

INFOWATCH

InfoWatch Device Control Adapter. Руководство по установке и конфигурированию

26/03/2021

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 3

2 Обзор InfoWatch Device Control Adapter 4

2.1 Схема работы InfoWatch Device Control Adapter 4

2.2 Информация, передаваемая в InfoWatch Traffic Monitor 5

2.3 Состав InfoWatch Device Control Adapter 7

2.4 Аппаратное и программное обеспечение для InfoWatch Device Control Adapter 7

3 Установка Device Control Adapter 9

3.1 Подготовка к установке Device Control Adapter 9

3.1.1 Варианты установки InfoWatch Device Control Adapter 9

3.1.2 Подготовка учетных записей Device Control Adapter 11

3.1.2.1 Подготовка учетной записи для работы службы Device Control Adapter 11

3.1.3 Используемые порты 13

3.2 Установка плагина для InfoWatch Traffic Monitor 13

3.3 Порядок установки InfoWatch Device Control Adapter 14

3.4 Удаление InfoWatch Device Control Adapter 17

4 Конфигурирование Интеграционной платформы и InfoWatch Device Control Adapter 18

4.1 Общие настройки InfoWatch Integration Adapter 18

4.2 Настройка InfoWatch Device Control Adapter 20

5 Мониторинг Device Control Adapter 24

5.1 Журнал приложений Windows для мониторинга Device Control Adapter 24

5.2 Счетчики производительности Windows для мониторинга Device Control Adapter 24

5.3 Диагностика и устранение неисправностей 24

5.3.1 Ошибки 25

5.3.2 Предупреждения 25

6 Глоссарий Infowatch Device Control Adapter 26

1 Введение

Информация, содержащаяся в данном Руководстве, предназначена для пользователей, выполняющих установку и администрирование InfoWatch Integration Adapter и InfoWatch Device Control Adapter.

В настоящем руководстве **не** рассматриваются вопросы установки и настройки сервера SecureWave Sanctuary Device Control, Lumension Device Control и Dprint. За получением необходимых сведений вы можете обратиться к документации сервера.

Аудитория

Информация, содержащаяся в руководстве, предназначена для администраторов, выполняющих установку и настройку Device Control Adapter.

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

2 Обзор InfoWatch Device Control Adapter

Infowatch Device Control Adapter – служба, осуществляющая передачу теневых копий заданий на печать и файлов, получаемых с помощью систем SecureWave Sanctuary Device Control, Lumension Device Control и Dprint, в систему InfoWatch Traffic Monitor (сервисы событий - *Обмен файлами*, *Принтер и МФУ*; типы событий - *Внешнее устройство*, *Печать*).

Основные функции Device Control Adapter:

- передача данных в InfoWatch Traffic Monitor с помощью XML-транспорта;
- фильтрация теневых копий по размеру и типу (сигнатуре) файла;
- получение теневых копий с Device Control Application Server (сервера системы, с которой производится интеграция), хранящихся как в его локальной файловой системе, так и на удаленном сетевом ресурс;
- поддержка нескольких серверов Device Control одним приложением Device Control Adapter.

В этой главе:

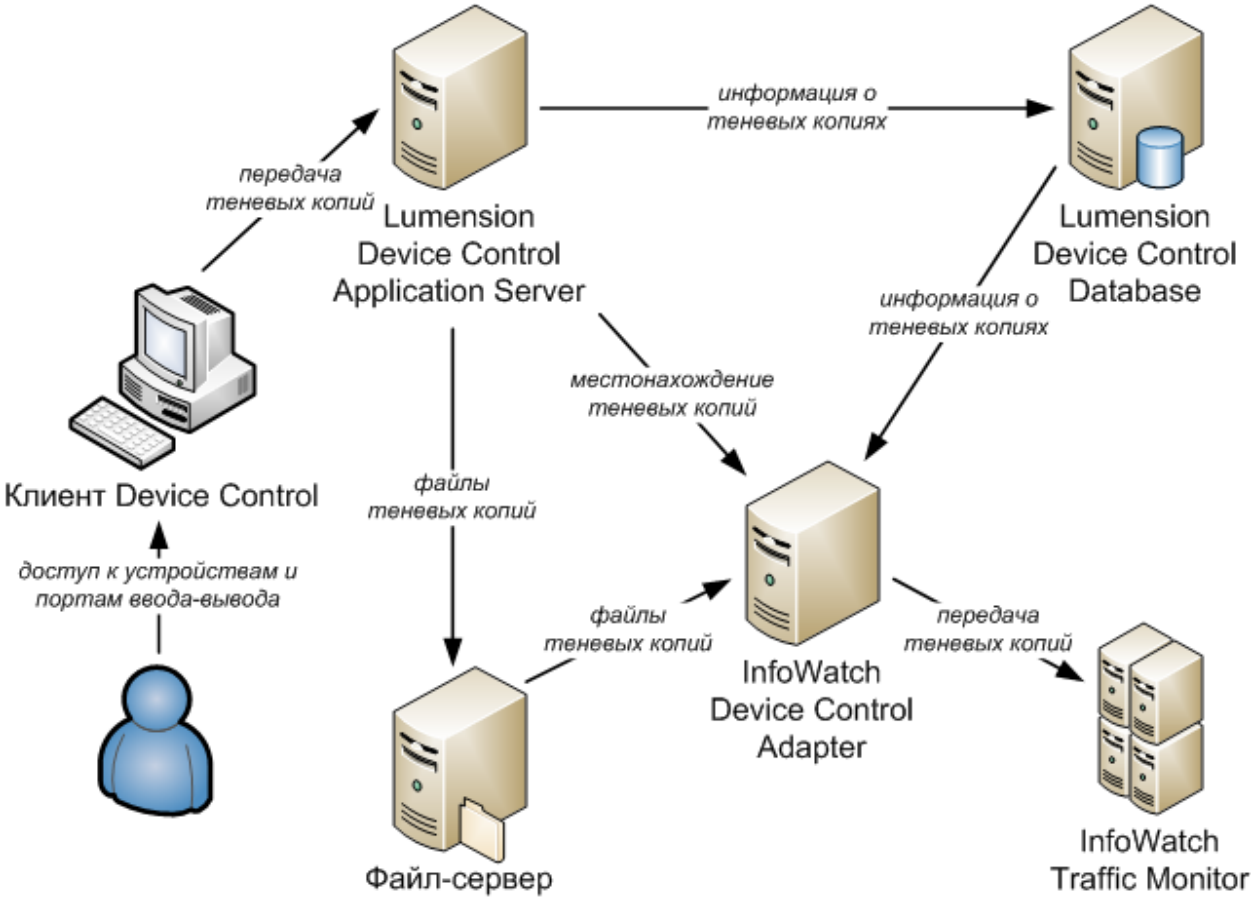
- Схема работы InfoWatch Device Control Adapter
- Информация, передаваемая в InfoWatch Traffic Monitor
- Состав InfoWatch Device Control Adapter
- Аппаратное и программное обеспечение для InfoWatch Device Control Adapter

2.1 Схема работы InfoWatch Device Control Adapter

На рисунке показан принцип работы InfoWatch Device Control Adapter с хранением файлов теневых копий на сетевом ресурсе на примере Lumension Device Control. Схема интеграции с SecureWave Sanctuary Device Control и Dprint будет выглядеть идентично ввиду аналогичной с Lumension Device Control структуры решений.

На схеме ниже и далее во всем документе:

- Lumension Device Control Application Server (LDC AS) – сервер Lumension или другой системы, с которой происходит интеграция DCA;
- Lumension Device Control Database – база данных Lumension или другой системы, с которой происходит интеграция DCA;
- Device Control Adapter (DCA) – сервер, на который устанавливается Device Control Adapter.



