

INFOWATCH

InfoWatch Sample Documents Autoupdate 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 Общие сведения об Infowatch Sample Documents Autoupdate Adapter 4

2.1 Состав InfoWatch Integration Adapter 4

2.2 Аппаратное и программное обеспечение 5

3 Установка InfoWatch Sample Documents Autoupdate Adapter 7

3.1 Установка плагина для InfoWatch Traffic Monitor 7

3.2 Порядок установки InfoWatch Sample Documents Autoupdate Adapter 8

3.3 Удаление InfoWatch Sample Documents Autoupdate Adapter 11

4 Конфигурирование InfoWatch Sample Documents Autoupdate Adapter ... 12

4.1 Общие настройки InfoWatch Integration Adapter 12

4.2 Настройка InfoWatch Sample Documents Autoupdate Adapter 14

4.2.1 Создание задачи обновления ЭД 15

4.2.2 Запуск задачи обновления ЭД 18

5 Каталоги ЭД 20

6 Глоссарий для InfoWatch Sample Documents Autoupdate Adapter 21

1 Введение

Информация, содержащаяся в данном Руководстве, предназначена для пользователей, выполняющих установку и администрирование InfoWatch Integration Adapter и Адаптера InfoWatch Sample Documents Autoupdate Adapter.

Аудитория

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

2 Общие сведения об Infowatch Sample Documents Autoupdate Adapter

Infowatch Sample Documents Autoupdate Adapter - интеграционный адаптер, который выполняет синхронизацию содержимого каталога эталонных документов в Traffic Monitor с источником данных - сетевым каталогом.

2.1 Состав InfoWatch Integration Adapter

InfoWatch Integration Adapter состоит из следующих частей:

- Служба Windows;
- Конфигуратор – приложение с графическим интерфейсом для настройки;
- Плагин InfoWatch Sample Documents Autoupdate Adapter.

Служба Windows и конфигуратор состоят из следующих компонентов:

Компонент	**Описание**	**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
InfoWatch Traffic Monitor Connector	Обеспечение взаимодействия 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 InfoWatch.PluginPlatform.Service.Core.Contract.dll 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

Компонент	Описание	Имя файла
Microsoft Enterprise Libraries	Библитека Microsoft для разработчиков, используется для логгирования	Microsoft.Practices.EnterpriseLibrary.Common.dll Microsoft.Practices.EnterpriseLibrary.Logging.dll Microsoft.Practices.ServiceLocation.dll Microsoft.Practices.Unity.dll Microsoft.Practices.Unity.Interception.dll
PushApi thrift protocol	Описание протокола pushApi thrift	Thrift.dll 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 InfoWatch.PluginPlatform.Service.Configurator .resources.dll
Service	Исполняемый файл службы Windows	InfoWatch.PluginPlatform.exe
Service configuration file	Конфигурационный файл службы	InfoWatch.PluginPlatform.exe.config
Configurator	Исполняемый файл конфигуратора	InfoWatch.PluginPlatform.Service.Configurator.exe
Configurator configuration file	Конфигурационный файл конфигуратора	InfoWatch.PluginPlatform.Service.Configurator.exe .config

2.2 Аппаратное и программное обеспечение

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 Windows Vista SP2.
- Microsoft .NET Framework 4.5.1.

3 Установка InfoWatch Sample Documents Autoupdate Adapter

Установка InfoWatch Integration Adapter происходит автоматически при установке плагина-адаптера Sample Documents Autoupdate Adapter. Для корректного функционирования интеграционной платформы необходимо выполнить следующие действия:

1. Сгенерировать лицензию для InfoWatch Traffic Monitor (лицензирование сторонних перехватчиков для издателя **IW_ADAPTERS** и любого протокола мессенджера Skype).
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 Sample Documents Autoupdate Adapter.
5. Запустить Конфигуратор InfoWatch Integration Adapter, внести изменения в настройки.

> **Важно!**
>
> Доступ к управлению эталонными документами в ТМ предоставляется вне зависимости от наличия лицензии на модуль автообновления ЭД. Адаптер Infowatch Sample Documents Autoupdate Adapter является частью поставки ТМ и не требует отдельной лицензии.

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.

