The FBS-Access Control System

– Short Description –

State: August 2022

Internet: www.irfp.de
E-Mail: info(at)irfp.de

Adress: iRFP e. K.
Institut für Regional- und Fernverkehrsplanung
Hochschulstraße 45
01069 Dresden

Phone: +49 351 4706819

Table of Contents

1. Short Description of FBS-Access Control System 2
1.1. Issue and Aproach 2
1.2. Organisation (for Network Administrators) 3
1.3. Configuration (for Users and Network Administrators) 4
1.3.1. FBS Access Dispatcher 4
1.3.2. Setup FBS-Workplace (once per Workplace) 5
1.3.3. Setup of FBS Files for Access Control System 6
1.4. Working with Access Control (for Users) 7
2. Possible Signal Colours and their Meanings 9

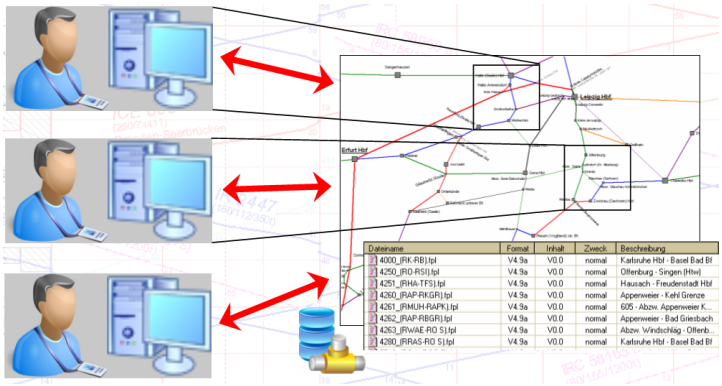
1. Short Description of FBS-Access Control System

1.1. Issue and Aproach

Previously, several users could access the same file in FBS simultaneously via one network. In in the event of saving, previously stored data was overwritten by the most recently saved data.

The FBS access control system enables

- prevention of "mutual overwriting" of data,
- several users to work simultaneously in the same network under certain conditions.



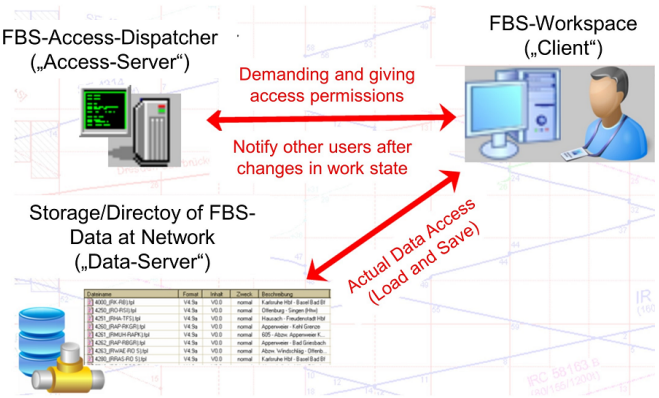
The following basic rules apply:

- Only one user can have "write permission" to an FBS network section (i.e., an FPL file) at a time.
- Write permission is required to save files.
- Any number of other users can have "read access", i.e., have the files open for reading. Some editing in the broader sense is also possible; however, these cannot be saved.
- Switching between read and write mode (i.e., receiving and giving write permission) can be done without closing and opening the files again.
- To edit an iPLAN network - i.e., both the network topology and network objects (drivers and customers timetables, circulation plans and interval graphics), the write permission to the network file and all of its FPL files is required.
- Working with FBS access control system is only possible with a continuously available network connection ("dedicated line") to the correspondingly configured server(s).

1.2. Organisation (for Network Administrators)

The FBS access control system has been designed and built to be fully compatible for working with local files ("offline"). The user does not necessarily have to be aware beforehand whether the files to be opened are subject to access control system or not.

- Access control system requires a key program provided by iRFP ("**FBS Access Dispatcher**").
- Each workstation (client) needs direct network access to the FBS access dispatcher (server) via TCP/IP. The server "listens" to **port 62001** - if not configured differently.



