INFOWATCH

InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию

InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию

© АО “ИнфоВотч”
Тел./Факс +7 (495) 229-00-22
http://www.infowatch.com
Дата редакции: 2016-08-08

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 4

2 ОБЗОР DEVICELOCK ADAPTER 5

2.1 Схема работы InfoWatch DeviceLock Adapter 5
2.2 Состав InfoWatch DeviceLock Adapter 6

3 ПОДГОТОВКА К УСТАНОВКЕ DEVICELOCK ADAPTER 7

3.1 Требования к аппаратному и программному обеспечению DeviceLock Adapter 7
3.2 Варианты установки DeviceLock Adapter 7
3.3 Подготовка учетных записей DeviceLock Adapter 9
3.3.1 Подготовка учетной записи для работы службы DeviceLock Adapter 9

4 УСТАНОВКА DEVICELOCK ADAPTER 11

4.1 Шаг 1. Начало установки Device Lock Adapter 11
4.2 Шаг 2. Выбор каталога для установки Device Lock Adapter 11
4.3 Шаг 3. Выбор типа установки компонентов Device Lock Adapter 12
4.4 Шаг 4. Настройка рабочих параметров Device Lock Adapter 12
4.5 Шаг 5. Настройка параметров соединения с сервером DeviceLock 14
4.6 Шаг 6. Настройка соединения Device Lock Adapter с InfoWatch Traffic Monitor 15
4.7 Шаг 7. Подтверждение установки Device Lock Adapter 17
4.8 Шаг 8. Завершение установки Device Lock Adapter 17

5 НАСТРОЙКА DEVICELOCK ADAPTER 18

5.1 Описание конфигурационных разделов 18
5.1.1 Раздел <applicationSettings> 18
5.1.2 Раздел <TMConnector> 19
5.1.2.1 Элемент <EventFilter> 22
5.1.2.2 Элемент <DeviceLockServers> 22
5.1.3 Раздел <system.diagnostics> 22
5.1.3.1 Элемент <trace> 23
5.1.3.2 Элемент <sources> 23
5.1.3.3 Элемент <switches> 24
5.2 Настройка уровня протоколирования 25

6 МОНИТОРИНГ DEVICELOCK ADAPTER 26

6.1 Журнал приложений Windows 26
6.2 Счетчики производительности Windows 26

7 УДАЛЕНИЕ INFOWATCH DEVICELOCK ADAPTER 28

7.1 Глоссарий 28

1 ВВЕДЕНИЕ

InfoWatch DeviceLock Adapter – служба, осуществляющая передачу теневых копий текстов и файлов, получаемых с помощью системы DeviceLock 6.3, в систему InfoWatch Traffic Monitor версии 6.x.
В настоящем руководстве вы можете найти сведения по установке, администрированию и удалению InfoWatch DeviceLock Adapter.
В настоящем руководстве не рассматриваются вопросы установки и настройки сервера DeviceLock. За получением необходимых сведений вы можете обратиться к соответствующей документации. Официальный сайт производителя DeviceLock: http://www.devicelock.com/ru/.

Аудитория

Информация, содержащаяся в руководстве, предназначена для пользователей, выполняющих установку InfoWatch DeviceLock Adapter.
Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

2 ОБЗОР DEVICELOCK ADAPTER

В этой главе содержится следующая информация:

- Схема работы InfoWatch DeviceLock Adapter;
- Состав InfoWatch DeviceLock Adapter.

2.1 Схема работы InfoWatch DeviceLock Adapter

На рисунке 1 показан принцип работы InfoWatch DeviceLock Adapter.

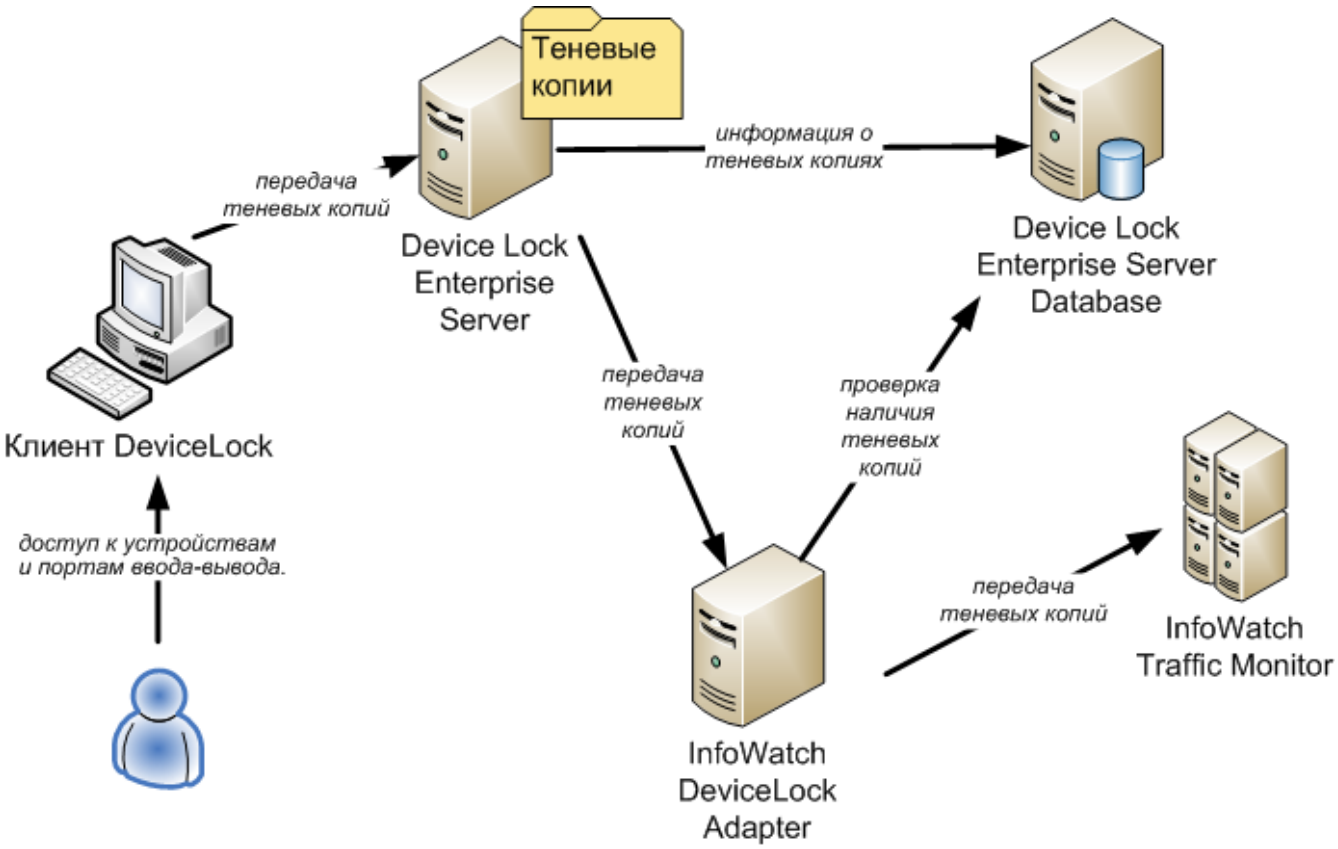


Рисунок 1. Принцип работы InfoWatch DeviceLock Adapter

InfoWatch DeviceLock Adapter работает следующим образом:

1. Подключается к базе данных DeviceLock Enterprise Server, которая содержит информацию о расположении теневой копии (это может быть сама база данных или локальная папка сервера Device Lock C:\Windows\DLSTORE).