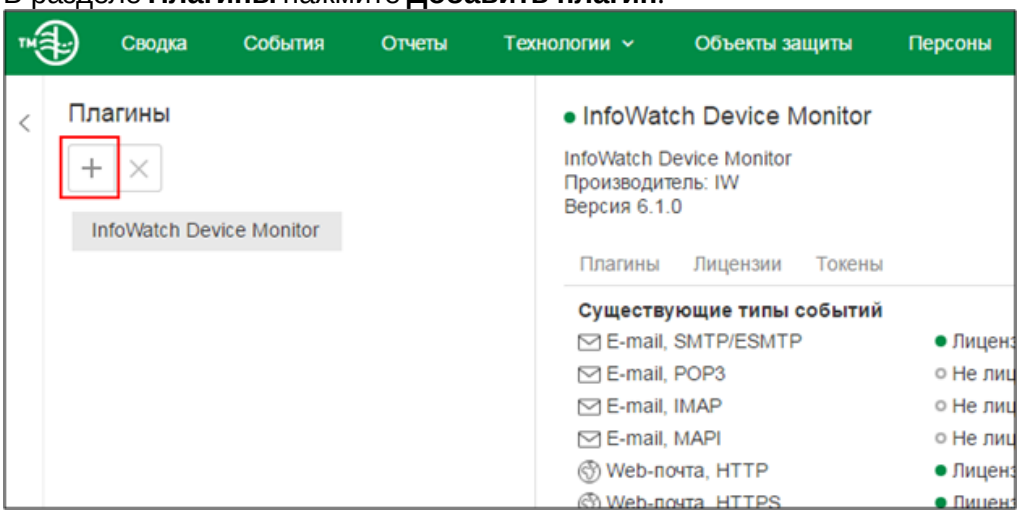
На вкладке настроек плагина необходимо:

1. Ввести токен доступа к InfoWatch Traffic Monitor (можно получить на странице установленного ранее плагина для InfoWatch Traffic Monitor). Подробнее см. "Настройка InfoWatch Sample Documents Autoupdate Adapter".
2. Нажать **Сохранить**. Плагин автоматически перезапустится.

3.1 Установка плагина для InfoWatch Traffic Monitor

Для установки плагина InfoWatch Traffic Monitor:

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



2. В появившемся окне нажмите **Загрузить.**
3. Выберите файл плагина (`TmPlugin_SampleDocuments.zip`). Если в открывшемся окне добавления плагина установлен статус *Лицензирован*, то установлена корректная лицензия на синхронизацию эталонных документов.
4. Для завершения установки нажмите **Установить**.

Описание файла плагина:

```
{
        "PLUGIN_ID": "791DFFB37098450EB8D2AB5B5DE8C6CB791DFFB3",
        "DISPLAY_NAME": "InfoWatch Sample documents Autoupdate Adapter",
        "DESCRIPTION": "Предустановленный плагин для адаптера автообновления эталонных документов",
        "VERSION": "1.0.0",
        "IS_SYSTEM": false,
        "VENDOR": "IW",
        "DATATYPE": [{
                "VALUE": "stamper",
                "TYPE": "DE"
        }],
        "PATTERN_SEARCH_LICENSE": "{\"operator\": \"and\", \"conditions\": [{\"cas\": \"stamper\"}]}",
        "LICENSE": []
}
```

3.2 Порядок установки InfoWatch Sample Documents Autoupdate Adapter

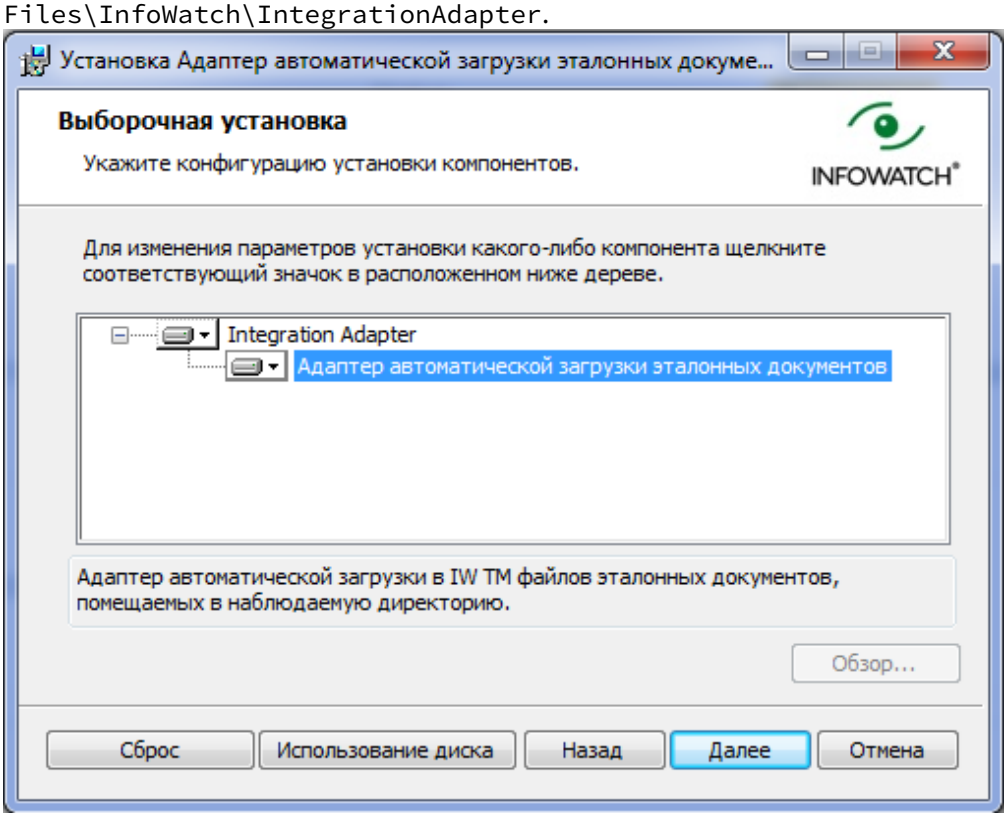
> **Важно!**
>
> Пользователь, выполняющий установку, должен обладать правами локального администратора на данном компьютере.

