**NATIONAL SETTLEMENT DEPOSITORY**

**User Guide**

**NSD’s EDI File Gateway**

Version 3

Moscow, 2019

**Annotation**

NSD’s EDI File Gateway User Guide identifies options of a workplace of EDI participant of a Windows NSD’s EDI File Gateway application.

NSD’s EDI File Gateway User Guide is intended for NSD’s EDI participants who use the automatic exchange of preliminary prepared files of e-mail messages with NSD.

On matters of installation, setup and addressing of problems during the application operation, please contact NSD’s technical support service by e-mail: soed@nsd.ru or by phone: +7 (495) 956-09-34.

**Table of Contents**

[**1. Introduction 5**](#_Toc5006472)

[**1.1. Purpose of the Document 5**](#_Toc5006473)

[**1.2. Terms and Abbreviations 5**](#_Toc5006474)

[**2. General Information about the FG Application 6**](#_Toc5006475)

[**2.1. Purpose of the FG Application 6**](#_Toc5006476)

[**2.2. FG Installation 6**](#_Toc5006477)

[**3. Technical Requirements 7**](#_Toc5006478)

[**4. FG Installation 8**](#_Toc5006479)

[**4.1. Installation of a New Version 8**](#_Toc5006480)

[**4.2. The Problem Related to the Installation of Older Versions 9**](#_Toc5006481)

[**5. Interface 10**](#_Toc5006482)

[**5.1. "Summary" Tab 10**](#_Toc5006483)

[**5.2. Incoming Packets 11**](#_Toc5006484)

[**5.3. Outgoing Packets 13**](#_Toc5006485)

[**5.4. Sending Errors 14**](#_Toc5006486)

[**5.5. Task Queue 14**](#_Toc5006487)

[**5.6. Log 15**](#_Toc5006488)

[**6. Settings 18**](#_Toc5006489)

[**6.1. General Settings 19**](#_Toc5006490)

[**6.2. Proxy Server Configuration 20**](#_Toc5006491)

[**6.3. Data Interchange Channels 21**](#_Toc5006492)

[**6.3.1. Creation of a Channel 22**](#_Toc5006493)

[**6.3.2. Deactivation of a Channel 25**](#_Toc5006494)

[**6.3.3. Deletion of a Channel 25**](#_Toc5006495)

[**6.3.4. WSL Channel Settings 25**](#_Toc5006496)

[**6.3.5. Setting Parameters of the LKR Channel 27**](#_Toc5006497)

[**6.3.6. Setup of the E-Voting Channel 29**](#_Toc5006498)

[**6.3.6.1. Setting Parameters of the E-Voting Channel 30**](#_Toc5006499)

[**6.3.6.2. E-Voting Messaging Algorithms 35**](#_Toc5006500)

[**7. Principle of Operation 38**](#_Toc5006501)

[**7.1. General Procedure for Sending Packets 38**](#_Toc5006502)

[**7.2. Rules for Naming ED Files 39**](#_Toc5006503)

[**7.3. Rules for Naming packageInfo.xml Files 40**](#_Toc5006504)

[**8. Sending Packets 42**](#_Toc5006505)

[**8.1. FpML-Documents 42**](#_Toc5006506)

[**8.2. Corporate Actions and Depository and Clearing Activities Packets 42**](#_Toc5006507)

[**8.3. WINF.XML file 43**](#_Toc5006508)

[**8.4. Sending by Closed Envelope Method 44**](#_Toc5006509)

[**9. Sending Drafts Electronic Documents to the Repository Web Client 45**](#_Toc5006510)

[**10. Requirements for Attached Files 47**](#_Toc5006511)

[**10.1. Attachments to the Repository’s FpML Messages 47**](#_Toc5006512)

[**10.2. Attachments to the Corporate Action Messages 47**](#_Toc5006513)

[**11. Sending Results 48**](#_Toc5006514)

[**11.1. Successful Sending 48**](#_Toc5006515)

[**11.2 .Sending Error 48**](#_Toc5006516)

[**12. Receipt of Packets 49**](#_Toc5006517)

[**13. "Participants of Transit" Directory 50**](#_Toc5006518)

[**13.1. Formation of the Directory of Participants 51**](#_Toc5006519)

[**13.2. Selection of a WSL channel 51**](#_Toc5006520)

[**13.3. Adding a Participant 52**](#_Toc5006521)

[**13.4. Download of Certificates 53**](#_Toc5006522)

[**13.5. Addition of a power of attorney 55**](#_Toc5006523)

[**13.6. Delete of a Certificate 56**](#_Toc5006524)

[**13.7. Deletion of a Participant from the List 56**](#_Toc5006525)

[**14. FG Console Version 58**](#_Toc5006526)

[**14.1. FG Stoppage 58**](#_Toc5006527)

[**14.2. Help Topics 58**](#_Toc5006528)

[**14.3. Run with settings located in another folder 59**](#_Toc5006529)

[**15. Run FG without an Interactive Session 61**](#_Toc5006530)

[**15.1. Setup of FG Channels 65**](#_Toc5006531)

* 1. **Introduction**

**1.1. Purpose of the Document**

The Guide describes the functions of the File Gateway designed for the electronic file interchange via the Web Service channel.

**1.2. Terms and Abbreviations**

Table 1

| No. | Name | Description |
| --- | --- | --- |
|  | File Gateway (FG) | Specialized software, part of NSD’s local workplace (LWP) of Electronic Data Interchange system (EDIS), which allows to automatically send a Participant's message to NSD via the WEB-service channel and to receive NSD messages via the WEB-service channel. |
|  | NSD Electronic Data Interchange (EDI) Rules | Appendix 1 to the Electronic Data Interchange Agreement concluded between NSD and the Participant of NSD EDI. |
|  | EDIS (Electronic Data Interchange System) | The organizational and technical system, including a set of software, information and hardware support of the EDIS Organizer, Organizers of EDIS subsystems, and Participants, which implements Electronic Data Interchange. |
|  | NSD EDIS (NSD’s Electronic Data Interchange System) | The organizational and technical subsystem of EDIS, including a set of software, information and hardware support of NSD and Participants, which implements Electronic Data Interchange. |
|  | WSL channel (Web Service) | A channel for data interchange via a software tool set on the side of NSD, which has an Internet address (URL) and is intended to ensure the electronic interaction between the Participant and NSD according to the established protocol. |
|  | LRK channel (Repository’s Web Client) | A channel for interchanging data between the Participants and NSD via the public Internet and/or Moscow Exchange’s Intranet.  FG uses this channel only for sending drafts to NSD Repository's Web Client. |

Other terms referred to in the Guide are used in the meaning defined by the EDI Rules of NSD and Russian Federation laws.

# General Information about the FG Application

* 1. **Purpose of the FG Application**

FG is designed for interchanging in preliminarily prepared messages with NSD via the Web Service.

FG supports:

1. Sending and receiving encrypted packets, including transit ones, defined by the EDI Rules of NSD as part of electronic interchange while providing the following services:

* repository activities;
* interaction during corporate actions;
* interaction between NSD’s EDI participants, including via NSD as a transfer agent of registrars;
* depository and clearing activities.

2. Sending draft electronic documents to the Repository's Web Client.

* 1. **FG Installation**

You can download FG on NSD website at the Software page (<https://www.nsd.ru/ru/workflow/system/programs/>).

# Technical Requirements

The following software should be installed on the client’s workplace for FG to operate:

* Certificate Storage;
* .NET Framework 4.0;
* Validata CIPF.

In order to work with NSD's Web Service, you need to make the settings as required by the Workplace Setup Instruction when connecting to NSD's WEB services via TLS connection on the website <https://www.nsd.ru/ru/workflow/system/programs/#index.php?36=906>.

The software selection is determined by the type of cryptography.



To work correctly on Windows XP, you should install the [KB2468871](https://www.microsoft.com/ru-ru/download/details.aspx?id=3556) update.

When using qualified certificates (GOST), you need to install the following software:

* Validata CIPF, full installation; HSS MICEX Client:
* Certificate storage, full installation and key certificates.

When using non-qualified certificates (RSA), you need to install the following software:

* MOEX EDIS Information Security Software: Certificate Storage, full installation and key certificates.

The required software can be downloaded on the Moscow Exchange website at <https://www.nsd.ru/ru/workflow/system/member/>.

Detailed information on the installation of cryptographic software is presented in sections of the Web Client documentation at <https://www.nsd.ru/ru/workflow/system/programs/#index.php?36=906>.

# FG Installation

* 1. ******Installation of a New Version**

To install FG, you need to download it by clicking the button and run the fgate-ru.exe (Russian version) or fgate-en.exe (English version).

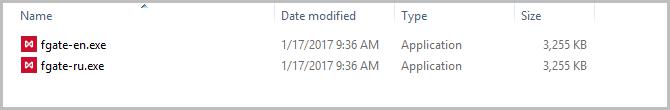


Figure 1. Selection of Installation File

Click the "Install" button in the window opened (Figure 2).

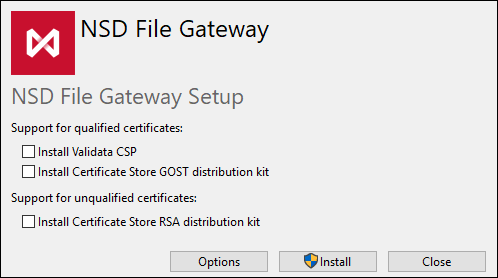


Figure 2. Starting the Installation

Optionally, you can change the FG installation folder (by default% PROGRAMFILES (X86)%\NSD File Gateway). To do this, click the "Parameters" button. Click the Browse button in the window opened and select a folder in Windows Explorer (Figure 3). When you click the "OK" button, you will go to the FG installation start window.

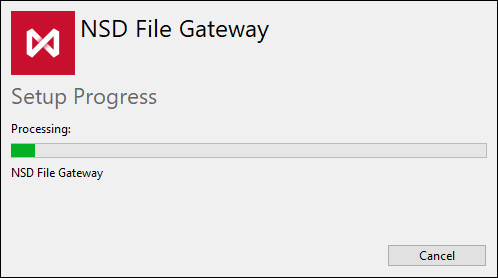


Figure 3. The FG installation start window

Depending on the operating system settings, the Windows’ security window may open. Click "Yes" button to continue the installation.

Upon completion of the installation, a window will open in which you should click the “Run” button to set and work with FG.

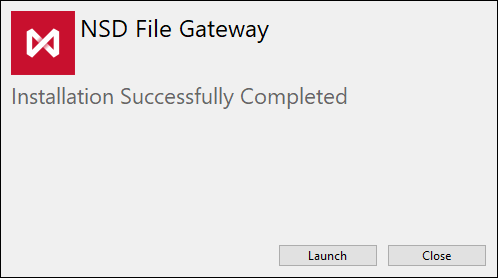


Figure 4. Completion of the Installation



A shortcut appears on the desktop to run FG.

* 1. **The Problem Related to the Installation of Older Versions**

If a newer version of FG is installed on the computer, then an error will be encountered while attempting to install an older version of FG (Figure 5).

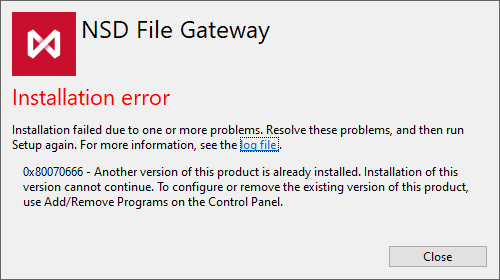


Figure 5. Older Version Installation Error

To solve it, you should uninstall current version of FG. All data and settings will be saved.

# 5. Interface

You can view general information about packets sent and uploaded via the FG interface.

* 1. **"Summary" Tab**

The "Summary" tab displays (Figure 6):

* A Line with the gateway status: run/stopped, in the process of run/stop;
* Gateway control buttons (Table 2);
* Statistics for the current day: the number of received/sent/sending errors of packets;
* Path to the INBOX, OUTBOX, SENT, ERRORS folders. The button http://docs.itglobal.ru/download/attachments/7833702/%D0%9A%D0%BE%D0%BF%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D1%82%D1%8C.png?version=1&modificationDate=1464277317090&api=v2 copies the path to the folder to the clipboard. The button http://docs.itglobal.ru/download/attachments/7833702/%D0%9E%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8C_%D0%BF%D0%B0%D0%BF%D0%BA%D1%83.png?version=1&modificationDate=1464277330407&api=v2 opens a folder in Windows explorer.

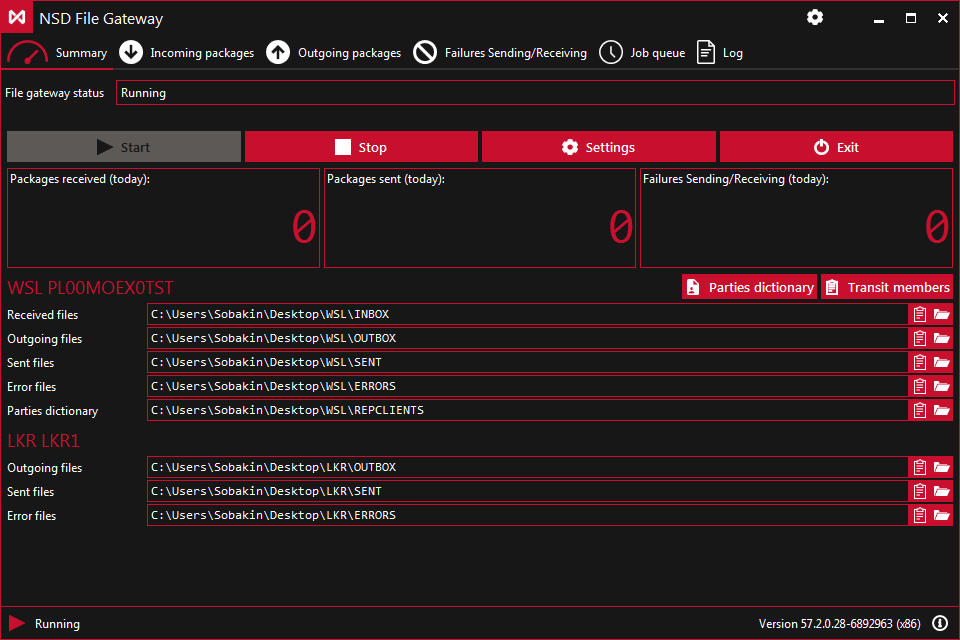


Figure 6. Summary Tab

Table 2. Running and Stopping FG

| **Button** | **Description** |
| --- | --- |
|  | Start to scan folders and send messages to the repository and the Repository Web Client |
|  | Stop FG operations |
|  | Go to the Transit Directory |
|  | Go to settings. Additional button http://docs.itglobal.ru/download/attachments/7833582/%D0%9A%D0%BD%D0%BE%D0%BF%D0%BA%D0%B0%D0%9D%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B8.png?version=1&modificationDate=1464095985193&api=v2 on the top panel |

When you right-click the FG icon, a list of commands will be opened on the right side of the Windows taskbar:

* Expand;
* Run;
* Stop;
* Settings;
* Escape.

Command descriptions are presented in Table 2.

* 1. **Incoming Packets**

The “Incoming Packets” tab displays information about packets unloaded from the Web Service for the selected time period (Figure 7).

