

INFOWATCH

# InfoWatch Cisco UCM 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

1.1 Аудитория ..... 3

2 Обзор InfoWatch Cisco UCM Adaper ..... 4

2.1 Общие сведения об InfoWatch Cisco UCM Adapter ..... 4

2.1.1 Ограничения ..... 4

2.2 Схема работы Infowatch Cisco UCM Adapter ..... 5

2.3 Состав InfoWatch Cisco UCM Adapter ..... 5

2.4 Аппаратное и программное обеспечение для InfoWatch Cisco UCM Adapter ..... 7

3 Установка InfoWatch Cisco UCM Adapter ..... 9

3.1 Установка плагина для InfoWatch Traffic Monitor ..... 9

3.2 Порядок установки InfoWatch Cisco UCM Adapter ..... 10

3.3 Удаление InfoWatch Cisco UCM Adapter ..... 13

4 Конфигурирование Интеграционной платформы и InfoWatch Cisco UCM Adapter ..... 15

4.1 Общие настройки InfoWatch Integration Adapter ..... 15

4.2 Настройка InfoWatch Cisco UCM Adapter ..... 17

5 Мониторинг функционирования InfoWatch Cisco UCM Adapter ..... 21

6 Глоссарий InfoWatch Cisco UCM Adapter ..... 22

# 1 Введение

InfoWatch Cisco UCM Adapter – служба, осуществляющая передачу событий теневых копий текстовых чатов и файлов. InfoWatch Cisco UCM Adapter получает события из базы данных Cisco UCM и передает их в систему InfoWatch Traffic Monitor версии 6.x.

Настоящее руководство содержит сведения по установке и мониторингу работы InfoWatch Cisco UCM Adapter.

## 1.1 Аудитория

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

Руководство рассчитано на пользователей, имеющих навыки администрирования в среде операционной системы Microsoft Windows.

# 2 Обзор InfoWatch Cisco UCM Adaper

В этой главе:


- Общие сведения об InfoWatch Cisco UCM Adapter
- Состав InfoWatch Cisco UCM Adapter
- Схема работы Infowatch Cisco UCM Adapter
- Аппаратное и программное обеспечение для InfoWatch Cisco UCM Adapter


## 2.1 Общие сведения об InfoWatch Cisco UCM Adapter

InfoWatch Cisco UCM Adapter – это .NET приложение, реализованное в виде службы Windows. Позволяет отправлять теневые копии текстовых чатов и файлов, передаваемых пользователями Cisco UCM (IM and Presence service), в InfoWatch Traffic Monitor версии 6.x.

Основные функции:

- передача данных в InfoWatch Traffic Monitor с помощью pushApi;
- поддержка нескольких серверов БД Cisco UCM;
- поддержка нескольких серверов - хранилищ файлов, передаваемых пользователями Cisco UCM;
- получение копий передаваемых файлов с файловых серверов Cisco UCM по протоколу SSH.

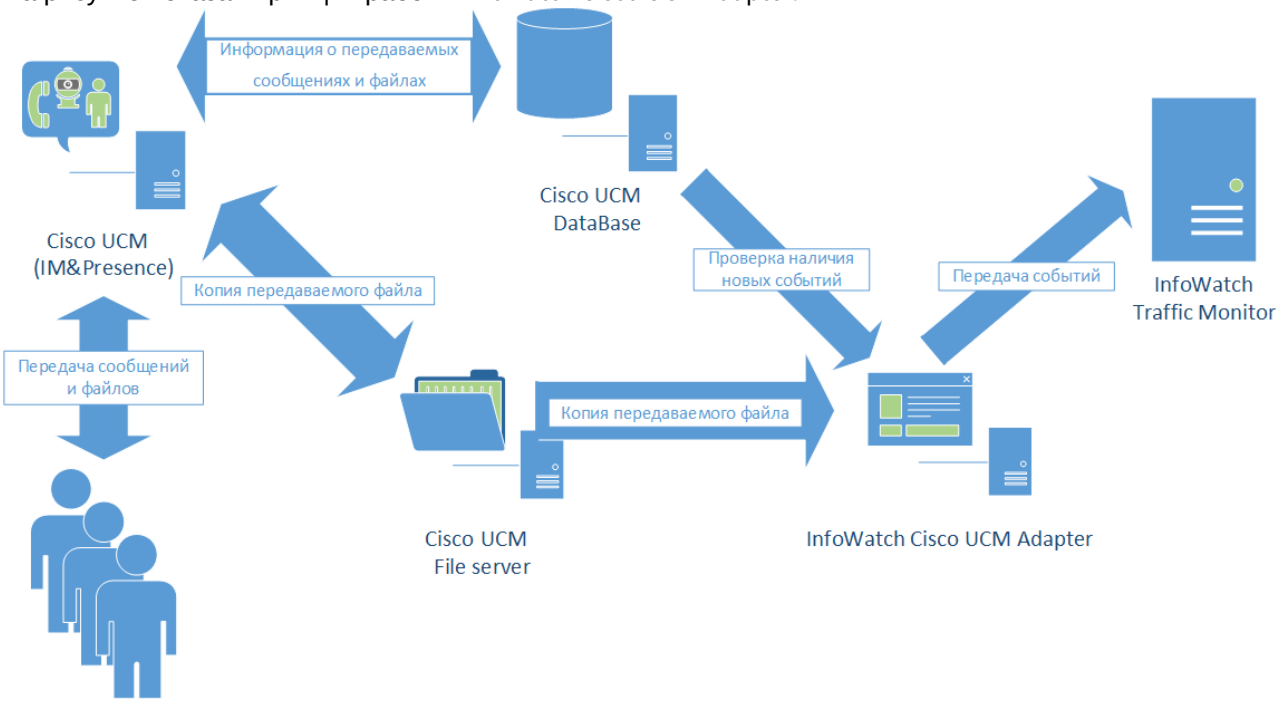
### 2.1.1 Ограничения

1. Для корректного извлечения из Cisco Unified Communications чатов и файлов на сервере с системой Cisco необходимо включить следующие опции:
    - логирование чатов (Message Archiver);
    - логирование передаваемых файлов (Managed File Transfer).
2. Извлечение файлов, переданных через Cisco Unified Communications, возможно, только если для подключения к к файловому серверу адаптер использует логин/пароль (или закрытый ключ) пользователя, от имени которого подключается непосредственно сам UCM для сохранения файлов на этом сервере.
3. Для идентификации отправителей/получателей с LDAP их идентификатор Jabber ID должен быть указан в карточке персоны.
4. Каждый перехваченный файл будет передаваться в Traffic Monitor в виде отдельного события. В склеенных диалогах будут отображаться только имена полученных и переданных файлов.
5. Работа в разрыв (режим *Блокировка*) не поддерживается.