Шаги установки:

1. На диске с дистрибутивом запустите один из файлов:

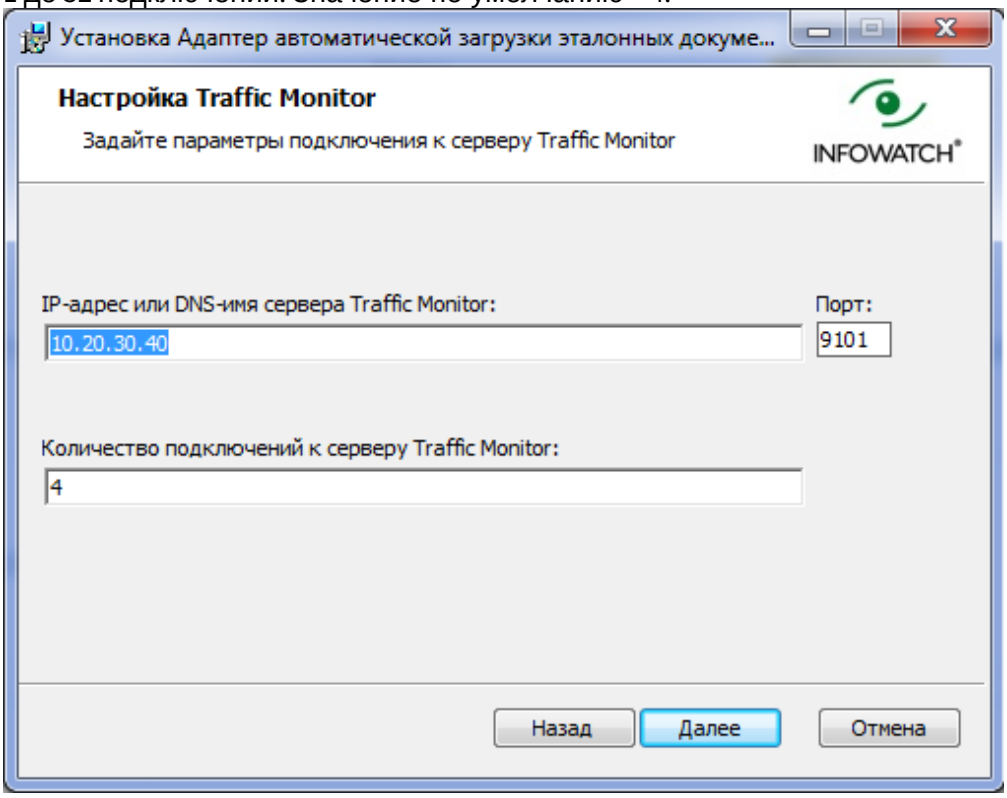
- Если используется 64-разрядная ОС:
  - `pluginplatform.3.2.0.x.SampleDocuments.x64.ru.msi` - для запуска мастера установки с русским языком интерфейса;
  - `pluginplatform.3.2.0.x.SampleDocuments.x64.en.msi` - для запуска мастера установки с английским языком интерфейса.
- Если используется 32-разрядная ОС:
  - `pluginplatform.3.2.0.x.SampleDocuments.x86.ru.msi` - для запуска мастера установки с русским языком интерфейса;
  - `pluginplatform.3.2.0.x.SampleDocuments.x86.en.msi` - для запуска мастера установки с английским языком интерфейса.

2. В окне приветствия мастера установки нажмите **Далее**.
3. Ознакомьтесь с условиями лицензионного соглашения 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 Infowatch Sample Documents Autoupdate 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`.