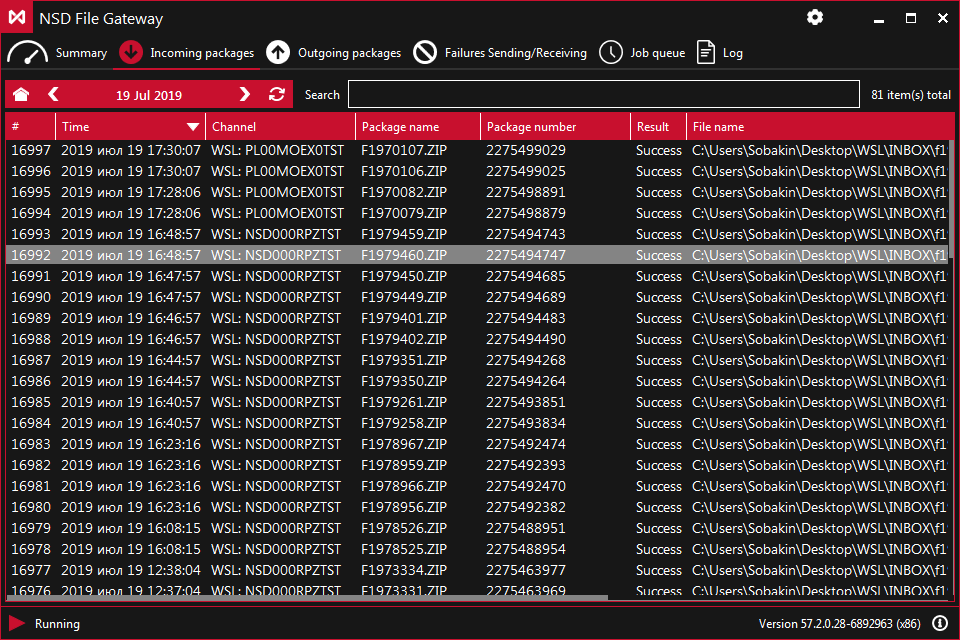


Figure 7. “Incoming Packets” Tab

Records are sorted by the download date of the FG message

* Serial number;
* Packet receipt time;
* Packet receipt channel;
* Packet name;
* Incoming packet number assigned by NSD;
* Result;
* Source file name;
* Status;
* Message subject;
* Sender;
* Recipient;
* Letter\_id;
* Contr\_letter\_id;
* Type;
* Date and time of creation.

Using the buttons on the top panel, the user can select records by days. To view the records for the current date, click the button .

The number of records for the said day is displayed in the right side of the form. . (Total: 10).

If the local time zone of the FG client is different from the MSK time zone (UTC +3), the messages from NSD to FG are downloaded on the basis of the MSK time zone (UTC +3).

On this tab, the list of records can display an archive containing a document sent from FG with an error occurred while processing it.

* 1. **Outgoing Packets**

The “Outgoing Packets” tab displays information about packets sent by FG:

* Serial number;
* Package sending time;
* Channel used for sending;
* Package name;
* Path to the source file;
* Status;
* Message subject;
* Sender;
* Recipient;
* Letter\_id;
* Contr\_letter\_id;
* Type;
* Date and time of creation.

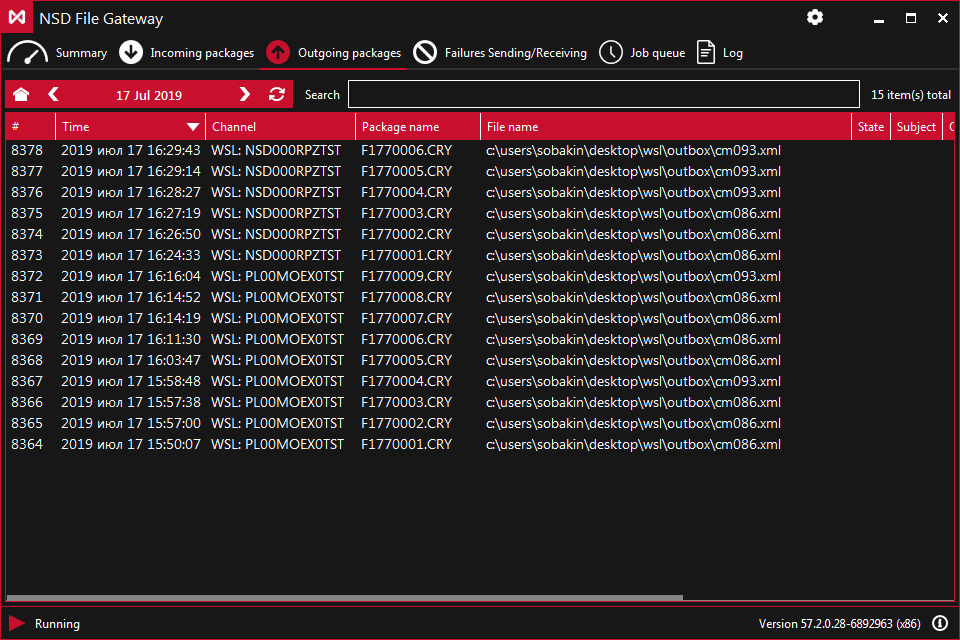


Figure 8. “Outgoing Packets” Tab

Using the buttons on the top panel, the user can select records by days. To view the records for the current date, click the button.

The number of records for the said day is displayed in the right side of the form. (Total: 10).

* 1. **Sending Errors**

A list of unsuccessfully sent files is displayed on the "Sending Errors" tab:The serial number of a record;

* Time of the attempt to send a packet;
* Channel used for sending;
* Path to the source file;
* Error information.

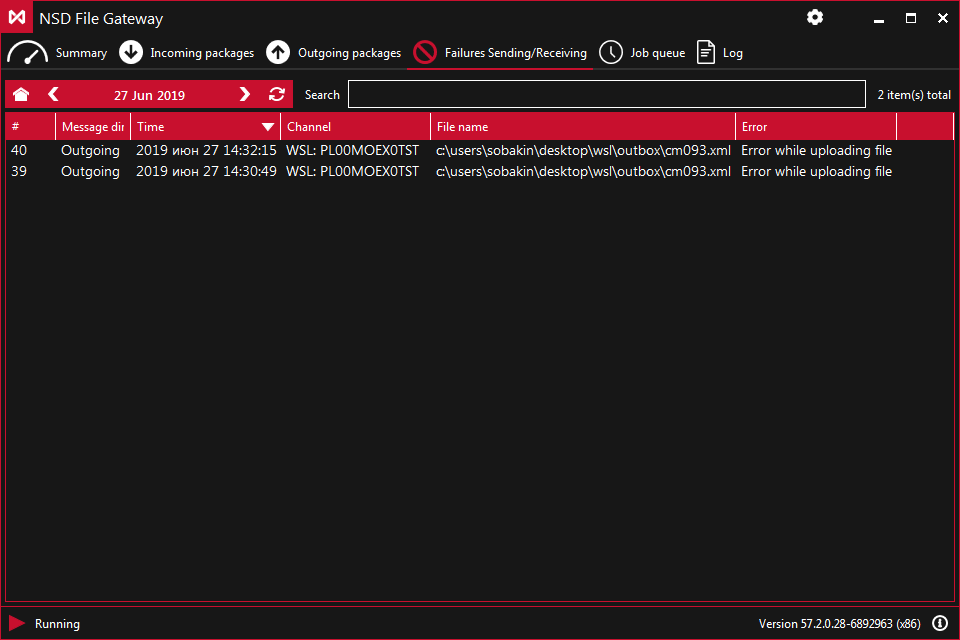


Figure 9. “Sending Errors” Tab



Using the buttons on the top panel, you can select the date of interest, for which you can see the history of sending packets. To view the records for the current date, click the button.

The number of records for the said day is displayed in the right part of the form. . (Total: 10).

* 1. **Task Queue**

The "Task Queue" tab displays messages about the results of sending packets:

* Created – the time when the message was queued for sending;
* Updated – the time when the status of the message was changed;
* Channel – the channel for sending messages;
* Task – a description of the operation performed by FG (operation type (sending/uploading packets), path to the file, file name);
* Status – task status:
* Canceled – the task is canceled by the user;
* Executed – the task was successfully executed;
* Failure - a failure occurred during the task execution;
* Standby – waiting for the completion of the packet generation;
* Processing – the task is being processed;
* In queue – the task is in the queue for processing;
* Sending message result.

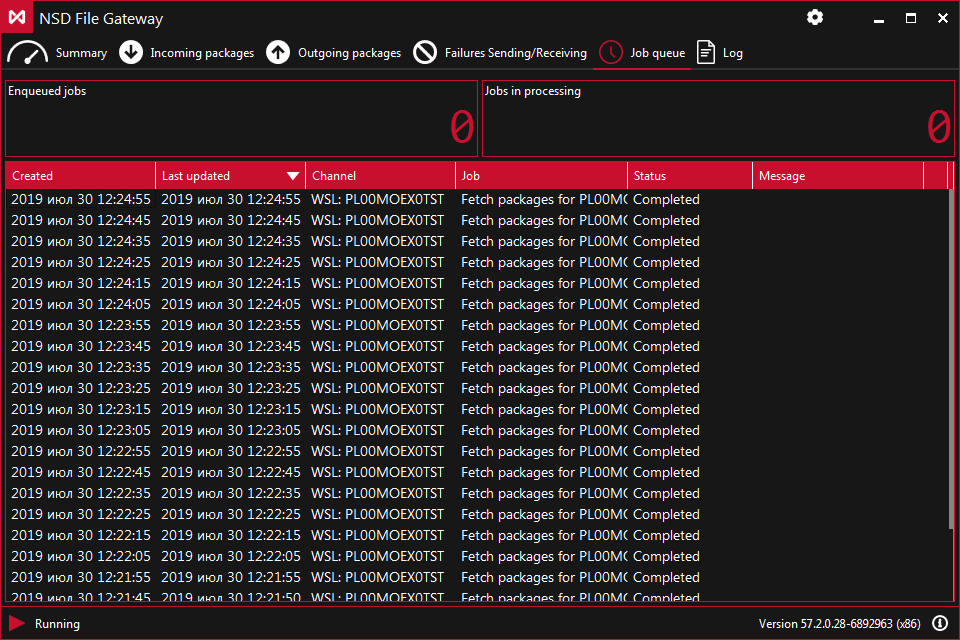


Figure 10. Task Queue Tab

You can cancel the sending of a packet during the standby by clicking the button at the end of the corresponding line. Records on the screen are deleted when sending new packets.

* 1. **Log**

The log contains information about events that occurred during the operation:

* The time when the event occurred;
* GATE – the component name that triggered the event;
* Description of the event.

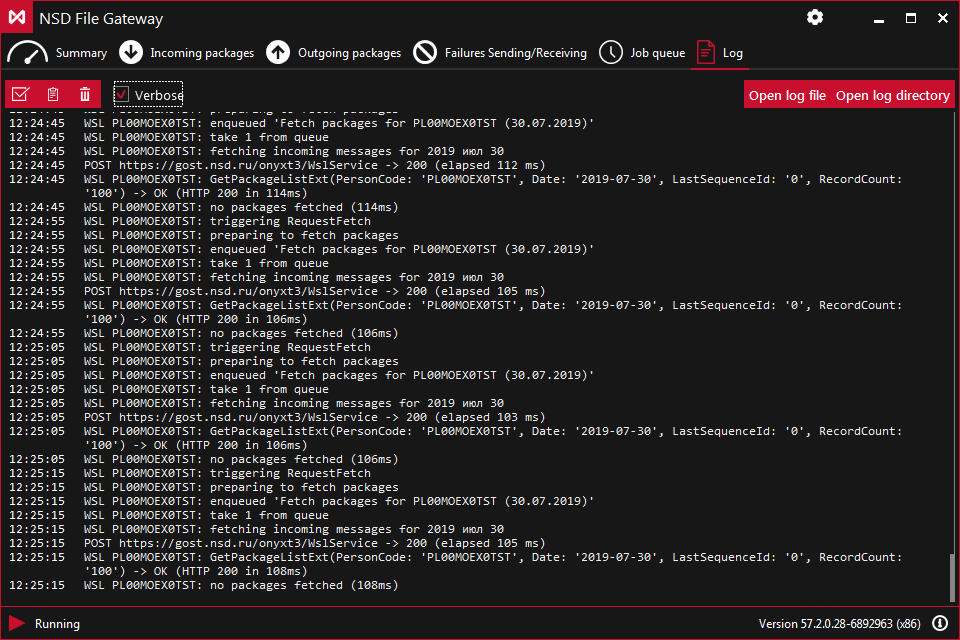


Figure 11. Log Tab

The following tools are available on the top panel:

1. select all records;
2. copy the selected records to the clipboard;
3. clear the Log tab of the records;
4. in details: show debug records;
5. open the log file in a text editor;
6. open the folder containing the log file.

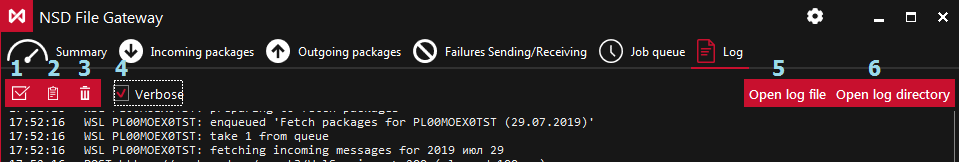
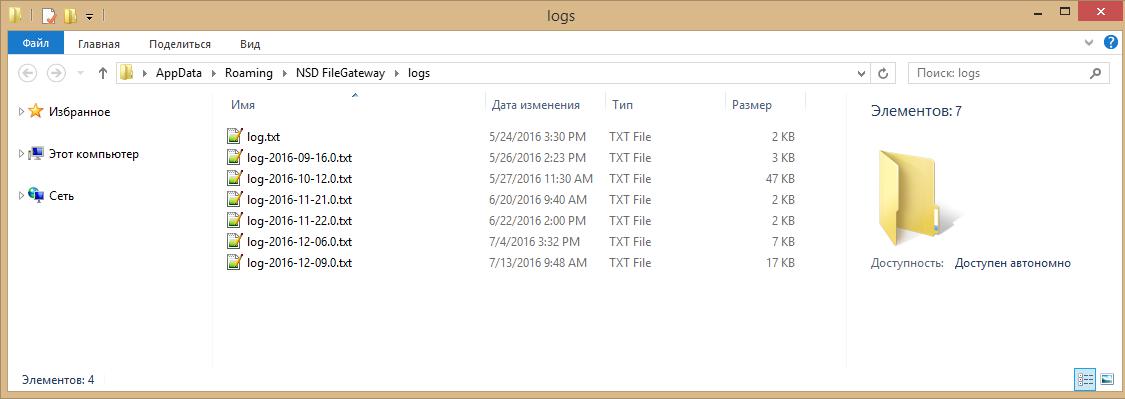


Figure 12. Tools of the Log Tab

If errors occurred, then you should send a log file to the technical support (item 6 in the list)

A new log file is generated every day. The log file for the current day is log.txt. Log files for the previous days are log-YYYY-MM-DD.N.txt, where N is the file number for the specified day. The maximum file size is 64 MB. The last 50 files are stored, and then they are automatically deleted. In view of this, the total size of the log does not exceed 3,200 MB.



13. Log File Folder

# 6. Settings

You can open the settings form by the following means:

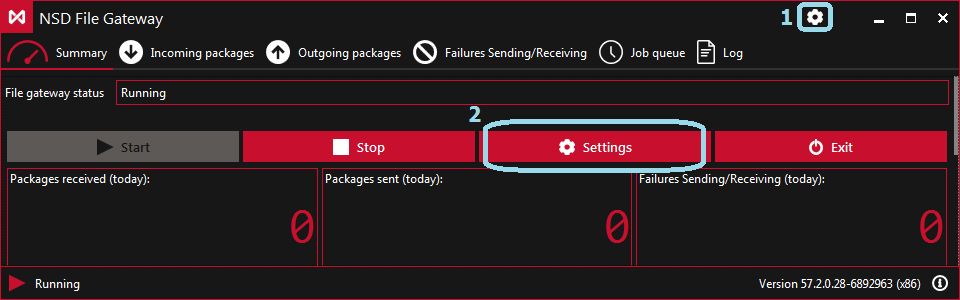
* Click the http://docs.itglobal.ru/download/attachments/7833582/%D0%9A%D0%BD%D0%BE%D0%BF%D0%BA%D0%B0%D0%9D%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B8.png?version=1&modificationDate=1464103185193&api=v2 button on the top panel;
* Click the “Settings” button in the main window (Figure 14);
* Right-click the icon in the right part of the Windows taskbar and select Settings.