InfoWatch Device Control Adapter работает следующим образом:

1. Подключается к базе данных Lumension Device Control и проверяет её на наличие теневых копий, удовлетворяющих следующим критериям:
   - размер файла попадает в указанный диапазон;
   - дата снятия теневой копии позднее, чем дата, заданная в конфигурации адаптера.
2. Получает с хоста LDC AS местонахождение файлов теневых копий.
3. Копирует найденные теневые копии на хост с адаптером и проверяет на соответствие сигнатурам, заданным в конфигурации адаптера.
4. Отправляет теневые копии, соответствующие какой-либо из заданных сигнатур, в Traffic Monitor.
5. Ведет учет идентификаторов отправленных копий во избежание повторной отправки.
6. В зависимости от настроек:
   - оставляет теневую копию в LDC DB без изменений;
   - удаляет файл теневой копии, оставляя информацию о ней в LDC DB;
   - удаляет файл теневой копии, а также всю информацию о ней из LDC DB.

2.2 Информация, передаваемая в InfoWatch Traffic Monitor

Ниже приведен список данных, передаваемых из LDC DB в TM, и названия полей TM, куда попадают переданные данные.

Поле LDC	Поле TM	Комментарий
–	Сервер перехвата	Имя сервера LDC AS, хранящего теневую копию. В Lumension Endpoint Security Management Console не отображается.
Computer	Рабочая станция	Машина, на которой совершена операция
Device Class	Тип устройства	Тип устройства, с которым произошла операция (например: Floppy, Cdrom, Removable). В Lumension Endpoint Security Management Console и LDC DB для одного и того же типа устройства используются разные названия типов. В TM передаются названия типов из LDC DB.
Device Model	Имя устройства	Имя устройства, с которым произошла операция. Обычно указывается производитель и/или модель устройства.
File Name (Full)	Конечный файл	Полный путь и имя файла, с которого снята теневая копия
Process Name	Приложение	Приложение, совершившее операцию. LDC всегда оставляет это поле пустым.
Size	Размер объекта	Размер файла, с которого снята теневая копия.
Transferred On (UTC)	Дата перехвата	Локальное время на сервере LDC AS в момент регистрации теневой копии в LDC DB. Примечание: Если адаптер не может запросить часовой пояс сервера LDC AS, то используется часовой пояс машины, на которой установлен адаптер.
Type	Операция	Действие пользователя, в результате которого была создана теневая копия. В TM передаются события только для следующих типов: ▪ WRITE-GRANTED (в TM - *Запись разрешена*) ▪ WRITE-DENIED (в TM - *Запись запрещена*) ▪ READ-GRANTED (в TM - *Чтение разрешено*) ▪ READ-DENIED (в TM - *Чтение запрещено*)
User	domain	Домен пользователя, совершившего операцию. В Lumension Endpoint Security Management Console отображается вместе с именем пользователя.

User	login	Имя пользователя, совершившего операцию. В Lumension Endpoint Security Management Console отображается вместе с доменом пользователя.
User	Отправитель	Комбинированное значение домена и имени пользователя. TM генерирует значение этого поля из полей domain и login.

2.3 Состав InfoWatch Device Control Adapter

Компоненты, входящие в состав InfoWatch Device Control Adapter:

Компонент	Назначение	Имя файла
Database provider	Библиотека, обеспечивающая работу с БД	`InfoWatch.DeviceMonitor.Database.Core.dll`
Service Core	Общие компоненты службы Device Control Adapter (осуществление бизнес-логики работы с Lumension Device Control и вспомогательные компоненты)	`InfoWatch.DeviceControlAdapter.Service.Core.dll`
InfoWatch Traffic Monitor Connector	Обеспечение взаимодействия с InfoWatch Traffic Monitor	`InfoWatch.DeviceControlAdapter.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.DeviceControlAdapter.exe`
Service Configuration File	Конфигурационный файл службы Device Control Adapter	`InfoWatch.DeviceControlAdapter.exe.config`

2.4 Аппаратное и программное обеспечение для InfoWatch Device Control Adapter

Требования к аппаратному обеспечению:

- Процессор Pentium 4 с частотой 3 ГГц и выше;
- Оперативная память - не менее 1 ГБ;
- Сетевая карта - 100/1000 Мбит/с.

Требования к программному обеспечению:

- Lumension Device Control, SecureWave Sanctuary Device Control или Dprint;
- Операционная система на выбор:
    - Microsoft Windows 2008 Server Service Pack 1 и более поздние;
    - Microsoft Windows Server 2016;
    - Microsoft Windows Server 2019.
- Microsoft .NET Framework 4.5.1.

3 Установка Device Control Adapter

Установка InfoWatch Integration Adapter происходит автоматически при установке адаптера Infowatch DeviceControl Adapter. Для корректного функционирования интеграционной платформы необходимо выполнить следующие действия:

1. Определить и подготовить учетные записи для взаимодействия службы DCA и БД.
2. Сгенерировать лицензию для InfoWatch Traffic Monitor.
3. Установить плагин в InfoWatch Traffic Monitor.
4. На сервер, где будет работать адаптер, установить Microsoft .Net Framework 4.5.1 (если не установлено).
5. Установить Infowatch DeviceControl Adapter.
6. Запустить Конфигуратор InfoWatch Integration Adapter, внести изменения в настройки.

После успешной установки плагин появится в списке установленных плагинов. Чтобы система загрузила плагин, необходимо выделить его и нажать **Сохранить**. При этом служба InfoWatch Integration Adapter будет перезапущена.

После перезапуска службы в Конфигураторе появится вкладка настроек плагина.

На вкладке настроек плагина необходимо:

1. Ввести токен доступа к InfoWatch Traffic Monitor (можно получить на странице установленного ранее плагина для InfoWatch Traffic Monitor). Подробнее см. "Настройка InfoWatch Device Control Adapter".
2. Ввести параметры подключения (см. "Общие настройки InfoWatch Integration Adapter").
3. Нажать **Сохранить**. Плагин автоматически перезапустится.

3.1 Подготовка к установке Device Control Adapter

В этой главе:

- Варианты установки InfoWatch Device Control Adapter
- Подготовка учетных записей Device Control Adapter
- Используемые порты

3.1.1 Варианты установки InfoWatch Device Control Adapter

Варианты установки приведены на примере Lumension Device Control. Установка с SecureWave Sanctuary Device Control и Dprint будет выглядеть идентично ввиду аналогичной с Lumension Device Control структуры решений.

При установке Device Control Adapter вам потребуется указать:

- учетную запись, под которой будет работать служба DCA (локальная учетная запись (LOCAL_SYSTEM) или специально созданная учетная запись – см. "Подготовка учетной записи для работы службы Device Control Adapter");
- способ авторизации на сервере MS SQL, где работает база данных Device Control (авторизация в Windows или встроенная учетная запись SQL Server).

Локальная учетная запись (LOCAL_SYSTEM) может быть использована, только если DCA и LDC AS установлены на одной машине. Во всех остальных случаях необходимо создавать специальную учетную запись.

Способ авторизации на сервере LDC DB определяется параметрами учетной записи службы DCA. Авторизация Windows может быть использована в двух случаях:

- если служба DCA будет работать под специально созданной учетной записью;
- если служба DCA устанавливается на тот же компьютер, где расположена LDC DB.

Во всех остальных случаях необходимо указывать параметры учетной записи SQL Server имеющей роли **db_datareader** и **db_datawriter** на базу LDC (по умолчанию sx).

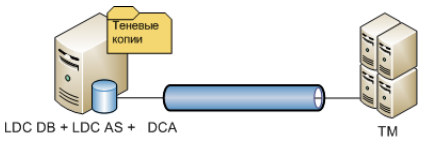
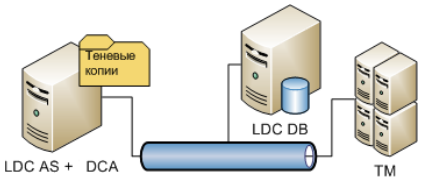
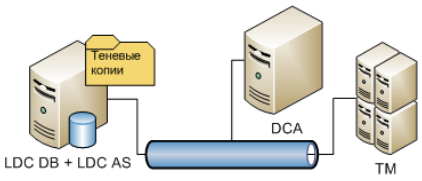
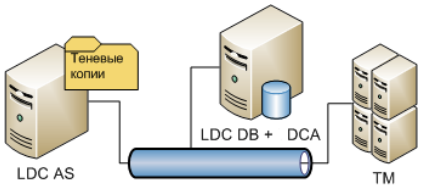
Возможности выбора параметров учетной записи службы DCA зависят от того, где LDC AS хранит теневые копии и куда будет устанавливаться сама служба DCA. Ниже рассмотрены различные варианты расположения этих объектов и описаны соответствующие им параметры установки.