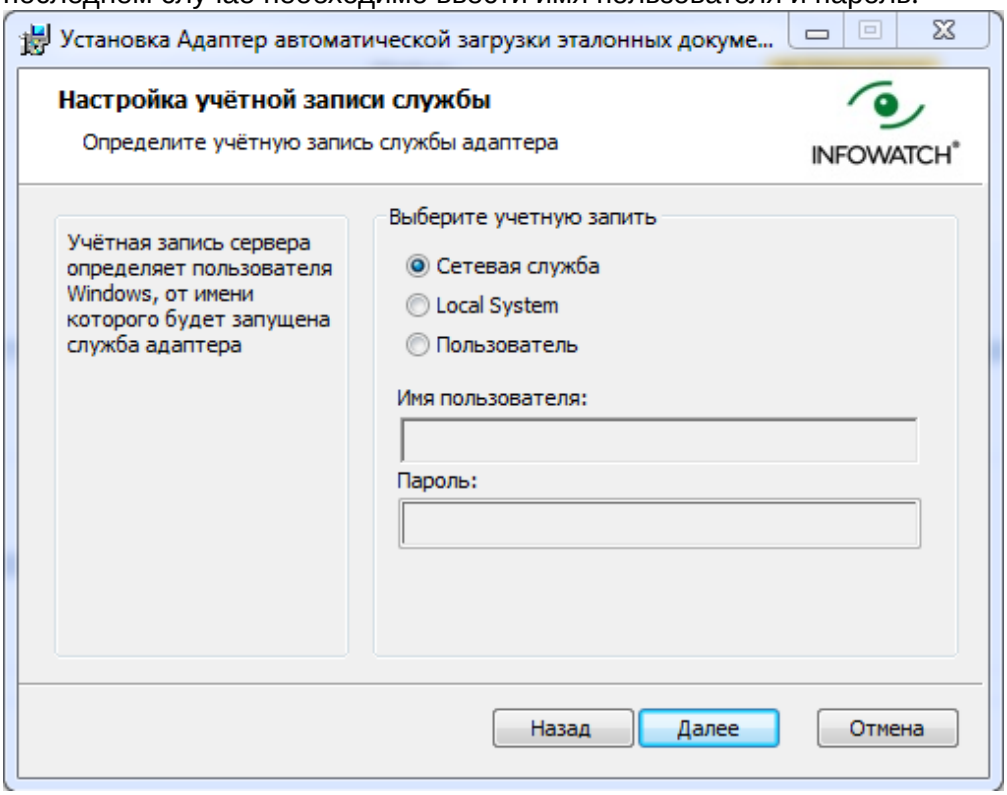


6. Нажмите **Далее**.
7. Настройте параметры соединения с сервером InfoWatch Traffic Monitor. Укажите:
   - IP-адрес или DNS-имя сервера InfoWatch Traffic Monitor;
   - Порт сервера InfoWatch Traffic Monitor, через который будут доставляться события (по умолчанию 9101);

- Количество подключений к серверу InfoWatch Traffic Monitor. Вы можете указать от 1 до 32 подключений. Значение по умолчанию – 4.



8. Нажмите **Далее**.
9. 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.



10. Нажмите **Далее.**

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

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

3.3 Удаление InfoWatch Sample Documents Autoupdate Adapter

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

После удаления адаптера средствами ОС Windows, удалите каталоги файловой очереди и ошибочных сообщений вручную.

Чтобы удалить InfoWatch Sample Documents Autoupdate Adapter:

1. Запустите файл инсталятора, 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.SampleDocuments.x64.ru.msi`.
2. Нажмите **Далее**.
3. В окне выбора доступных действий нажмите **Удалить**.
4. В окне подтверждения нажмите **Удалить**. Все файлы InfoWatch Sample Documents Autoupdate Adapter будут удалены с компьютера вместе с созданными в процессе установки папками.
5. Для завершения процесса удаления нажмите **Готово**.

4 Конфигурирование InfoWatch Sample Documents Autoupdate 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**:

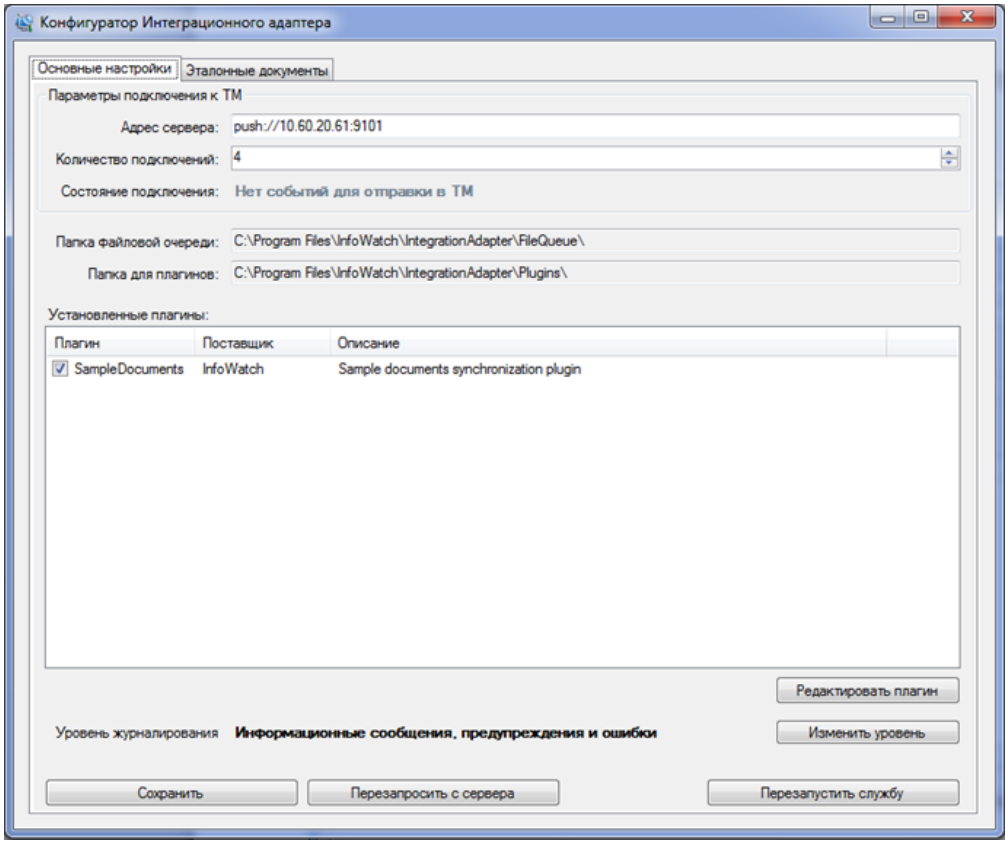
- воспользуйтесь ярлыком на рабочем столе **Конфигуратор Интеграционного адаптера**;
- в меню **Пуск** -> **Все программы** -> **InfoWatch** -> **IntegrationAdapter** выберите пункт **Конфигуратор Интеграционного адаптера**;
- в папке, где установлен InfoWatch Integration Adapter, запустите приложение `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 Sample Documents Autoupdate Adapter перейдите на вкладку **Эталонные документы** (см. "Настройка InfoWatch Sample Documents Autoupdate 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.