> **Важно!**
>
> Адаптер разработан под Cisco Unified Communications версии 11.0, подключенной к СУБД PostgreSQL. Возможно использование адаптера также с версиями 10.5.2 - 11.5 и другими СУБД, поддерживаемыми Cisco, однако работа адаптера с этими версиями не тестировалась).

## 2.2 Схема работы Infowatch Cisco UCM Adapter

На рисунке показан принцип работы InfoWatch Cisco UCM Adapter.




InfoWatch Cisco UCM Adapter работает следующим образом:

1. Подключается к базе данных Cisco UCM и проверяет её на наличие новых событий (событие должно быть создано позднее, чем дата, заданная в конфигурации).
2. Отправляет найденные события в InfoWatch Traffic Monitor на анализ.
3. Ведет учет идентификаторов событий во избежание повторной отправки.

## 2.3 Состав InfoWatch Cisco UCM Adapter

InfoWatch Cisco UCM Adapter состоит из следующих частей:

- служба Windows;
- конфигуратор – приложение с графическим интерфейсом для настройки адаптера;
- плагин.

Служба Windows и конфигуратор состоят из следующих компонентов:

| Компонент | Назначение | Имя файла |
|---|---|---|
| `Plugin Contract` | Библиотека, обеспечивающая взаимодействие с плагинами | `InfoWatch.PluginPlatform.Contract.dll` |
| `Configuration library` | Библиотека с описанием структуры конфигурации службы | `InfoWatch.PluginPlatform.Service.Configiration.dll` |

| Компонент | Назначение | Имя файла |
| --- | --- | --- |
| InfoWatch Traffic Monitor Connector | Обеспечивает взаимодействие с InfoWatch Traffic Monitor по протоколу pushApi | InfoWatch.PluginPlatform.Service.Connector.dll |
| Common components | Общие компоненты для взаимодействия службы и конфигуратора | InfoWatch.PluginPlatform.Service.Core.dll<br>InfoWatch.PluginPlatform.Service.Core.Contract.dll<br>InfoWatch.PluginPlatform.Service.Core.Logger.dll |
| Plugin manifest | Описание манифеста плагина в формате JSON | InfoWatch.PluginPlatform.Service.Core.PluginHost.JsonPluginManifest.dll |
| Event context | Описание контекстов событий, получаемых от плагинов | InfoWatch.PluginPlatform.Service.FileQueue.JsonContext.dll |
| Microsoft Enterprise Libraries | Библиотека Microsoft для разработчиков, используется для логирования | Microsoft.Practices.EnterpriseLibrary.Common.dll<br>Microsoft.Practices.EnterpriseLibrary.Logging.dll<br>Microsoft.Practices.ServiceLocation.dll<br>Microsoft.Practices.Unity.dll<br>Microsoft.Practices.Unity.Interception.dll |
| PushApi thrift protocol | Описание протокола pushApi thrift | Thrift.dll<br>pushapi-thrift.dll |
| Ionic Zip | Библиотека Ionic zip для поддержки ZIP | Ionic.Zip.dll |
| Newtonsoft Json | Библиотека, обеспечивающая сериализацию и десериализацию в JSON | Newtonsoft.Json.dll |
| Ru resources | Дополнительные ресурсы | InfoWatch.PluginPlatform.Service.Core.resources.dll<br>InfoWatch.PluginPlatform.Service.Configurator.resources.dll |
| Service | Исполняемый файл службы Windows | InfoWatch.PluginPlatform.exe |
| Service configuration file | Конфигурационный файл службы | InfoWatch.PluginPlatform.exe.config |

| Компонент | Назначение | Имя файла |
|---|---|---|
| `Configurator` | Исполняемый файл конфигуратора | `InfoWatch.PluginPlatform.Service.Configurator.exe` |
| `Configurator configuration file` | Конфигурационный файл конфигуратора | `InfoWatch.PluginPlatform.Service.Configurator.exe.config` |

В состав плагина для Cisco UCM (IM and Presence) входят следующие компоненты:

| Компонент | Назначение | Имя файла |
|---|---|---|
| `Manifest` | Манифест плагина | `manifest.json` |
| `Plugin core` | Основной файл плагина | `InfoWatch.PluginPlatform.Plugin.CiscoIm.dll` |
| `Database provider` | Библиотека, обеспечивающая работу с БД | `InfoWatch.DeviceMonitor.Database.Core.dll`<br>`Mono.Security.dll`<br>`Npgsql.dll`<br>`Oracle.DataAccess.dll` |
| `Ssh provider` | Библиотека, обеспечивающая работу с удаленными файловыми серверами по SSH | `Renci.SshNet.dll` |
| `Ru resources` | Дополнительные ресурсы | `InfoWatch.DeviceMonitor.Database.Core.resources.dll`<br>`InfoWatch.PluginPlatform.Plugin.CiscoIm.resources.dll` |

## 2.4 Аппаратное и программное обеспечение для InfoWatch Cisco UCM Adapter

**Требования к аппаратному обеспечению:**

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

**Требования к программному обеспечению:**

- Операционная система на выбор:
  - Microsoft Windows 2008 Server Service Pack 2 и более поздние;
  - Microsoft Windows Server 2016;
  - Microsoft Windows Server 2019.

- Microsoft .NET Framework 4.5.