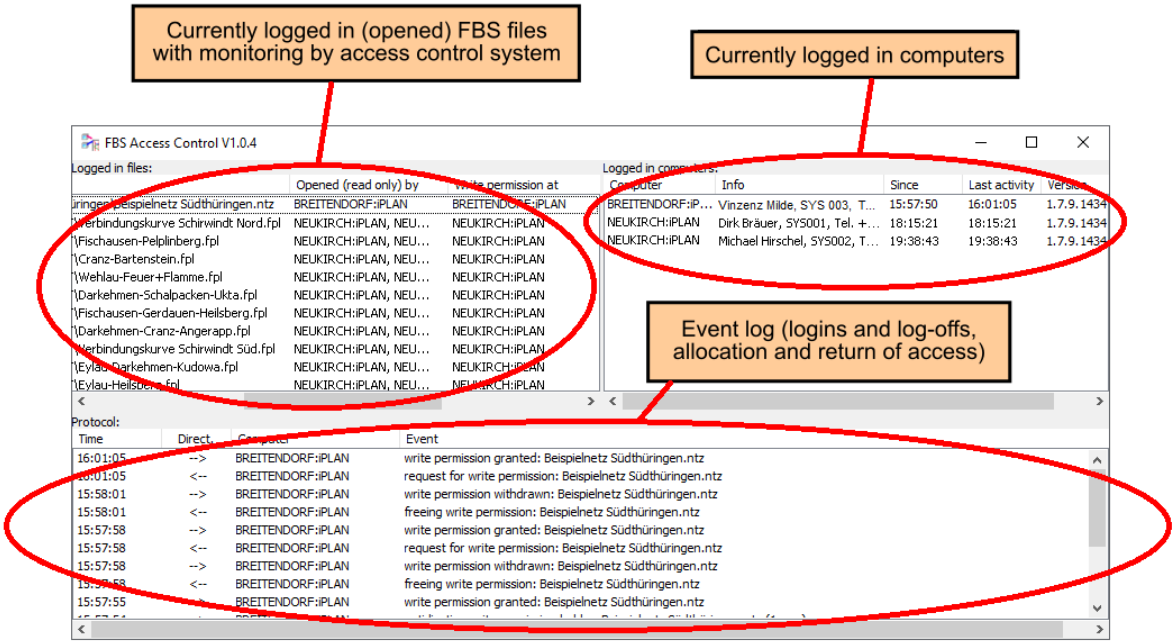
- The FBS Access Dispatcher must be permanently available - as long as at least one workstation wants to work with FBS data that is subject to access control system.
- The actual data (FBS files) must be located on a **shared network directory**. This can, but does not have to be on the same computer as the FBS access dispatcher. The network directory must be as permanently available as the FBS Access Dispatcher.
- Access to the FBS files from each workstation must always be via **UNC paths** (Uniform Naming Convention - paths structured like \\computer name\share\...). It is valid to substitute the UNC path with a local drive letter (virtual drive; DOS command *subst*). Nevertheless, it is important that all workstations involved access the same share, i.e., the computer name and share name of the UNC paths actually used must be identical for all workstations. This is to be considered in particular, if the file server is used as workstation at the same time: Then this workstation must access itself by UNC file name (e.g., \localhost\freigabe\...) and/or virtual (!) drive letter.
- Each workstation needs potential **read and write permission to the FBD files at file level**, i.e., access at file level must not be restricted initially. Under certain circumstances, the creation or deletion of files in the network directory may be restricted.

1.3. Configuration (for Users and Network Administrators)

1.3.1. FBS Access Dispatcher

The FBS Access Dispatcher requires no installation and no special system requirements. It consists of the executable program file (**FBSZgrDisp.exe**) and an optional configuration file (**FBSZgrDisp.ini**) only. The program can be started from any directory. It sould be considered to start the program e.g., via an "Autostart group". A future version to offer the program as a stand-alone service (no login required, no screen displays) is planned.

The screen displays of the FBS Access Dispatcher are only used for status display and, if necessary, troubleshooting and cannot be configured.



The optional configuration file must be located in the same directory and have the same name as the program, excpt for the file extension ".ini". If required, it can be created and edited with a text editor. The following configurations are possible:

```
[FBS]
ZgrDispPort=61001
ZgrDispProt=D:\Temp\FBSZgrDispProt.txt
```

ZgrDispPort is used to configure a port number that may differ from the default. If the configuration file or line does not exist, 61001 is used. The port number must not be occupied by other programs on the server or on any of the workstations involved. Port numbers must be between 1 and 65535. The range from 1 to 1024 is reserved, numbers up to about 5000 are used by Windows, so only port numbers between 5001 and 65535 should be used here. The range from 49152 to 65535 is recommended.

ZgrDispProt is used to set an optional log file in which the individual requests, assignments, and deliveries of rights are logged. In case of doubt, it helps to verify when which right was requested and granted. A valid path and file name must be specified; for path and file name

the FBS access dispatcher must have write permission. If the configuration file or line does not exist, no log file is kept.

Attention: If log files are also configured for workstations (clients), do not enter the same path and file name into the FBS Access Dispatcher and the workstations! The FBS Access Dispatcher and each workstation must have their own log file. Two programs cannot write to the same log.