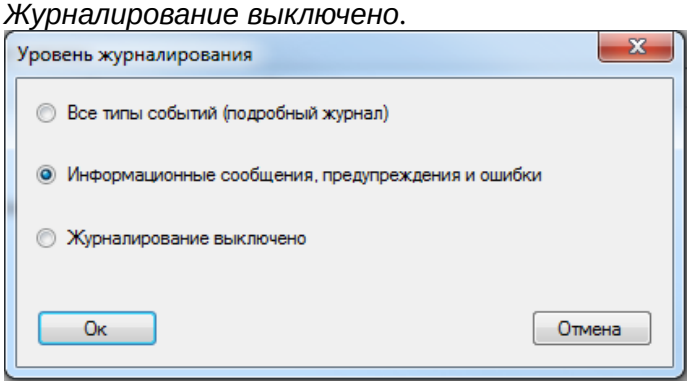
В списке **Установленные плагины** отмечены загруженные в платформу плагины.

Вкладка содержит следующие настройки:

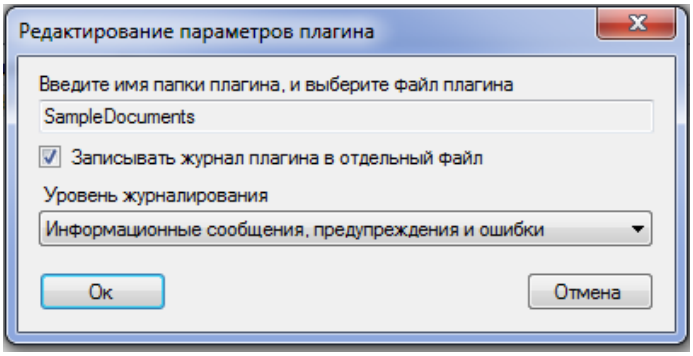
1. В области **Параметры подключения к ТМ**:
   - **Адрес сервера** InfoWatch Traffic Monitor в формате: `push://host:port`, где host – доменное имя или IP-адрес сервера InfoWatch Traffic Monitor, а port – порт сервера InfoWatch Traffic Monitor, через который будут доставляться события (по умолчанию 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*.

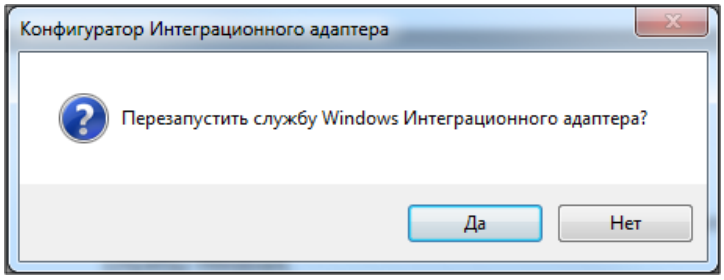


4. Чтобы изменить уровень журналирования для отдельного плагина:
   a. Выберите нужный плагин в списке и нажмите **Редактировать плагин**.
   b. В открывшемся окне укажите, нужно ли вести журнал плагина в отдельном файле, и выберите уровень жуналирования.



c. Нажмите **OK**.

