

INFOWATCH

InfoWatch Sample Documents Autoupdate Adapter. Setup and Configuration Guide

26/03/2021

© JSC “InfoWatch”

Tel/Fax +7 (495) 229-00-22

http://www.infowatch.com

Table of Contents

1 Introduction 3

1.1 Who should read this guide 3

2 General Information about Infowatch Sample Documents Autoupdate Adapter 4

2.1 Composition of InfoWatch Integration Adapter 4

2.2 Hardware and Software 5

3 Installing InfoWatch Sample Documents Autoupdate Adapter 6

3.1 Installing the plugin for InfoWatch Traffic Monitor 6

3.2 Installation procedure for InfoWatch Sample Documents Autoupdate Adapter 7

3.3 Uninstalling InfoWatch Sample Documents Autoupdate Adapter 10

4 Configuring InfoWatch Sample Documents Autoupdate Adapter 11

4.1 InfoWatch Integration Adapter - General Settings 11

4.2 InfoWatch Sample Documents Autoupdate Adapter Configuration 13

4.2.1 Creating Sample Documents Update Task 14

4.2.2 Staring Sample Documents Update Task 16

5 Sample Documents Catalogues 17

6 Glossary for InfoWatch Sample Documents Autoupdate Adapter 18

1 Introduction

This guide contains information on installation, configuration and administration of InfoWatch Integration Adapter and InfoWatch Sample Documents Autoupdate Adapter.

1.1 Who should read this guide

The guide is intended for users familiar with the basics of the Microsoft Windows OS.

2 General Information about Infowatch Sample Documents Autoupdate Adapter

InfoWatch Sample Documents Autoupdate Adapter - an integration adapter, established to syncronize the sample documents catalog content in InfoWatch Traffic Monitor with data source - network catalog.

2.1 Composition of InfoWatch Integration Adapter

InfoWatch Integration Adapter consists of:

- Windows service;
- Configurator - an application with user interface to configure the System;
- InfoWatch Sample Documents Autoupdate Adapter plugin

Windows service and configurator contain the following components:

Component	**Description**	**Filename**
Plugin Contract	Library networking with plugins	InfoWatch.PluginPlatform.Contract.dll
Configuration library	Library containing configuration service structure described	InfoWatch.PluginPlatform.Service.Configiration.dll
InfoWatch Traffic Monitor Connector	Networking with InfoWatch Traffic Monitor via pushApi protocol	InfoWatch.PluginPlatform.Service.Connector.dll
Common components	Common components to provide networking between configurator and service	InfoWatch.PluginPlatform.Service.Core.dll InfoWatch.PluginPlatform.Service.Core.Contract.dll InfoWatch.PluginPlatform.Service.Core.Logger.dll
Plugin manifest	JSON manifest plugin description	InfoWatch.PluginPlatform.Service.Core.PluginHost.JsonPluginManifest.dll
Event context	Description of event context received from plugins	InfoWatch.PluginPlatform.Service.FileQueue.JsonContext.dll
Microsoft Enterprise Libraries	Microsoft library used by developers for logging	Microsoft.Practices.EnterpriseLibrary.Common.dll Microsoft.Practices.EnterpriseLibrary.Logging.dll Microsoft.Practices.ServiceLocation.dll Microsoft.Practices.Unity.dll Microsoft.Practices.Unity.Interception.dll

Component	Description	Filename
PushApi thrift protocol	PushApi thrift protocol description	Thrift.dll pushapi-thrift.dll
Ionic Zip	Ionic zip library to support zip	Ionic.Zip.dll
Newtonsoft Json	Library providing serialization and deserialization within JSON	Newtonsoft.Json.dll
Ru resources	Additional resources	InfoWatch.PluginPlatform.Service.Core .resources.dll InfoWatch.PluginPlatform.Service.Conf igurator .resources.dll
Service	Windows service executible file	InfoWatch.PluginPlatform.exe
Service configuration file	Service configuration file	InfoWatch.PluginPlatform.exe.config
Configurator	Configurator executible file	InfoWatch.PluginPlatform.Service.Conf igurator.exe
Configurator configuration file	Configurator configuration file	InfoWatch.PluginPlatform.Service.Conf igurator.exe .config

2.2 Hardware and Software

Hardware requirements:

- Processor 1 GHz and higher;
- RAM not less than 1 GB;
- Network card - 100/1000 Mbps.

Software requirements:

- Operating systems:
    - Microsoft Windows 2008 Server Service Pack 2 and later;
    - Microsoft Windows Server 2016;
    - Microsoft Windows Server 2019;
    - Microsoft Windows Vista SP2.
- Microsoft .NET Framework 4.5.1.

3 Installing InfoWatch Sample Documents Autoupdate Adapter

InfoWatch Integration Adapter installation is performed automatically when installing Sample Documents Autoupdate Adapter plugin. To provide the correct work of configuration platform the following actions are to be taken:

1. Generate a license for InfoWatch Traffic Monitor (vendor interceptors licenses for **IW_ADAPTERS** editor and any protocol of Skype messenger).
2. Install the generated license into InfoWatch Traffic Monitor.
3. Install Microsoft .Net Framework 4.5.1on the server where the adapter is to be operating (if not installed yet).
4. Install Infowatch Sample Documents Autoupdate Adapter.
5. Start InfoWatch Integration Adapter Configurator, implement required changes in settings.

