	INTERSECT	PRIVILEGES	UPDATE
CURRENT	INTO	PUBLIC	USER
DATE	IS	RAW	VALIDATE
DECIMAL	LEVEL	RENAME	VALUES
DEFAULT	LIKE	RESOURCE	VARCHAR
DELETE	LOCK	REVOKE	VARCHAR2
DESC	LONG	ROW	VIEW
DISTINCT	MAXEXTENTS	ROWID	WHENEVER
DROP	MINUS	ROWNUM	WHERE
ELSE	MLSLABEL	ROWS	WITH

9 Настройка сетевых правил доступа

Для корректной работы Системы должны быть разрешены соединения:

Компонент Системы, для работы которого необходимо соединение	Взаимодействие между компонентами		Порт	Назначение порта	
	Источник	**Получатель**			
Сервер Device Monitor (DM)	Консоль управления DM	Сервер DM	TCP 15003	Взаимодействие сервера DM с Консолью управления DM	
	Агент DM	Сервер DM	TCP 15004	Защищенное соединение Сервера DM с Агентами	Передача теневых копий (шифрованный канал)
	Агент DM	Сервер DM	UDP 15100		Уведомление Агентов
	Сервер DM	Агент DM			
	Агент DM	Сервер DM	TCP 15101		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	
Агент DM на ОС семейства Linux	Сервер DM	Рабочая станция	TCP 22	Установка Агента	
Агент DM на ОС Windows	Сервер DM	Агент DM	TCP 135	Установка Агента	Локатор удаленного вызова процедур (RPC)
	Сервер DM	Агент DM	UDP 137		Сервис регистрации и преобразования имен NetBIOS Name
	Сервер DM	Агент DM	UDP 138		Сервис распространения для связи без установления соединения NetBIOS Datagram

	Сервер DM	Агент DM	TCP 139		Служба сеансов для связи с установлением соединения NetBIOS Session
	Сервер DM	Агент DM	TCP 445		Обмен необходимыми в процессе установки Агента файлами по протоколу SMB
	Агент DM	Сервер DM			
	Сервер DM	Агент DM	TCP 593		HTTP в качестве транспорта RPC (RPC-over-HTTP)
	Агент DM	Сервер DM	TCP 15506	Сбор логов, запуск и остановка Агентов	

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 через диспетчер задач или выполнив команду в cmd:
`net 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. Чтобы изменить порт подключения консоли управления (TCP 15003), в файле `C:\Program Files\InfoWatch\Device Monitor\Server\InfoWatch.DeviceMonitor.Server.exe.config` отредактируйте значение параметра `RemotingPort`.
d. Включите службу Сервера DM через диспетчер задач или выполнив команду в cmd:
`net start iwdms`