2. Проверяет хранилище на наличие теневых копий, удовлетворяющих заданным критериям таким как:
    - размер файла не меньше минимального и не больше максимального;
    - тип (сигнатура) файла есть в списке сигнатур, заданном в конфигурации адаптера;
    - дата снятия теневой копии позднее, чем заданная в конфигурации адаптера.
3. Отправляет найденные теневые копии на Traffic Monitor.
4. Ведет учет идентификаторов отправленных копий во избежание повторной отправки.

2.2 Состав InfoWatch DeviceLock Adapter

Компоненты, входящие в состав InfoWatch DeviceLock Adapter, перечислены в таблице 1.
Таблица 1. Компоненты InfoWatch DeviceLock Adapter

Компонент	**Назначение**	**Имя файла**
Database provider	Библиотека, обеспечивающая работу с БД.	`InfoWatch.DeviceMonitor.Database.Core.dll`
Service Core	Общие компоненты службы InfoWatch DeviceLock Adapter (осуществление бизнес-логики работы с DeviceLock Enterprise Server и вспомогательные компоненты).	`InfoWatch.DeviceLockAdapter.Service.Core.dll`
InfoWatch Traffic Monitor Connector	Обеспечение взаимодействия с InfoWatch Traffic Monitor.	`InfoWatch.DeviceLockAdapter.Service.Connector.dll`
File type detector	Обеспечение детектирования типов файлов.	`InfoWatch.DeviceLockAdapter.Core.FileType.dll`
Encoding detector	Обеспечение детектирования кодировок текстовых файлов.	`EncodingTools.dll.`
Service	Исполняемый файл службы Windows.	`InfoWatch.DeviceLockAdapter.exe`
Service Configuration File	Конфигурационный файл службы DeviceLock Adapter.	`InfoWatch.DeviceLockAdapter.exe.config`

3 ПОДГОТОВКА К УСТАНОВКЕ DEVICELOCK ADAPTER

В этой главе содержится следующая информация:

- Требования к аппаратному и программному обеспечению DeviceLock Adapter;
- Варианты установки DeviceLock Adapter;
- Подготовка учетных записей DeviceLock Adapter.

3.1 Требования к аппаратному и программному обеспечению DeviceLock Adapter

Требования к аппаратному обеспечению, необходимому для работы InfoWatch DeviceLock Adapter, перечислены в таблице 2.

Таблица 2. Аппаратное обеспечение InfoWatch DeviceLock Adapter

Оборудование	**Минимальные требования**
Процессор	Pentium 4 с частотой 3 ГГц
Оперативная память	1 Гб
Сетевая карта	100/1000 Мбит/с

Требования к программному обеспечению:

- операционная система Microsoft Windows 2003 Server Service Pack 1 и выше;
- Microsoft .NET Framework 3.0.

3.2 Варианты установки DeviceLock Adapter

При установке InfoWatch DeviceLock Adapter вам потребуется указать

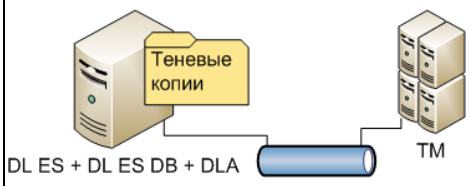
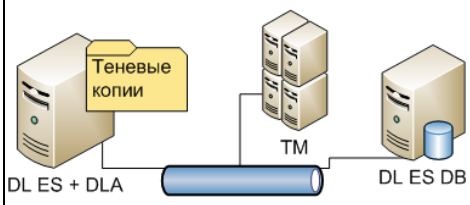
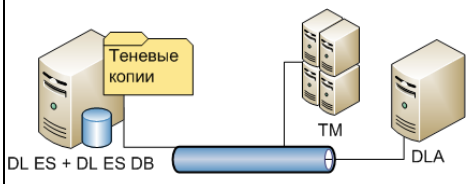
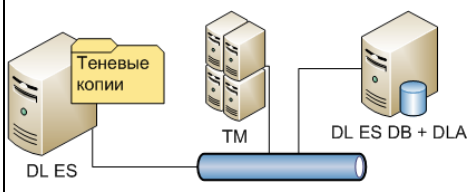
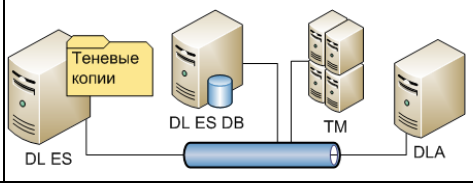
- Учетную запись, под которой будет работать служба DLA (локальная учетная запись или специально созданная учетная запись – см. статью "Подготовка учетной записи для работы службы DeviceLock Adapter");
- Способ авторизации на сервере MS SQL, где работает база данных DeviceLock Enterprise Server (авторизация в Windows или встроенная учетная запись SQL Server).

8

Способ авторизации на сервере, где работает БД DL ES, определяется параметрами учетной записи службы DLA. Авторизацию в Windows вы можете использовать в двух случаях: если служба DLA будет работать под специально созданной учетной записью; а также если служба DLA устанавливается на тот же компьютер, где расположена БД DL ES. Во всех остальных случаях вам необходимо указывать параметры учетной записи SQL Server с ролью **db_owner**.

Возможности выбора параметров учетной записи службы DLA зависят от того, где DeviceLock Enterprise Server хранит теневые копии, и куда будет устанавливаться сама служба DLA. Ниже рассмотрены различные варианты расположения этих объектов и описаны соответствующие им параметры установки.

Приведенные варианты описаны с учетом того, что теневые копии хранятся в файловой системе компьютера, на котором работает DeviceLock Enterprise Server. Это стандартная настройка, рекомендованная для DeviceLock. Если в вашей системе теневые файлы хранятся в другом месте, учитывайте это при выборе варианта и определении настроек установки службы DeviceLock Adapter.

Сервер, куда устанавливается DeviceLock Adapter	**Схема расположения серверов DLA, TM, DL ES и DL ES DB**	**Параметры установки**
Тот же, где хранятся теневые копии и находится БД DL ES		Служба DLA **может** работать под учетной записью локальной системы.
Тот же, где хранятся теневые копии. При этом БД DeviceLock находится на другом сервере		Служба DLA **может** работать под учетной записью локальной системы.
Отличный от того, где хранятся теневые копии и работает БД DeviceLock		Служба DLA **не может** работать под учетной записью локальной системы.
Тот же, где находится БД DL ES, теневые копии хранятся на другом сервере		Служба DLA **не может** работать под учетной записью локальной системы.
InfoWatch DeviceLock Adapter и БД DeviceLock находятся на разных серверах, теневые копии хранятся на третьем сервере.		Служба DLA **не может** работать под учетной записью локальной системы.

3.3 Подготовка учетных записей DeviceLock Adapter

При установке InfoWatch DeviceLock Adapter необходимо определить учетные записи, с помощью которых будет работать служба DLA и производиться соединение с базой данных DeviceLock Enterprise Server. В зависимости от варианта установки (см. статью "Варианты установки DeviceLock Adapter") вы можете выбрать следующие варианты:

- **Служба DLA будет работать под учетной записью локальной системы, при доступе к БД DL ES будет использоваться авторизация в Windows** – это возможно только если служба DLA запускается на том же компьютере, где расположена БД DL ES. При этом никаких дополнительных учетных записей подготавливать не требуется.
- **Служба DLA будет работать под учетной записью локальной системы, при авторизации в БД DL ES будет использоваться запись SQL Server** – необходимо подготовить встроенную запись SQL сервера, назначив ей роль **db_owner**.
- **Служба DLA не может работать под учетной записью локальной системы, при доступе к БД DL ES будет использоваться авторизация в Windows** – вы можете выбрать один из вариантов:

- подготовить специальную учетную запись домена Windows (см. статью "Подготовка учетной записи для работы службы DeviceLock Adapter"), назначив ей роль **db_owner**.