> **Warning!**
>
> Access to sample documents within InfoWatch Traffic Monitor is granted regardless of whether you have the license for sample documents autoupdate module or not. Infowatch Sample Documents Autoupdate Adapter is a part of InfoWatch Traffic Monitor and requires no separate license.

After the installation, the plugin can be found in the list of installed plugins. To upload the plugin, mark it and click **Save**. Thus InfoWatch Integration Adapter will be restared.

After the System has been restared, you may find a tab with plugin settings within Configurator.

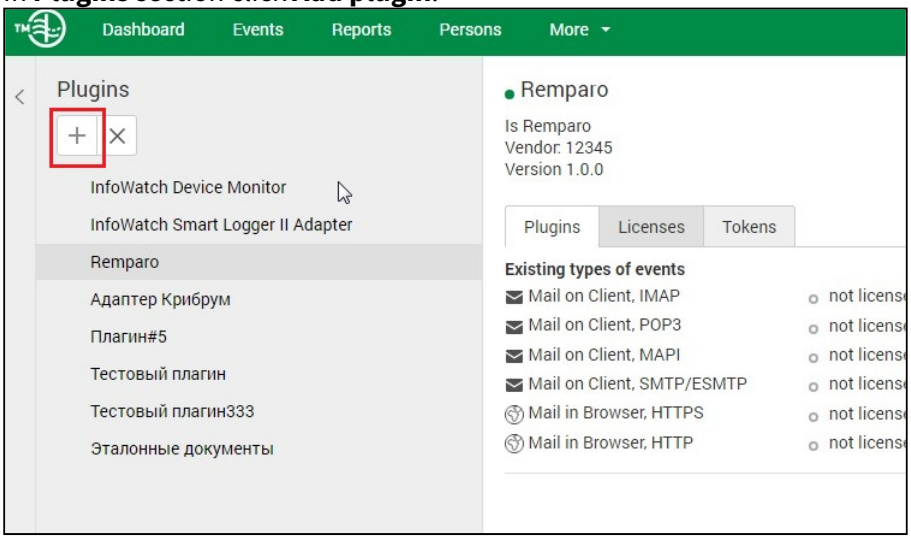
On this tab you should do the following:

1. Enter the access token for InfoWatch Traffic Monitor (it can be found on the page with prior installed plugin for InfoWatch Traffic Monitor). For details see "InfoWatch Sample Documents Autoupdate Adapter Configuration".
2. Press **Save**. The plugin will restart automatically.

3.1 Installing the plugin for InfoWatch Traffic Monitor

To install InfoWatch Traffic Monitor plugin:

1. In **Plugins** section click **Add plugin**.



2. In the window that appears, click **Upload**.
3. Select the plugin file (`TmPlugin_SampleDocuments.zip`). If you see the status *Licensed* in the opened window, that means the correct license for sample documents synchronization has been installed.
4. To finalise the installation, click **Install**.

File plugin description:


```
{
        "PLUGIN_ID": "791DFFB37098450EB8D2AB5B5DE8C6CB791DFFB3",
        "DISPLAY_NAME": "InfoWatch Sample documents Autoupdate Adapter",
        "DESCRIPTION": "Sample Documents Autoupdate Adapter pre-installed plugin",
        "VERSION": "1.0.0",
        "IS_SYSTEM": false,
        "VENDOR": "IW",
        "DATATYPE": [{
                "VALUE": "stamper",
                "TYPE": "DE"
        }],
        "PATTERN_SEARCH_LICENSE": "{\"operator\": \"and\", \"conditions\": [{\"cas\": \"stamper\"}]}",
        "LICENSE": []
}
```