# 3 Установка InfoWatch Cisco UCM Adapter

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

1. Сгенерировать лицензию для InfoWatch Traffic Monitor.
2. Установить сгенерированную лицензию в InfoWatch Traffic Monitor.
3. На сервер, где будет работать адаптер, установить Microsoft .Net Framework 4.5.1 (если не установлено).
4. Установить Infowatch Cisco UCM Adapter.
5. 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.

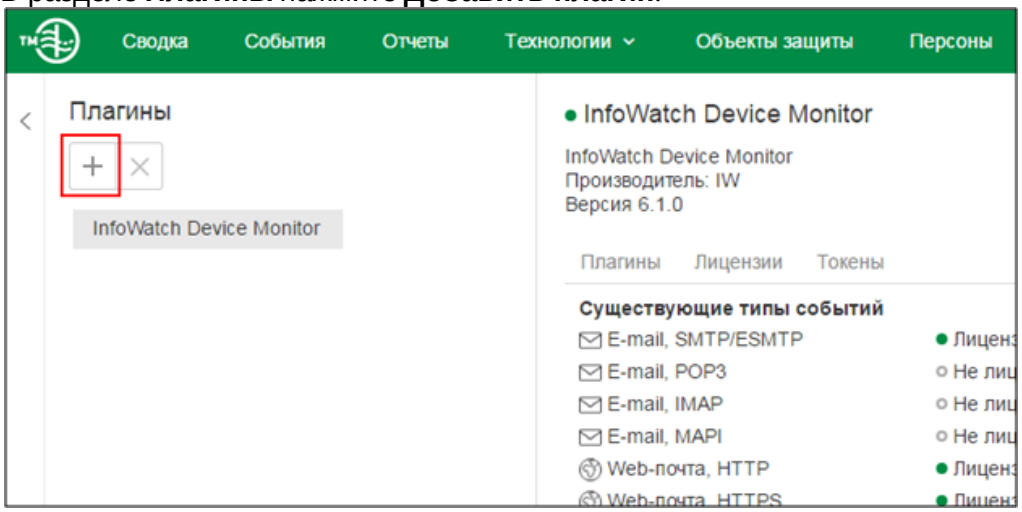
На вкладке настроек плагина необходимо:

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

## 3.1 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**.

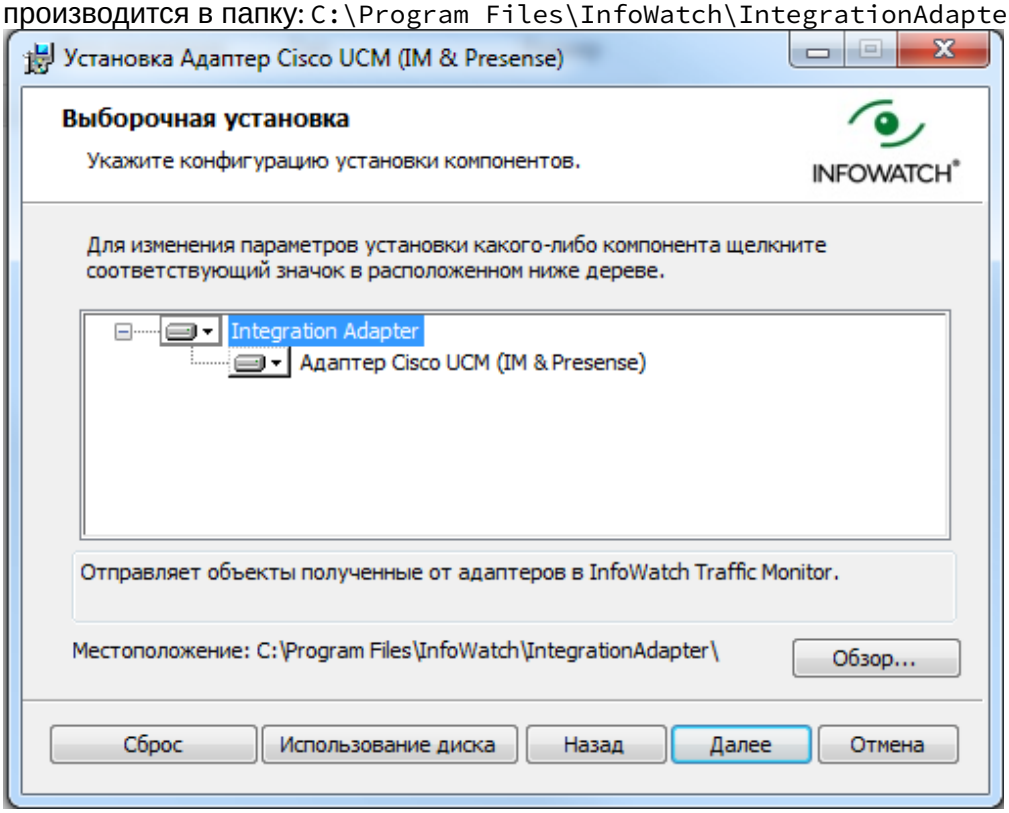
## 3.2 Порядок установки InfoWatch Cisco UCM Adapter

> **Важно!**
>
> Пользователь, выполняющий установку, должен обладать правами локального администратора на данном компьютере.