- в качестве учетной записи службы указать уже существующую учетную запись с правами на базу данных DL ES (например, использовавшуюся при установке DL ES), подготовив ее так, как описано в статье "Подготовка учетной записи для работы службы DeviceLock Adapter".

- **Служба DLA не может работать под учетной записью локальной системы, при авторизации в БД DL ES будет использоваться учетная запись SQLServer** – необходимо подготовить две записи: учетную запись домена Windows (см. статью "Подготовка учетной записи для работы службы DeviceLock Adapter") и встроенную запись SQL сервера, назначив ей роль **db_owner**.

3.3.1 Подготовка учетной записи для работы службы DeviceLock Adapter

Если работа InfoWatch DeviceLock Adapter под учетной записью локальной системы невозможна, то необходимо заранее подготовить специальную учетную запись домена Windows, под которой будет работать служба InfoWatch DeviceLock Adapter.

Чтобы подготовить учетную запись домена Windows для службы InfoWatch DeviceLock Adapter, выполните следующие действия:

1. Создайте учетную запись домена Windows.
2. Предоставьте этой записи права администратора на DeviceLock Enterprise Server.
3. Разрешите подготовленной учетной записи запускать процесс как службу:
    - 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.

4. Включите созданную запись в состав учетных записей БД DeviceLock Enterprise Server.
5. Если соединение с БД DL ES будет производиться с помощью авторизации Windows, то назначьте подготовленной записи роль базы данных DL ES **db_owner**.

4 УСТАНОВКА DEVICELOCK ADAPTER

Установка DeviceLock Adapter происходит в следующем порядке.

4.1 Шаг 1. Начало установки Device Lock Adapter

Важно!

Пользователь, выполняющий установку, должен обладать на данном компьютере правами администратора.

На диске с дистрибутивом найдите и запустите файл `Setup.Service.ru.msi` (для русскоязычного интерфейса мастера установки) или `Setup.Service.en.msi` (для англоязычного интерфейса мастера установки).

После этого на экран будет выведено окно приветствия мастера установки.

Нажмите кнопку **Далее**.

4.2 Шаг 2. Выбор каталога для установки Device Lock Adapter

Так как InfoWatch DeviceLock Adapter реализован в виде службы, то он устанавливается в общую папку `C:\Program Files\InfoWatch\DeviceLock Adapter\Service` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\DeviceLock Adapter\Service` для 64-битных систем. InfoWatch DeviceLock Adapter доступен для всех пользователей того компьютера, на который производится установка. Изменить папку установки вы сможете на следующем шаге.

Нажмите кнопку **Далее**.

4.3 Шаг 3. Выбор типа установки компонентов Device Lock Adapter

На данном шаге необходимо выбрать тип установки InfoWatch DeviceLock Adapter (см. рис. 2).

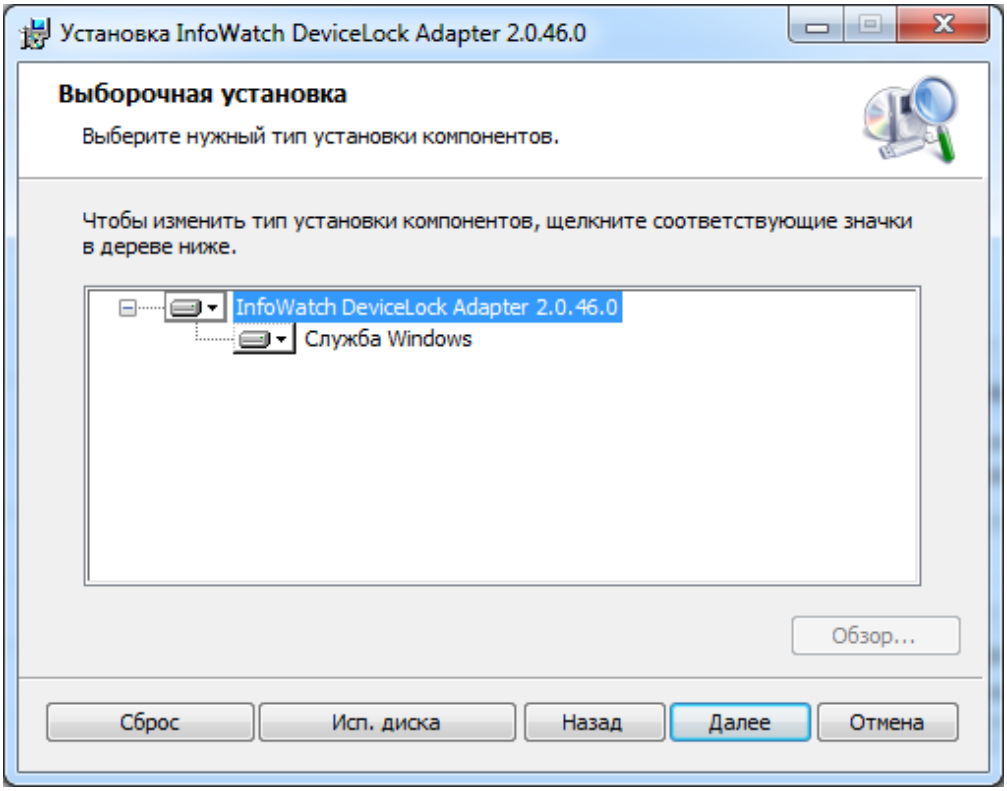


Рисунок 2. Выбор типа установки компонентов Device Lock Adapter

Чтобы изменить папку, в которую будет произведена установка, в дереве компонентов выберите **Служба Windows** и нажмите **Обзор**. В открывшемся окне укажите папку установки.

Нажмите кнопку **Далее**.

4.4 Шаг 4. Настройка рабочих параметров Device Lock Adapter

На данном шаге необходимо настроить основные параметры работы InfoWatch DeviceLock Adapter (см. рис. 3).