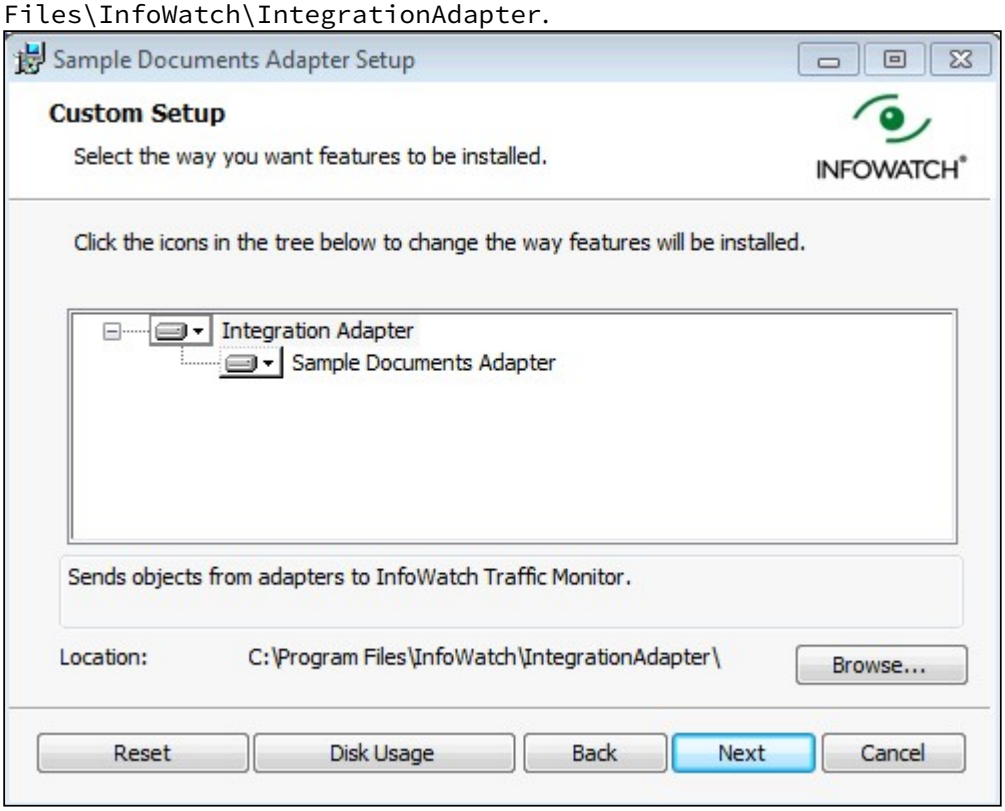

3.2 Installation procedure for InfoWatch Sample Documents Autoupdate Adapter

> **Warning!**
>
> The user performing the installation should have local administrator's privileges on the workstation.

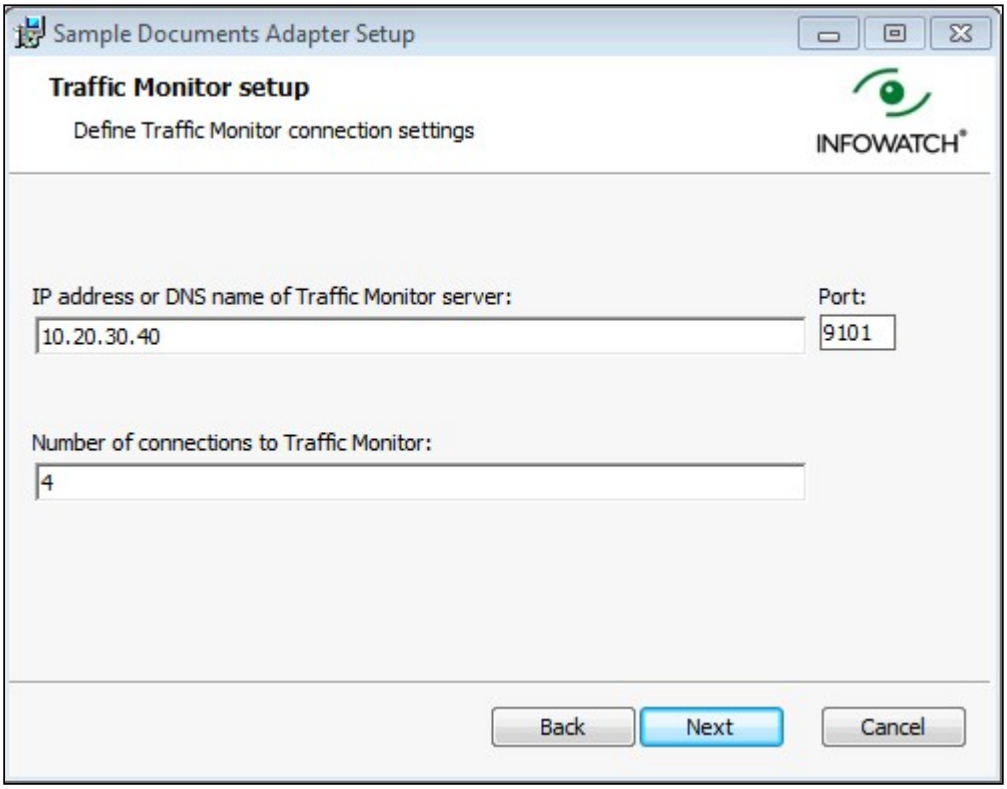
Installation steps:

1. On distributive disk run one of the files as follows:
   - If you use 64-bit operating system:
     - `pluginplatform.3.2.0.x.SampleDocuments.x64.ru.msi` - to start the setup wizard with interface in Russian;
     - `pluginplatform.3.2.0.x.SampleDocuments.x64.en.msi` - to start the setup wizard with interface in English.
   - If you use 32-bit operating system:
     - `pluginplatform.3.2.0.x.SampleDocuments.x86.ru.msi` - to start the setup wizard with interface in Russian;
     - `pluginplatform.3.2.0.x.SampleDocuments.x86.en.msi` – to start the setup wizard with interface in English.
2. In the welcoming window of the wizard press **Next**.
3. Read the terms of license agreement, check the box to accept it and press **Next**.
4. InfoWatch Integration Adapter operates as Windows service, so it cannot be installed per user and will be installed in the common users folder. Click **Next**.