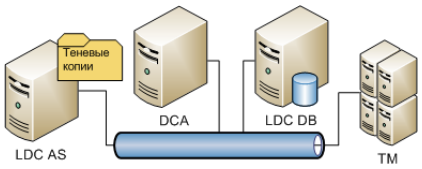
Приведенные варианты описаны с учетом того, что теневые копии хранятся в файловой системе компьютера, на котором работает Device Control Application Server. Это стандартная настройка, установленная для Device Control по умолчанию. Если в вашей системе теневые файлы хранятся в другом месте, то учетная запись DCA должна иметь доступ на чтение/запись этих файлов.

В случае если DCA и LDC AS установлены на различных машинах, и файлы теневых копий хранятся локально на сервере LDC AS, учетная запись DCA должна иметь доступ на чтение/запись административного ресурса, соответствующего диску, где хранятся теневые копии. Например, если теневые копии хранятся в **C:\DataFileDirectory**, учетная запись DCA должна иметь доступ по сети к **C$**.

В случае если DCA и LDC AS установлены на различных машинах, на стороне LDC AS должна работать стандартная служба Windows “**Удаленный реестр**” (Remote Registry service), и учетная запись DCA должна иметь доступ на чтение следующих ключей:

- `HKLM\SYSTEM\CurrentControlSet\Services\sxs\parameters`
- `HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`

Сервер, на который устанавливается DCA	Схема расположения серверов DCA, TM, LDC DB и LDC AS	Ограничения
Тот же, где установлены LDC AS и LDC DB		Служба DCA **может** работать под учетной записью локальной системы
Тот же, где установлен LDC AS. При этом LDC DB находится на другом сервере		Служба DCA **может** работать под учетной записью локальной системы. Авторизация в LDC DB через учетную запись SQL Server
Отличный от того, где установлены LDC AS и LDC DB		Служба DCA **не может** работать под учетной записью локальной системы. Авторизация в LDC DB через учетную запись SQL Server
Тот же, где установлена LDC DB. LDC AS установлен на отдельном сервере		Служба DCA **не может** работать под учетной записью локальной системы

Отличный от того, где установлены LDC AS и LDC DB. LDC AS и LDC DB установлены на различные сервера		Служба DCA **не может** работать под учетной записью локальной системы. Авторизация в LDC DB через учетную запись SQL Server

3.1.2 Подготовка учетных записей Device Control Adapter

Подготовка учетных записей приведена на примере Lumension Device Control. Учетные записи для установки с SecureWave Sanctuary Device Control и Dprint будут иметь идентичные параметры ввиду аналогичной с Lumension Device Control структуры решений.

При установке Device Control Adapter необходимо определить учетные записи, с помощью которых будет работать служба DCA и производиться соединение с базой данных Lumension Device Control. В зависимости от типа установки (см. "Варианты установки InfoWatch Device Control Adapter") вы можете выбрать следующие варианты:

- Служба DCA будет работать под учетной записью локальной системы (LOCAL_SYSTEM), при доступе к LDC DB будет использоваться авторизация в Windows – возможно, только если служба DCA запускается на том же компьютере, где установлен LDC AS и расположена LDC DB. При этом никаких дополнительных учетных записей подготавливать не требуется.
- Служба DCA будет работать под учетной записью локальной системы (LOCAL_SYSTEM), при авторизации в LDC DB будет использоваться запись SQL Server – необходимо подготовить встроенную запись SQL сервера, назначив ей роли **db_datareader** и **db_datawriter** на базу LDC.
- Служба DCA не может работать под учетной записью локальной системы (LOCAL_SYSTEM), при доступе к LDC DB будет использоваться авторизация в Windows – вы можете выбрать один из вариантов:
  - подготовить специальную учетную запись Windows (см. "Подготовка учетной записи для работы службы");
  - в качестве учетной записи службы указать уже существующую учетную запись с правами на LDC DB (например, использовавшуюся при установке Lumension Device Control), подготовив ее так, как описано на странице "Подготовка учетной записи для работы службы".
- Служба DCA не может работать под учетной записью локальной системы (LOCAL_SYSTEM), при авторизации в LDC DB будет использоваться учетная запись SQL Server – необходимо подготовить две записи: учетную запись Windows (см. "Подготовка учетной записи для работы службы") и встроенную запись SQL сервера, назначив ей роли **db_datareader** и **db_datawriter** на базу LDC.

Подготовка учетной записи для работы службы Device Control Adapter

Если работа Device Control Adapter под учетной записью локальной системы невозможна, то необходимо заранее подготовить специальную учетную запись Windows, под которой будет запущена служба Device Control Adapter.

Если машины с LDC AS, LDC DB и DCA находятся в домене, то, чтобы подготовить учетную запись домена Windows для службы Device Control Adapter, выполните следующие действия:

1. Создайте учетную запись домена Windows.
2. Предоставьте этой записи права локального администратора на машине, где установлен DCA (неободимо для создания счетчика производительности Windows).
3. Если LDC AS хранит файлы теневых копий на локальном диске, дайте учетной записи DCA права локального администратора на машине с LDC AS (необходимо для доступа к локальному диску через административные ресурсы C$, D$ и т.д.).
4. Если LDC AS установлен на машине с ОС **Windows Server 2008**, и хранит файлы на локальном диске, необходимо добавить в реестр этой машины **DWORD** параметр **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy** со значением 1. Это позволит DCA подключаться к административным ресурсам C$, D$ и т.д. на этой машине.
5. Если LDC AS хранит файлы теневых копий на файловом сервере, дайте учетной записи DCA права на чтение/запись этих файлов (права на запись нужны только при использовании DCA в режимах удаления теневых копий после передачи их в ТМ).
6. Разрешите подготовленной учетной записи запускать процесс как службу, для этого на контроллере домена:
   a) В **Панели управления** откройте компонент **Администрирование ► Доменная политика безопасности**.
   b) В открывшемся диалоговом окне выберите узел **Локальные политики ► Назначение прав пользователя**.
   c) Справа в области сведений дважды щелкните право **Вход в качестве службы**.
   d) На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.
7. Если для доступа к LDC DB планируется использовать авторизацию Windows:
   a) Включите созданную запись в состав учетных записей СУБД MS SQL Server на сервере, где находится LDC DB.
   b) Назначьте подготовленной записи роли **db_datareader** и **db_datawriter** на базу LDC (по умолчанию sx).

Если машины с LDC AS, LDC DB и DCA находятся НЕ в домене, то, чтобы подготовить учетную запись Windows для службы Device Control Adapter, выполните следующие действия:

1. Создайте идентичные учетные записи Windows на машинах с DCA и LDC AS.
2. Предоставьте права локального администратора для записи на машине, где установлен DCA (неохбодимо для создания счетчика производительности Windows).
3. На машине с DCA разрешите подготовленной учетной записи запускать процесс как службу, для этого:
   a) В **Панели управления** откройте компонент **Администрирование ► Локальная политика безопасности**.
   b) В открывшемся диалоговом окне выберите узел **Локальные политики ► Назначение прав пользователя**.
   c) Справа в области сведений дважды щелкните право **Вход в качестве службы**.
   d) На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.
4. Если LDC AS хранит файлы теневых копий на локальном диске, дайте учетной записи DCA права локального администратора на машине с LDC AS (необходимо для доступа к локальному диску через административные ресурсы C$, D$ и т.д.).
5. Если LDC AS установлен на машине с ОС **Windows Server 2008**, и хранит файлы на локальном диске, необходимо добавить в реестр этой машины **DWORD** параметр

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy со значением 1. Это позволит DCA подключаться к административным ресурсам C$, D$ и т.д. на этой машине.