Figure 14. Moving to FG Settings

Parameters are split into 3 groups:

* general settings;
* proxy server configuration;
* setup of data interchange channels.

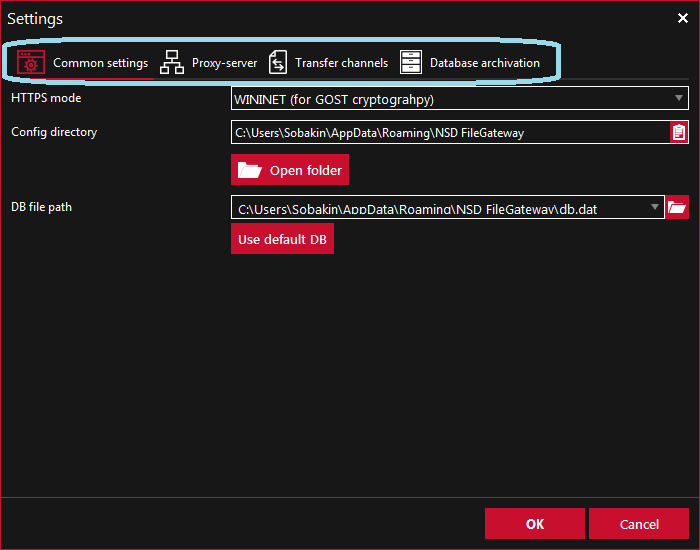


Figure 15. FG Settings

To go to FG settings, you should click the Configuration Folder button on the General Settings tab. You can save settings (the “OK” button in any of the tabs) if the required fields of all three settings groups are filled.

* 1. **General Settings**

To work on the “General Settings” tab, you should specify the https-connection mode:

* Select automatically;
* Default (used for RSA cryptography);
* WININET (used for GOST cryptography).

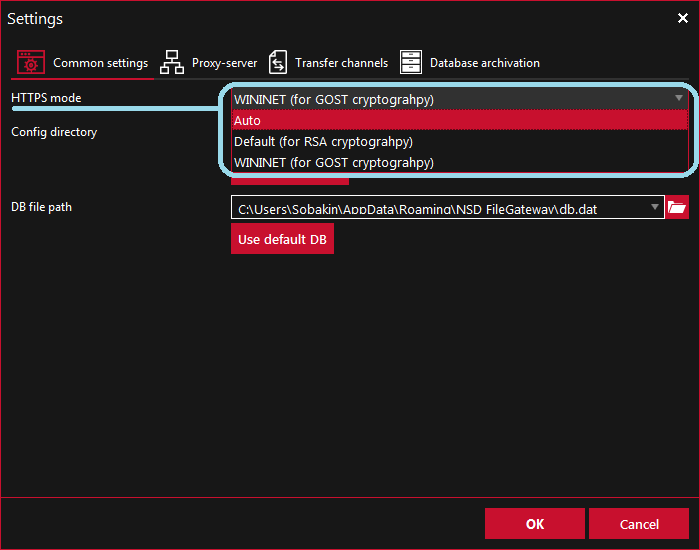
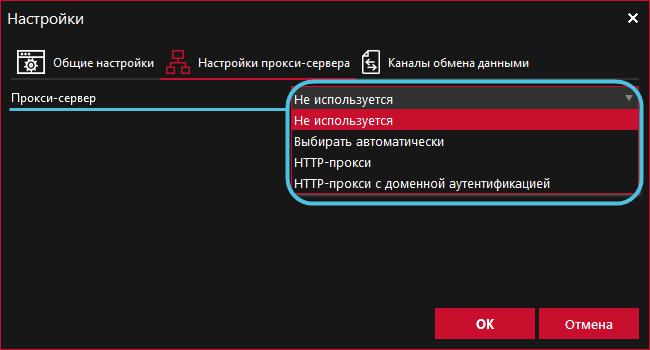


Figure 16. Web Client Address

The “Configuration Folder” button is used to go to FG settings. After entering the settings on the General Settings tab, you should set the next tab.

* 1. **Proxy Server Configuration**

In the Proxy server drop-down list, you should select the mode and fill settings’ parameters.



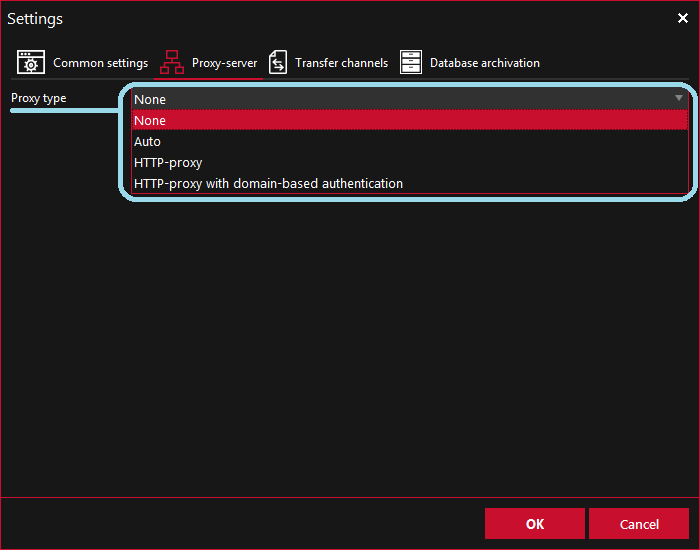


Figure 17. Configuring a Proxy Server



You can check the settings of the current proxy server with your system administrator.

You must click the "OK" button to save all settings. Saving is not possible until the required fields are filled in all three tabs.

The “Not Used” mode is set in case if the proxy will not be used to work with NSD Web Service.

The "Select automatically" mode is selected automatically. The proxy server specified in the Internet Explorer settings will be used.

In the settings of the "HTTP proxy" mode, you should specify the user on whose behalf the authentication will be performed. Connection settings include:

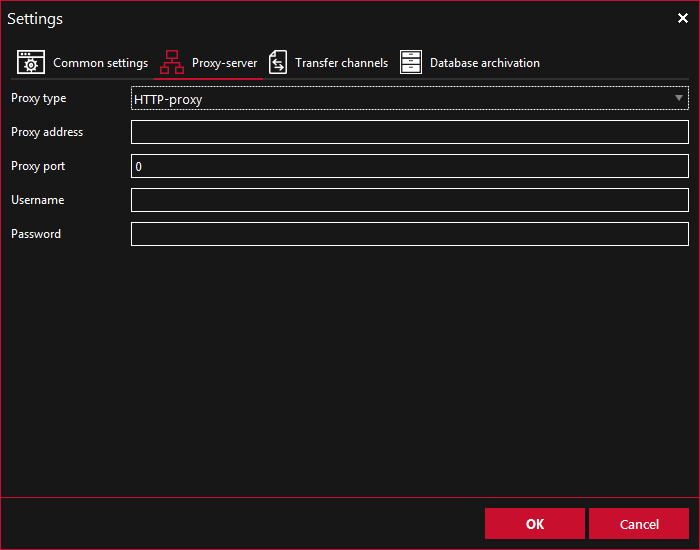
* IP address of the proxy server;
* Port number of the proxy server;
* User name for the proxy server;
* User password for the proxy server.

Figure 18. HTTP Proxy Mode

In the settings of the “HTTP proxy with domain authentication” mode, you should specify the user on whose behalf the FG will be run. Connection settings:

* IP address of the proxy server
* Port number of the proxy server

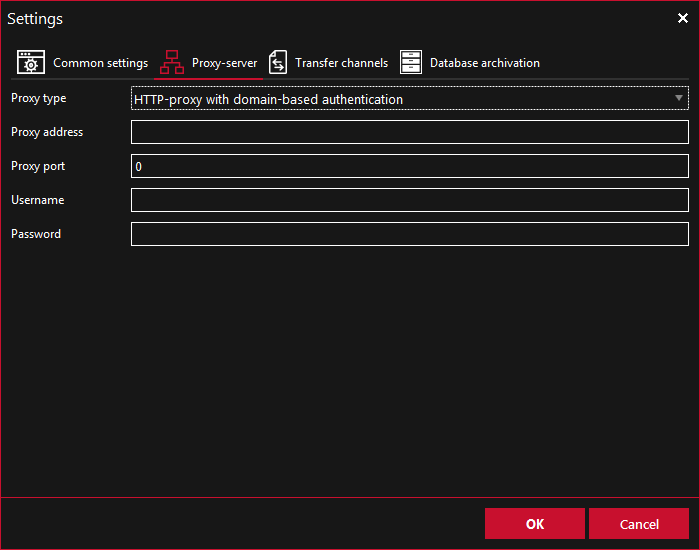


Figure 19. HTTP Proxy with Domain Authentication

* 1. **Data Interchange Channels**

Messages are exchanged through the active channels:

* The WSL channel is used to send and receive NSD’s EDI files.
* The LKR channel is used only for sending draft electronic documents to NSD Repository Web Client.

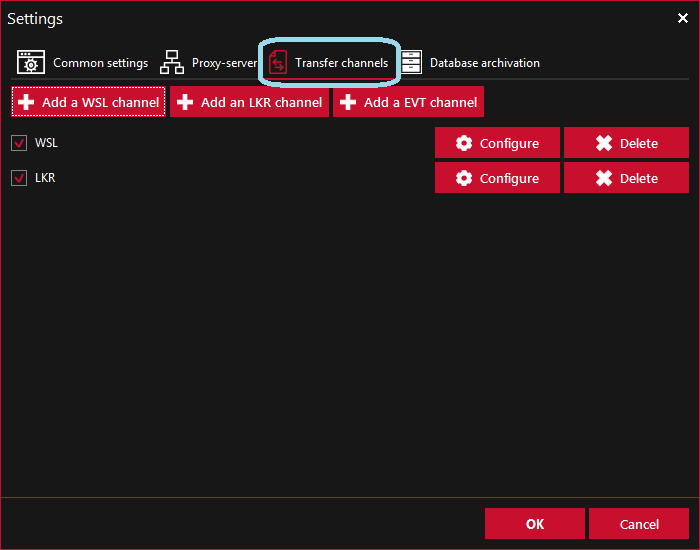


Figure 20. Data Interchange Channels Tab

Through the FG interface, you can configure the ability of several channels of the same type to operate simultaneously. Each channel uses its own set of folders and depository code. With respect to each channel, you can specify URL of the Web Service, or the Repository Web Client.

* + 1. **Creation of a Channel**

To create a channel, you should:

* 1. сlick the button  / .
  2. fill in the settings in the window opened. The description of settings for the WSL and LKR channels is presented in the tables below (see pp. 6.3.4, 6.3.5);

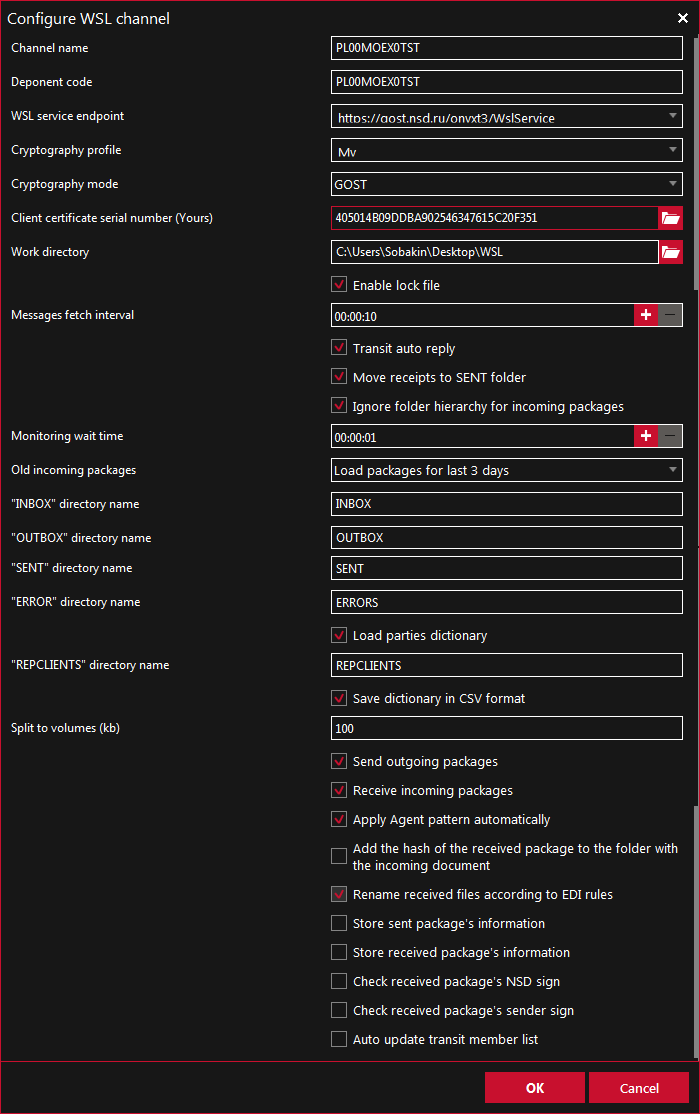


Figure 21. Settings for the WSL Channel

Before saving, make sure that the “General Settings”, “Proxy Server Configuration” tabs and the “Settings for the WSL/LKR channel” window are filled. Click “OK” to save the settings.

The created channel will be displayed on the “Settings” screen form on the “Data Interchange channels” tab.

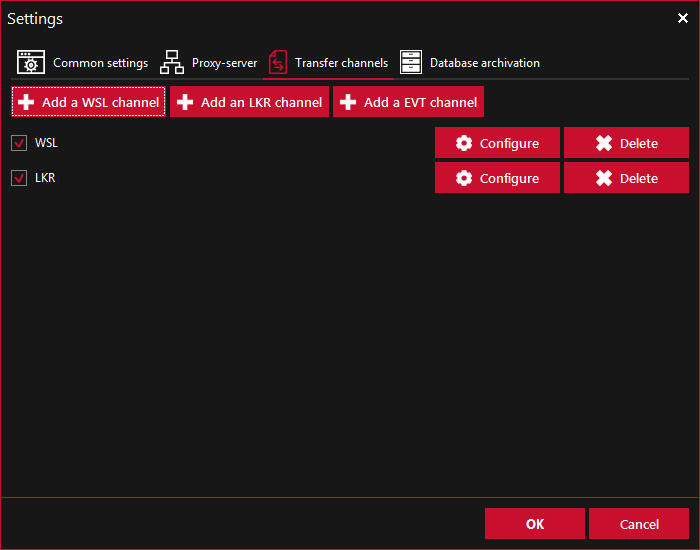


Figure 22. Created Channel

* 1. Click the "OK" button.

To edit the channel settings, click the “Configure” button and make changes in the opened window and save by clicking “OK” button.

To run gateway click the “Run”  button on the Summary tab and then folders will be displayed in the working folder of each created channel, named by default:

* ERRORS,
* INBOX (the INBOX folder is not created for LKR channels),
* OUTBOX,
* SENT.