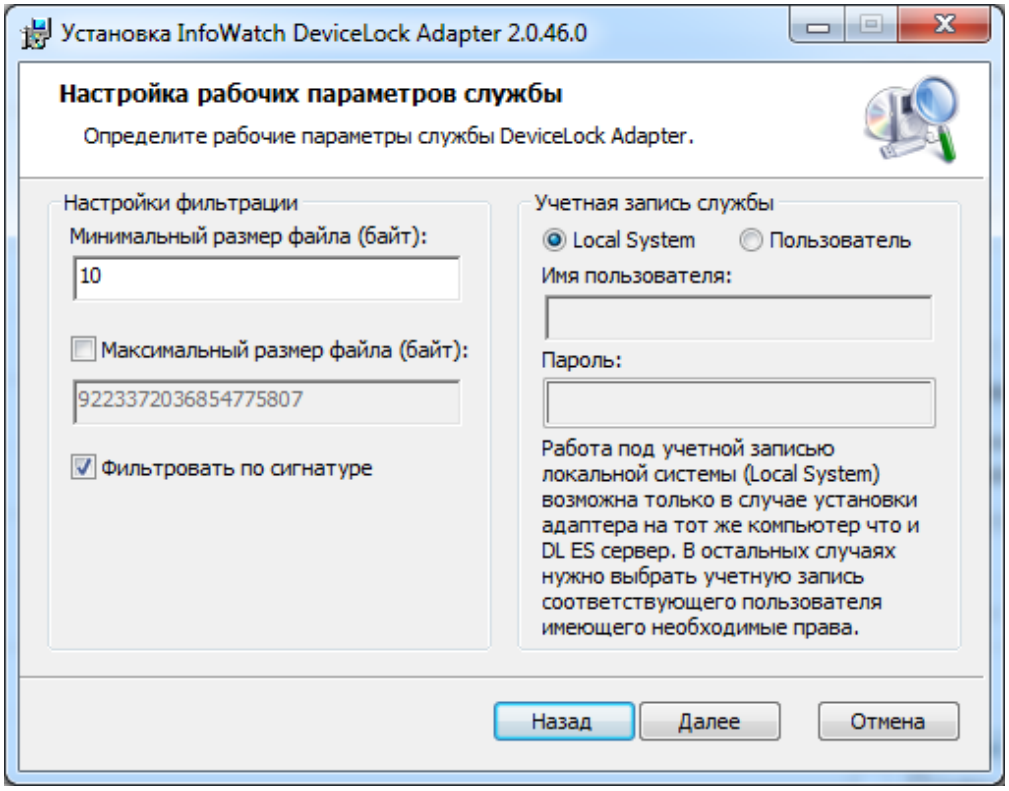


Рисунок 3. Настройка рабочих параметров

Укажите настройки фильтрации:

- **Минимальный размер файла (байт)** — определяет минимальный размер файла, отправляемого в InfoWatch Traffic Monitor, в байтах. Файлы меньше этого размера отправляться не будут. Допустимые значения от 0 до 9223372036854775806. Значение по умолчанию 10.
- **Максимальный размер файла (байт)** — определяет максимальный размер файла, отправляемого в InfoWatch Traffic Monitor. Файлы больше этого размера отправляться не будут. Допустимые значения от 1 до 9223372036854775807. Значение по умолчанию 9223372036854775807.
- **Фильтровать по сигнатуре** — определяет, производить ли фильтрацию файлов, отправляемых в InfoWatch Traffic Monitor, по их типу (сигнатуре). Если файл не попадает ни под одну из представленных сигнатур — его отправка не производится (файл отфильтровывается).

Примечание:

Переопределить настройки фильтрации, а также изменить список сигнатур файлов можно при настройке InfoWatch DeviceLock Adapter, в элементе конфигурационного файла <EventFilter>: см. статью "Элемент <EventFilter>".

Выберите учетную запись службы с учетом варианта установки InfoWatch DeviceLock Adapter по отношению к месту хранения теневых файлов (см. статью "Варианты установки DeviceLock Adapter"):

- для работы службы под учетной записью локальной системы выберите **Local System**;

- для работы под другой учетной записью выберите **Пользователь** и укажите **Имя пользователя** и **Пароль** учетной записи, подготовленной как описано в статье "Подготовка учетных записей DeviceLock Adapter".

Нажмите кнопку **Далее**.

4.5 Шаг 5. Настройка параметров соединения с сервером DeviceLock

На данном шаге необходимо настроить параметры соединения с сервером DeviceLock (см. рис. 4).

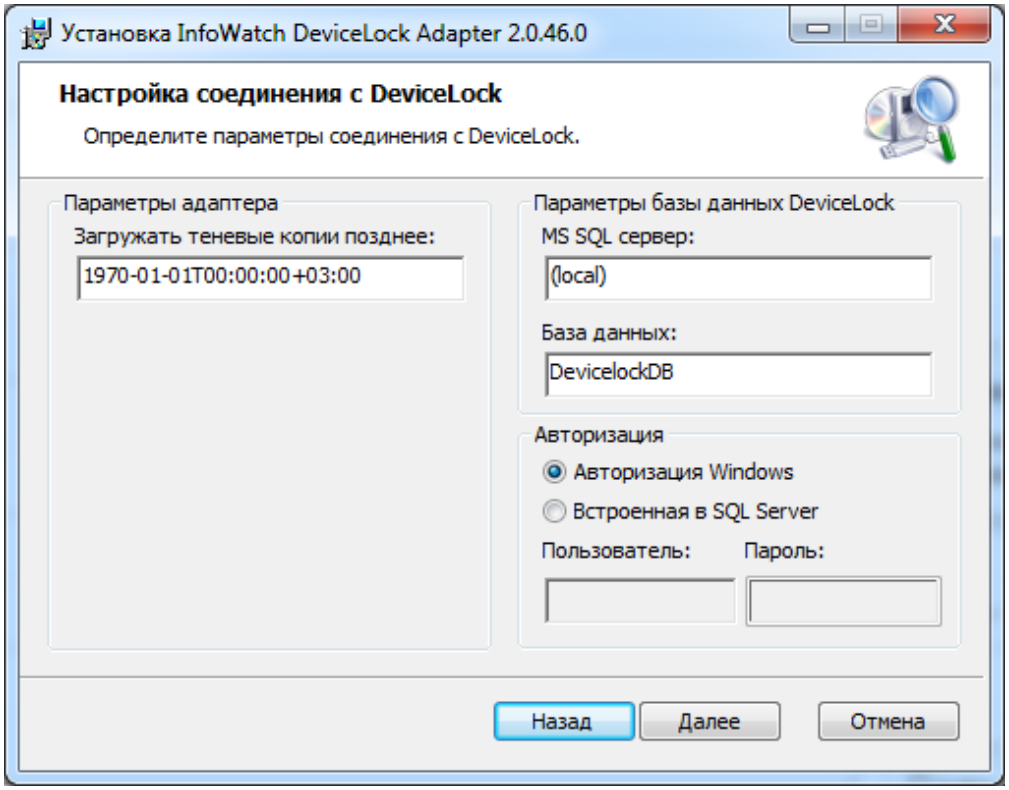


Рисунок 4. Настройка параметров соединения с сервером DeviceLock

Укажите параметры адаптера:

- **Загружать теневые копии позднее** — определяет начальную дату и время создания теневых копий. Т.е. все теневые копии, полученные позднее этой даты, должны отправляться в InfoWatch Traffic Monitor. Более ранние копии отправляться не будут. Формат даты: ГГГГ-ММ-ДДТЧЧ:ММ:СС+ЧЧ:ММ, например: 1970-01-01T00:00:00+03:00 — 1-е января 1970 года, полночь; время по Гринвичу плюс три часа (московское время).

Укажите параметры базы данных:

- **MS SQL сервер** — NetBIOS имя сервера СУБД Microsoft SQL Server, где расположена база данных DeviceLock; или NetBIOS\<имя экземпляра>, если этот сервер имеет именованные экземпляры;
- **База данных** — имя базы данных DeviceLock.

Выберите параметры авторизации:

- **Авторизация в Windows** — авторизация в DeviceLock Enterprise Server выполняется с использованием учетных записей, принадлежащих к домену Windows.

> **Примечание:**
>
> Вы не можете выбрать этот вариант, если на шаге 4 выбрали в качестве учетной записи службы **Local System**, кроме того случая, когда служба DLA запускается на том же компьютере, где расположена БД DL ES.