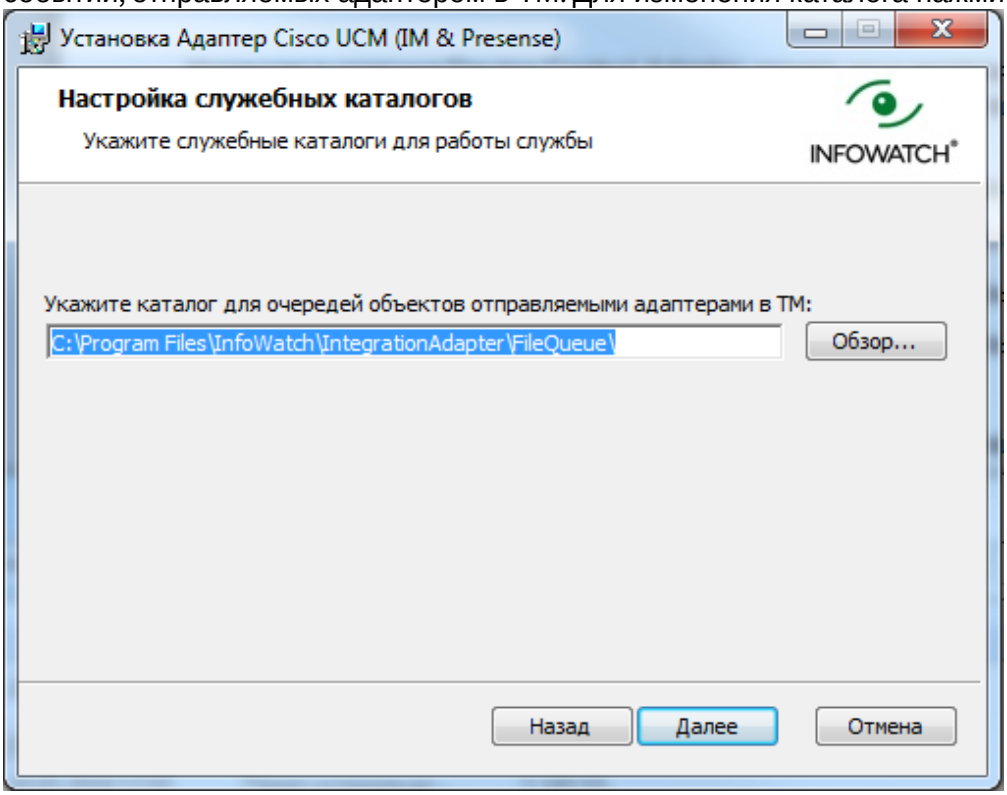
Шаги установки:

1. На диске с дистрибутивом запустите один из файлов:
   - Если используется 64-разрядная ОС:
     - `pluginplatform.3.2.0.x.CiscoIm.x64.ru.msi` - для запуска мастера установки с русским языком интерфейса;
     - `pluginplatform.3.2.0.x.CiscoIm.x64.en.msi` - для запуска мастера установки с английским языком интерфейса.
   - Если используется 32-разрядная ОС:
     - `pluginplatform.3.2.0.x.CiscoIm.x86.ru.msi` - для запуска мастера установки с русским языком интерфейса;
     - `pluginplatform.3.2.0.x.CiscoIm.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 адаптера Cisco UCM Adapter происходит совместно с установкой Интеграционной платформы. 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`.

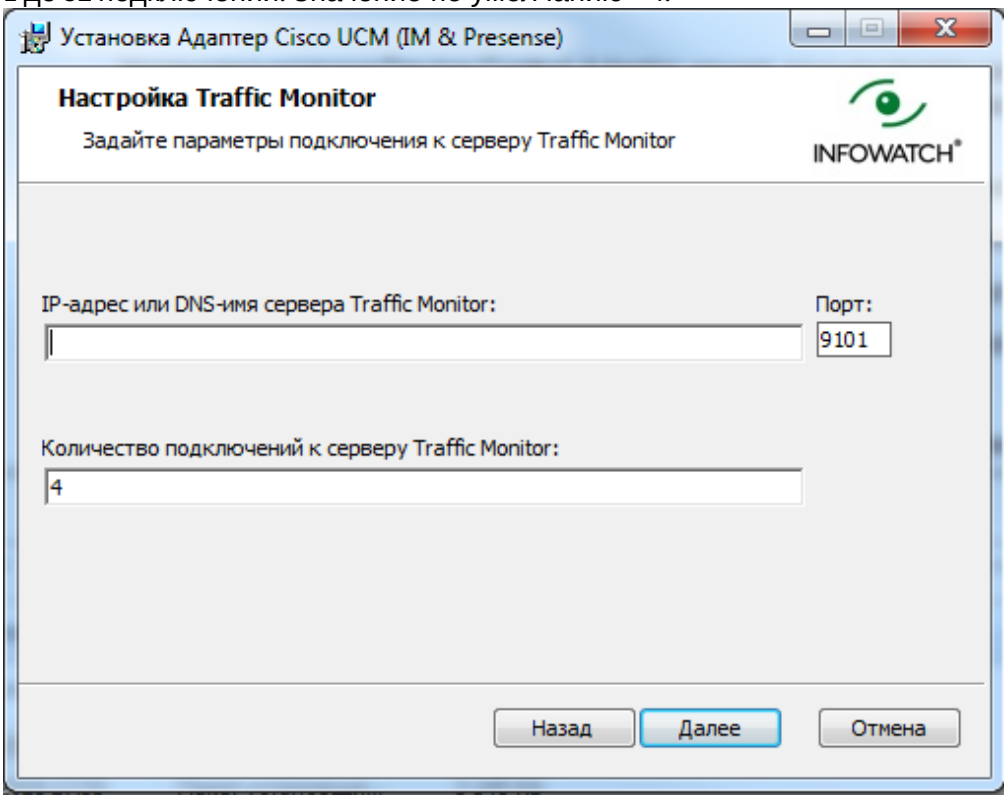



6. Нажмите **Далее**.
7. Укажите каталог очередей объектов - каталог, в котором создаются файловые очереди событий, отправляемых адаптером в TM. Для изменения каталога нажмите **Обзор**.