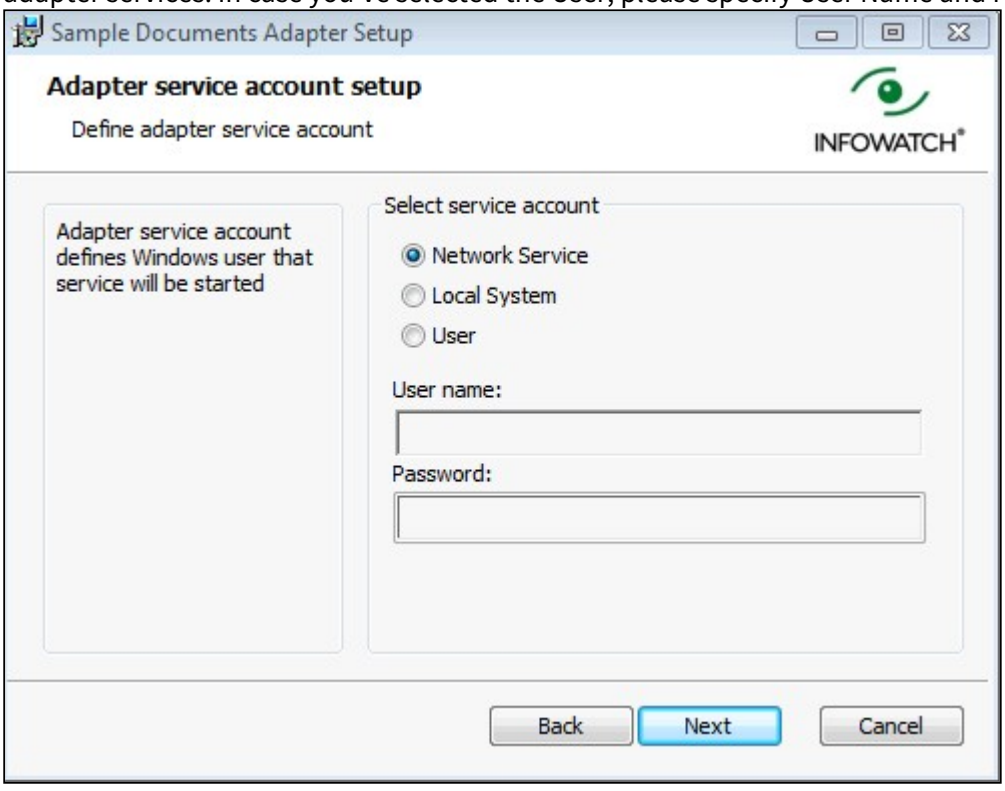
5. InfoWatch Sample Documents Autoupdate Adapter is to be installed together with Integration platform. Change the installion folder (if required). To do this select **Integration Adapter** component and press Browse. By default the installation will be held in `C:\Program Files\InfoWatch\IntegrationAdapter`.



6. Press **Next**.
7. Configure the connection with InfoWatch Traffic Monitor. To do this, please specify the following parameters:
    - IP address or DNS name of InfoWatch Traffic Monito server;
    - Port of InfoWatch Traffic Monitor server to transfer the events (default value 9101);
    - Number of connections to InfoWatch Traffic Monitor server. You may specify the number from the range of 1 to 32 connections. The default value is 4.



8. Press **Next**.
9. Specify the adapter service acount: **Network Service**, **Local System** or **User**, the one to start the adapter services. In case you've selected the User, please specify User Name and Password.



10. Press **Next**.

> **Warning!**
>
> InfoWatch Integration Adapter can be connected only to InfoWatch Traffic Monitor due to pushApi connection protocol used.

11. Click **Install** to begin the installation, thus confirming the correct data input.
12. Once the installation is completed, the setup wizard will display the notification window. Click **Finish**.

3.3 Uninstalling InfoWatch Sample Documents Autoupdate Adapter

You may remove the adapter from Control Panel by means of OS Windows or you may run the installation package.

After the adapter has been uninstalled, delete the file queue catalogs and error messages manually.

To uninstall InfoWatch Sample Documents Autoupdate Adapter, the following actions are to be taken:

1. Run the installer file, you've used for initial installation. For example, if you've started the setup wizard with interface in Russian for 64-bit operating system, you should run the file `pluginplatform.3.2.0.x.SampleDocuments.x64.ru.msi`.
2. Then click **Next**.
3. In the window with options provided click **Remove**.
4. To confirm the action click **Remove** in the newly opened window. All InfoWatch Sample Documents Autoupdate Adapter files will be removed from your computer, including the folders created while installation.
5. Click **Finish** to finalise the unistalling process.

4 Configuring InfoWatch Sample Documents Autoupdate Adapter

Integration adapter provides the plugin with interface to perform the graphic configuration, it also stores the binary data settings sent to plugin while its starting which can be changed. The configurator loads the widget, performed by plugin into proper tab.