- **Встроенная в SQL Server** — при авторизации в DeviceLock Enterprise Server используются учетные записи СУБД Microsoft SQL Server. Для этого типа авторизации укажите имя пользователя и пароль встроенной запись SQL сервера, которой назначена роль **db_owner**.

> **Примечание:**
>
> Если требуется, чтобы DeviceLock Adapter поддерживал работу одновременно с несколькими серверами DeviceLock, то дополнительные сервера и их параметры можно указать при настройке InfoWatch DeviceLock Adapter, в элементе конфигурационного файла <DeviceLockServers>: см. раздел "Элемент <DeviceLockServers>".

Нажмите кнопку **Далее**.

4.6 Шаг 6. Настройка соединения Device Lock Adapter с InfoWatch Traffic Monitor

На данном шаге необходимо настроить параметры соединения с сервером InfoWatch Traffic Monitor (см. рис. 5).

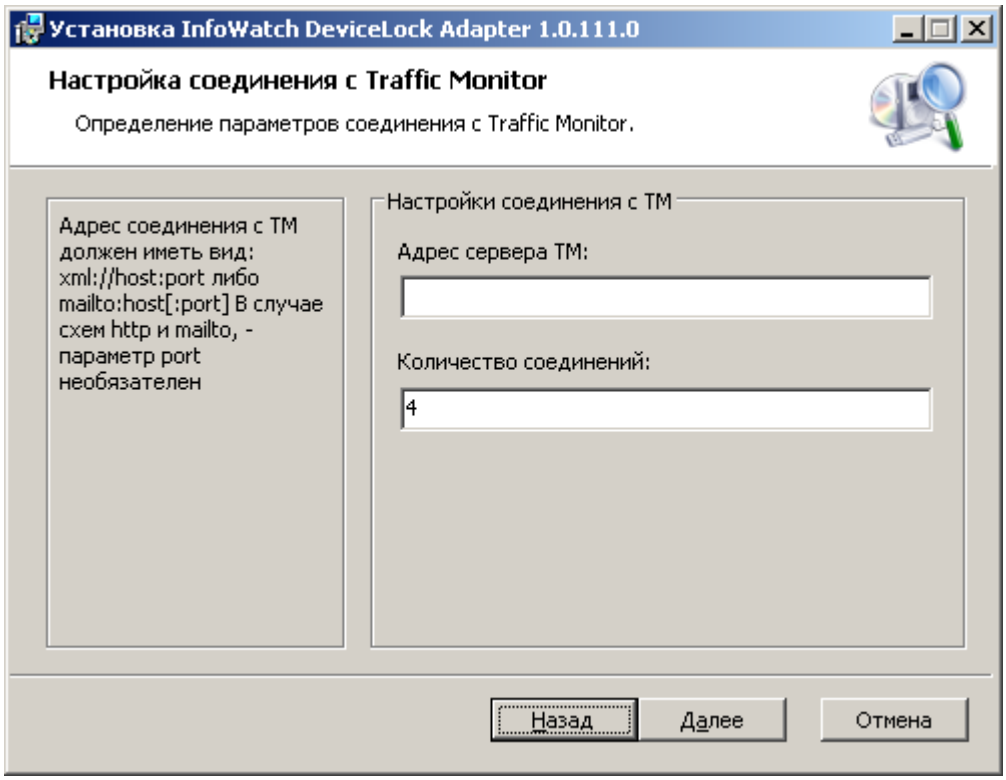


Рисунок 5. Настройка соединения с InfoWatch Traffic Monitor

Укажите параметры для взаимодействия с сервером InfoWatch Traffic Monitor:

- **Адрес сервера ТМ**. Адрес сервера InfoWatch Traffic Monitor.
  Для InfoWatch Traffic Monitor версии 2.x взаимодействие осуществляется по *mailto (smtp)* схеме. Формат записи адреса – mailto:host[:port], где host — доменное имя или IP-адрес сервера InfoWatch Traffic Monitor, а port — порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий. Если порт не задан явно, то по умолчанию используется порт 25.
  Для InfoWatch Traffic Monitor версии 3.x взаимодействие осуществляется по *xml* схеме. Формат записи адреса – xml://host:port, где *host* — доменное имя или IP-адрес сервера InfoWatch Traffic Monitor, а *port* — порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий (для ТМ 3.x этот порт обычно имеет значение 4101). Оба параметра записи являются обязательными.

- **Количество соединений**. Количество соединений с сервером InfoWatch Traffic Monitor. Вы можете задать от 1 до 32 соединений.

Нажмите кнопку **Далее**.

Если, задавая адрес соединения с InfoWatch Traffic Monitor, вы указали SMTP-схему (то есть настраивается соединение с InfoWatch Traffic Monitor версии 2.x), то вам необходимо выполнить дополнительный шаг установки, определив параметры почтового транспорта (см. рис 6).

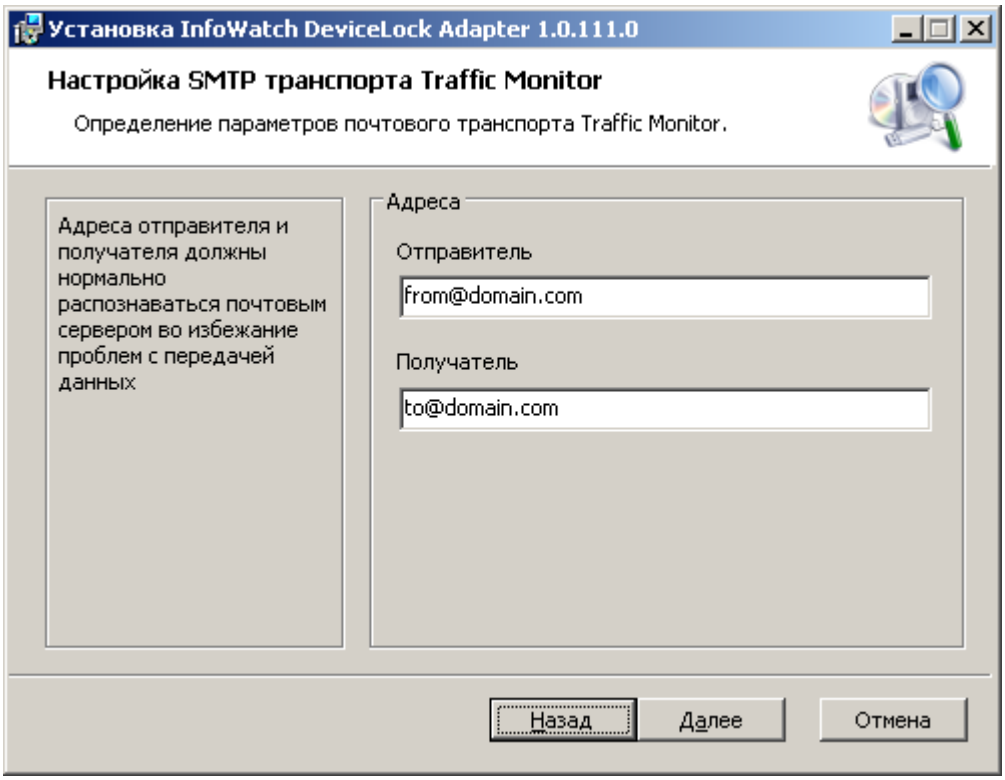


Рисунок 6. Настройка SMTP транспорта InfoWatch Traffic Monitor

Укажите адреса:

- **Отправитель** – адрес отправителя сообщения;
- **Получатель** – адрес получателя сообщения.

Нажмите кнопку **Далее**.