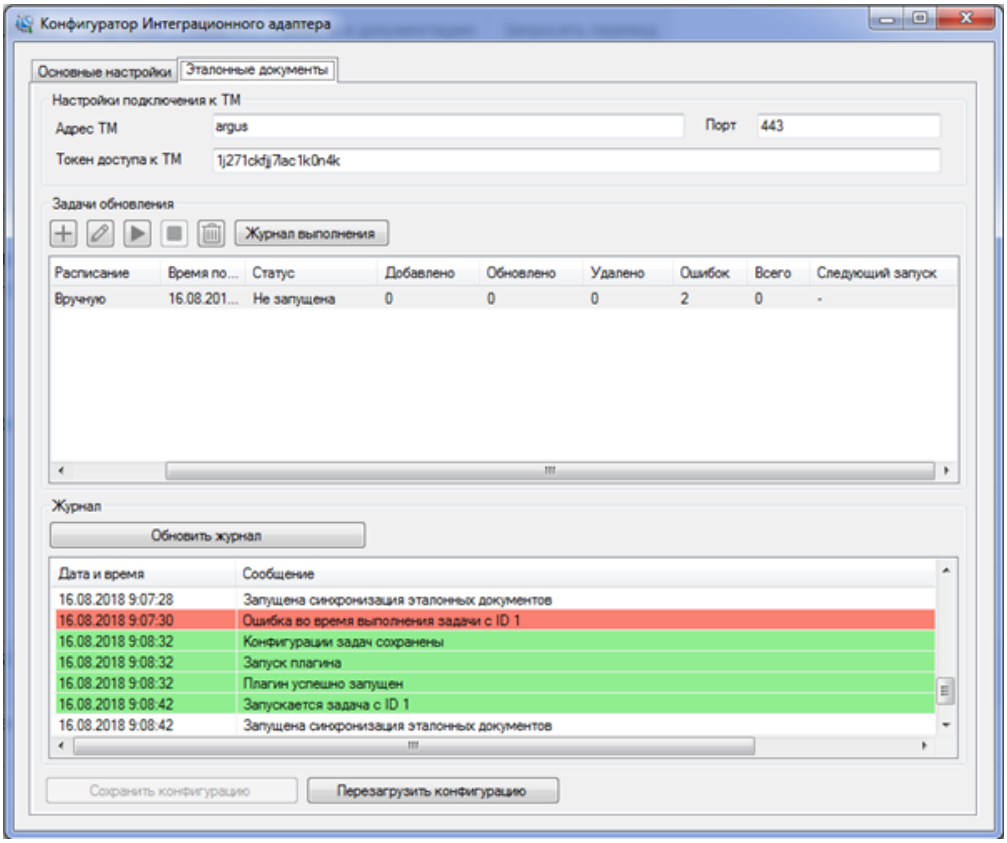
После изменения настроек нажмите **Сохранить**. Будет выведен запрос на перезапуск службы Windows.



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

4.2 Настройка InfoWatch Sample Documents Autoupdate Adapter

Для настройки плагина запустите приложение **Конфигуратор Интеграционного адаптера** и перейдите на вкладку **Эталонные документы**.



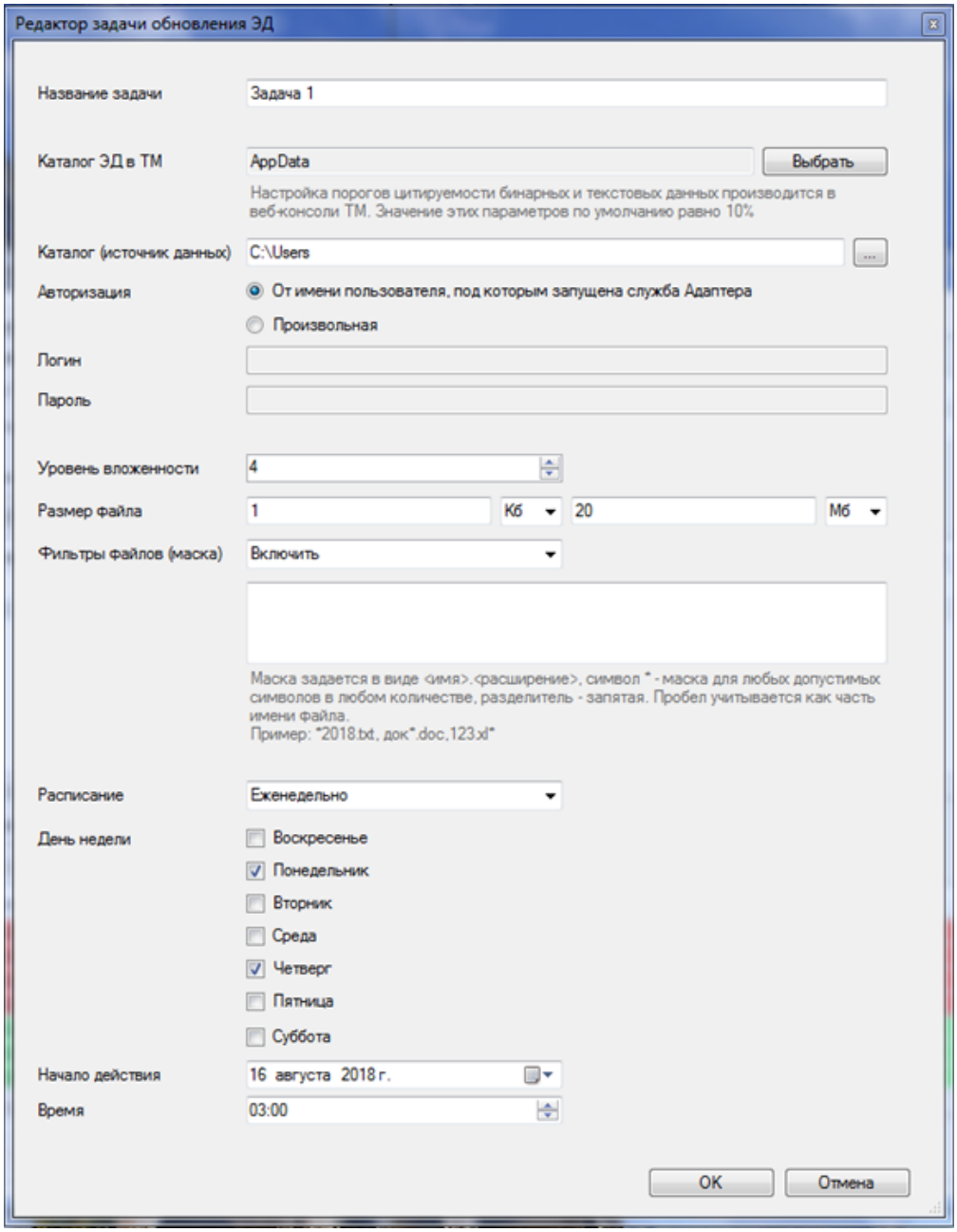
- Для настройки синхронизации эталонных документов вам потребуется:
  1. Указать параметры подключения к серверу Traffic Monitor:
     - Адрес ТМ – адрес сервера Traffic Monitor;
     - Порт – номер SSL-порта (по умолчанию: 443);
     - Токен доступа – строка является видимой только для плагина и InfoWatch Traffic Monitor. Токен доступа к ТМ можно получить в Консоли управления Traffic Monitor, раздел **Плагины**, для издателя **IW_ADAPTERS**.
  2. Создать задачу обновления ЭД. Для этого в области **Задачи обновления** нажмите  и в открывшейся форме заполните необходимые поля (см. Создание задачи обновления ЭД).
     Чтобы отредактировать параметры задачи, выберите нужную задачу в списке и нажмите . Чтобы удалить задачу из списка, нажмите .