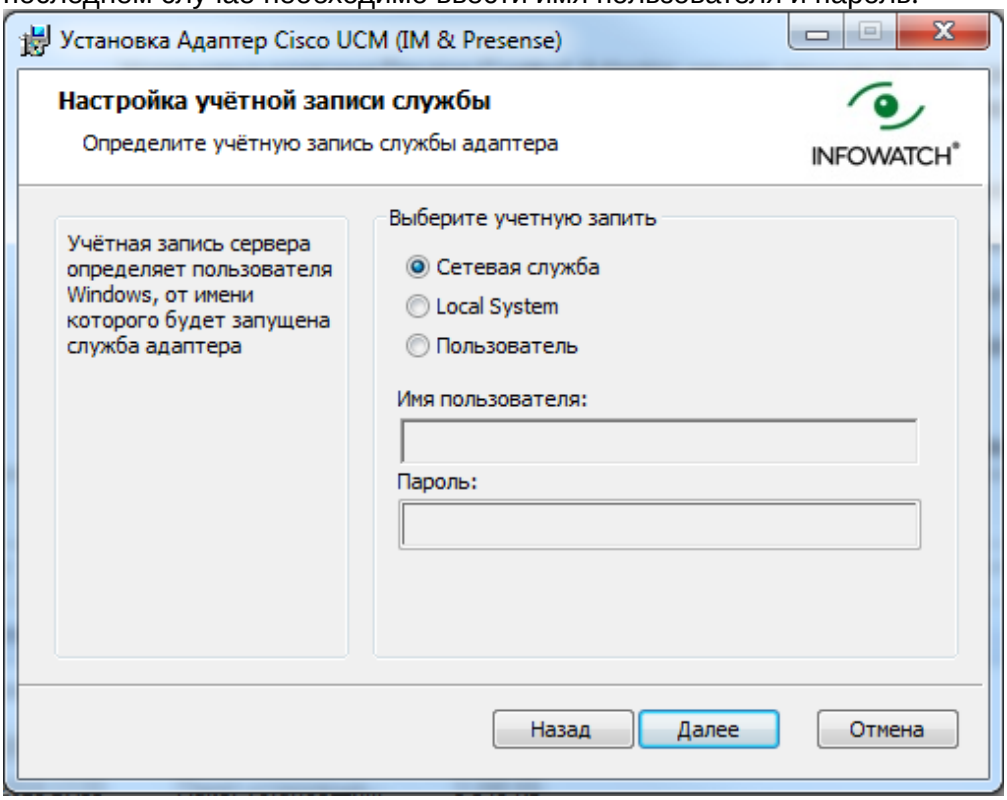

8. Нажмите **Далее**.
9. Настройте параметры соединения с сервером InfoWatch Traffic Monitor. Укажите:

- IP-адрес или DNS-имя сервера InfoWatch Traffic Monitor;
- порт сервера InfoWatch Traffic Monitor, через который будут доставляться события (по умолчанию 9101);
- количество подключений к серверу InfoWatch Traffic Monitor. Вы можете указать от 1 до 32 подключений. Значение по умолчанию – 4.




10. Нажмите **Далее**.
11. Определите учетную запись службы адаптера: **Сетевая служба, Local System** или **Пользователь**, от имени которого будет запущена служба адаптера. В

последнем случае необходимо ввести имя пользователя и пароль.




12. Нажмите **Далее.**

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

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

## 3.3 Удаление InfoWatch Cisco UCM Adapter

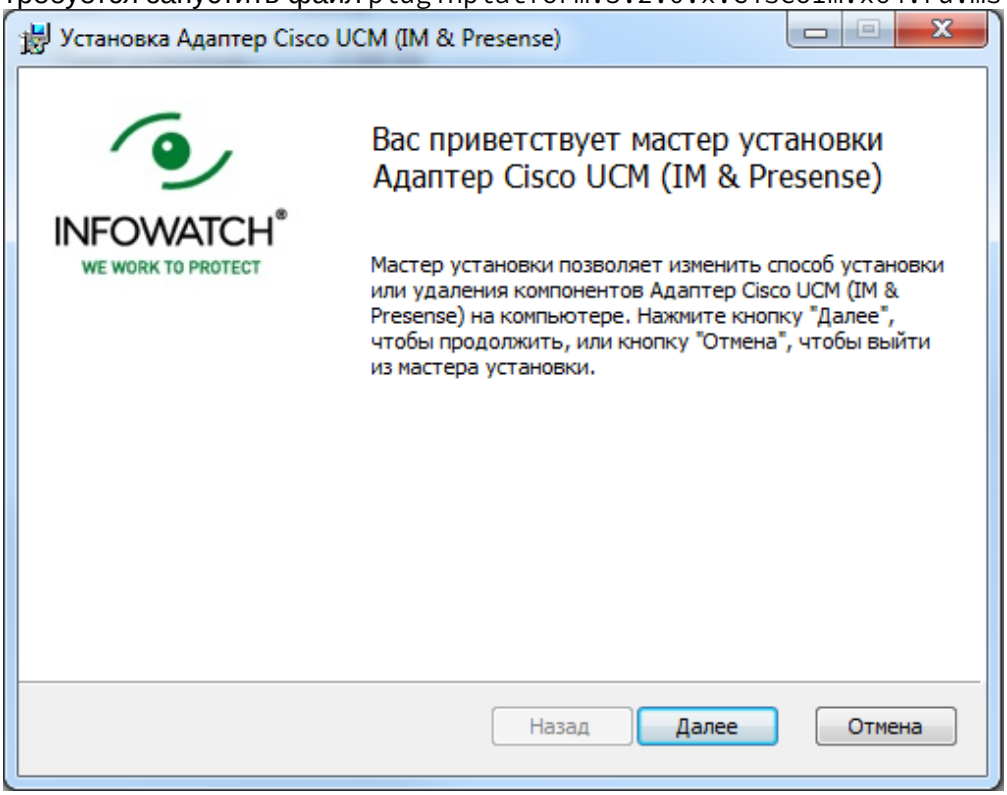
Вы можете удалить Адаптер либо средствами ОС Windows из Панели Управления, либо запустив установочный пакет.

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

Чтобы удалить InfoWatch Cisco UCM 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.3.2.0.x.CiscoIm.x64.ru.msi`.