4.7 Шаг 7. Подтверждение установки Device Lock Adapter

Подтвердите правильность указанных на предыдущих шагах параметров установки, нажав кнопку **Далее**.

4.8 Шаг 8. Завершение установки Device Lock Adapter

После успешного завершения установки InfoWatch DeviceLock Adapter мастер установки отобразит окно с уведомлением.

Нажмите кнопку **Готово**.

5 НАСТРОЙКА DEVICELOCK ADAPTER

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

Примечание:

По умолчанию после установки Сервер расположен в каталоге `C:\Program Files\InfoWatch\DeviceLock Adapter\Service`.

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

В этой главе содержится следующая информация:

- Описание конфигурационных разделов;
- Настройка уровня протоколирования.

5.1 Описание конфигурационных разделов

Раздел содержит описание конфигурационных разделов:

- Раздел <applicationSettings>;
- Раздел <TMConnector>;
- Раздел <system.diagnostics>;

5.1.1 Раздел <applicationSettings>

Данный раздел состоит из двух подразделов, определяющих настройки компонентов InfoWatch DeviceLock Adapter:

- `<InfoWatch.DeviceLockAdapter.Service.Connector.Properties.Settings>` — базовые настройки коннектора Traffic Monitor Server.
- `<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>` — настройки низкоуровневого драйвера базы данных.

Эти подразделы имеют одинаковую структуру – состоят из набора элементов `<setting>`, предназначенных для настройки параметров компонента. Каждый элемент `<setting>` имеет следующие атрибуты:

- `name` — имя параметра;

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

Значения параметров компонента определяются дочерним элементом <value>. Например:

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

Описание параметров для каждого компонента приводится в таблице.

Таблица 2. Параметры раздела <applicationSettings>

Имя параметра	Описание, возможные значения
<InfoWatch.DeviceLockAdapter.Service.Connector.Properties.Settings>	
DBPollTime	Период (в миллисекундах) опроса базы данных, в процессе которого проверяется наличие событий в базе данных
CultureName	Язык диагностических и других сообщений компонента. Возможные значения: • ru – русский • en - английский
NumberOfConnections	Количество соединений с InfoWatch Traffic Monitor. Значение по умолчанию 4 Максимальное значение 32
QueueSendLimit	Максимальное количество событий, которые могут быть переданы из базы данных в InfoWatch Traffic Monitor за одну транзакцию. Значение по умолчанию 200
<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>	
CultureName	Язык диагностических и других сообщений компонента. Возможные значения: • ru - русский • en - английский

5.1.2 Раздел <TMConnector>

Раздел предназначен для расширенных настроек коннектора InfoWatch Traffic Monitor. В разделе определяется структура и различные параметры сообщений, отправляемых в InfoWatch Traffic Monitor.

- <TMAddress>. Адрес сервера InfoWatch Traffic Monitor.

Взаимодействие осуществляется по *xml* схеме. Формат параметра - xml://host:port, где *host* — доменное имя или IP-адрес сервера InfoWatch Traffic Monitor, а *port* — порт сервера InfoWatch

Traffic Monitor, через который будет осуществляться доставка событий. Порт по умолчанию: 4101. Раздел определяет следующие параметры:

- <Prefix>. Префикс, который будет добавляться к именам всех атрибутов xml-сообщения.

- <MailHeaderPrefix>. Префикс, который будет добавляться к именам всех заголовков почтового сообщения.
- <UserLogin>. Имя заголовка, в котором будет отправляться информация об учетной записи пользователя (без указания домена).
- <UserDomain>. Имя заголовка, в котором будет отправляться информация об учетной записи пользователя (без указания домена).
- <From>. Адрес отправителя сообщения.
- <To>. Адрес получателя сообщения.
- <SubjectTemplate>. Шаблон темы почтового сообщения. В качестве параметров шаблона можно использовать имена атрибутов из параметров <CommonAttributes> и <ShadowAttributes>.

Параметр задается следующим образом:
$(<имя атрибута>)
Например:
$(Destination)
Вместо параметра $(Destination) будет подставлено имя файла на съемном носителе, в который производилась запись. Имена атрибутов в шаблоне необходимо указывать в точном соответствии с XML-схемой (<Attribute>name).
Например,

```
<SubjectTemplate>DLA. Shadow copy of:
 [$(Destination)] from:
 [$(WorkstationAddress)] account:
 [$(UserAccount)]</SubjectTemplate>
```

В этом шаблоне будет произведена подстановка имени файла, созданного (путем копирования или записи) на съемном носителе. Также здесь содержатся сведения о контролируемой рабочей станции, на которой была перехвачена операция создания файла, и об имени пользователя, выполнившем данную операцию.
В разделе <TMConnector> также определены атрибуты сообщений, отправляемых в InfoWatch Traffic Monitor.

Важно!

Значения атрибутов менять не разрешается.

Атрибуты определены в следующих подразделах:

- <CommonAttributes>. Определение общих атрибутов сообщений, отправляемых в InfoWatch Traffic Monitor. Внутреннее имя атрибута в InfoWatch DeviceLock Adapter определяется элементом name. Значение этого элемента менять не разрешается.
- <ShadowAttributes>. Для событий теневого копирования. Внутреннее имя атрибута в InfoWatch DeviceLock Adapter определяется элементом name. Значение этого элемента менять не разрешается.

Описание параметров приведено в таблице.

Таблица 3. Параметры подразделов <CommonAttributes> и <ShadowAttributes>

Имя параметра	**Описание**
<CommonAttributes>	
Id	Идентификатор события
Interceptor	Перехватчик (в настоящее время только Shadow)
Action	Заблокировано ли событие перехватчиком (Device Lock). Значение по умолчанию: Allowed
EventType	Тип события (в настоящее время ShadowFull — событие с теневой копией)
Operation	Перехваченная операция (запись, печать и т.д.)
ServerName	Имя сервера DL ES
WorkstationAddress	Имя рабочей станции, с которой была снята теневая копия
UserAccount	Учетная запись пользователя, выполнившего перехваченную операцию
Application	Приложение, выполнившее перехваченную операцию
OccurredAt	Дата и время операции
WorkstationDns	DNS-имя рабочей станции
WorkstationIp	IP-адрес рабочей станции
WorkstationType	Тип устройства
<ShadowAttributes>	
DeviceName	Имя устройства
Destination	Имя конечного файла или документа (если речь идет о печати)
Size	Размер теневой копии в байтах
ShadowId	Идентификатор теневой копии в БД DL ES
Direction	Направление операции
ShadowCopy	Наличие теневой копии
DeviceType	Тип устройства

Также в разделе <TMConnector> настраивается фильтрация теневых копий, отправляемых в InfoWatch Traffic Monitor (см. статью "Элемент <EventFilter>") и подключенные к адаптеру серверы DeviceLock (см. статью "Элемент <DeviceLockServers>").