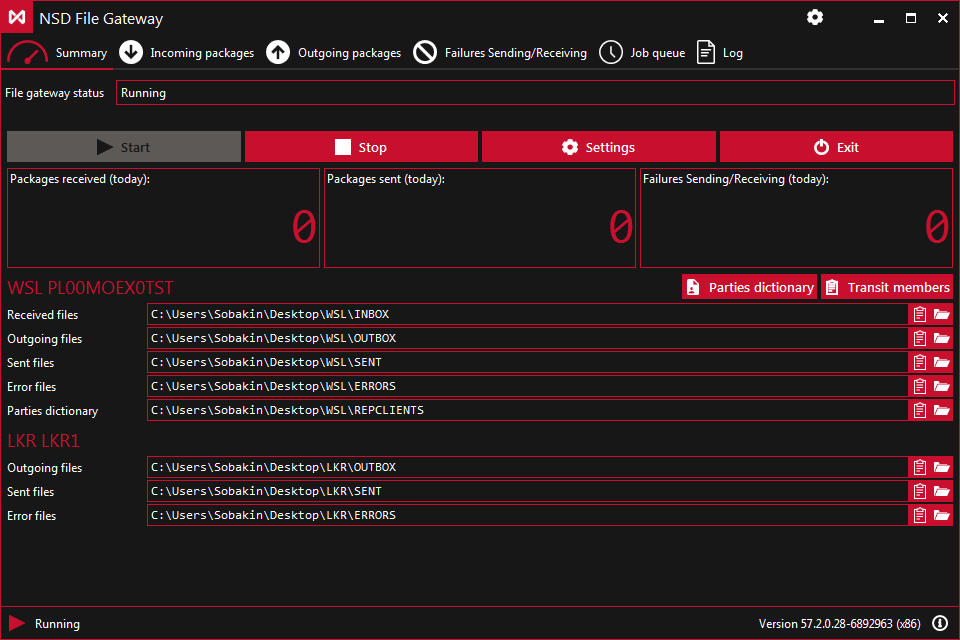


Figure 23. Created Channel Folders

* + 1. **Deactivation of a Channel**

To deactivate a channel, you should uncheck the box and save the changes by clicking the “OK” button on the “Data Interchange Channels” tab.

* + 1. **Deletion of a Channel**

To remove a channel, you should click the Delete button and save the changes by clicking the OK button on the Data Interchange Channels tab.

* + 1. **WSL Channel Settings**

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Client code | On behalf of the specified code, the channel will send and receive messages. |
| WSL service address | NSD Web Service address with which FG interacts to interchange messages (including those related to Corporate actions). In the drop-down list, you should select one of the addresses or manually enter your address.  **GOST**  <https://gost-g.nsd.ru/onyxgs/WslService> – GUEST, test environment for clients (current software version installed in PROM);  <https://edog.nsd.ru/onyxpr/WslService> – PROM, production environment;  <https://gost.nsd.ru/onyxpl/WslService> – PL, test environment for beta testing (prospective software version).  **RSA**  <https://rsa-g.nsd.ru/onyxgs/WslService> – GUEST, test environment for clients (current software version installed in PROM);  <https://edor.nsd.ru/onyxpr/WslService> – PROM, production environment;  <https://rsa.nsd.ru/onyxpl/WslService> – PL, test environment for beta testing (prospective software version). |
| Serial number of NSD electronic signature certificate | The serial number of the client certificate which is saved in the system storage. It is used to encrypt cry-packets being sent to NSD. The number must be copied from the certificate storage. |
| Cryptographic profile | The Validata profile is used, “My” (all certificates saved in the system storage) is proposed to use by default. |
| Cryptography mode | Cryptography type – GOST (set by default) or RSA |
| Serial number of client certificate (Yours) | The serial number of a client certificate. Clicking the http://docs.itglobal.ru/download/attachments/7833702/%D0%9E%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8C_%D0%BF%D0%B0%D0%BF%D0%BA%D1%83.png?version=1&modificationDate=1464270130407&api=v2 button opens a window in which you need to select a certificate.    It is used to access the HTTPS channel. |
| Path to the working folder | The working folder is a folder in which a channel automatically creates its own folders of incoming, outgoing, sent, and error messages. Clicking on http://docs.itglobal.ru/download/attachments/7833702/%D0%9E%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8C_%D0%BF%D0%B0%D0%BF%D0%BA%D1%83.png?version=1&modificationDate=1464270130407&api=v2 button will open the Window Explorer, in which you need to select a folder. |
| Use a semaphore file | If this mode is enabled, when accessing the working folder, then FG will block the “.LOCK” file in the working folder root.  If this file has been already locked, then FG will wait for it to be unlocked. |
| Interval for unloading messages from WSL channel | Interval for refreshing incoming messages in the HH:MM:SS format.  For example, 00:01:30 is 1 min 30 sec  Minimum value – 00:00:10 |
| Automatic sending of notifications | Enable automatic sending of EDI transit packet receipts. |
| Transfer receipts to the SENT folder | The mode in which the receipts received from NSD's Web Service are downloaded in the folder for sent messages (by default the SENT folder) with the name **Received.xml** or **ReceivedNDC.xml**. |
| Ignore folder nesting when processing incomings | The mode in which the folder structure changes when receiving reports. When this option is selected, FG does not create multiple subfolders, but downloads the files in one folder, and assigns to it the name of the attached file. |
| Waiting time for sending | Waiting time for downloading multiple attached files, if multiple files are downloaded in one folder  Interval of waiting for outgoing messages in the HH:MM:SS format  For example, 00:01:30 is 1 min 30 sec  It is recommended to set 10 sec  The minimum value is 00:00:01 |
| Old incoming packets | From the drop-down list you need to choose: how many packets and days you need to unload. FG uploads only those packets that were not uploaded before. |
| INBOX/OUTBOX/SENT/ERROR folder | The names of the folders for incoming, outgoing, sent messages and for sending errors.  Specified by default:  •INBOX  •OUTBOX  •SENT  •ERROR  You can also specify a path to the folder, for example, OUTBOX\_folder\FpML\_folder |
| Download the Directory of Participants | Saving the Directory of Participants in the working folder of the channel. |
| Split a packet into parts | Sending/receiving packet in parts |
| Enable packet sending | Enabling packet sending |
| Enable packet receipt | Enabling packet receipt |
| Apply automatically the Agent scheme | Sending/receiving of new documents under the Agent scheme |
| Add the received packet’s hash to the inbox folder name | A line equal to the HASH function calculated from the incoming packet is added. |
| Rename outgoing files automatically | Renaming outgoing files according to the EDI Rules |
| Save information about a sent packet | After sending, a packageInfo.xml file with information about the packet will be saved in the SENT folder next to the packet. |

* + 1. **Setting Parameters of the LKR Channel**

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| URL of the Repository Web-Client | NSD’s Web Client address, which FG interacts with to send drafts. In the drop-down list, you need to select one of the addresses or manually enter your address.  URL (test environment):  <http://repository1.itglobal.ru/lkr/>, corresponds to [https://gost.nsd.ru/onyxpl/WslService](https://rsa.nsd.ru/onyxpl/WslService), <https://rsa.nsd.ru/onyxpl/WslService>,  <http://repository3.itglobal.ru/lkr/>, corresponds to <https://gost-g.nsd.ru/onyxgs/WslService>, <https://rsa-g.nsd.ru/onyxgs/WslService>,  URL (product environment):  GOST and RSA – <https://cabinet.nsd.ru/repository/>, corresponds to <https://edog.nsd.ru/onyxpr/WslService> and <https://edor.nsd.ru/onyxpr/WslService>. |
| User name | User name of the account in the Web Client |
| Password | Password of the account in the Web Client. The password is stored in a configuration file in an encrypted form. |
| Cryptographic profile | Validata profile used, proposed by default “My” - all certificates saved in the system storage. |
| Cryptography mode | Cryptography type – GOST (set by default) or RSA |
| Serial number of client certificate (Yours) | Serial number of the client certificate. Clicking the http://docs.itglobal.ru/download/attachments/7833702/%D0%9E%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8C_%D0%BF%D0%B0%D0%BF%D0%BA%D1%83.png?version=1&modificationDate=1464270130407&api=v2 button opens a window in which you need to select a certificate.    It is used to access the HTTPS channel. |
| Use a semaphore file | Whether to use a semaphore file when working with a working folder.  If this mode is enabled, when accessing the working folder, then FG will block the “.LOCK” file in the working folder root.  If this file is already locked, then FG will wait for it to be unlocked. |
| Path to the working folder | Working folder is a folder in which a channel automatically creates its own folders of incoming, sent and error messages |
| Waiting time for sending | Waiting time for downloading multiple attached files, if multiple files are downloaded in one folder  The interval of waiting for outgoing messages in the HH:MM:SS format  For example, 00:01:30 is 1 min 30 sec  It is recommended to set 10 sec  Minimum value is 00:00:01 |
| OUTBOX/SENT/ERROR folder | The names of the folders for outgoing, sent messages and for sending errors. Specified by default:  •OUTBOX  •SENT  •ERROR  You can also specify path to the folder, for example, OUTBOX\_folder\FpML\_folder |

* + 1. **Setup of the E-Voting Channel**

The E-voting channel is used to exchange documents through API (web service) E-voting. There is the “Add EVT channel” button in the FG interface’s “Settings/Data interchange channels” section.

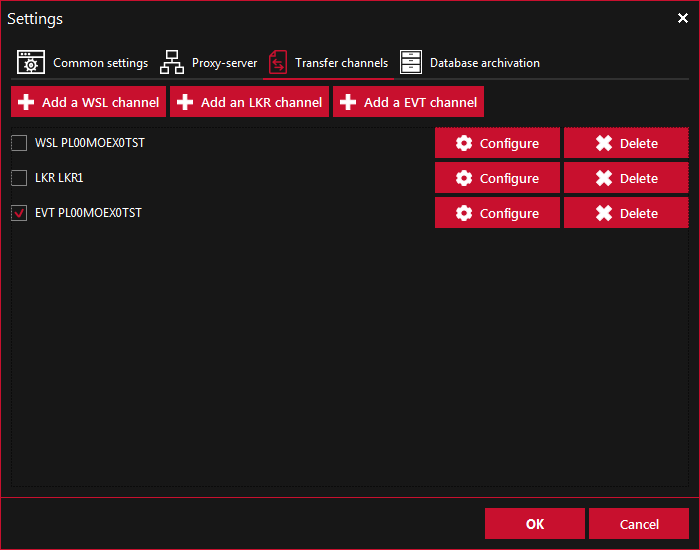


Figure 24. “Settings” Screen Form

You need to press the “Add EVT channel” button, after which the settings window for this type of channel will open: receive payments on a special depository account.

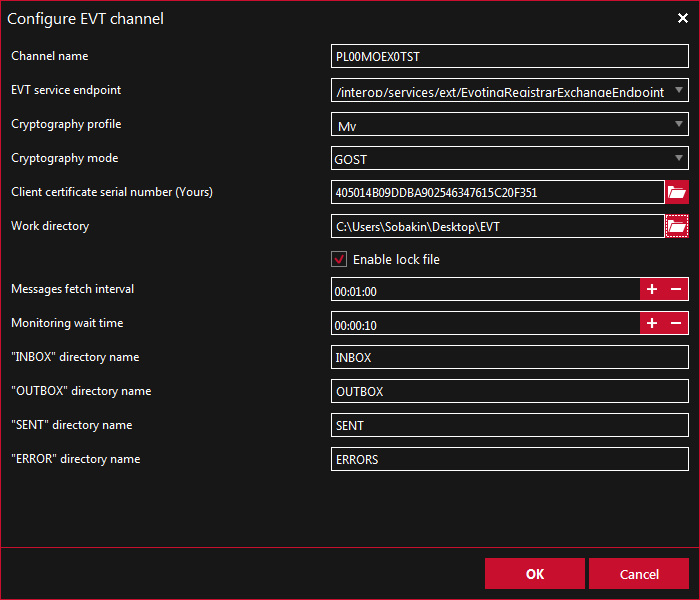


Figure 25. “Configure the EVT Channel” Screen Form

After filling the channel parameters, click the “OK” button to save the new settings.

* + - 1. **Setting Parameters of the E-Voting Channel**

|  |  |
| --- | --- |
| **Parameter** | **Description** |
| Channel name | Manual entry of the channel name |
| EVT service address | NSD Web Service address (E-Voting) with which FG interacts to exchange messages.   <https://gw.nsd.ru/e-voting-ui-pl/interop/services/ext/> **The current address is provided by NSD Technical Support.** |
| Cryptographic profile | Validata profile in-use |
| Cryptography mode | Cryptography type – GOST (by default) |
| Serial number of a client certificate | The serial number of a client certificate that is used to access the HTTPS channel and to apply an electronic signature on the sent e-document. |
| Path to the working folder | Working folder is a folder in which a channel creates its own folders of incoming, outgoing, sent and error messages. |
| Use a semaphore file | Whether to use a semaphore file when working with a working folder. If this mode is enabled, when accessing the working folder, then FG will block the “.LOCK” file in the working folder root. If this file is already locked, then FG will wait for it to be unlocked (see the “Use of a Semaphore File” section). |
| Message upload interval | Interval of accessing to WS E-voting to refresh incoming messages in HH: MM: SS format  For example, 00:01:30 is 1 min 30 sec  The minimum value is 00:00:10 |
| Waiting time for sending | Waiting time for downloading multiple attached files, if multiple files are downloaded in one folder. The interval of waiting for outgoing messages in the HH:MM:SS format. For example, 00:01:30 is 1 min 30 sec. It is recommended to set 10 sec. The minimum value is 00:00:01. |
| “INBOX” folder | The INBOX by default in the working folder specified above  The folder is intended for documents received in FG FG does not additionally convert files when receiving them. |
| “OUTBOX” folder | The OUTBOX by default in the working folder specified above  The folder is intended for documents prepared for sending. The file gateway periodically scans this folder for changes and analyzes the content of the folder.  Documents prepared for sending should be in a subfolder (with an arbitrary name) OUTBOX \% FolderName% rather than in the OUTBOX folder root.  FG does not additionally convert files when sending them. |
| “SENT” folder | The SENT by default in the working folder specified above  The “OUTBOX” folder’s documents successfully sent to the recipient (E-voting service) are transferred to the folder. Documents are transferred to the said folder without additional conversions made by the file gateway. |
| “ERROR” folder | The ERRORS by default in the working folder specified above  Folder for unsuccessfully sent files. |

After setting and selecting the EVT channel the main **"Summary" tab** looks like this:

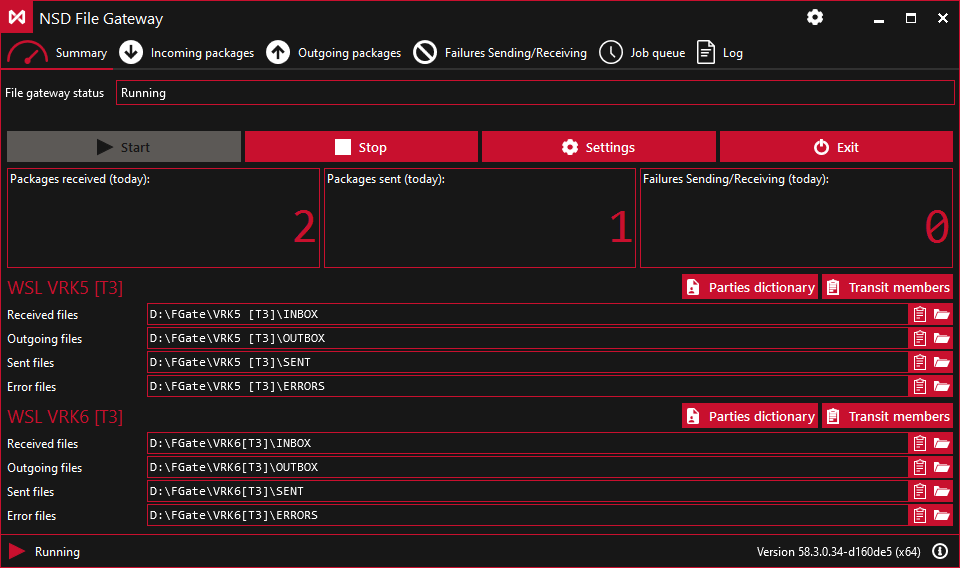


Figure 26. Summary Tab

**Incoming Packets Tab:**

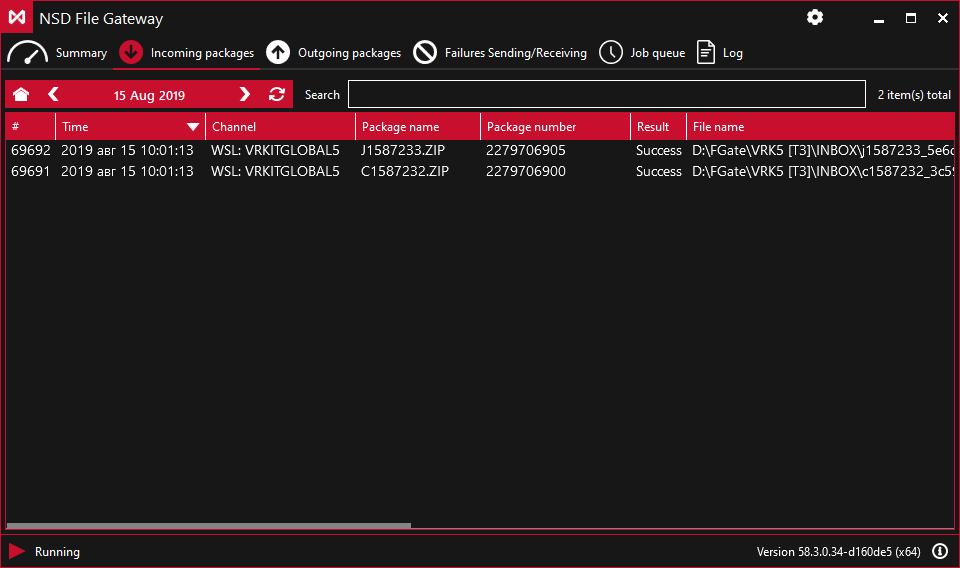


Figure 27. Incoming Packets Tab

**Outgoing Packets Tab:**

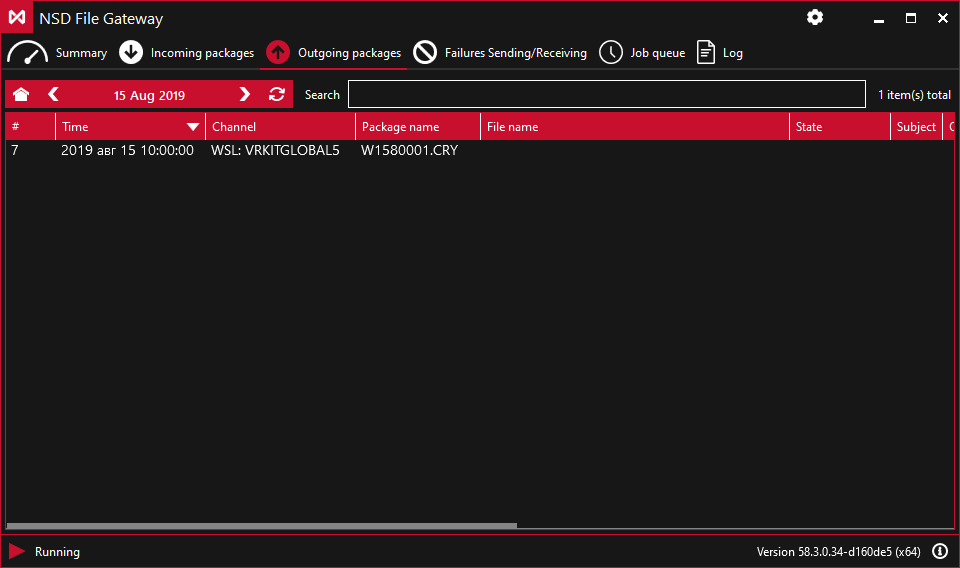


Figure 28. Outgoing Packets Tab

**Sending/Receiving Errors Tab:**

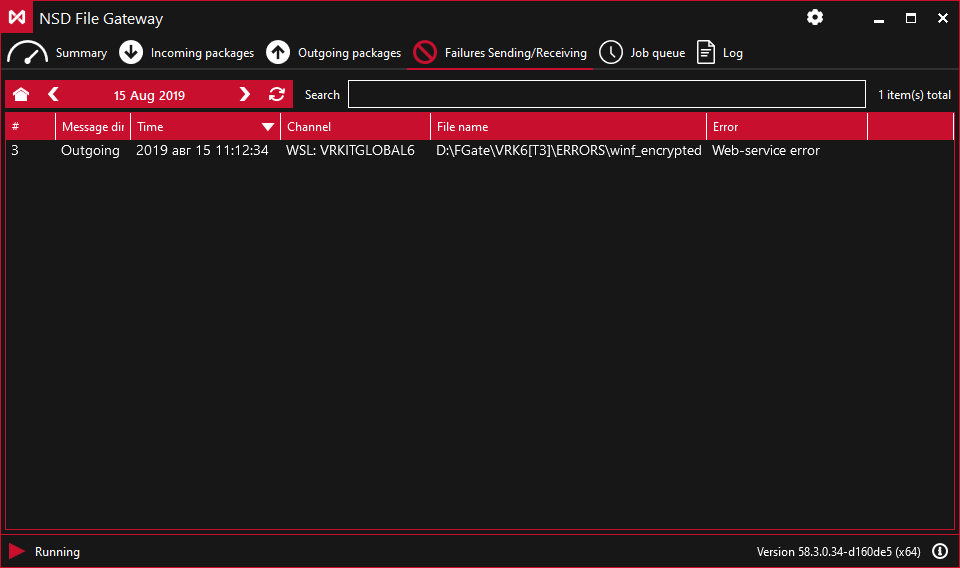


Figure 29. Sending/Receiving Errors Tab

**Task Queue Tab:**

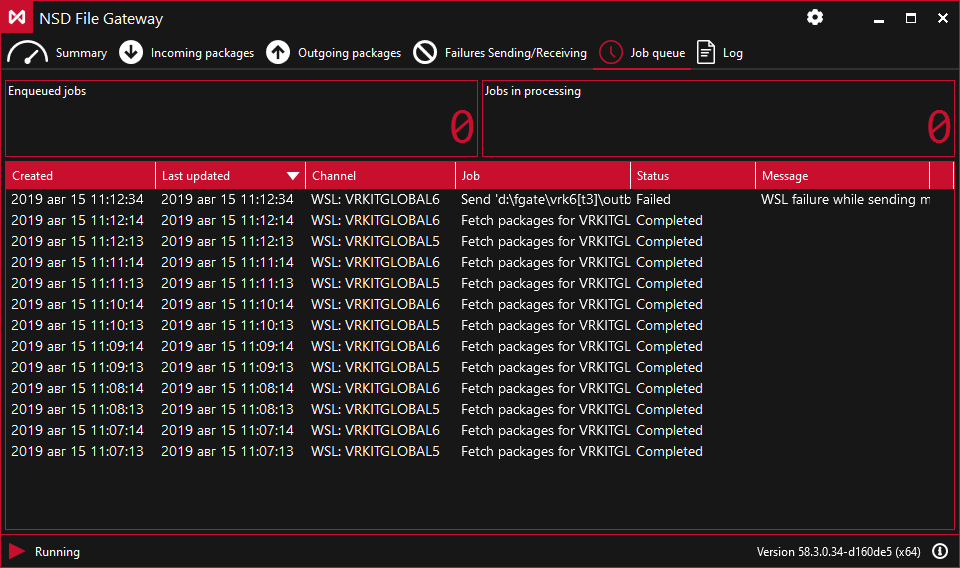


Figure 30. Task Queue Tab

**Log Tab:**

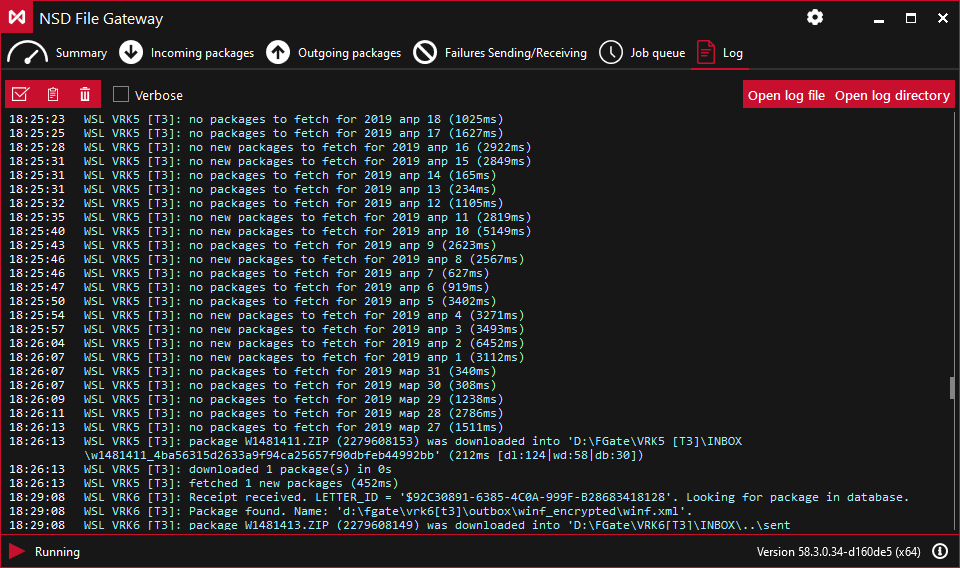


Figure 31. Log Tab

* + - 1. **E-Voting Messaging Algorithms**

6.3.6.2.1 **Receiving Messages from E-Voting**Receiving messages from E-Voting occurs automatically with an interval of 30 seconds, but you need to monitor possible errors. The process of receiving messages consists of the following steps:

1. E-voting forms an ISO message packet on its side and assigns it a unique identifier.
2. FG automatically initiates successive requests to the E-voting service for the existence of messages to the registrar.
3. When receiving files, FG automatically generates a status message to E-voting on the successful receipt of these files (*SendMessageStatus*), sequentially for each received packet from step (2).   
   Each message will contain one status per one packet.

The received files (which are ZIP-archives with attached xml-documents) will be put in the INBOX folder of the working folder of the EVT channel.  
FG does not provide additional processing/unpacking.

More information about the error you can find in the “Sending/Receiving Errors” tab or in the “Log” tab.

6.3.6.2.2 **Sending Messages to E-Voting**

To send messages to **E-voting**, you need to put the sent ISO20022 message packet in a ZIP archive format, with an attached xml OUTBOX \% Arbitrary\_name\_folder% \% sent\_package% .ZIP.

In case of successful sending, this packet will be moved to the SENT folder of the working folder of the EVT channel. In case of error sending, the packet will be moved to the ERRORS folder of the working folder of the EVT channel.

More information about an error you can find in the “Sending/Receiving Errors” tab or in the “Log” tab.

6.3.6.2.2 **Formation of the ISO 20022 Messages Packet**

ISO 20022 messages are transmitted between the interchange participants in the form of a packet of electronic documents signed by the sender's ES. The packet of electronic documents is formed as follows:

1. Each ISO 20022 message is saved in a separate file.

Requirements for the Name of the ISO 20022 Message File

| Position or number of characters in the name | Content |
| --- | --- |
| 1 to 5 characters | The value of the/AppHdr/BizSvc element of the ISO 20022 messages |
| 1 character | The separator is the underscore character: "\_". |
| 1 to 35 characters | The value of the BizMsgIdr (AppHdr/BizMsgIdr) element of an ISO 20022 message (business message identifier).  The business message identifier must not contain an underscore character: “\_”. |
| 1 character | The separator is the underscore character: "\_". |
| 20 characters | The creation time of an ISO 20022 message, equal to the value of the/AppHdr/CreDt element of the ISO message header, in the format:  CCYY-MM-DDThh+mm+ssZ  where,  CCYY – year;  MM –month;  DD – day;  T – constant "T";  hh – hours;  mm – minutes;  ss – seconds.  Z – constant «Z»;  Time Zone: UTC. |
| 4 characters (file extension). | Line: ".xml" |

Example of xml file name, "CA012" form code:   
***CA012\_a9327938866f42dc81082a1f9e1a3f0d\_2001-01-02T19+32+52Z.xml***

1. ISO 20022 message files are packed in a ZIP-archive, there are no requirements for the archive name, and however, it is recommended to name the archive with respect to the attached xml file.  
   Possible methods of archive compression:

uncompressed – without compression;

deflate – «deflate» method.

1. The exchange participant monitors the size of the ZIP-archive (maximum packet size is 2 MB).
2. The ISO 20022 message packet file (ZIP-archive) is put in the OUTBOX folder of the EVT channel working folder, further see p. 6.3.6.2.2.

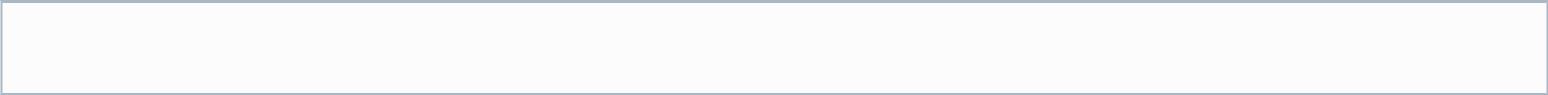
# 7. Principle of Operation

* 1. **General Procedure for Sending Packets**

The working folder is shown in the settings for each channel (see Section 6.3). FG creates target folders in this folder.

The following folders are created for the LRK-type channels (sending draft electronic documents to NSD Repository Web Client):

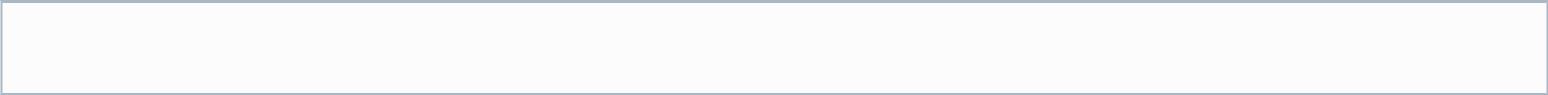
* OUTBOX – for outgoing files,
* SENT – for files which were sent successfully,
* ERRORS – for files which were sent with errors.



The folder name is set in the channel settings (see section 6.3.5).

The following folders are created for the WSL-type channels (sending and receiving NSD EDI files):

* INBOX – for incoming files,
* OUTBOX – for outgoing files,
* SENT – for files which were sent successfully,
* ERRORS – for files which were sent with errors.



The folder name is set in the channel settings (see section 6.3.4).

The file gateway maintains sending of the following files:

* \*.XML files;
* documents concerning corporate actions;
* WINF.XML files;
* attachments.

To transfer files, you need to create a directory (folder) with any name in the OUTBOX folder. Then you should place the files prepared for the transfer to the created directory. The directory is deleted if the files have been transferred. In case of successful sending, the original subfolder will be moved from the OUTBOX folder to the SENT folder, and in case of an error – to the ERRORS folder. To send new files, you need to create a new directory in the OUTBOX folder.

The response message is uploaded to the **\INBOX\{Packet name in EDI**} folder (this item is applicable only to the WSL-type channels).

If a file/folder with the same name is already in the directory of messages sent or incoming, then a new file/folder name is formed by adding the suffix \_N, where N is a decimal integer.

The packet will be formed with the first letter **K** for the Register of holders under the meeting, with respect to reports – with the first letter **Q**.

* 1. **Rules for Naming ED Files**

ED files are assigned names based on the following general requirements:

* the file name can have only letters of the Latin alphabet (regardless of the case), numbers and the # character (hash);
* the length of the file name (except for extension) must not exceed 8 characters if the first character is different from # and up to 25 characters if the first character is #;
* the file name with a length of 8 characters is formed according to the requirements specified in Table 1, with a length of up to 25 characters – Table 2.