2. Нажмите **Далее**.
3. Выберите **Удалить**.
4. Убедитесь, что Cisco UCM 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 Cisco UCM 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**:

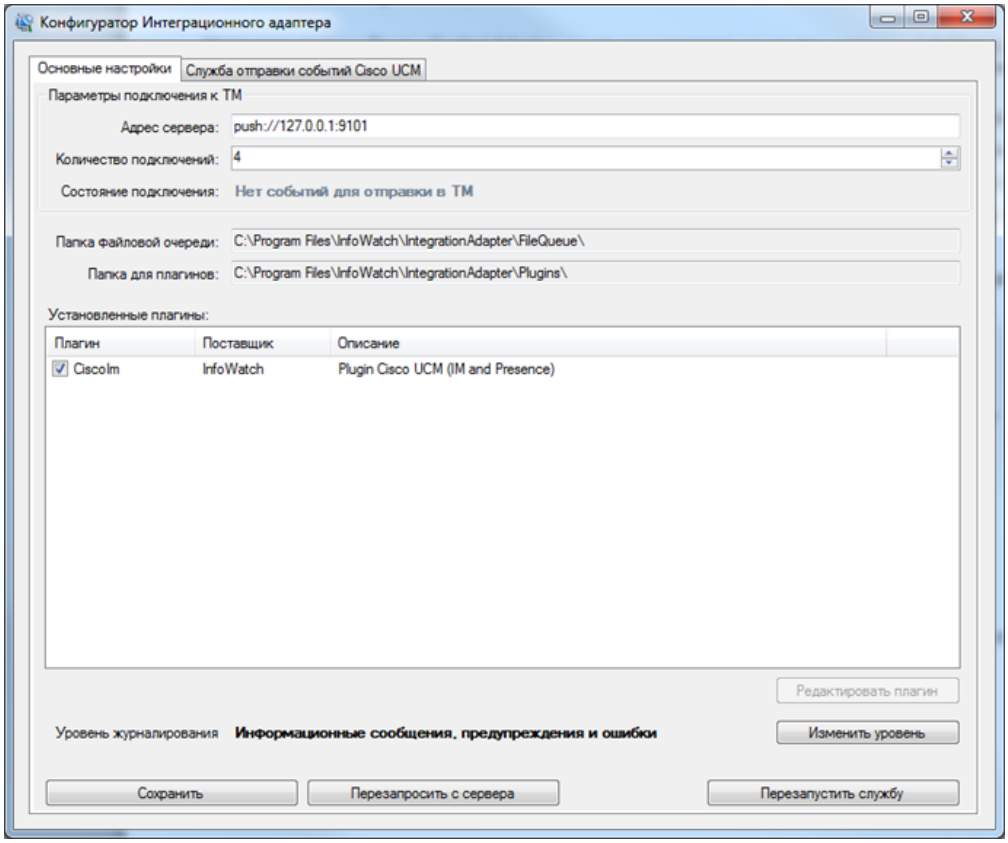
- воспользуйтесь ярлыком на рабочем столе **Конфигуратор Интеграционного адаптера**;
- в меню **Пуск** -> **Все программы** -> **InfoWatch** -> **IntegrationAdapter** выберите пункт **Конфигуратор Интеграционного адаптера**;
- в папке, где установлен InfoWatch Integration Adapter, запустите приложение `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 Cisco UCM Adapter перейдите на вкладку **Служба отправки событий Cisco UCM** (см. "Настройка InfoWatch Cisco UCM 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.



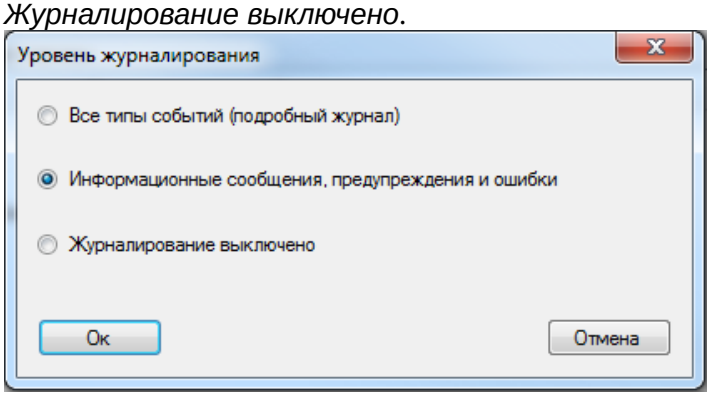
В списке **Установленные плагины** отмечены загруженные в платформу плагины.

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.

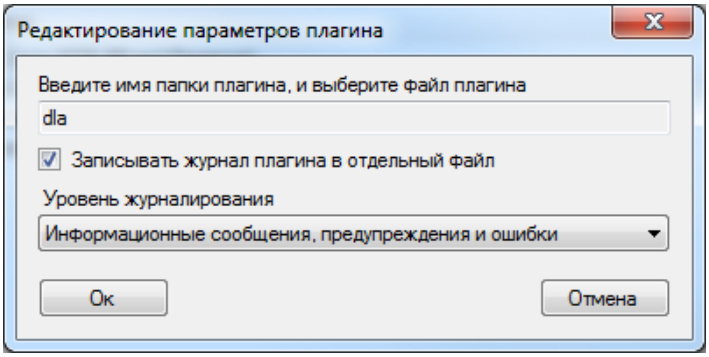
> **Важно!**
>
> Так как как Windows-служба InfoWatch Integration Adapter работает с правами пользователя «NETWORK SERVICE», необходимо убедится, что данному пользователю предоставлен доступ к указанным папкам.

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*.



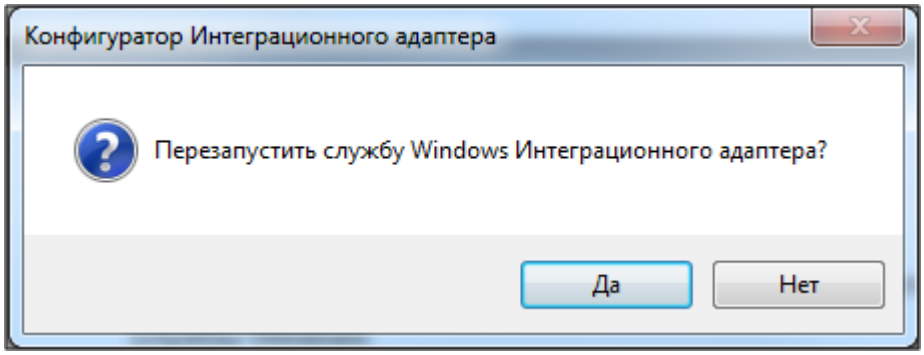

Чтобы изменить уровень журналирования для отдельного плагина:

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**.