6. Если LDC AS хранит файлы теневых копий на файловом сервере, создайте на файловом сервере учетную запись идентичную созданным на шаге 1, и дайте ей права на чтение/запись теневых копий (права на запись нужны только при использовании DCA в режимах удаления теневых копий после передачи их в TM).
7. Если для доступа к LDC DB планируется использовать авторизацию Windows:
   a) Создайте на машине с LDC DB учетную запись идентичную записям, созданным на шаге 1.
   b) Включите созданную запись в состав учетных записей СУБД MS SQL Server на сервере, где находится LDC DB.
   c) Назначьте записи роли **db_datareader** и **db_datawriter** на базу LDC (по умолчанию sx).

3.1.3 Используемые порты

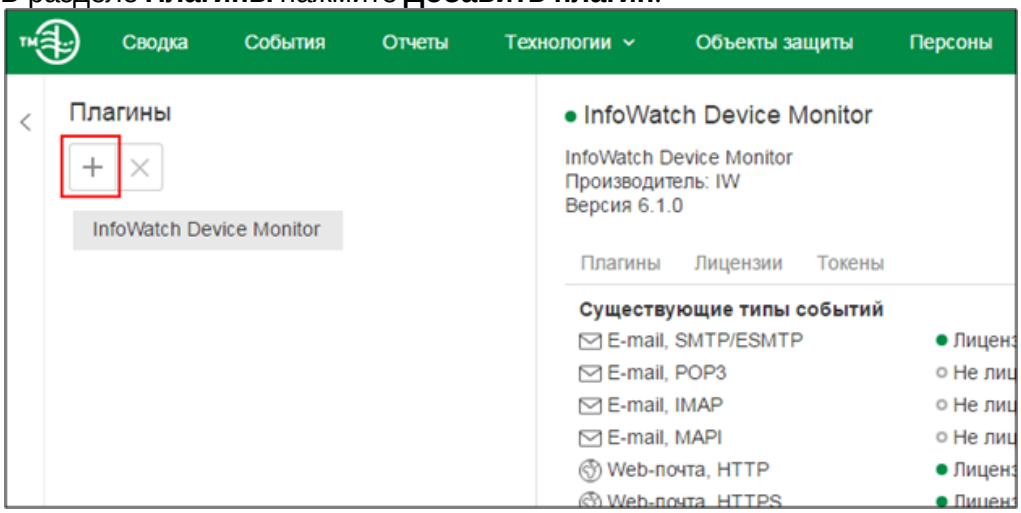
Если между DCA и серверами LDC находится брандмауэр, необходимо разрешить машине с DCA подключения по следующим портам:

- TCP 1433 – для подключения к LDC DB;
- TCP 139 и 445 – для подключения к файловому серверу или серверу LDC AS, если файлы хранятся локально;
- TCP 139 – для подключения к службе удаленного реестра на сервере LDC AS;
- TCP 9101 – для подключения к серверу TM.

3.2 Установка плагина для InfoWatch Traffic Monitor

Чтобы установить плагин для InfoWatch Traffic Monitor:

1. В разделе **Плагины** нажмите **Добавить плагин**.



2. В появившемся окне нажмите **Загрузить**
3. Выберите файл плагина (`.zip`). Если напротив плагина установлен статус *Не лицензирован*, то:
   a. убедитесь, что в файле плагина (`.zip`) присутствуют **manifest.json** и файл лицензии (`.license`).

b. откройте **manifest.json** на редактирование и пропишите в параметре `LICENSE` путь до нужного файла лицензии. Путь укажите относительно файла **manifest.json**. Если файл лицензии и **manifest.json**находятся в одной директории,то:

```
"LICENSE": [
       { "PATH" : "tm_license.license" }
   ]
```

c. сохраните изменения и повторите действия пунктов 1-3.

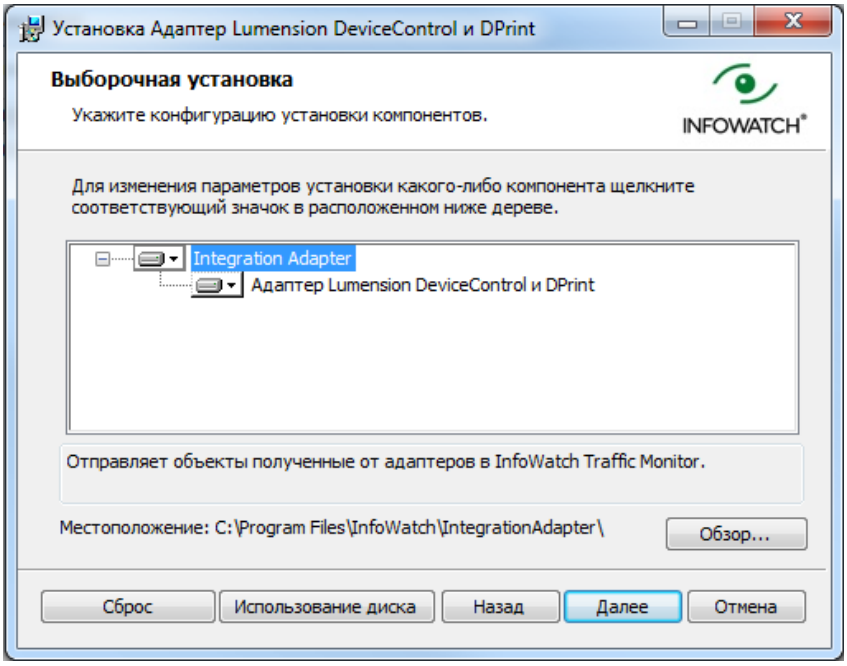
4. Убедитесь, что напротив плагина установлен статус *Лицензирован*. Установлена корректная лицензия перехватываемых типов событий.
5. Для завершения установки нажмите **Установить**.

3.3 Порядок установки InfoWatch Device Control Adapter

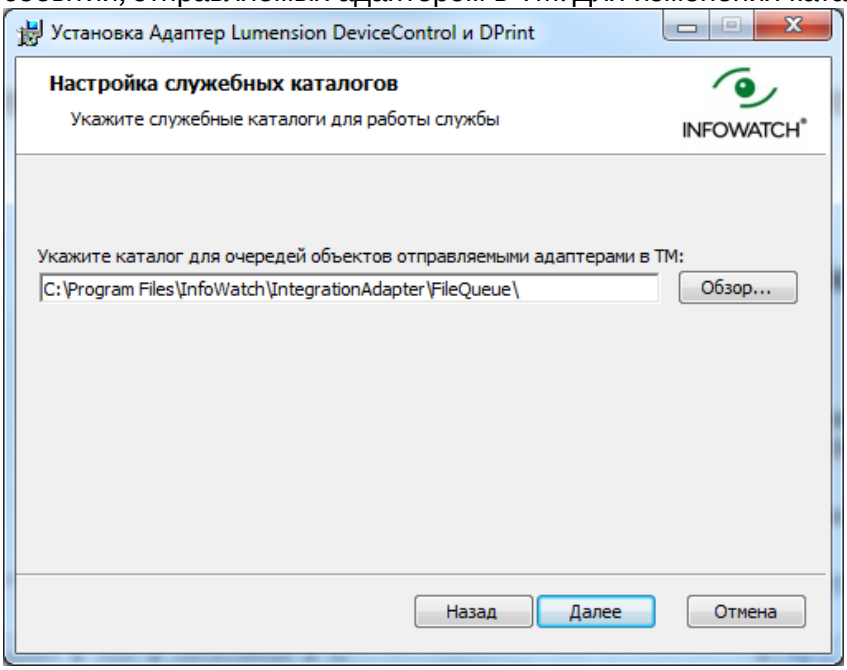
> **Важно!**
>
> Пользователь, выполняющий установку, должен обладать правами администратора.