**Table 1 – Rule No. 1 for Naming a Packet of Documents**

|  |  |  |
| --- | --- | --- |
| **1 character** | **2-4 character** | **5-8 character** |
| Feature of ED | DDM (day, month: 1-9, A, B,C.) | The unique ED file number for the specified day. |

**Table 2 – Rule No. 2 for Naming a Packet of Documents**

|  |  |  |  |
| --- | --- | --- | --- |
| **1 character** | **2-6 character** | **7-12 character** | **13-25 character** |
| # | Type of ED | DDMMYY (date of ED formation) | The unique ED file number for the specified day. |

|  |  |
| --- | --- |
| **Table 3 - List of Documents** |  |

|  |  |  |
| --- | --- | --- |
| **Name of the document/group of documents** | **Type of ED** | **First character, feature of ED** |
| Incoming message from the client to AMS (application management system) | FOXML | # |
| Outgoing message from AMS to the client | FOXRP | # |
| Notification of the acceptance (non-acceptance) of a notice on the crediting of securities to NSD account in the Register/List of securities holders | CONF | C |
| Notification of the receipt of the packet of electronic documents | CONFH | C |
| Notification of an error occurred when processing packets of electronic documents | ERRH | C |
| Notification of the receipt of the packet of electronic documents | XCONF | C |
| Notification of acceptance (non-acceptance) of the List of holders of securities for execution | CNF | D |
| Notification of acceptance (non-acceptance) of the List of owners of securities for execution | RE | D |
| Repository documents | RPZTR | F |
| Payment Request Register/Notification | PAYMN | G |
| Report on the average monthly balance of securities in NSD accounts | MIDAM | H |
| Notification of the generation of the report on the execution/non-execution of the depository order | BRREP | I |
| Information message | INF | I |
| Open information message in HTML format | INF\_H | I |
| Notifications of income payment | PMNI | I |
| Refreshing directories | DICT | J |
| Depository instruction/Notice of acceptance (non-acceptance) of depository instructions | ORD42 | K |
| Instruction/Ordinance | ORDXM | K |
| Notification of acceptance (non-acceptance) of instructions/orders | REORD | K |
| List of electronic documents transmitted and received by NSD for the certain period | LST | L |
| List of operations for the certain period (attached to the invoice) | FACTP | M |
| Disclosure Consent Notice | CONSN | P |
| XML report | XMLRP | Q |
| Depository instruction /Notice of acceptance (non-acceptance) of depository instructions | ORD36 | S |
| Notification of securities crediting to NSD's account in the Registry/ Notification of securities debiting from NSD's account in the Registry | UVD | U |
| Notification of the receipt of transit packet of documents | BTRAN | W |
| Transit packet of documents | TRANS | W |
| Notification of the receipt of transit packet of documents | TRBRC | W |
| Receipt for processing FATCA form | FAINF | Y |
| FATCA form | FATCA | Y |
| Requests for corporate actions | GS061 | Z |
| Payment documents | INV | Z |
| Report on transactions executed based on depository instructions | RPT | Z |

* 1. **Rules for Naming packageInfo.xml Files**

PackageInfo.xml files contain information about packets sent/received.

File names are specified with extensions. The file is put in the same folder as the sent/received packet. With respect to the sent packets, a file is created only if the “Save information about the sent packet” option is enabled. With respect to received packets, a file is created if the “Verify the signature of received transit files” option is enabled.

| **Name of the document/group of documents** | **Type of ED** | **First character, feature of ED** |
| --- | --- | --- |
| Payment document in SWIFT FIN format | PMSWT | # |
| Depository instruction in SWIFT FIN format | ORDSW | # |
| Depository report in SWIFT FIN format | RPTSW | # |
| Report on payments in SWIFT FIN format | PMSWR | # |

|  |  |
| --- | --- |
| **Table 1 - List of Documents** |  |

# Sending Packets

* 1. **FpML-Documents**

To transfer a file, you need to put attachments in the root/subfolder of the OUTBOX folder. A CRY packet is formed from the message and attached files:

1. Each of the files being sent is signed by ES using Validata.
2. All signed files are packed in a ZIP archive.

The identifier of the sent packet is formed by the mask: “FDDMNNNN”, where:

* F – letter identifying the type of packet,
* DD – day of sending packet (decimal number),
* M – month of sending packet (decimal number),
* NNNN – serial number of the packet sent by FG for the current day (decimal number).

A CRY packet is sent via the https protocol to NSD Web service. In case of successful sending, and also if the “Save information about the sent packet” option is enabled, the packageInfo.xml file will be automatically generated.



The requirements for attached files for fpml messages are presented in section 10.

* 1. **Corporate Actions and Depository and Clearing Activities Packets**

To transfer a file/an attached file, they must be put in a subfolder of the OUTBOX folder. A CRY packet is formed from the message file:

* 1. Each of the sent files is signed by ES using Validata.
  2. All signed files are packed in a ZIP archive.
  3. ZIP-archive is encrypted using the Validata software.

The identifier of the sent packet is formed by the mask: “КDDMNNNN”, where:

* К – letter identifying the type of packet,
* DD – day of sending packet (decimal number),
* M – month of sending packet (hexadecimal number),
* NNNN – serial number of the packet sent by FG for the current day (decimal number).

The message file is renamed by the mask “XXXXXXXX.XML”, where XXXXXXXX is the identifier of the packet being sent. A CRY packet is sent via the https protocol to NSD Web service. In case of successful sending, and also if the “Save information about the sent packet” option is enabled, the packageInfo.xml file will be automatically generated.



The requirements for attached files for corporate actions messages are presented in section 10.

* 1. **WINF.XML file**

The WINF.XML file containing the description of the transit packet can be created, for example, like this:

<?xml version="1.0" encoding="Windows-1251"?>

<COVERING\_LETTER>

<ORIGINATOR>

<CONTRAGENT>

<CONTRAGENT\_CODE> *sender code* </CONTRAGENT\_CODE>

</CONTRAGENT>

</ORIGINATOR>

<RECIPIENT>

<CONTRAGENT>

<CONTRAGENT\_CODE> *receiver code* </CONTRAGENT\_CODE>

</CONTRAGENT>

</RECIPIENT>

<DOC CONTR\_DOC\_ID="1" STORE\_IN\_NDC="YES" ENCRYPTED[[1]](#footnote-1)="NO" TRANSFER\_AGENT\_CONTRACT[[2]](#footnote-2)="NO">

<DOC\_TYPE>TRZT\_PRM[[3]](#footnote-3)</DOC\_TYPE>

<ORIGINAL\_FILE\_NAME>4restr08.xml</ORIGINAL\_FILE\_NAME>

<IDENT\_CODE> code TEDIK (for example, 4RESTR08) </IDENT\_CODE>

</DOC>

<DOC CONTR\_DOC\_ID="10001693CG" STORE\_IN\_NDC="YES" ENCRYPTED="NO" TRANSFER\_AGENT\_CONTRACT="NO">

<FILE\_NAME>10001693CG.rtf</FILE\_NAME>

<DOC\_TYPE>TRZT\_WRD[[4]](#footnote-4)</DOC\_TYPE>

<ORIGINAL\_FILE\_NAME>10001693CG.rtf</ORIGINAL\_FILE\_NAME>

<IDENT\_CODE>1200</IDENT\_CODE>

</DOC>

</COVERING\_LETTER>

To transfer the WINF.XML file and attached files, they must be put in a subfolder of the OUTBOX folder. The identifier of the packet being sent is formed by the following mask: “WDDMNNNN”, where:

* W – the letter W, which identifies the type of packet,
* DD – day of sending packet (decimal number),
* M – month of sending packet (hexadecimal number),
* NNNN – serial number of the packet sent by FG for the current day (decimal number).

A CRY packet containing the following files is created:

* WINF.XML file,
* Message file, renamed by the mask “XXXXXXXX.XML”, where XXXXXXXX is the identifier of the packet being sent,
* ZIP archive with attached files with the type name “XXXXXXXX.ZIP”, where XXXXXXXX is the identifier of the packet being sent. This file is not added in the absence of attached files.

A CRY packet in encrypted form is sent via the https protocol to NSD Web service. If the packet has been sent successfully, and also if the “Save information about the sent packet” option is enabled, the packageInfo.xml file will be automatically generated.



A description of the interaction format is presented on NSD official website in the section “EDI document/documents Appendix 4 to NSD EDI Rules “Ensuring the transit of electronic documents through NSD EDIS”.

* 1. **Sending by Closed Envelope Method**

Unlike sending transit documents in a standard way, the XML file of the document is additionally encrypted on all certificates for which a valid power of attorney is specified in the Directory of Transit Participants (for this wsl channel).

The method of sending packets (the standard one or the closed envelope method) is specified when generating a file description:



DOC/@ENCRYPTED, «YES» ( )

In case of successful sending, and also if the “Save information about the sent packet” option is enabled, the packageInfo.xml file will be automatically generated.



A description of the interaction format is presented on NSD official website in the Section “Appendix 4 to NSD EDI Rules “Ensuring the transit of electronic documents through NSD EDIS”.

# Sending Drafts Electronic Documents to the Repository Web Client

To send draft electronic documents to the Repository Web Client, you need to put the file with the .xml extension in the OUTBOX folder/subfolder.



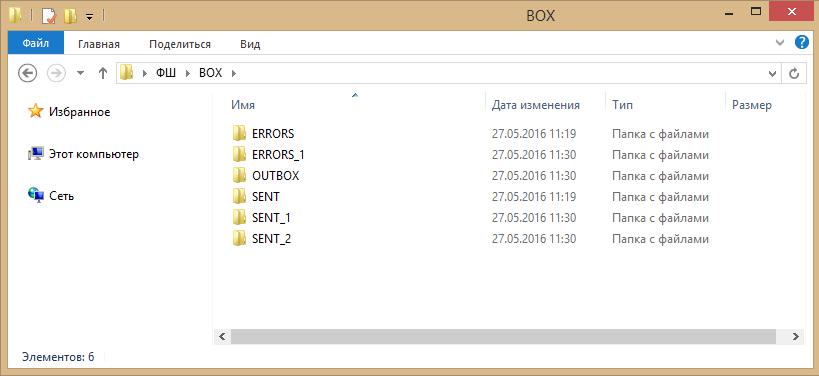
Requirements for attached files are presented in section 10.

When running, FG scans files and folders in the OUTBOX folder.

Files with the .xml extension are considered as FpML documents and sent to the Repository Web Client as drafts. If any of the attached files is missing or unavailable for reading, the sending of the whole message is postponed. A retry will be made the next time you scan the OUTBOX folder.

In case of successful sending, all files involved in drafting are moved to the SENT folder/subfolder. In case of a packet sending error, all files are moved to the ERRORS folder/subfolder.

In our example, we put 3 files to be sent in the root of the OUTBOX folder. As a result, 2 files were successfully downloaded to the Repository Web Client (two SENT\_1/SENT\_2 folders were displayed in the working folder), and one file was not downloaded (one ERROR\_1 folder was displayed in the working folder).



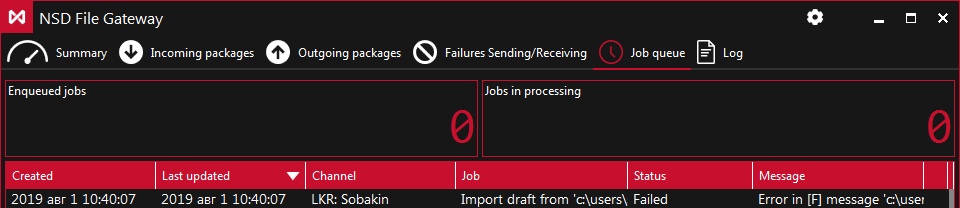
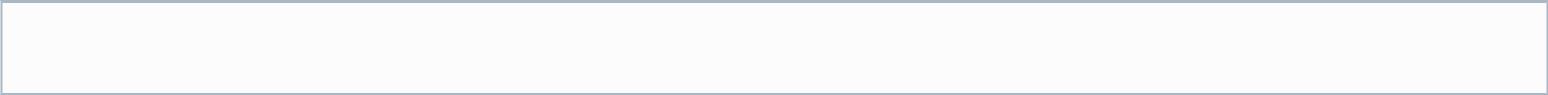


Figure 32. Result of Sending Files



More information on the processing of sending results is available in section 11.

# Requirements for Attached Files

* 1. **Attachments to the Repository’s FpML Messages**

Requirements:

1. There can be only one attached file per message.
2. The attached file must be put in the same folder as the message file.
3. The XML file of the message should contain a link to the attached file in accordance with the FpML format.



Figure 33. Link to Attachment



If the file is missing or cannot be read, the sending of a message is postponed. A retry will be made the next time you scan the OUTBOX folder.

* 1. **Attachments to the Corporate Action Messages**

Requirements:

* 1. There can be only one attached file per message.
  2. The file name must match the message file name.  
     For example, the message is message.xml, the attachment is message.pdf.
  3. The file extension of an attachment must be different from the file extension of a message.

# Sending Results

* 1. **Successful Sending**

In case of sending a packet successfully, all files involved in the packet generation are moved to a subfolder of the SENT folder, and in case of an error – to the ERRORS folder.

Additional subfolders can be created in each target folder. FG does not impose restrictions on the depth of attached folders. In this case, the path to the destination folders will be as follows:

* Files sent from the root of the OUTBOX folder will be moved to the SENT or ERRORS folder.
* Files sent from the OUTBOX\ABC subfolder will be moved to the SENT\ABC or ERRORS\ABC folder.
* Files sent from the OUTBOX\ABC\DEF subfolder will be moved to the SENT\ABC\DEF or ERRORS\ABC\DEF folder.

If the folder already exists, then a new unique folder name is formed by adding the suffix \_N, where N is a decimal integer. The number 1 is used as number N. If the file or folder with the obtained name already exists, the number is increased by 1. The process is repeated as necessary until a unique file or folder name is formed.

* 1. **.Sending Error**

In case of an error related to sending a packet, all files involved in the packet assembly are moved to the ERRORS folder. The ERROR.XML file is generated, which specifies:

* time – the date and time of an error;
* description – text description of an error.

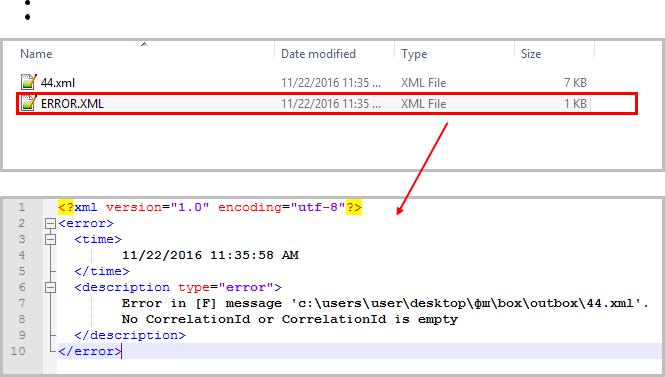


Figure 34. ERROR.XML

# Receipt of Packets

FG checks for the presence of new messages in NSD Web Service with the specified frequency (the Message upload interval parameter in the WSL channel settings). Each new message is uploaded according to the following rules:

* files that could be decrypted are put in the\INBOX\{package name in EDI} subfolder (for example,\INBOX\F2990001);
* files that could not be decrypted are put in the root of the INBOX folder "as is" (for example,\INBOX\CERROR01).



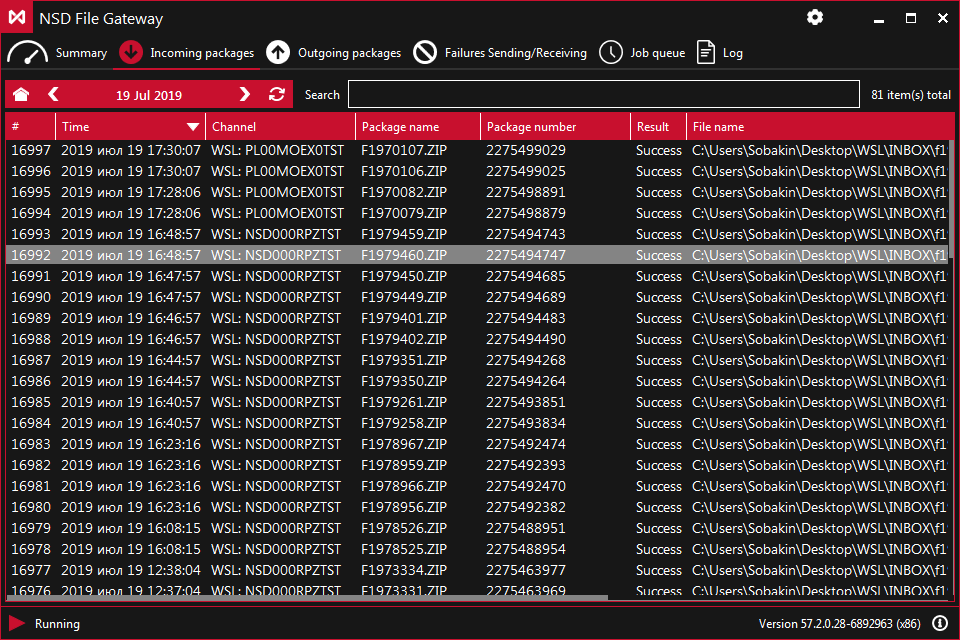
After receiving transit packets, unpacked files are assigned original names, which are taken from the ORIGINAL\_FILE\_NAME fields in the WINF.xml file.