5.1.2.1 Элемент <EventFilter>

Данный элемент содержит определение настроек фильтрации теневых копий, отправляемых в InfoWatch Traffic Monitor.
Элемент содержит атрибут `isFilterBySignatures` определяющий использовать или нет фильтрацию теневых копий по сигнатурам. Значение true включает фильтрацию, `false` выключает.
Элемент содержит следующие дочерние элементы, определяющие настройки фильтрации:

- `<MinFileSizeInBytes>`. Определяет минимальный размер файла, отправляемого в InfoWatch Traffic Monitor, в байтах. Файлы меньше этого размера отправляться не будут. Допустимые значения от 0 до 9223372036854775806. Значение по умолчанию 10.
- `<MaxFileSizeInBytes>`. Определяет максимальный размер файла, отправляемого в InfoWatch Traffic Monitor, в байтах. Файлы больше этого размера отправляться не будут. Допустимые значения от 1 до 9223372036854775807. Значение по умолчанию 9223372036854775807.
- `<AcceptableSignatures>`. Определяет список сигнатур файлов, отправляемых в InfoWatch Traffic Monitor. Если файл не попадает ни под одну из представленных сигнатур, — он не отправляется (отфильтровывается). Элемент содержит дочерние элементы <Signature>, каждая из которых определяет имя сигнатуры.

5.1.2.2 Элемент <DeviceLockServers>

Данный элемент определяет настройки подключения к каждому из серверов DeviceLock, с которыми должен работать InfoWatch DeviceLock Adapter.
Элемент содержит один или несколько дочерних элементов `<Server>`, по одному на каждый из серверов DL ES.
Элемент `<Server>` содержит следующие дочерние элементы, определяющие настройки соединения с БД DL ES:

- `<DBConnectionString>`. Определяет строку соединения с БД в формате ADO.NET для данного экземпляра сервера DeviceLock.

Пример:

```
Data Source=(local);Initial Catalog=DevicelockDB;Integrated Security=True
```

> **Примечание:**
>
> Если несколько серверов DeviceLock работают с одной и той же БД, то InfoWatch DeviceLock Adapter отправляет в InfoWatch Traffic Monitor все копии, записи о которых хранятся в этой БД, независимо от того, с какого сервера DeviceLock они получены и где хранятся.

- `<TransferShadowsLaterThen>`. Определяет начальную дату и время теневых копий. Т.е. все теневые копии, полученные позднее этой даты, должны отправляться в InfoWatch Traffic Monitor. Более ранние копии отправляться не будут. Формат даты: ГГГГ-ММ-ДДТЧЧ:ММ:СС+ЧЧ:ММ, например: 1970-01-01T00:00:00+03:00, — 1-е января 1970 года полночь, время по Гринвичу плюс три часа (московское время)

5.1.3 Раздел <system.diagnostics>

Раздел предназначен для настройки параметров диагностики работы адаптера. Включает в себя следующие элементы:

- `<trace>` — общие настройки диагностики.
- `<sources>` — настройки, необходимые для диагностики отдельных компонентов адаптера.
- `<switches>` — управление уровнем протоколирования диагностической системы в целом. Если для разных компонентов требуются разные настройки протоколирования, то их можно настроить с помощью фильтра в элементе `<sources>`.

5.1.3.1 Элемент <trace>

Используется для описания глобальных настроек диагностики.
Элемент `<trace>` имеет следующие атрибуты:

- `autoflush` — параметр сохранения данных из потока диагностических сообщений на жесткий диск: `true` – данные сохраняются, `false` – сохранение не производится;
- `indentsize` — величина отступов в сообщениях.

5.1.3.2 Элемент <sources>

Используется для настройки отдельных компонентов приложения. Включает в себя дочерние элементы `<source>` – по одному на каждый компонент приложения.
Элемент `<source>` имеет следующие атрибуты:

- `name` — имя компонента;
- `switchName` — имя компонента, определяющего уровень протоколирования диагностических сообщений (детализатора);
- `switchType` — тип компонента, определяющего уровень протоколирования диагностических сообщений. Всегда имеет значение `System.Diagnostics.SourceSwitch`.

В каждом элементе <source> также содержится определение приемников диагностических сообщений (<listeners>). Приемниками диагностических сообщений могут быть:

- журнал приложений Windows (Application log) – является приемником по умолчанию;
- системный отладочный вывод (можно просматривать с помощью специальных инструментов, например DebugView: http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx);
- текстовый файл.

Элемент `<listeners>` может включать в себя следующие дочерние элементы:

- `<remove>` — удаление приемника диагностических сообщений по умолчанию (журнал приложений Windows).

Чтобы исключить журнал приложений Windows из перечня приемников сообщений:
установите имя элемента равным `Default`:

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

- `<add>` — добавление нового приемника диагностических сообщений. Элемент содержит следующие атрибуты:
- `name` — имя приемника диагностических сообщений.
- `type` — полное имя типа приемника диагностических сообщений: из библиотеки классов .NET Framework или собственного типа.

Примечание:

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).

- `initializeData`. Идентификатор компонента адаптера. Как правило, это значение совпадает с именем соответствующего компонента (см. статью "Состав InfoWatch DeviceLock Adapter"). Если в качестве приемника используется журнал приложений Windows, этот идентификатор будет отображаться для событий InfoWatch DeviceLock Adapter в столбце **Source**.

Элемент <add> также содержит фильтр диагностических сообщений. Данный фильтр выводит только те сообщения с уровнем важности, не превышающим заданный в настройках фильтра.

Чтобы определить фильтр диагностических сообщений:
укажите необходимый уровень протоколирования, например:
`<filter type="System.Diagnostics.EventTypeFilter" initializeData="Information"/>`
В приведенном примере будут протоколироваться события с уровнем **Warning**, **Error**, **Critical** и **Information**

Примечание:

Подробнее о настройке уровня протоколирования см. статью "Настройка уровня протоколирования"

5.1.3.3 Элемент <switches>

Определяет глобальный (для всего сервера) уровень протоколирования сообщений диагностической системы. Если отдельным компонентам адаптера требуется более низкий уровень протоколирования, то в этом случае можно воспользоваться фильтром в элементе `<sources>`.
По-умолчанию элемент `<switches>` содержит только один дочерний элемент:
`<add name="eventLog" value="Warning"/>.`
Уровень протоколирования задается как значение атрибута `value`.

Примечание:

Подробнее о настройке уровня протоколирования см. статью "Настройка уровня протоколирования".

5.2 Настройка уровня протоколирования

Определяя уровень протоколирования, можно настроить вывод только тех диагностических сообщений, чей уровень превышает заданный в настройках. Определены следующие уровни протоколирования (приведены в порядке возрастания):

- **Critical**. Критический уровень. Регистрируются только серьёзные нарушения в работе, которые могут привести к неработоспособности адаптера.
- **Error**. Уровень ошибок. Регистрируются ошибки, мешающие корректной работе Системы (т.е. ошибки, требующие исправления).
- **Warning**. Уровень предупреждения. Помимо событий, входящих в уровни **Critical** и **Error**, регистрируются некритичные ошибки в работе адаптера, такие как неожиданное прекращение соединения с сервером DeviceLock или Traffic Monitor, истекший таймаут соединения и пр.
- **Information**. Информационный уровень. Помимо событий, входящих в уровни **Critical**, **Error** и **Warning**, регистрируются события, не связанные с ошибками, такие как, например, информация об изменении параметров сервера.
- **Verbose**. Отладочный уровень, в журнале регистрируются все события. Данный уровень нужно применять только для отладки адаптера. Не разрешается устанавливать данный уровень для адаптера, работающего в нормальном режиме, так как это приводит к значительному снижению производительности.

Уровень протоколирования диагностических сообщений настраивается в двух местах конфигурационного файла:

- В элементе `<switches>` — глобальный уровень для всего адаптера;
- В элементе `<add>` для каждого из `<listeners>` элемента `<source>` —для каждого из компонентов.