Шаги установки:

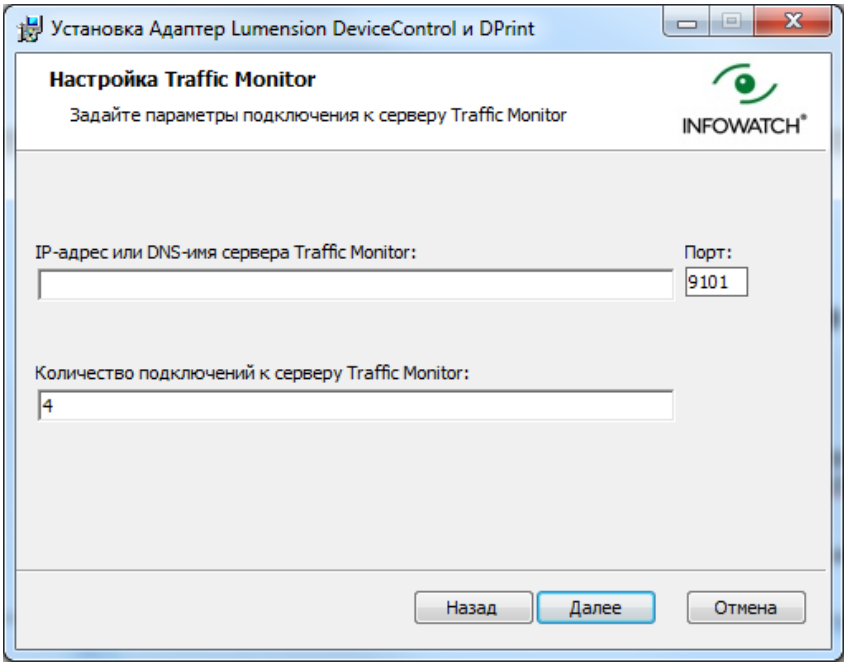
1. На диске с дистрибутивом запустите один из файлов:
   - Если используется 64-разрядная ОС:
     - `pluginplatform.3.0.0.x.Lumension.x64.ru.msi` - для запуска мастера установки с русским языком интерфейса;
     - `pluginplatform.3.0.0.x.Lumension.x64.en.msi` - для запуска мастера установки с английским языком интерфейса.
   - Если используется 32-разрядная ОС:
     - `pluginplatform.3.0.0.x.Lumension.x86.ru.msi` - для запуска мастера установки с русским языком интерфейса;
     - `pluginplatform.3.0.0.x.Lumension.x86.en.msi` - для запуска мастера установки с английским языком интерфейса.
2. В окне приветствия мастера установки нажмите **Далее**
3. Ознакомьтесь с лицензионным соглашением и нажмите **Далее**, чтобы принять его.
4. InfoWatch Integration Adapter реализован в виде службы Windows, не поддерживает установку для отдельных пользователей и устанавливается в общую для всех пользователей папку. Нажмите **Далее**.
5. Установка плагина происходит совместно с установкой Интеграционной платформы. Выберите плагин DeviceLock и установите ему опцию **Будет установлен на локальный жесткий диск**.
6. Измените папку установки (если необходимо). Для этого выберите компонент **Integration Adapter** и нажмите **Обзор**. По умолчанию установка производится в папку : `C:\Program Files\InfoWatch\IntegrationAdapter`.



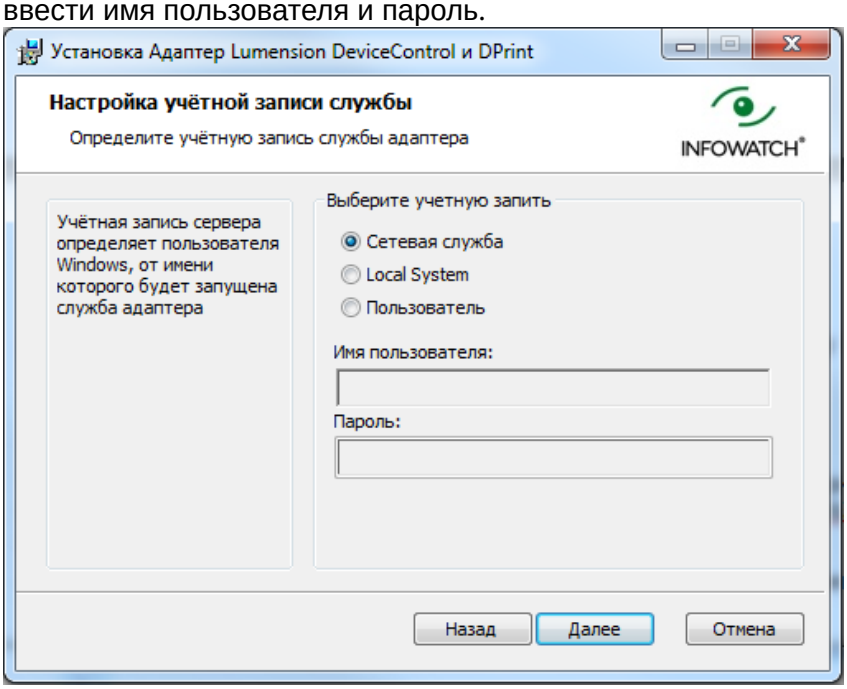
7. Нажмите **Далее**.
8. Укажите каталог очередей объектов - каталог, в котором создаются файловые очереди событий, отправляемых адаптером в ТМ. Для изменения каталога нажмите **Обзор**.



9. Нажмите **Далее**.
10. Настройте параметры соединения с сервером InfoWatch Traffic Monitor. Укажите:
    - IP-адрес или DNS-имя сервера InfoWatch Traffic Monitor;
    - порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий (по умолчанию 9101);
    - количество подключений к серверу InfoWatch Traffic Monitor. Вы можете указать от 1 до 32 подключений. Значение по умолчанию – 4.



11. Нажмите **Далее**.
12. Определите учетную запись службы адаптера: **Local System** или **Пользователь**, от имени которого будет запущена служба адаптера. В последнем случае необходимо ввести имя пользователя и пароль.



13. Нажмите **Далее**.

> **Важно!**
>
> InfoWatch Integration Adapter может установить подключение только к InfoWatch Traffic Monitor, так как используется протокол pushApi.

14. Подтвердите правильность указанных параметров установки, нажав **Установить**.
15. После успешного завершения установки мастер установки отобразит окно с уведомлением. Нажмите **Готово**.

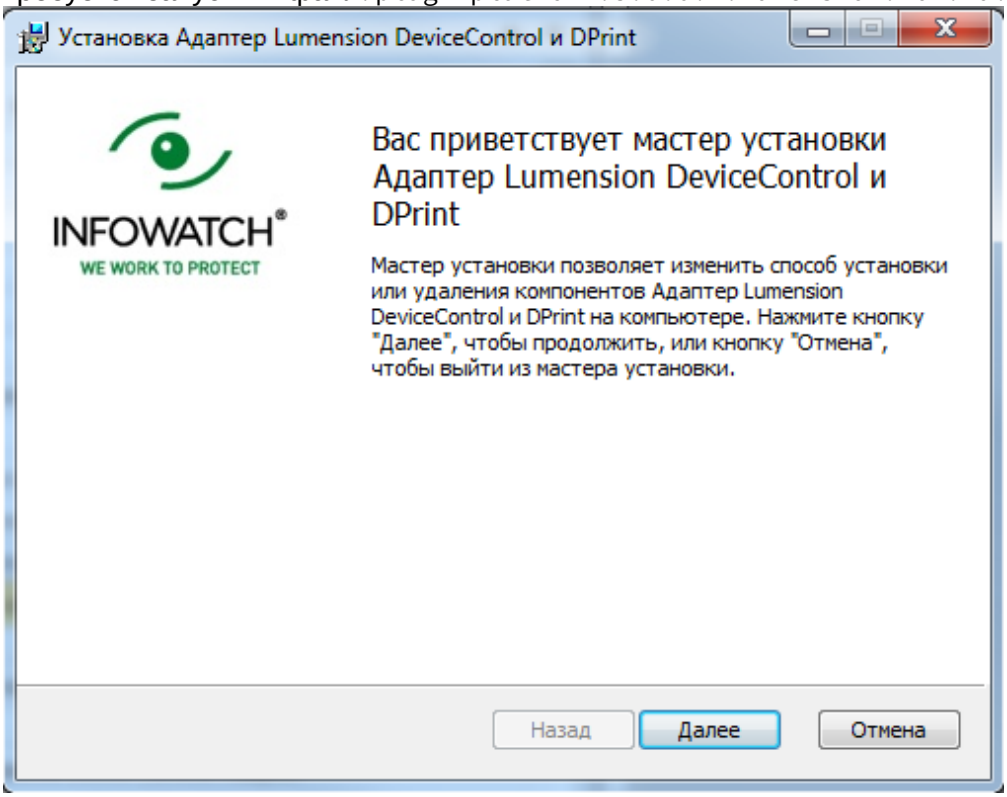
3.4 Удаление InfoWatch Device Control Adapter

Вы можете удалить Адаптер либо средствами ОС Windows из Панели Управления, либо запустив установочный пакет.