To start **Integration Adapter Configurator** application, you should do the following:

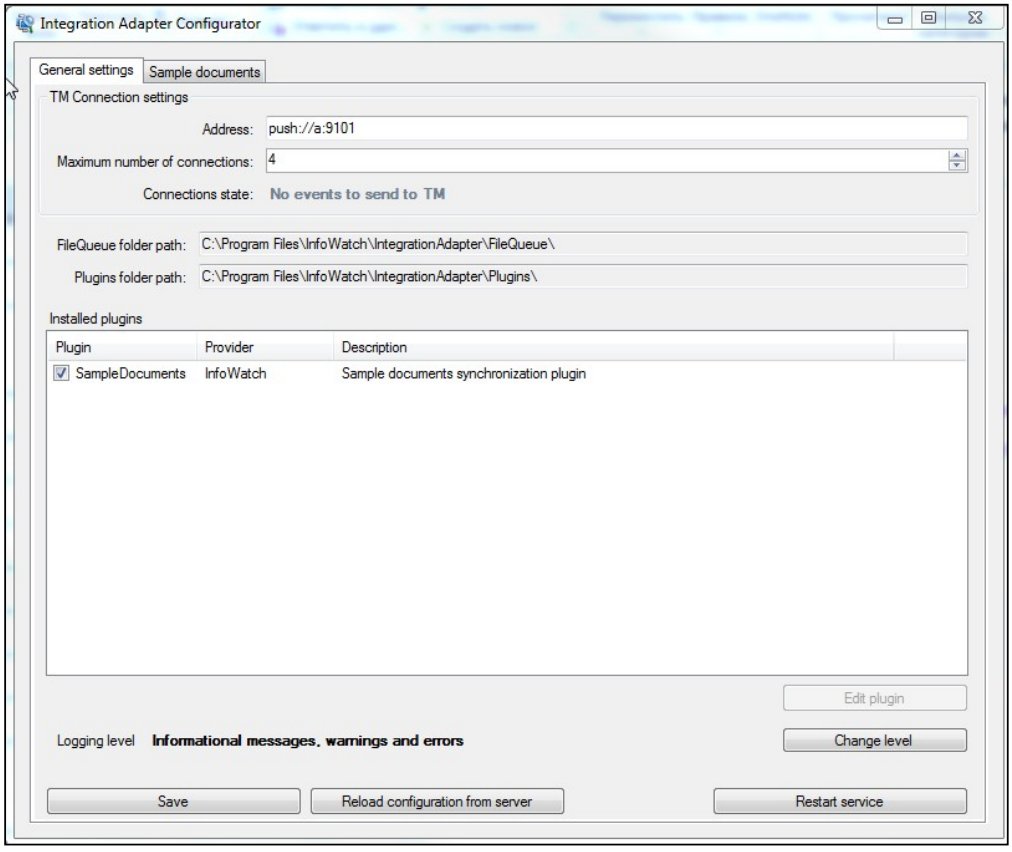
- use the desktop shortcut **Integration Adapter Configurator**;
- in menu **Start** -> **All programmes** -> **InfoWatch** -> **Integration Adapter** select the point **Integration Adapter Configurator**;
- in the folder, where InfoWatch Integration Adapter has been installed, run the application `InfoWatch.PluginPlatform.Service.Configurator.exe`.

The parameters of InfoWatch Integration Adapter service, you've entered while installing can be found in **General settings** tab (see "InfoWatch Integration Adapter - General Settings").

To configure InfoWatch Sample Documents Autoupdate Adapter go to **Sample Documents** tab (see "InfoWatch Sample Documents Autoupdate Adapter Configuration").

4.1 InfoWatch Integration Adapter - General Settings

On the tab **General settings** of **Integration Adapter Configurator** you can find the parameters of InfoWatch Integration Adapter, you've entered while installing the application.



In the list of **Installed plugins** you may find the plugins loaded into the platform.

The tab contains the settings to be edited if required:

1. In **TM connection settings** area:
   - InfoWatch Traffic Monitor **Address** in a format: `push://host:port`, where host is an ip address or domain name of InfoWatch Traffic Monitor server, and port is InfoWatch Traffic Monitor server port, used to deliver the events (the dafault one is 9101);
   - Maximum number of connections to InfoWatch Traffic Monitor server.
2. Service directories:
   File Queue folder, where the events file queues of all running plugins are created;
   Plugins folder, where the plugins and their settings are stored.

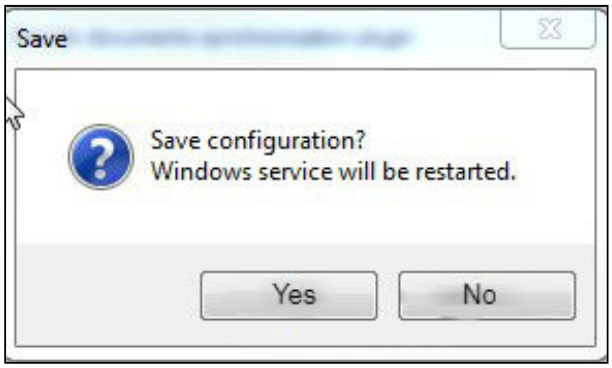
   > **Warning!**
   >
   > Since Windows service of InfoWatch Integration Adapter works with «NETWORK SERVICE» user privilleges, you should make sure the user has access to specified folders.