The path to the inbox (INBOX by default) can be specified in the WSL channel settings (details, see section 6.3.4). The list of incoming messages is displayed on the Incoming Packets tab.



Records are displayed by the date of receipt by FG, but not by the date the packet appeared in EDI.

Figure 35. Incoming Messages List in the FG Interface



A description of the interaction format is presented on NSD website in the Appendices to NSD Electronic Data Interchange Rules.

# "Participants of Transit" Directory

The "Participants of Transit" Directory contains certificates of counterparties with which it is planned to exchange transit documents by a closed envelope method. The directory is used to provide encryption on the private key of the sender of packets using keys with valid certificates of the recipients.

To go to the directory, you need to click the "Participants of Transit" button.

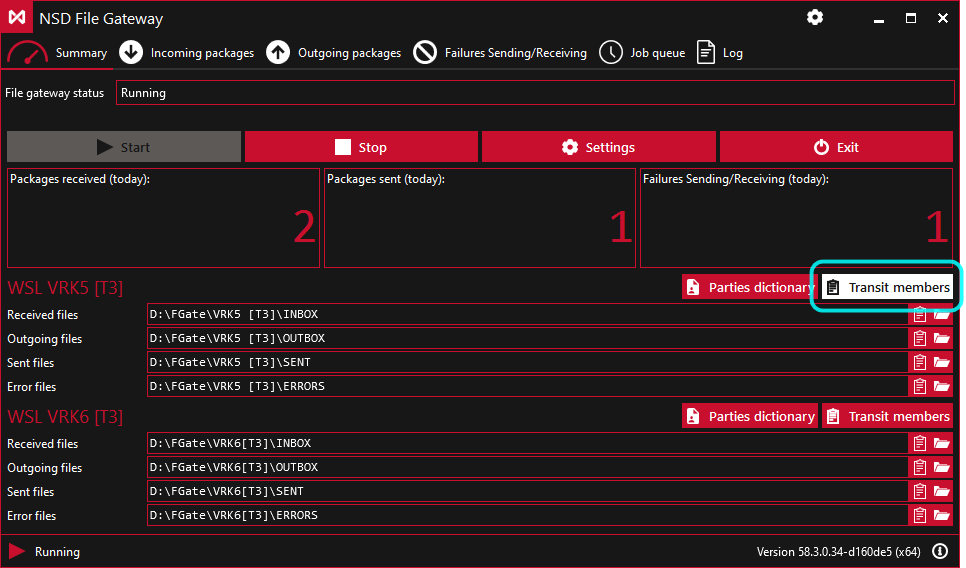


Figure 36. Go to the Directory

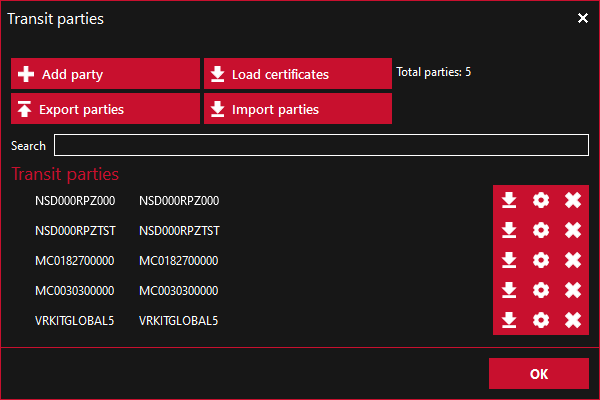


Figure 37. “Participants of Transit” Directory

* 1. **Formation of the Directory of Participants**

The procedure for the formation of the directory:

* 1. select a WSL channel from the list of current channels (a directory is formed for each WSL channel separately);
  2. add participants to the directory;
  3. download certificates manually, or send a request to NSD's web service;
  4. specify powers of attorney for certificates that will be used to encrypt documents.



Certificates are requested only for those participants who are included in the List of participants of transit

**13.2. Selection of a WSL channel (Not actual for now)**

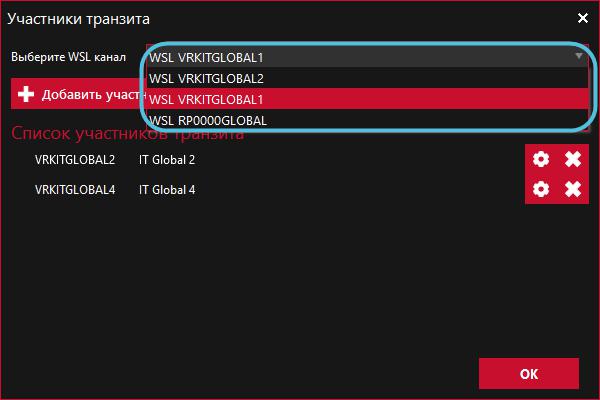
Channels are selected from the current active channels specified in FG settings.

Figure 38. Selection of a Channel

* 1. **Adding a Participant**

To add a new participant, you must click the Add Participant button.

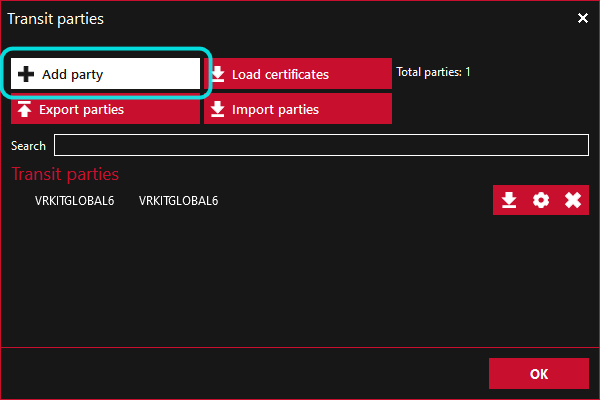


Figure 39. Add Participant Button

In the window opened, you need to specify:

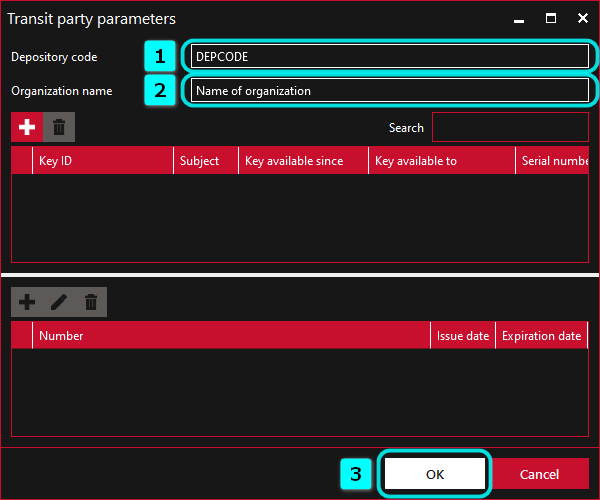
* Depository code;
* Name of organization;
* Click OK button.

Figure 40. Participant Settings

The first block displays information about the certificates of a participant. Information will be displayed after downloading participants’ certificates (see section 13.4). The second block displays information about powers of attorney. The power of attorney is indicated after the addition of certificates.

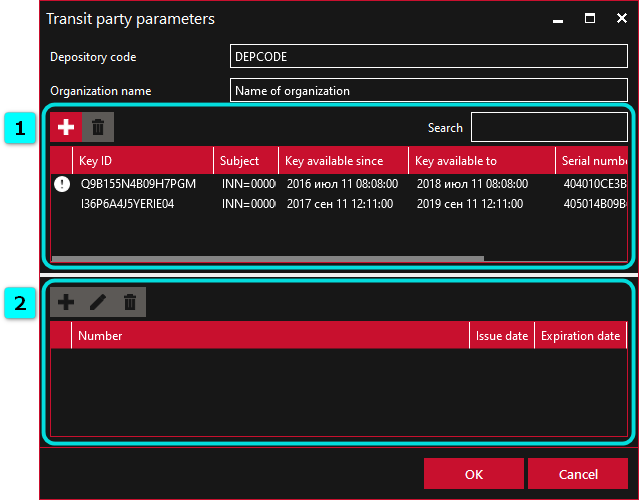


Figure 41. Participant Settings

The icon http://docs.itglobal.ru/download/attachments/9044505/icon.png?version=1&modificationDate=1481622593750&api=v2 is placed opposite the expired certificates/powers of attorney.

* 1. **Download of Certificates**

To obtain counterparty certificates, you must click the "Download Certificates" button. The button will become inactive until the response to the request comes.

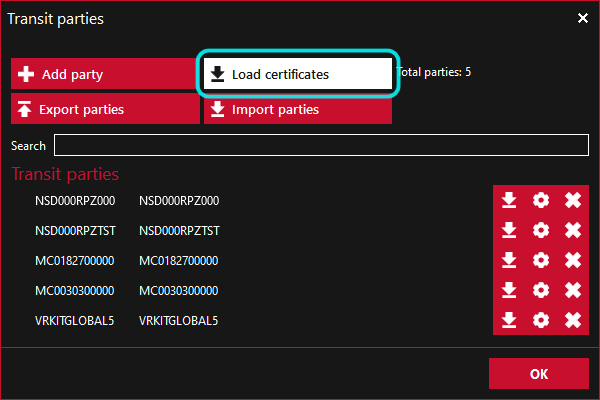


Figure 42. Download of Certificates

As a result, a request to NSD will be generated with a list of codes of depositors, which are included in the list of participants of transit. After receiving the response, the received certificates will automatically be added to the participants of transit directory and to the local Certificate Storage.

Also, you can download a certificate manually for each participant separately. To do this, you should:

* click the http://docs.itglobal.ru/download/attachments/9044505/%D0%94%D0%BE%D0%B1%D0%B0%D0%B2%D0%B8%D1%82%D1%8C%20%D1%83%D1%87%D0%B0%D1%81%D1%82%D0%BD%D0%B8%D0%BA%D0%B0.png?version=1&modificationDate=1481535942170&api=v2 button (1);



Figure 43. Addition of a certificate (the second way)

* select a certificate in DER-encoding (**.cer**) via Windows Explorer.

Information about the certificate is displayed in the Participant Settings window (2). To save changes, press the “OK” button (3).



You must specify a power of attorney for certificates that will be used to encrypt packets.

* 1. **Addition of a power of attorney**

To add information about powers of attorney, you should:

* 1. select a certificate for which the power of attorney is specified;

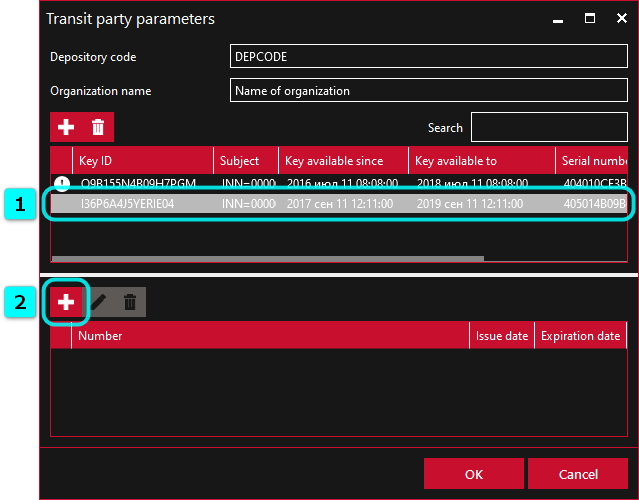


Figure 44. Selection of a Certificate



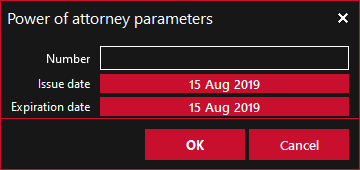
* 1. press the button;
  2. enter the number, the date of issue and the expiration date of the power of attorney;.

Figure 45. Form for the Addition of Power of Attorney доверенности

* 1.  press the OK button.

To edit information about the power of attorney, click the  button, enter the changes in the window opened and save the data. To delete a power of attorney, click the button.

.

* 1. **Delete of a Certificate**

To delete a certificate, you need to open the Participant settings form (1), select certificate (2) and click the button (3). Then you need to save the changes by clicking “OK” (4).

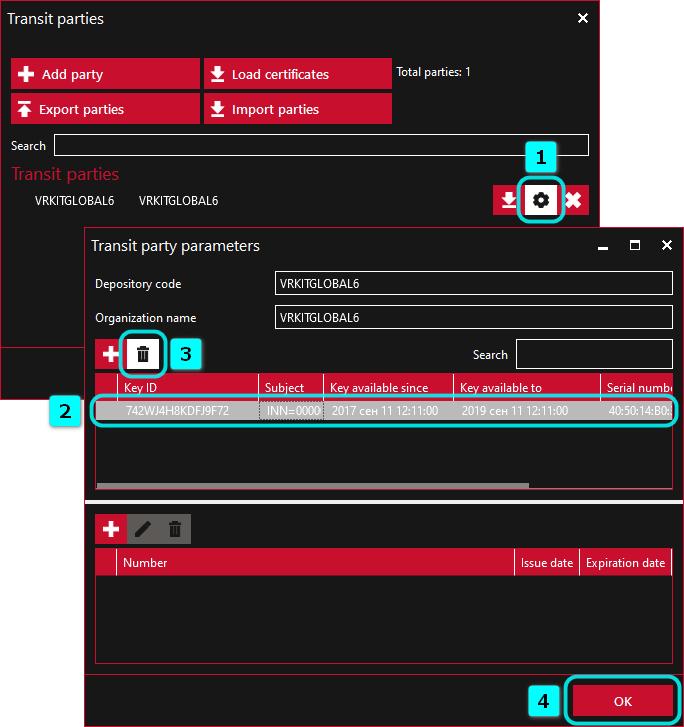


Figure 46. Deletion of a Certificate

* 1.  **Deletion of a Participant from the List**

To delete a participant, click the button.

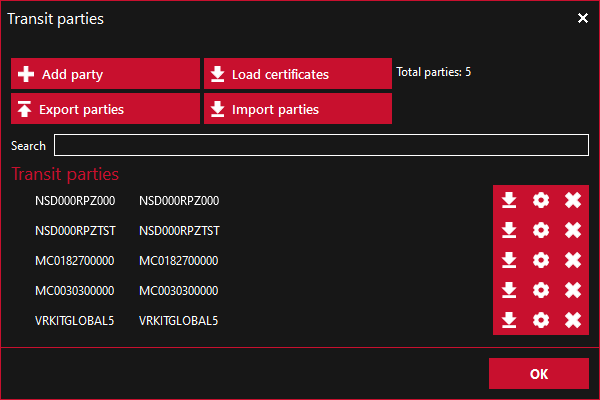
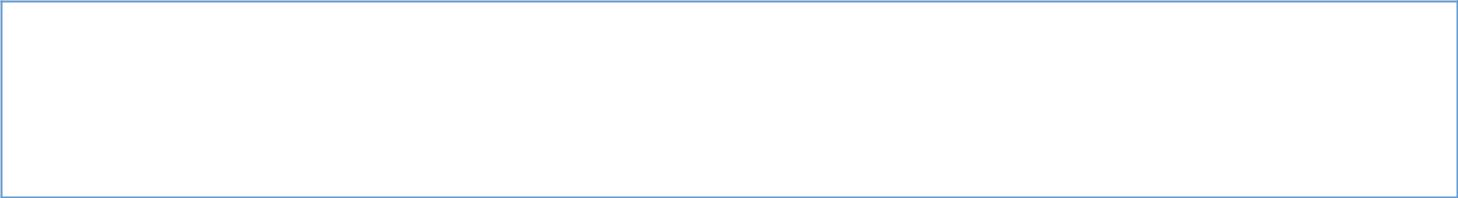


Figure 47. Deletion of a Participant

# FG Console Version

FG of version 41 and higher has the fgate-cli.exe file in the installation folder, which can be run from the console. The general order of the console version operation is similar to the principle of the desktop version operation (more details are available in sections 8 and 12). You can run the gateway in the following ways:

* 1. double click the fgate-cli.exe file in the% Program Files (x86)%\NSD FileGateway folder;
  2. go to the FG installation folder in the console, enter the fgate-cli command and press Enter.