После удаления адаптера удалите каталоги файловой очереди и ошибочных сообщений вручную.

Чтобы удалить InfoWatch DeviceControl Adapter:

1. Запустите файл инсталлятора, который использовался при установке. Например, если вы устанавливали Адаптер с русским языком интерфейса на 64-разрядной ОС, требуется запустить файл: `pluginplatform.3.0.0.x.Lumension.x64.ru.msi`.



2. Нажмите **Далее**.
3. Выберите действие **Удалить**.
4. Убедитесь, что Lumension Device Control не запущен, и нажмите **Далее**.
5. В окне подтверждения нажмите **Удалить**. Все файлы InfoWatch Integration Adapter будут удалены с компьютера вместе с созданными в процессе установки папками.

4 Конфигурирование Интеграционной платформы и InfoWatch Device Control Adapter

Интеграционный адаптер предоставляет плагину интерфейс для графического конфигурирования, а также хранит двоичные данные настроек, передаваемых плагину в момент его запуска, и позволяет изменить эти данные. Конфигуратор загружает элемент управления, реализуемый плагином, в собственную вкладку.

Чтобы запустить приложение **Конфигуратор Интеграционного адаптера**:

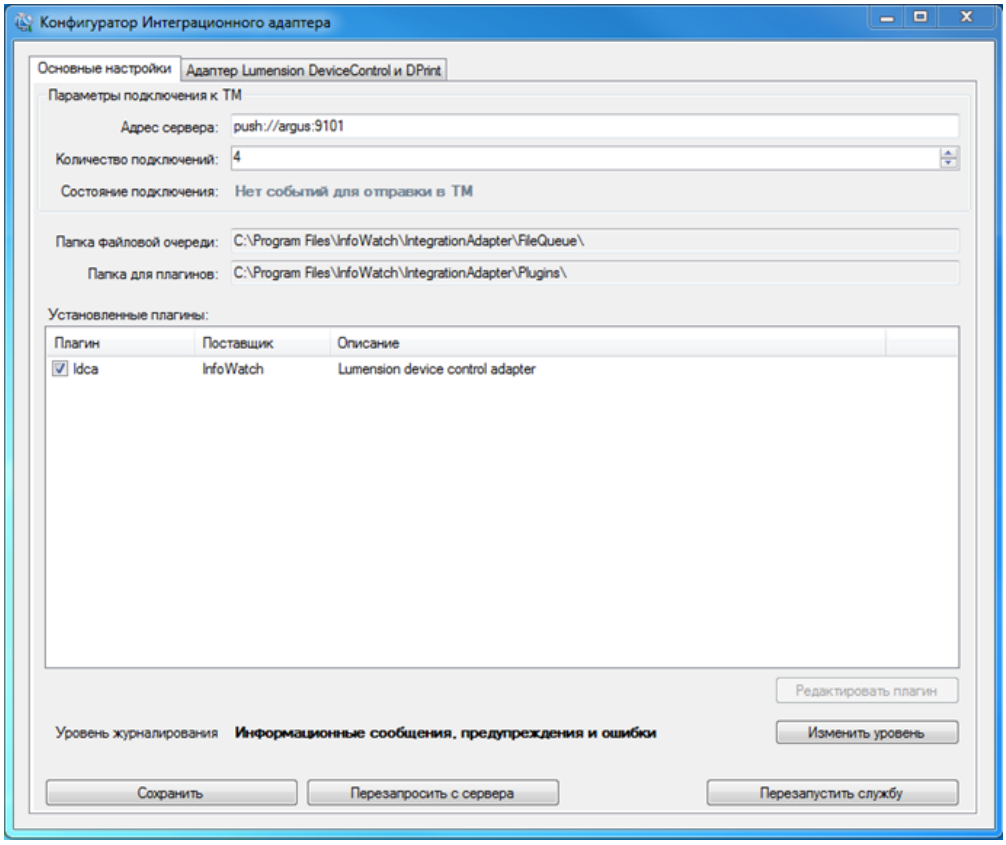
- воспользуйтесь ярлыком на рабочем столе **Конфигуратор Интеграционного адаптера**;
- в меню **Пуск** -> **Все программы** -> **InfoWatch** -> **IntegrationAdapter** выберите пункт **Конфигуратор Интеграционного адаптера**;
- в папке, где установлен InfoWatch Integration Adapter, запустите приложение `InfoWatch.PluginPlatform.Service.Configurator.exe`.

Параметры службы InfoWatch Integration Adapter, введенные в процессе установки, содержатся на вкладке **Основные настройки** (см. "Общие настройки InfoWatch Integration Adapter").

Для настройки InfoWatch Device Control Adapter перейдите на вкладку **Адаптер Lumension DeviceControl и DPrint** (см. "Настройка InfoWatch Device Control Adapter").

4.1 Общие настройки InfoWatch Integration Adapter

На вкладке **Основные настройки** приложения **Конфигуратор Интеграционного адаптера** содержатся параметры службы InfoWatch Integration Adapter, введенные в процессе установки.



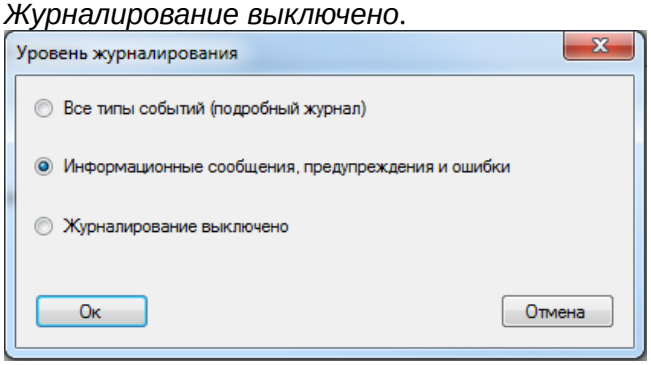
В списке **Установленные плагины** отмечены загруженные в платформу плагины.

Для редактирования доступны следующие настройки:

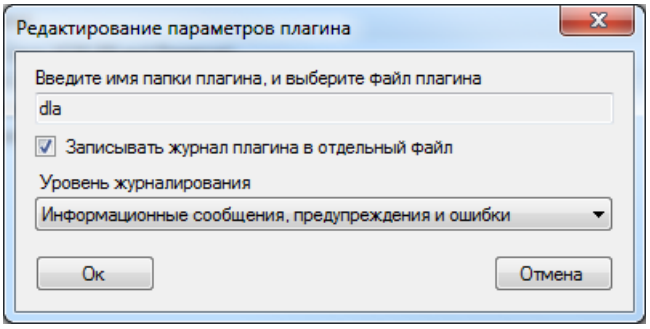
1. В области **Параметры подключения к ТМ**:
   - **Адрес сервера** InfoWatch Traffic Monitor в формате: `push://host:port`, где host – доменное имя или IP-адрес сервера InfoWatch Traffic Monitor, а port – порт сервера InfoWatch Traffic Monitor, через который будут доставляться события (по умолчанию 9101);
   - **Количество подключений** к серверу InfoWatch Traffic Monitor.
2. Служебные папки:
   - **Папка файловой очереди**, в которой создаются файловые очереди событий всех запущенных плагинов;
   - **Папка для плагинов**, в которой хранятся плагины и их настройки.

   > **Важно!**
   >
   > Так как Windows-служба InfoWatch Integration Adapter работает с правами пользователя «NETWORK SERVICE», необходимо убедится, что данному пользователю предоставлен доступ к указанным папкам.

3. Уровень журналирования. Чтобы выбрать уровень журналирования для всех зарегистрированных плагинов, нажмите **Изменить уровень** и укажите, какие данные должны сохраняться в журнал InfoWatch Integration Adapter. Доступны следующие уровни:
   - *Все типы событий (подробный журнал)*;
   - *Информационные сообщения, предупреждения и ошибки*;
   - *Журналирование выключено*.