3. Logging level. To select the log level for all registered plugins, click **Change level** and specify the ones to be stored within InfoWatch Integration Adapter log. The following levels are available:
   - *All events* (verbose log);
   - *Infomational messages, warnings and errors*;
   - *Logging off*.



4. To change the logging level of a plugin:
   a.Select the required plugin in the list and click **Edit plugin**.
   b. In the opened window specify if the plugin log should be written in a separate file and specify the logging level.
   c. Click **OK**.

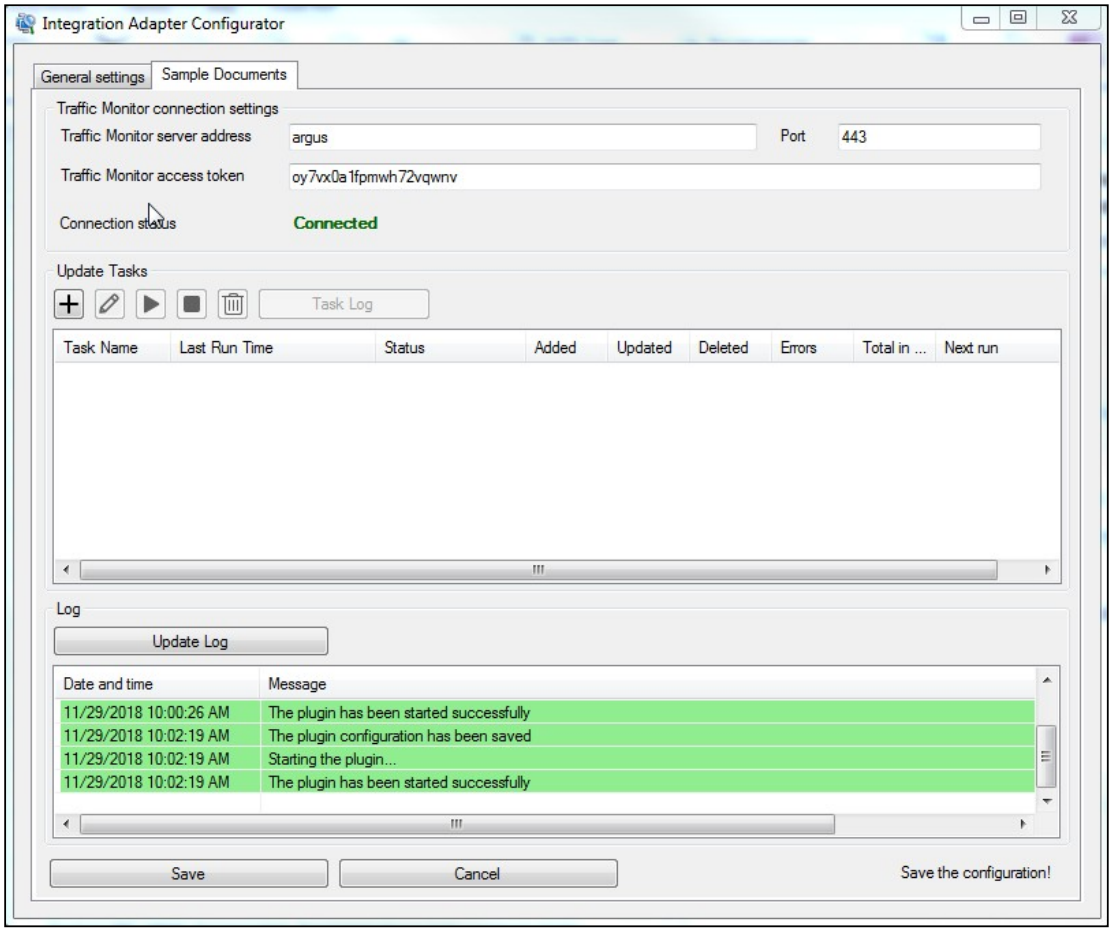
After the configuration has been changed click Save. The request for configuration saving will be displayed. Windows service will be restared.



Click **Yes**. Configurator window will be closed and then a window with new settings will be opened.

4.2 InfoWatch Sample Documents Autoupdate Adapter Configuration

To configure the plugin, start the application **Integration Adapter Configurator** and go to **Sample Documents** tab.



To configure sample documents synchronization you should:

1. Specify Traffic Monitor server connection parameters:
   - TM Address - InfoWatch Traffic Monitor server address;
   - Port - SSL port number (default valuy is 443);
   - Access token - the string is available only for InfoWatch Traffic Monitor and plugin. Traffic Monitor access token can be found within Traffic Monitor Management Console, Plugins section for **IW_ADAPTERS** editor.