При определении глобального уровня протоколирования необходимо следить, чтобы он был не меньше, чем, максимальный установленный уровень протоколирования компонентов. В противном случае события с более высоким уровнем, чем определено глобально, не будут регистрироваться.
Пример 1
Установлен глобальный уровень протоколирования **Verbose**, а для фильтра одного из компонентов – **Warning**. В таком случае для этого компонента будут протоколироваться события с уровнем **Warning**, **Error** и **Critical**, но отфильтровываться - события с уровнем **Information** и **Verbose**.
Пример 2
Установлен глобальный уровень протоколирования **Error**, а для фильтра одного из компонентов – **Warning**. В таком случае для этого компонента будут протоколироваться события с уровнем **Error** и **Critical**, но отфильтровываться - события с уровнем **Warning**, **Information** и **Verbose**. Это происходит потому, что общий уровень протоколирования — **Error**, т.е. вне зависимости от того, как настроены фильтры, регистрируются только сообщения с уровнем **Error** и меньше.

6 МОНИТОРИНГ DEVICELOCK ADAPTER

Мониторинг работы InfoWatch DeviceLock Adapter осуществляется с помощью следующих стандартных утилит:

- Журнал приложений Windows;
- Счетчики производительности Windows.

6.1 Журнал приложений Windows

Стандартный журнал приложений Windows (**Event Viewer -> Applications**) регистрирует сообщения от службы InfoWatch DeviceLock Adapter как поступившие от источников, начинающихся с `InfoWatch.DeviceLockAdapter` или `InfoWatch.DeviceMonitor`. Каждый источник определяет модуль службы, сгенерировавший данное журнальное сообщение:

- `InfoWatch.DeviceLockAdapter.Service.Connector` — модуль взаимодействия с TM;
- `InfoWatch.DeviceLockAdapter.Service.Core` — ядро службы;
- `InfoWatch.DeviceLockAdapter.Core.FileType` — детектор сигнатур;
- `InfoWatch.DeviceMonitor.Database.Core` — модуль взаимодействия с БД.

6.2 Счетчики производительности Windows

Мониторинг длины очереди событий, ожидающих отправки в TM, (отдельной для каждого из подключенных к InfoWatch DeviceLock Adapter серверов DeviceLock Enterprise Server) осуществляется с помощью счетчиков производительности Windows. Для каждого сервера DL ES определен свой экземпляр счетчика. Имя экземпляра счетчика состоит из имени сервера DL ES и цифры - идентификатора этого сервера в базе данных DL ES. Если на каком-либо сервере вы производили переустановку DeviceLock, то для этого сервера актуальным экземпляром счетчика является тот, у которого больше значение идентификатора.

Чтобы наблюдать длину очереди теневых копий, ожидающих отправки в TM:

1. Откройте стандартную оснастку мониторинга производительности (**Control Panel —> Administrative Tools —> Performance**).
2. Добавьте новый счетчик:

- В качестве категории счетчиков выберите `InfoWatch DeviceLock Adapter`.

В списке счетчиков длины очереди будет выбран единственный счетчик `DeviceLock Event Queue Length`.

- Выберите имя необходимого экземпляра сервера DeviceLock Enterprise Server или выберите счетчик `_Total` (суммарная длина очереди событий от всех серверов DL ES).

7 УДАЛЕНИЕ INFOWATCH DEVICELOCK ADAPTER

Для того чтобы удалить InfoWatch DeviceLock Adapter, запустите файл установки `Setup.Service.ru.msi` (для русскоязычного интерфейса мастера установки) или `Setup.Service.en.msi` (для англоязычного интерфейса мастера установки).

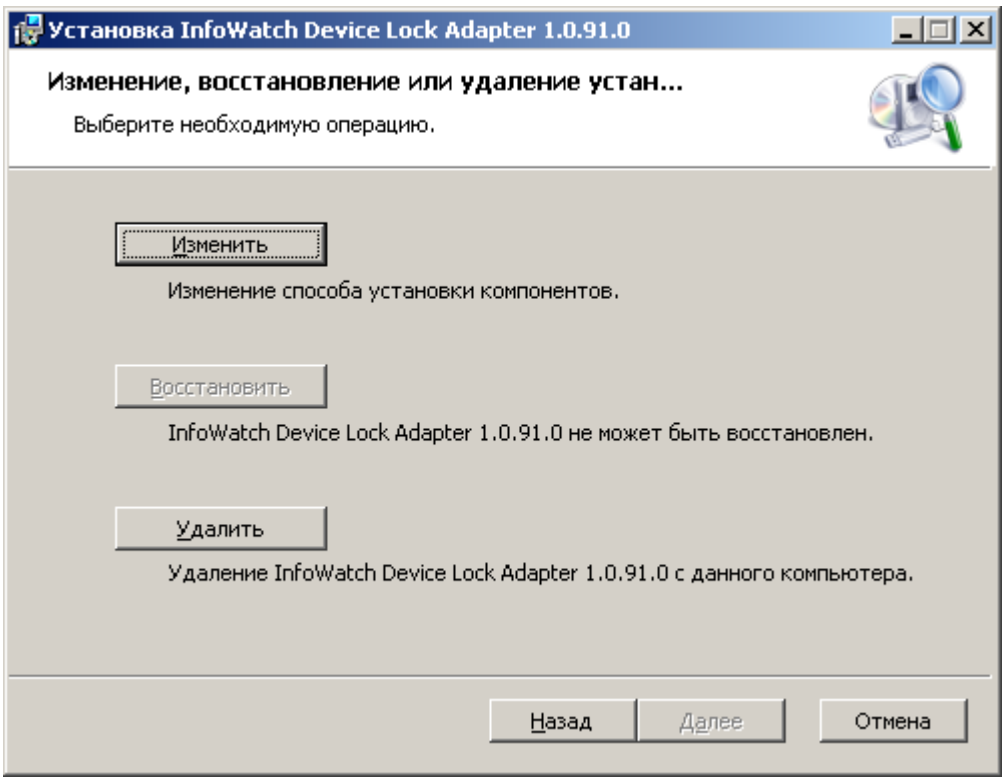


Рисунок 7. Удаление InfoWatch DeviceLock Adapter

Нажмите кнопку **Удалить**.

Все файлы InfoWatch DeviceLock Adapter будут удалены с компьютера вместе с созданными в процессе установки папками.

7.1 Глоссарий

DeviceLock
Система контроля доступа к периферийным устройствам компьютерной системы. Также производит мониторинг информации, переносимой с рабочих станций на съемные устройства или отправляемой на печать.

DL ES DB DeviceLock Database – база данных сервера системы DeviceLock.
DL ES DeviceLock Enterprise Server – сервер системы DeviceLock.
DLA Служба InfoWatch DeviceLock Adapter.
InfoWatch Traffic Monitor Система, предназначенная для перехвата, фильтрации и анализа информационных потоков компьютерной системы.
ТМ Система InfoWatch Traffic Monitor.
БД База данных.
Контроль доступа к периферийным устройствам Разграничение прав на работу с периферийными устройствами компьютерной системы. Определение уровня доступа к различным типам периферийных устройств выполняется в соответствии с требованиями корпоративной политики безопасности. Для разных групп пользователей и групп рабочих станций может быть настроен разный уровень доступа к тому или иному периферийному устройству.
СУБД Система управления базами данных.
Теневая копия текста Копия текста, выделенного из документа, отправленного на печать.
Теневая копия файла Копия файла, создаваемого на съемном устройстве. Создается только при успешном завершении операции сохранения файла на съемное устройство. Анализ теневых копий файлов выполняется в системе InfoWatch Traffic Monitor.