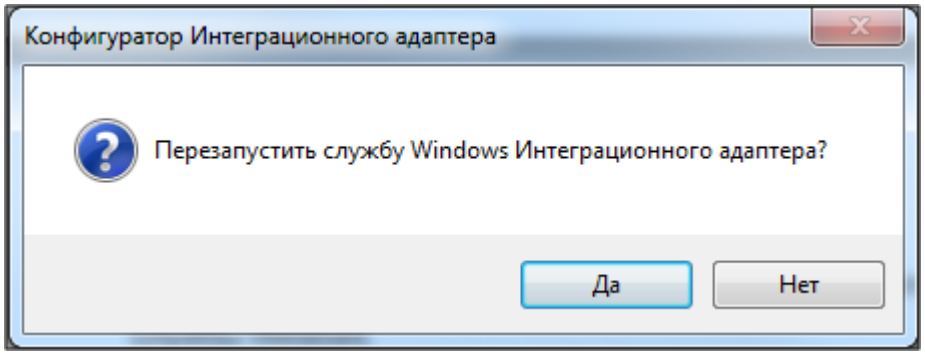
   

   Чтобы изменить уровень журналирования для отдельного плагина:
   a. Выберите нужный плагин в списке и нажмите **Редактировать плагин**.
   b. В открывшемся окне укажите, нужно ли вести журнал плагина в отдельном файле, и выберите уровень журналирования.



c. Нажмите **OK**.

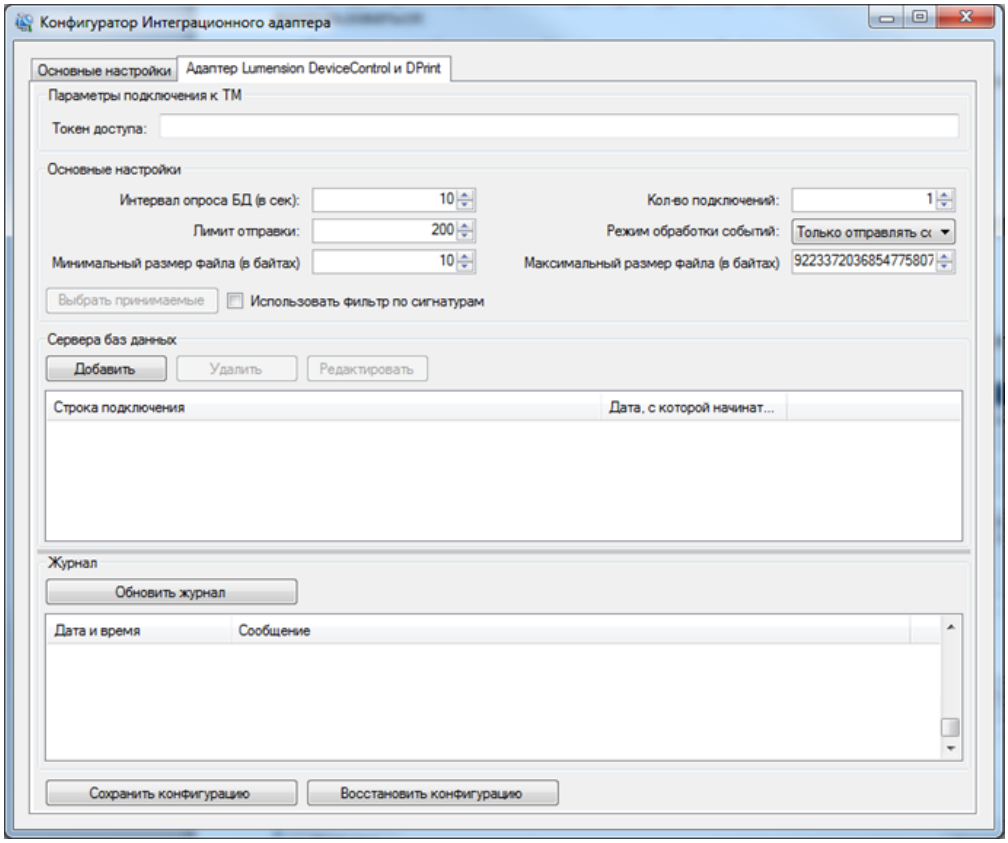
После изменения настроек нажмите **Сохранить**. Будет выведен запрос на перезапуск службы Windows.



Нажмите **Да**. Окно Конфигуратора будет закрыто, а затем открыто уже с новыми настройками.

4.2 Настройка InfoWatch Device Control Adapter

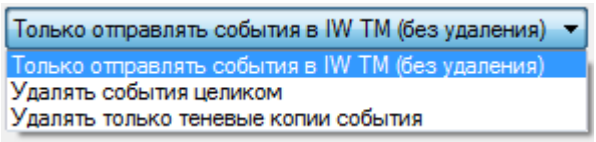
Для настройки плагина запустите приложение **Конфигуратор Интеграционного адаптера** и перейдите на вкладку **Адаптер Lumension DeviceControl и DPrint**.



Для функционирования плагина необходимо указать токен доступа. Строка **Токен доступа** отображается только для плагина и InfoWatch Traffic Monitor. Токен доступа к ТМ можно получить в окне ТМ, раздел **Плагины**, для издателя **IW _ADAPTERS**.

В области **Основные настройки** укажите следующие параметры:

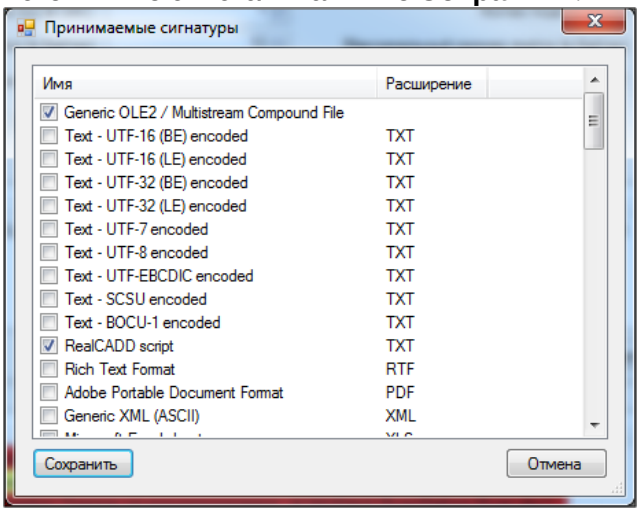
- **Интервал опроса БД (в сек)** – интервал опроса баз данных DeviceLock (в секундах). Список баз данных задается в области **Сервера баз данных**;
- **Количество подключений** – количество подключений, устанавливаемых плагином к каждой из баз данных DeviceLock;
- **Минимальный размер файла (в байтах)** – минимальный размер файла, отправляемого в InfoWatch Traffic Monitor. Файлы меньшего размера отправляться не будут. Допустимые значения от 0 до 9223372036854775806. Значение по умолчанию – 10;
- **Максимальный размер файла (в байтах)** – максимальный размер файла, отправляемого в InfoWatch Traffic Monitor. Файлы большего размера отправляться не будут. Значение по умолчанию – 9223372036854775807;
- **Лимит отправки** – количество событий, запрашиваемых из удаленной БД;
- **Режим обработки событий** – действия, которые будут выполняться с событиями. Возможные значения:



  - **Только отправлять события в IW TM (без удаления)** – оставлять файл теневой копии и информацию о нем в системе Lumension Device Control;
  - **Удалять события целиком** – удалять файл теневой копии и информацию о нем из системы Lumension Device Control;

- **Удалять только теневые копии события** – удалять только файл теневой копии, оставляя информацию о нем в системе Lumension Device Control.