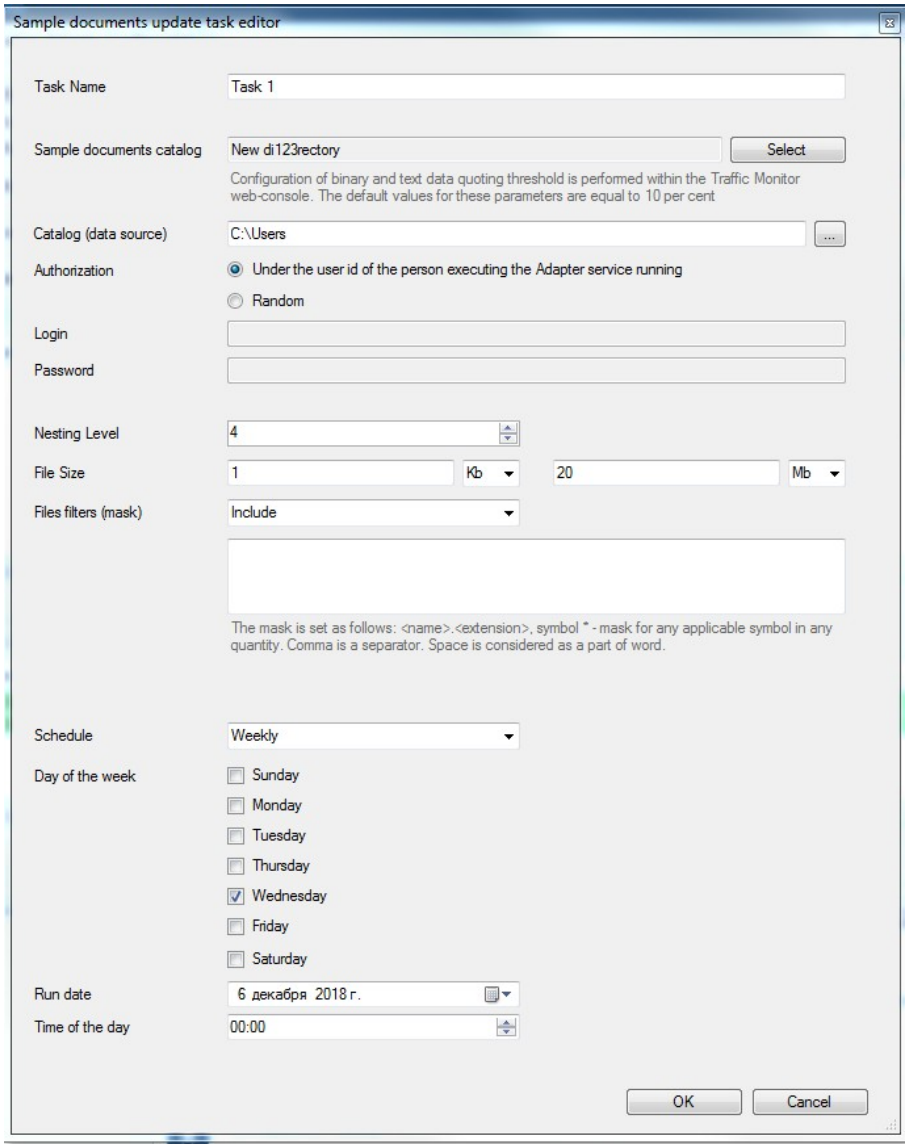
2. Create sample documents update task. For this, in the **Update Tasks** area, click  and, in the window that opens, specify required values (see Creating Sample Documents Update Task).

   To edit the task parameters, choose the required task in the list and click . To delete a task from the list, click .

4.2.1 Creating Sample Documents Update Task

To create a sample document update task, fill in the form fields:

- Task Name;
- Catalog of sample documents. It can be:
  - selected from existing catalogs in Traffic Monitor, or
  - created by user within Automatic sample documents catalog;
- Catalog (data source). You may specify a folder, disk or workstation within local network or local computer (e.g. C:\Users). For details, please see "Sample Documents Catalogues";
- Authorization. You may use the current user authorization, the person executing the Adapter service running or a random one. In case you've selected the random authorization, you should enter Login and Password accordingly;
- The following filtering options should be specified:
  - Folders nesting level (from 0 to 6);
  - Sample document file size (from 1 kB);
  - Files masks, that could be neither included into the filtering option, neither removed from it;
- Options to start the update task for sample documents:
  - Schedule (manually, once, daily, weekly, monthly);
  - Run date and time (if required the task can be run periodically).



Once the fields have been filled in, click **Ok**. The new task will be added to the update task list.

Warning!

Adapter checks documents' statuses, seekeing for documents' duplicates. The documents will not be uploaded, if in catalogue (data source) there are already sample documents' duplicates uploaded to TM earlier.