4.2.1 Создание задачи обновления ЭД

Чтобы создать задачу обновления ЭД, заполните поля формы:

- Название новой задачи;
- Каталог ЭД (на выбор):
  - из уже существующих в ТМ;
  - созданный пользователем в каталоге «Автоматические эталонные документы»;

- Каталог-источник данных. Это может быть папка, диск или рабочая станция внутри локальной сети, либо диск локального компьютера (например, C:\Users). Подробнее см. в разделе «Создание каталога ЭД»
- Способ авторизации. Это может быть авторизация от имени текущего пользователя, который запустил службу Интеграционного адаптера, либо произвольная авторизация. Во втором случае потребуется указать параметры доступа к учетной записи (Логин и Пароль);
- Необходимые параметры фильтрации:
    - Уровень вложенности папок (от 0 до 6);
    - Размер файла ЭД (от 1 КБ);
    - Маски файлов, которые можно как включать в фильтрацию, так и исключать.
- Параметры запуска задачи обновления ЭД:
    - Расписание (вручную, один раз, каждый день, каждую неделю, каждый месяц);
    - Дату и время начала (если необходимо запускать задачу периодически)



После заполнения всех полей нажмите **Ок**. Новая задача будет добавлена в список задач обновления.

> **Важно!**
>
> Адаптер проверяет статусы документов на дубликаты. Если в каталоге-источнике данных есть дубликаты эталонных документов, загруженных ранее в ТМ, то такие документы повторно загружаться не будут.

Примечание:

В случае если каталог-источник необходимо повторно синхронизировать с измененным каталогом-получателем в ТМ, прежний каталог-получатель в ТМ или его содержимое рекомендуется удалить из ТМ вручную.