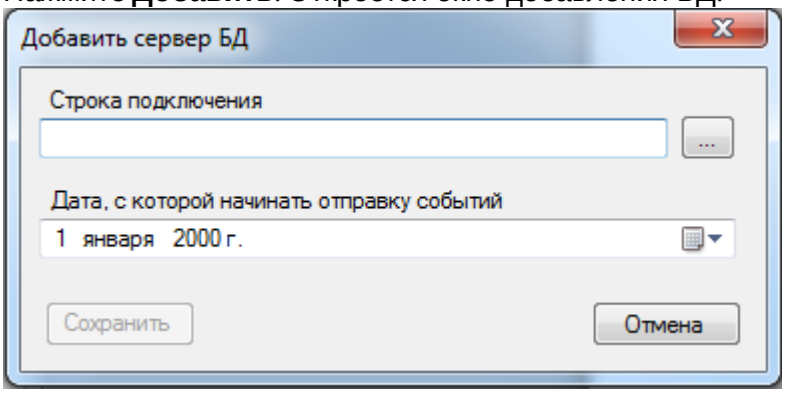
- **Использовать фильтр по сигнатурам** – отметьте эту опцию, если требуется фильтровать фонограммы по сигнатурам. В этом случае файлы, отправляемые в InfoWatch Traffic Monitor, будут фильтроваться по их типу (сигнатуре). Если файл не попадает ни под одну из представленных сигнатур, файл не отправляется. Для выбора сигнатур:
  1. Нажмите **Выбрать принимаемые**.
  2. В открывшемся окне **Принимаемые сигнатуры** выберите как минимум один источник из списка и нажмите **Сохранить**.



В области **Сервера баз данных** укажите список опрашиваемых серверов баз данных Device Lock.

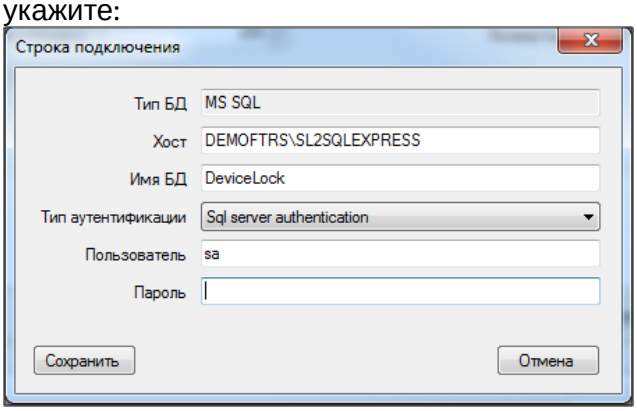
Для добавления сервера:

1. Нажмите **Добавить**. Откроется окно добавления БД.



2. Укажите строку подключения к базе данных. Строку можно ввести вручную либо нажать  для формирования строки подключения. В открывшемся диалогом окне

укажите:



- **Хост** – путь до экземпляра СУБД;
- **Имя БД** – имя просматриваемой базы данных;
- **Тип аутентификации**:
  - Проверка подлинности Windows (**Integrate security**) – можно использовать, если пользователь, от чьего имени запущена служба InfoWatch Integration Adapter, имеет доступ к требуемой базе данных;
  - Проверка подлинности SQL server (**SQL server authentication**).
- Имя пользователя учетной записи БД и пароль.

3. Нажмите **Сохранить** для формирования строки подключения
4. Укажите дату, начиная с которой нужно просматривать события (может понадобиться для первого запуска, чтобы не загружать очень старые сообщения);
5. Нажмите **Сохранить** для добавления сервера БД.

Для редактирования ранее добавленного сервера выберите нужный сервер в списке и нажмите **Редактировать**.

В области **Журнал** отображаются события, произошедшие в плагине. Журнал отображает последние 100 событий. Обновление журнала происходит автоматически каждые десять секунд.

Для фиксации событий, произошедших в плагине, реализован **Журнал** событий, который автоматически обновляется каждые десять секунд и отображает последние 100 событий. Для принудительного обновления нажмите **Обновить журнал**. Если необходимо отменить несохраненные изменения, нажмите **Восстановить конфигурацию**. После изменения настроек нажмите **Сохранить конфигурацию**. При этом настройки будут сохранены в постоянное хранилище InfoWatch Integration Adapter, а плагин будет перезапущен.

5 Мониторинг Device Control Adapter

Для мониторинга состояния Device Control Adapter используются:

- Журнал приложений Windows для мониторинга Device Control Adapter
- Счетчики производительности Windows для мониторинга Device Control Adapter

Для диагностики неполадок используется журнал EventLog (см. "Диагностика и устранение неисправностей").

5.1 Журнал приложений Windows для мониторинга Device Control Adapter

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

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

5.2 Счетчики производительности Windows для мониторинга Device Control Adapter

Мониторинг длины очереди событий, ожидающих отправки в TM, выполняется отдельно для каждого из подключенных к Device Control Adapter серверов Device Control. Для мониторинга используются счетчики производительности Windows. Для каждого сервера Device Control определен свой экземпляр счетчика. Имя экземпляра счетчика состоит из имени сервера и идентификатора этого сервера в LDC DB.

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

1. Откройте стандартную утилиту мониторинга производительности (**Control Panel** –> **Administrative Tools** –> **Performance**).
2. Добавьте новый счетчик:
   a. В качестве категории счетчиков выберите `InfoWatch DeviceControl Adapter`. В списке счетчиков длины очереди будет выбран единственный счетчик `Device Control Event Queue Length`.
   b. Выберите имя необходимого экземпляра сервера Device Control или выберите счетчик `_Total` (суммарная длина очереди событий от всех серверов Device Control).

5.3 Диагностика и устранение неисправностей

Сообщения об ошибках в работе адаптера записываются в EventLog. Ниже приведены примеры ошибок и предупреждений, которые могут быть выведены в EventLog, и общие рекомендации по их исправлению:

- Ошибки
- Предупреждения

5.3.1 Ошибки

Ниже приведены примеры ошибок, возможные причины и решения.

Текст ошибки	Причина	Решение
Ошибка конфигурации: <описание ошибки> **Пример:** Ошибка конфигурации: неверный режим обработки событий: 'Romember'.	Некорректно заданы параметры в конфигурационном файле	Проверьте конфигурационный файл на наличие некорректно заданных параметров и исправьте неверное значение. Перезапустите сервис адаптера.
Нет соединения с Traffic Monitor	Не получается установить соединение	Проверьте настройки соединения с TM, наличие связи между сервером адаптера и сервером TM, работоспособность сервера TM
Нет прав на использование реестра на <имя сервера>	Недостаточно прав для чтения реестра на сервере LDC	Проверьте настройки прав доступа для пользователя, от имени которого выполняется сервис адаптера
Ошибка при проверке связи с БД LDC: <текст ошибки>	Не удалось выполнить тестовый запрос к базе данных LDC	Проверьте конфигурацию адаптера, наличие связи между сервером адаптера и сервером БД LDC. Проверьте настройки БД LDC (разрешены ли подключения к БД по сети)

5.3.2 Предупреждения

Ниже приведены примеры предупреждений, возможные причины и решения.

Текст предупреждения	Причина	Решение
Есть <N> потерянных событий которые не были отправлены из-за ошибок. Отправляем.	Во время отправки событий ранее возникла какая-то ошибка. Будет осуществляться повторная передача событий	Проверьте системный лог адаптера на наличие ошибок
Установлено <N> из <M> соединений с TM **Примечание:** N < M	Не все соединения с TM удалось установить	Проверьте соответствие настроек адаптера настройкам TM в части количества соединений
Не найден файл <путь к файлу> теневой копии	Файл теневой копии был удалён или к нему нет доступа	Проверьте наличие прав доступа к файлу для пользователя, от имени которого запускается адаптер

6 Глоссарий Infowatch Device Control Adapter

Device Control, LDC Система контроля доступа к периферийным устройствам компьютерной системы. Также производит мониторинг информации, переносимой с рабочих станций на съемные устройства или отправляемой на печать.
LDC DB Lumension Device Control Database – база данных Lumension или другой Системы, с которой происходит интеграция DCA.
LDC AS Lumension Device Control Application Server – сервер Lumension или другой Системы, с которой происходит интеграция DCA, который отвечает за прием теневых копий от агентов LDC и загрузку их в LDC DB.
DCA Служба DeviceControl Adapter.
InfoWatch Traffic Monitor, TM Система, предназначенная для перехвата, фильтрации и анализа информационных потоков компьютерной системы.
InfoWatch Integration Adapter Универсальный Интеграционный Адаптер
БД База данных.
Теневая копия заданий на печать Копия текста или изображения, 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.