Note:

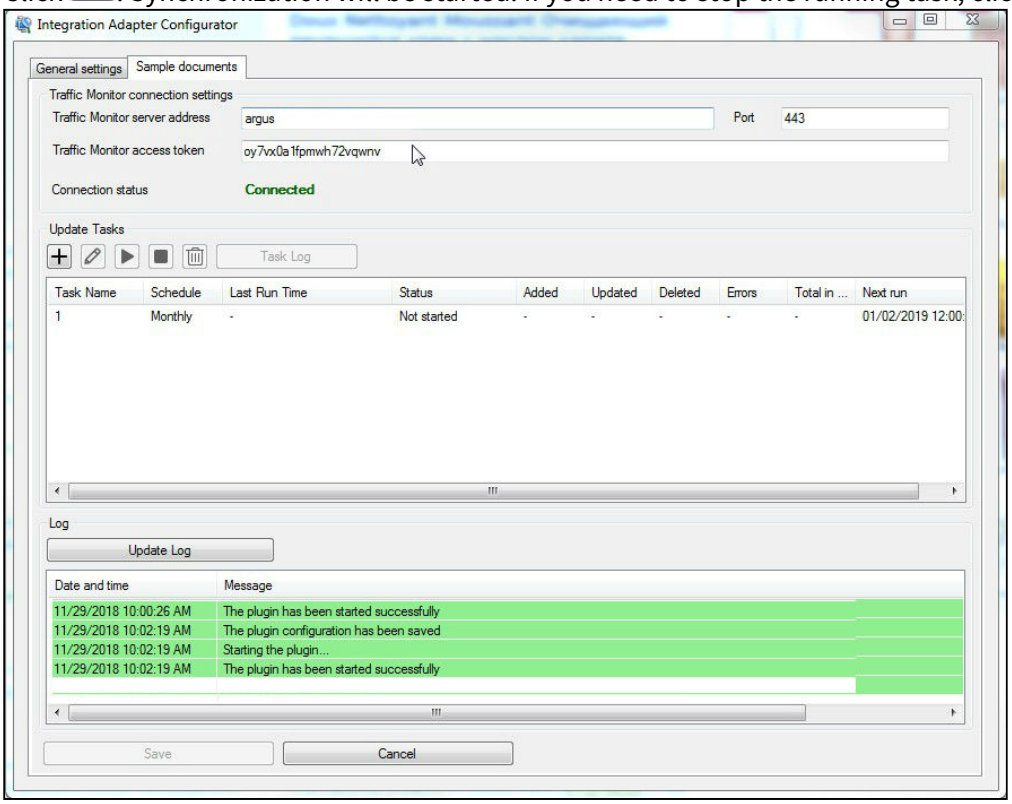
When resynchronizing source catalogue with a modified receiving Traffic Monitor catalogue, it is recommended to manually delete the previous receiving Traffic monitor catalogue or its content.

4.2.2 Staring Sample Documents Update Task

> **Warning!**
>
> After you've changed the configuration, click **Save** before you start the task. The changes will be saved to InfoWatch Integration Adapter regular storage. The plugin will be restarted.

To start sample documents update task, take the following steps:

1. Select the task from the list.
2. Click . Synchronization will be started. If you need to stop the running task, click .



To see the details of the task you've performed, click **Task Log**.

If you want to cancel unsaved changes, click **Restore configuration**.

To record the events within the plugin, you may use the event **Log**, that is updated automatically every 10 seconds and displays the latest 100 events. Use the **Update Log** button for manual refreshing.

5 Sample Documents Catalogues

All sample documents sent to InfoWatch Traffic Monitor by adapter are placed into parent directory **Automatic sample documents**.

To create a new catalogue take the following steps:

1. Go to *Sample documents update task editor->Sample documents catalogue->Review of sample documents catalogues in Traffic Monitor* by clicking **Select**.
2. Select the required catalogue (or specify the root directory **Automatic sample documents**).
3. Click  to create a new catalogue.
4. Enter the catalogue name and press **Enter**.

To remove the catalogue from the tree, you should select the required catalogue and click **Delete catalogue**.

Warning!

The catalogue used by another task or protected object, as well as the root directory **Automatic sample documents** cannot be deleted.

Example:

1. The following catalogue structure has been created:
   Root catalogue
   - **Working catalogue №1**
   - **Working catalogue №2**
2. Sample documents are imported to subfolders (**Working catalogue №1, Working catalogue №2**).
3. A Security Officer creates 2 security objects, one of which includes the **Root catalogue** and the other one includes **Working catalogue №2**.

In case **Working catalogue №2** is removed from the synchronized source and **Working catalogue №3** is added, synchronization of **Working catalogue №2** will result in an error since it is related to a user protected object and cannot be removed. When creating a structure of sample document catalogues in InfoWatch Traffic Monitor, you should take into account that this situation may lead to the policy false positives: if a protected object is related to the **Root catalogue**, then sample documents from the removed **Working catalogue №2** will trigger the protected object.

6 Glossary for InfoWatch Sample Documents Autoupdate Adapter

InfoWatch Traffic Monitor, TM The System intended to intercept, filter and analyse information flows of computer system.
InfoWatch Integration Adapter Universal Integration Adapter
InfoWatch Sample Documents Autoupdate Adapter Adapter intended to synchronize sample documents
SSL Secure Sockets Layer cryptographic protocols designed to provide communications security over a computer network
DB Database