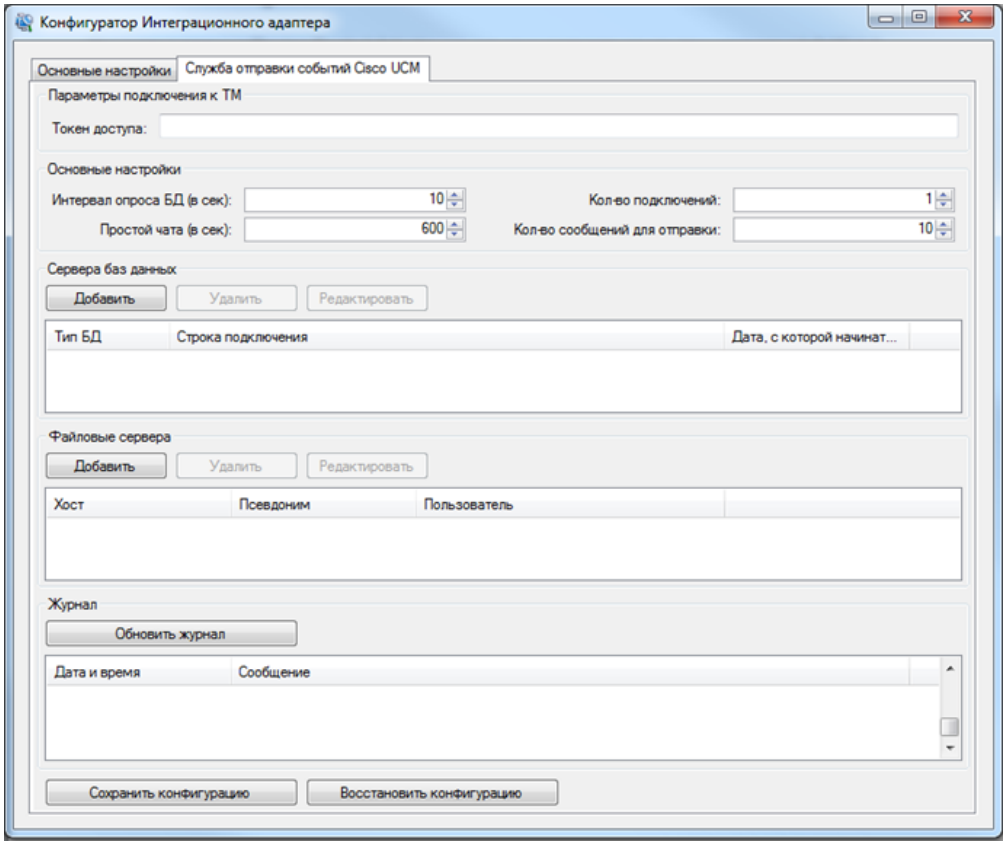
После изменения настроек нажмите **Сохранить**. Будет выведен запрос на перезапуск службы Windows.




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

## 4.2 Настройка InfoWatch Cisco UCM Adapter

Для настройки плагина запустите приложение **Конфигуратор Интеграционного адаптера** и перейдите на вкладку **Служба отправки событий Cisco UCM**.




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**.

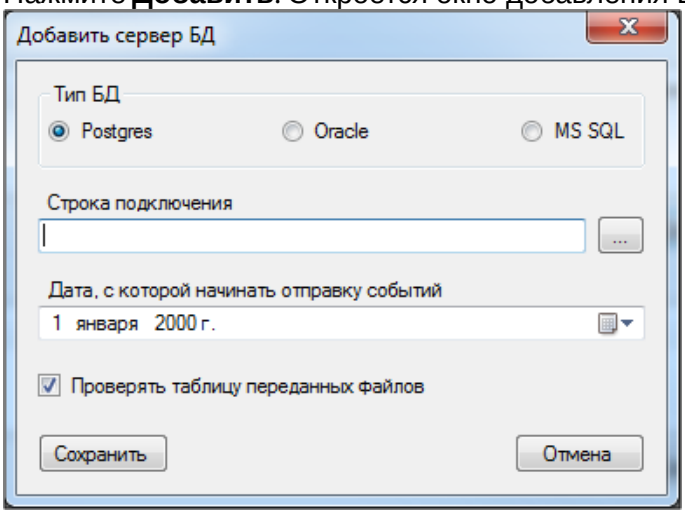
В области **Основные настройки** укажите следующие параметры:

- **Интервал опроса БД (в сек)** – интервал опроса баз данных Cisco UCM (в секундах). Список баз данных задается в области **Сервера баз данных**;
- **Количество подключений** – количество подключений, устанавливаемых плагином к каждой из баз данных Cisco UCM;
- **Простой чата** – время простоя события, по достижении которого содержимое отправляется в InfoWatch Traffic Monitor независимо от количества сообщений для отправки;
- **Количество сообщений для отправки** – количество сообщений в одном событии, по достижении которого содержимое события отправляется в InfoWatch Traffic Monitor.

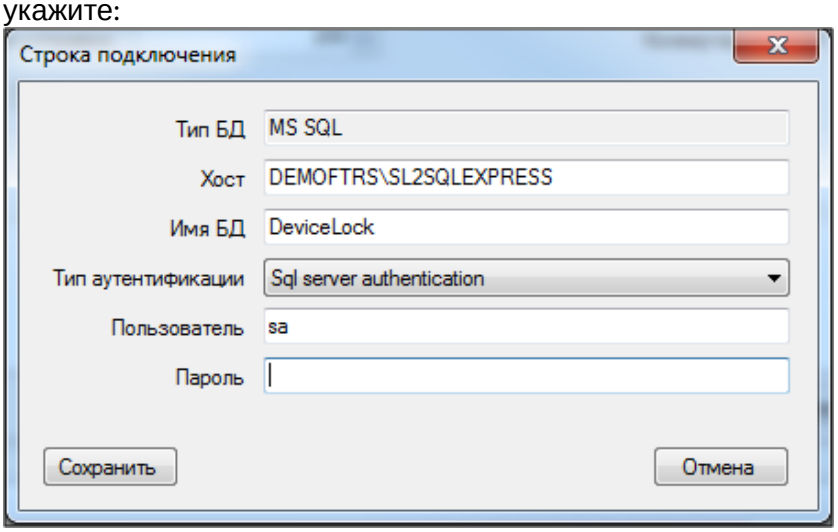
В области **Сервера баз данных** укажите список опрашиваемых серверов баз данных Cisco UCM.