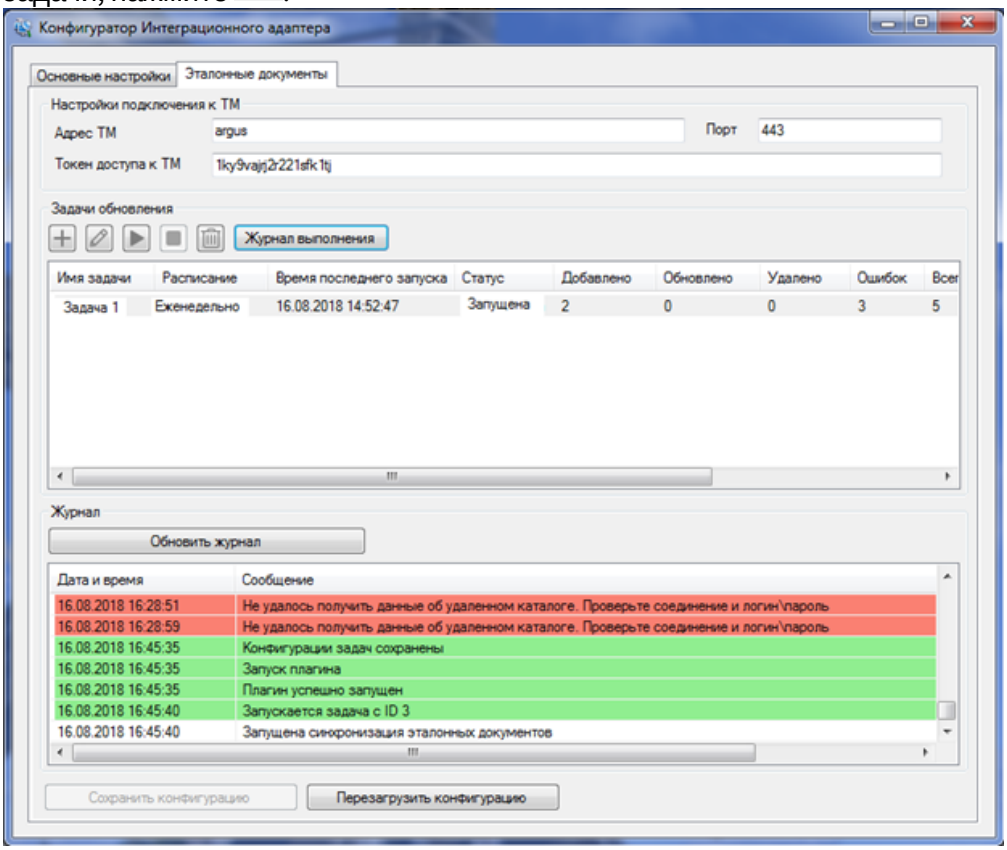
4.2.2 Запуск задачи обновления ЭД

Важно!

После изменения каких-либо настроек для запуска задачи нажмите **Сохранить конфигурацию**. При этом введенные настройки будут сохранены в постоянное хранилище InfoWatch Integration Adapter, а плагин будет перезапущен.

Чтобы запустить задачу обновления ЭД:

1. Выберите задачу, выделив ее в списке.
2. Нажмите . Начнется процесс синхронизации. Если нужно остановить выполнение задачи, нажмите .



Чтобы просмотреть подробности выполнения задачи, нажмите **Журнал выполнения**. Если необходимо отменить несохраненные изменения, нажмите **Восстановить конфигурацию**.

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**.

5 Каталоги ЭД

Все эталонные документы, поступившие в ТМ через Адаптер, помещаются в родительский каталог **Автоматические эталонные документы**.

Чтобы создать новый каталог:

1. Перейдите в *Редактор задачи обновления ЭД->Обзор каталогов ЭД в Traffic Monitor.*
2. Выделите нужный родительский каталог (или корневой каталог **Автоматические эталонные документы)**.
3. Нажмите **Создать каталог**.
4. Введите имя нового каталога и нажмите **Enter**.

Чтобы удалить каталог из дерева, необходимо его выделить и нажать **Удалить каталог**.

Важно!

Невозможно удалить каталог, который используется в другой задаче или ОЗ, как и корневой каталог **Автоматические эталонные документы.**

Пример:

1. Создана следующая структура каталогов ЭНТ:
   - **Корневой каталог**
     - **Рабочий каталог №1**
     - **Рабочий каталог №2**
2. В дочерние каталоги (**Рабочий каталог №1**, **Рабочий каталог №2**) импортируются ЭД.
3. Офицер безопасности создаёт два ОЗ, в один из которых входит **Корневой каталог**, а во второй - **Рабочий каталог №2**.

В ситуации, когда из структуры каталогов в синхронизируемом источнике удален подкаталог **Рабочий каталог №2** и добавлен **Рабочий каталог №3**, синхронизация **Рабочего каталога №2** завершится с ошибкой, так как он связан с пользовательским ОЗ и не может быть удален. При создании структуры каталогов ЭД в ТМ необходимо учитывать, что данная ситуация приведет к ложно-положительным срабатываниям политик, так как, если ОЗ настроен на **Корневой каталог**, он будет продолжать срабатывать на ЭД из удаленного в источнике данных **Рабочего каталога №2**.

6 Глоссарий для InfoWatch Sample Documents Autoupdate Adapter

InfoWatch Traffic Monitor, TM Система, предназначенная для перехвата, фильтрации и анализа информационных потоков компьютерной системы
InfoWatch Integration Adapter Универсальный Интеграционный Адаптер
InfoWatch Sample Documents Autoupdate Adapter Адаптер для синхронизации эталонных документов
SSL Secure Sockets Layer (уровень защищённых сокетов) - криптографический сетевой протокол, обеспечивающий защищенный обмен данными
БД База данных
ОЗ Объект защиты
ЭД Эталонные документы
ЭНТ Элемент настройки технологий