

INFOWATCH

SDK. Access to IWTM events for external systems

27/09/2019

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Purpose of DataExport API application programming interface 3

2 Aauthorization to access DataExport API 4

2.1 Work with plugins 4

2.1.1 Adding plugin 4

2.1.2 Plugin removal 4

2.2 Work with tokens 4

2.2.1 Adding token 4

2.2.2 Token's data editing 5

2.2.3 Token's value update 5

2.2.4 Copying token 5

2.2.5 Deleting token 5

3 DataExport API functionality 6

4 DataExport API third-party component registration 7

4.1 DataExport API third-party component registry file format 7

5 Functional description of DataExport API application programming interface 8

1 Purpose of DataExport API application programming interface

This application programming interface is intended to integrate InfoWatch Traffic Monitor with external data receiving systems. As a part of the implementation DataExport API external systems get the events content and metadata from InfoWatch Traffic Monitor. DataExport API supports only data reading operation from InfoWatch Traffic Monitor.

2 Aauthorization to access DataExport API

Authorization to access DataExport API is provided via tokens mechanism, similar to other InfoWatch Traffic Monitor API's. To get token and review DataExport API licensing status it is required adding new type of plugin into the System - Plugin for DataExport API. All the activities related to plugins are performed within the InfoWatch Traffic Monitor console.

2.1 Work with plugins

2.1.1 Adding plugin

To add plugin:

1. Go to **Administration - Plugins**;
2. Within the area **Plugins** click .
3. Click **Add**.
4. Review the plugin description and click **Install**.

> **Note:**
>
> To update a plugin, the updated version of this plugin should be added.

2.1.2 Plugin removal

To remove plugin:

1. Go to **Administration - Plugins**;
2. Within the area **Plugins** click 
3. Click **Yes** to confirm the deletion.

2.2 Work with tokens

Token is generated automatically after the plugin has been added. All the activities related to tokens are performed within the InfoWatch Traffic Monitor console.

2.2.1 Adding token

To add token:

1. Go to **Administration - Plugins**;
2. Choose the plugin within the **Plugins** area;
3. Go to **Tokens** bookmark;
4. Click .

Note:

Token's value is generated automatically when setting up a token and it cannot be set by user.

2.2.2 Token's data editing

To change token's data:

1. Go to **Administration - Plugins**;
2. Choose the plugin within the **Plugins** area;
3. Go to **Tokens** bookmark;
4. By double left button click, enter the required info within the fields *Name* and *Description*.

2.2.3 Token's value update

If the token was compromised or if there is a potential token leak to the third party, it is required generating a new token's value.

To update token's value:

1. Go to **Administration - Plugins**;
2. Choose the plugin within the **Plugins** area;
3. Go to **Tokens** bookmark;
4. Click  .

2.2.4 Copying token

To copy token's value into the clipboard:

1. Go to **Administration - Plugins**;
2. Choose the plugin within the **Plugins** area;
3. Go to **Tokens** bookmark;
4. Click  .

2.2.5 Deleting token

To delete token:

1. Go to **Administration - Plugins**;
2. Choose the plugin within the **Plugins** area;
3. Go to **Tokens** bookmark;
4. Click  .

3 DataExport API functionality

The functionality of DataExport API includes the following:

- Able to specify the number of attributes to be included within the result:
    - Event ID;
    - Senders: list of contacts and authentication result, taking into account the potential conflicts;
    - Recipients: list of contacts, and authentication result, taking into account the potential conflicts;
    - Sender's computer, taking into account the potential conflict;
    - Type of event;
    - Date and time of interception;
    - Protocol;
    - Level of violation;
    - Verdict;
    - User's decision;
    - Path to file;
    - Web resource address;
    - Security objects and catalogues;
    - User's decision;
    - Event's size;
    - Tags;
- Able to specify the number of attributes to filtrate:
    - Date and time of interception;
    - Type of event;
    - Protocol;
    - Security objects and catalogues;
    - User's decision;
    - Event's size;
    - Tags;
- Separate event metadata obtaining with the ability to specify the number of attributes to be included within the result. In this regard, if the event contains few enclosed objects, all the extracted text to be assembled into one file;
- Obtaining all the extracted text of an event;
- Obtaining binary data of an event.

4 DataExport API third-party component registration

To integrate third-party receiving system with InfoWatch Traffic Monitor the following actions are to be taken:

1. Register the authentication type string of company - the component user in Infowatch JSC. Thus letting to connect a user company to the license, to be installed within the InfoWatch Traffic Monitor System;
2. Obtain the developer's license related to company's ID. This would let unloading the events data from InfoWatch Traffic Monitor;
3. Create third-party component registry file in accordance with the format below. The license, obtained as per the point 2 is to be added to the file;
4. Download the third-party component registry file toInfoWatch Traffic Monitor System using the InfoWatch Traffic Monitor console interface. Section "Administration" - "Plugins". (see "Traffic Monitor. Administration guide");
5. Obtain an access token within the downloaded third-party component's properties;

The System is ready to send the company's events data.

4.1 DataExport API third-party component registry file format

Plugin is a .zip format archive. The archive includes:

- **licenses** folder, containing license files;
- **icon** folder, containing the files with pictograms used for registered events (optionally);
- **manifest.json** file, containing information on a plugin.

For external systems, receiving data from TM **manifest.json** should contain age following information:

Title	If it is mandatory	Description
Version	Yes	Plugin version
Developing company's ID	Yes	In accordance with company name, specified within the license
Name	Yes	Plugin name
Systems-data receivers	Yes	List of systems, receiving data from IWTM, registered within this Plugin.
Description	Yes	Plugin description.
"Preset" feature	No	If it is a part of the System.
Unique ID	Yes	Unique 128-bit plugin ID (UUID).

5 Functional description of DataExport API application programming interface