Для добавления сервера:

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




2. Выберите тип БД: **Postgres**, **Oracle** или **MS SQL**.
3. Укажите строку подключения к базе данных. Строку можно ввести вручную либо нажать ... для формирования строки подключения. В открывшемся диалогом окне укажите:

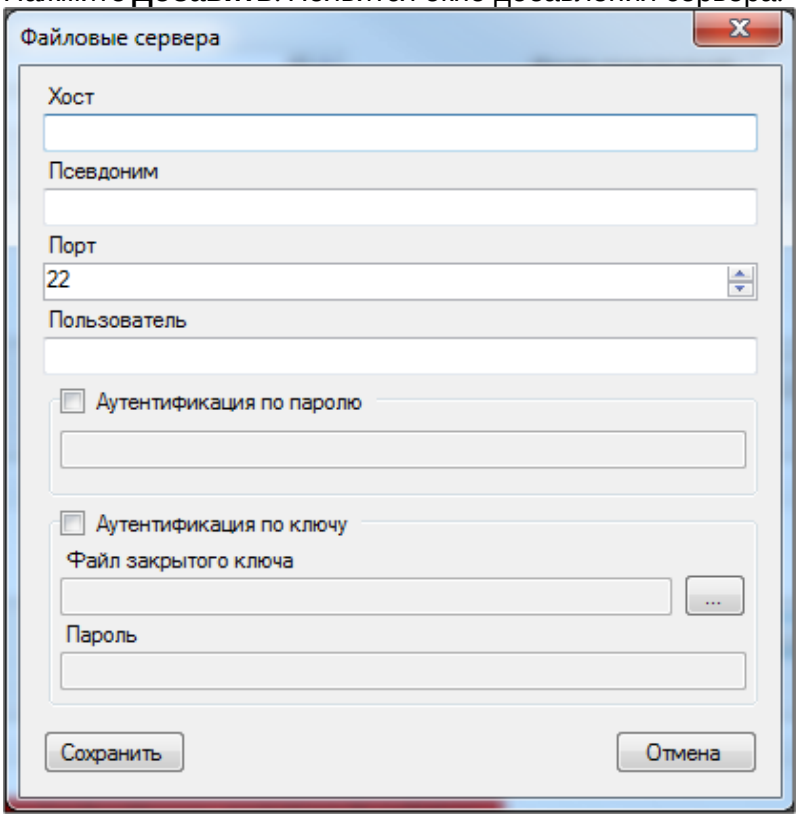



   - **Хост** – путь до экземпляра СУБД;
   - **Имя БД** – имя просматриваемой базы данных;
   - **Тип аутентификации**:
     - Проверка подлинности Windows (**Integrate security**) – можно использовать, если пользователь, от чьего имени запущена служба InfoWatch Integration Adapter, имеет доступ к требуемой базе данных;
     - Проверка подлинности SQL server (**SQL server authentication**).
   - Имя пользователя учетной записи БД и пароль.
4. Нажмите **Сохранить** для формирования строки подключения
5. Укажите дату, начиная с которой нужно просматривать события (может понадобиться для первого запуска, чтобы не загружать очень старые сообщения).
6. Нажмите **Сохранить** для добавления сервера БД.

В области **Файловые сервера** укажите список серверов, на которых хранятся передаваемые пользователями Cisco UCM файлы. Доступ к данным серверам осуществляется по SSH.

Для добавления файлового сервера:

1. Нажмите **Добавить**. Появится окно добавления сервера.




2. В открывшемся окне укажите настройки файлового сервера:
   - **Хост** – доменное имя или IP-адрес сервера;
   - **Псевдоним** – альтернативное имя (необязательно), также доменное имя или IP-адрес;
   - **Порт**, на котором настроен SSH-сервер;
   - **Пользователь** - имя пользователя (должно совпадать с именем пользователя, под которым Cisco UCM записывает файлы на файловый сервер, так как при записи Cisco UCM выставляет права "только для пользователя";
   - Способ аутентификации: **Аутентификация по паролю** или **Аутентификация по ключу**. Закрытый ключ должен быть в формате SSH.
3. Нажмите **Сохранить**.

Для редактирования ранее добавленного сервера баз данных или файлового 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 функционирования InfoWatch Cisco UCM Adapter

Функционирование Адаптера можно проверить в Журнале приложения InfoWatch Cisco UCM Adapter. Он находится в папке установки Адаптера (по умолчанию `C:\Program Files\InfoWatch\IntegrationAdapter\Logs` для 32-х разрядных ОС либо `C:\ProgramFiles (x86)\InfoWatch\IntegrationAdapter\` для 64-х разрядных ОС).

Папка содержит следующие файлы:

- **iwps.txt** – основной файл журнала InfoWatch Integration Adapter. В этом журнале:
  - отмечаются события, связанные с загрузкой плагинов;
  - показано, выполнено ли подключение к InfoWatch Traffic Monitor,
  - фиксируются ошибки, возникающие при отправке событий в InfoWatch Traffic Monitor.
- **configurator.txt** – файл журнала приложения Конфигуратор;
- **plugin_cisoim.txt** – файл журнала плагина Cisco UCM;
- службы ОС Windows.

Для проверки функционирования службы Windows InfoWatch Integration Adapter откройте **Панель Управления - > Администрирование -> Службы** и выберите службу **InfoWatch Integration Adapter Service**. В столбце **Состояние** отображается, работает ли служба в данный момент.

# 6 Глоссарий InfoWatch Cisco UCM Adapter

| |
|---|
| **InfoWatch Traffic Monitor, TM**<br>Система, предназначенная для перехвата, фильтрации и анализа информационных потоков компьютерной системы. |
| **InfoWatch Integration Adapter**<br>Универсальный Интеграционный Адаптер |
| **Контроль доступа к периферийным устройствам**<br>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. |
| **БД**<br>База данных |
| **Теневая копия текстового чата**<br>Копия текста, выделенного из документа, отправленного на печать. |
| **Теневая копия файла**<br>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. |