* Run console with default settings.

C:\>cd %PROGRAMFILES(x86)%\NSD File Gateway\

C:\Program Files (x86)\NSD File Gateway>fgate-cli

FG will run with the current settings of the desktop version.

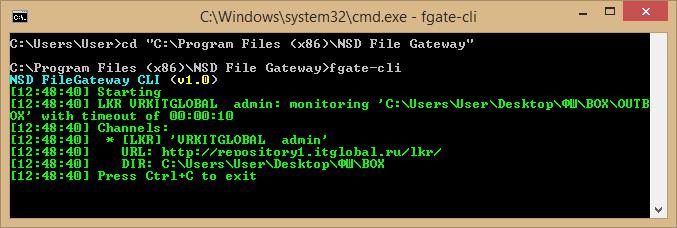


Figure 48. Run the Console Version



It is not recommended to run both the FG console and desktop simultaneously, since the console version by default uses the same setting file as the desktop version. Simultaneous operation is possible if different settings (folder and file) are specified for the versions.

* 1. **FG Stoppage**

Pressing Ctrl + C stops the FG operation.

* 1. **Help Topics**

To display a list of available commands on the console, you need to enter fgate-cli --help.

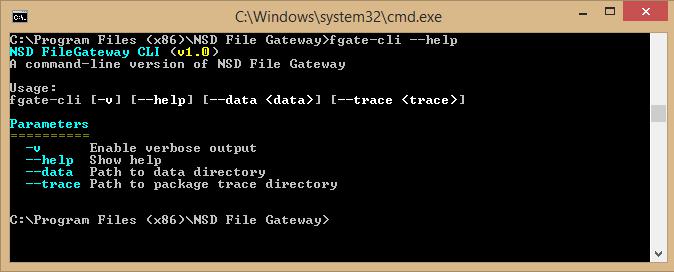


Figure 49. List of Commands

* 1. **Run with settings located in another folder**

You can only specify the setting folder in the console. It is not possible to edit settings via the console.

In order to specify a folder with other FG settings (by default, the % APPDATA%\NSD FileGateway folder), the --data "\_\_" parameter is used, for example:



* ,"PATH\_TO\_DATA\_DIRECTORY".

fgate-cli --data "PATH\_TO\_DATA\_DIRECTORY"

* 1. **Run with duplication of incoming and outgoing CRY-packets**

In order to enable the debug mode with duplication of incoming and outgoing CRY packets into the folder, the –-trace parameter "\_\_" is used, for example:



# CRY- "PATH\_TO\_TRACE\_DIRECTORY".

fgate-cli --trace "PATH\_TO\_TRACE\_DIRECTORY"

This mode is recommended only to diagnose problems.

* 1. **Record of Log Files**

Log files are recorded in the logs-cli folder, which is located in the settings folder. Logging setup commands are:

* - . fgate-cli -v
* , "PATH\_TO\_TRACE\_DIRECTORY", - . fgate-cli --data "PATH\_TO\_TRACE\_DIRECTORY" -v

# Run FG without an Interactive Session

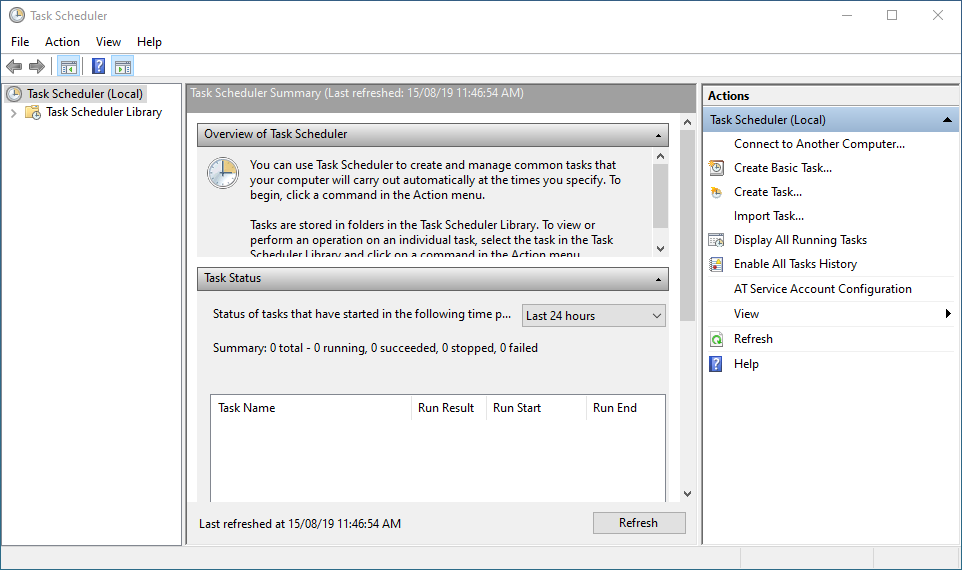


To work with FG, you should use a crypto profile that does not require entering a PIN code.

The FG console version can be run without an interactive session. In order to do so, you need to:

* 1. Run Task Scheduler through the Start menu.
  2. Click the "Create Task" button.

Figure 50. Task Scheduler



* 1. In the window opened, you should:
  2. Enter task name, for example, FG (1).
  3. Set the switch “Run” for all users (2);

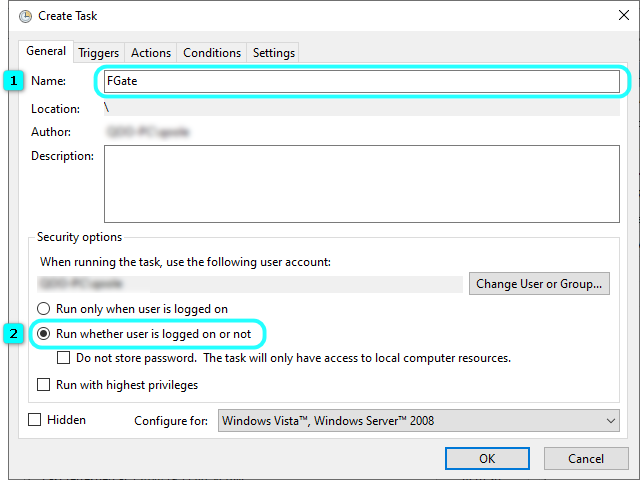


Figure 51. Created Tasks

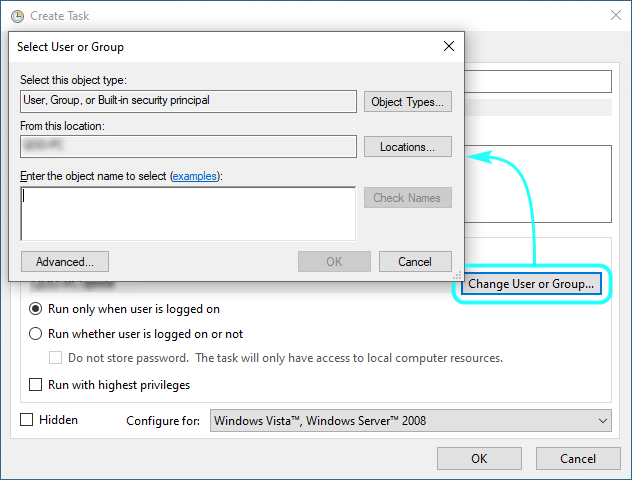
* 1. (optionally) Specify the user on whose behalf FG will be run

Figure 52. Selection of a User

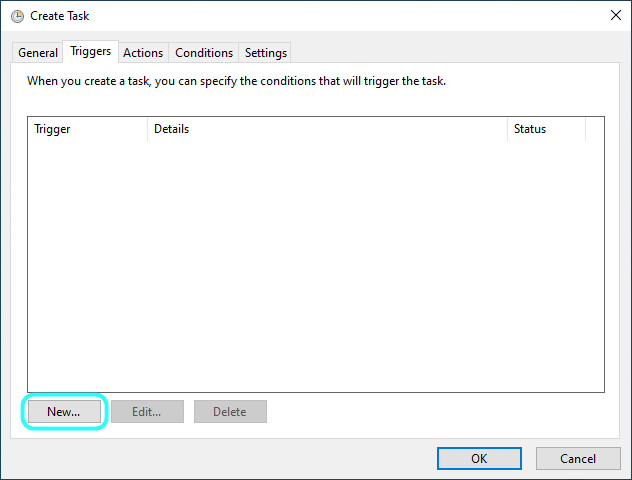
* 1. Go to the Triggers tab and click the "Create ..." button.

Figure 53. Triggers

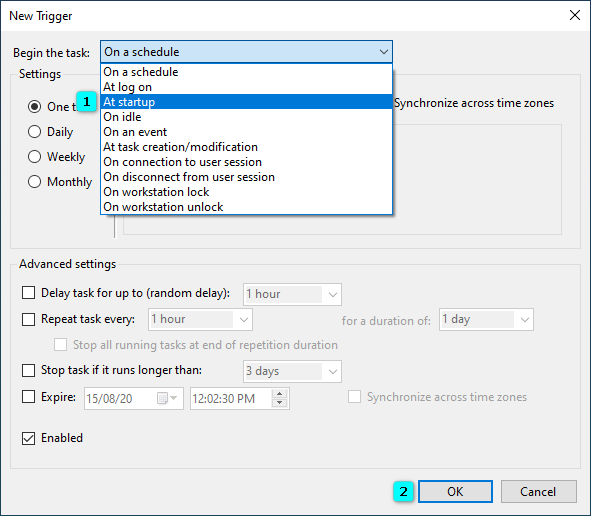
* 1. Select "On Startup" (1) in the "Start Task" menu and click "OK" button (2).

Figure 54. Creation of a Trigger

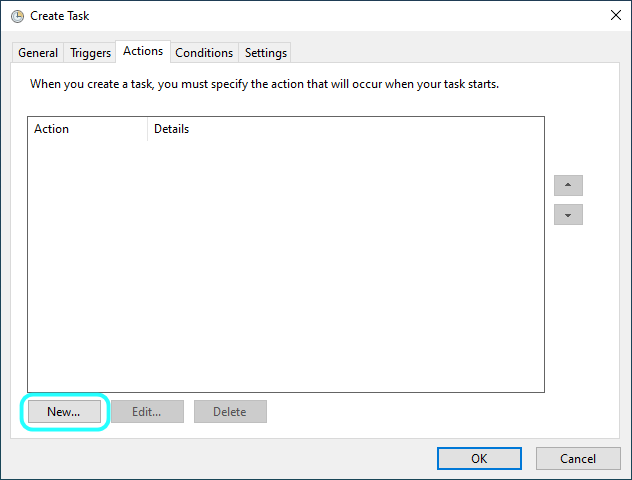
* 1.  Go to the "Actions" tab and click "Create…”

Figure 55. Actions

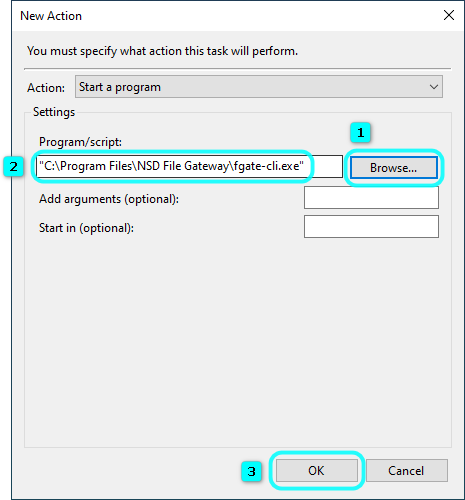
* 1. Click the "Browse ..." button (1), specify the path to the fgate-cli.exe file (by default, the % PROGRAMFILES (X86)%\NSD File Gateway) the FG installation folder (2), and click the OK button (3).

Figure 56. Creation of an Action

Further, a window will open in which you must enter the password for the account under which the FG will be used. After that, a line with the created task will appear in the Task Scheduler (item 1 in Figure 49).

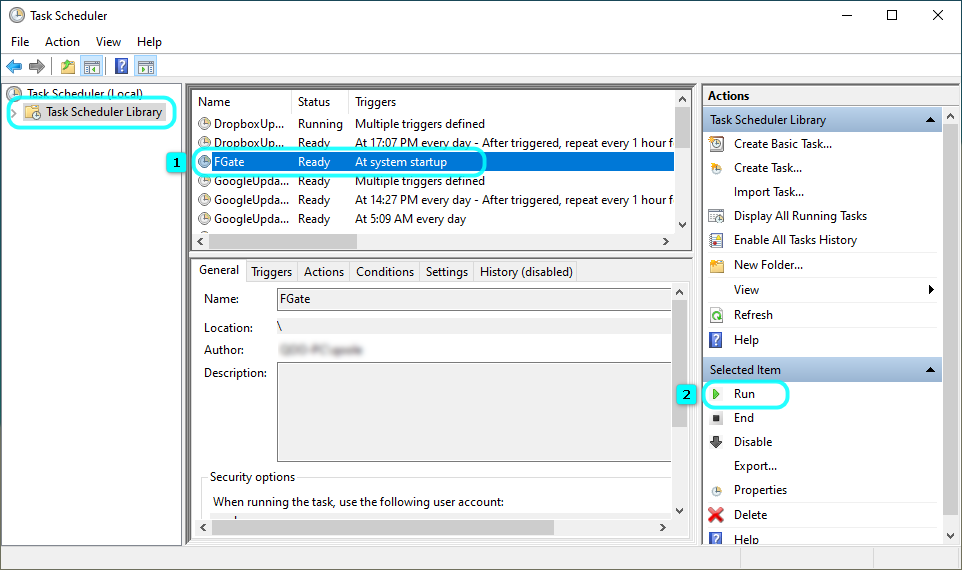


Figure 58. Created Task

You can run the task in one of the following ways:

* press the “Run” button (item 2 in Figure 49);
* reboot a computer. The task will start automatically when the computer starts.
  1. **Setup of FG Channels**

To set up channels, you should initially run FG in one of the following ways:

* Double click the icon on the desktop (created when installing the program),
* Double click the fgate.exe file (by default it is located in the% PROGRAMFILES (X86)%\NSD File Gateway folder).

After setting up the channels (the description is presented here), you should close the program.

If the setup is performed under an account other than the one that was specified when configuring FG, then the following steps should be made:

1. Open the folder:



C:\Users\\_\_\_\%APPDATA%\Roaming\NSD FileGateway

1. Copy the config.json file;
2. Open the folder:

C:\Users\\_\_\_\_\_\_\_\%APPDATA%\Roaming\NSD FileGateway

1. Put the config.json file in it.

Then you need to restart FG. This can be done in two ways:

* 1. Reboot the computer;
  2. Stop the task by clicking the “Finish” button in the task scheduler first and then start it by pressing the “Run” button.

1. Feature: by a closed envelope or not. [↑](#footnote-ref-1)
2. . Feature: according to the transfer agent scheme or not. [↑](#footnote-ref-2)
3. Constant for a type safe transit. [↑](#footnote-ref-3)
4. Constant for an untyped document. [↑](#footnote-ref-4)