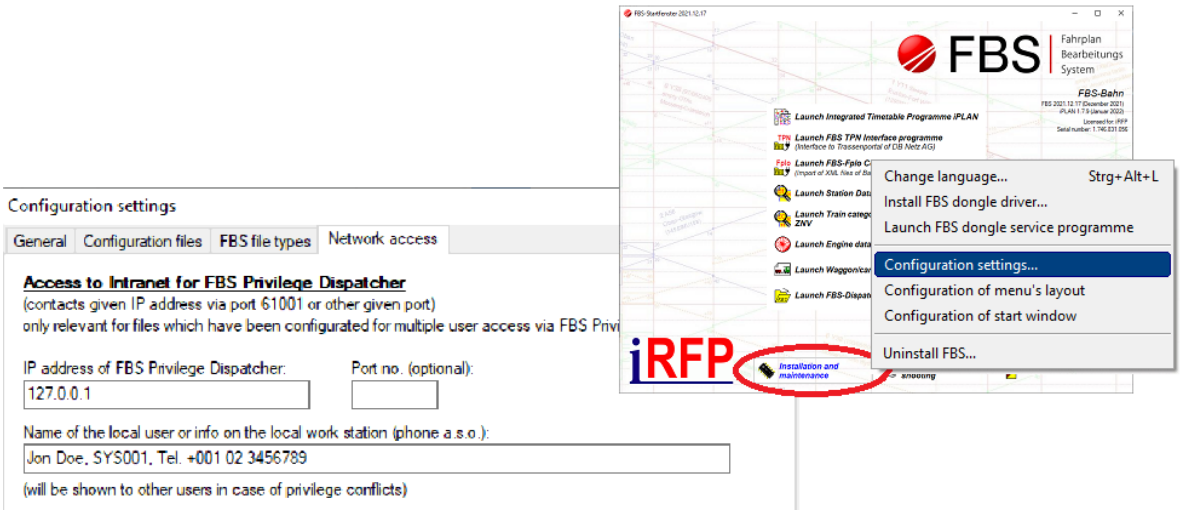
1.3.2. Setup FBS-Workplace (once per Workplace)

At each FBS workstation, the following must be setup

- network address of FBS access dispatcher,
- unique port number of FBS access dispatcher (if different from the standard) and
- a name and/or a unique identifier of the workstation

These settings can be changed afterwards.

They are configured in the FBS start window (program FBS.exe) under Installation and Maintenance FBS/Configuration Settings/Network Access:



Specify the IP address of the computer on which FBS access dispatcher is running. If the network configuration supports name resolution (DNS address set up), you can alternatively specify the name of the computer. Do not use any other introductory or terminating characters (no // or similar).

Specify the port number if it differs from the default (61001). The port number must not be occupied by other programs on the server or on any of the workstations involved. Port numbers must be between 1 and 65535. The range from 1 to 1024 is reserved, numbers up to about 5000 are used by Windows, so only port numbers between 5001 and 65535 should be used here. The range from 49152 to 65535 is recommended.

Enter a name and/or a designation of the workstation in the second input line. This can be the name of the user or an abbreviation for the workstation or, for example, a telephone number. This information should be unique, concise and not too long. It is displayed in the FBS access dispatcher as well as at other FBS workstations to identify this workstation when requesting access rights. It tells other workstations, for example, who currently has write permission or who is requesting it.

The settings are saved in the current configuration file (see *Configuration files* tab page). If

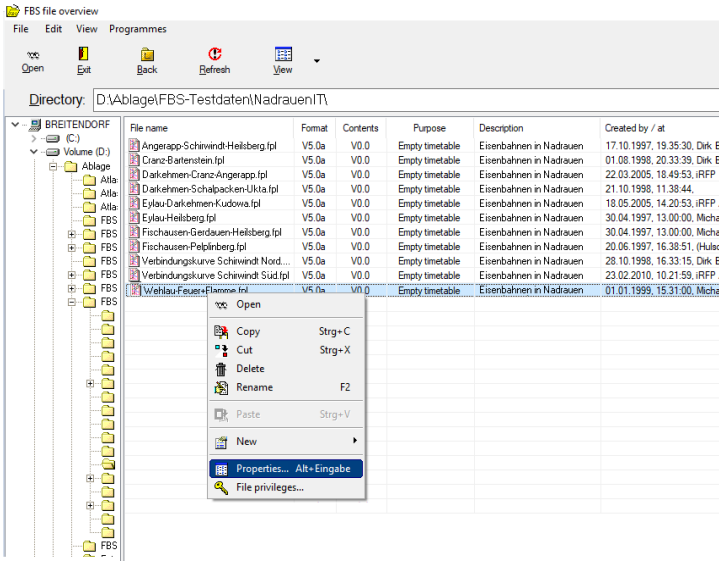
user-specific configuration files are set there, they must be setup once for each user.
The settings take effect after the next restart of the relevant FBS program.

1.3.3. Setup of FBS Files for Access Control System

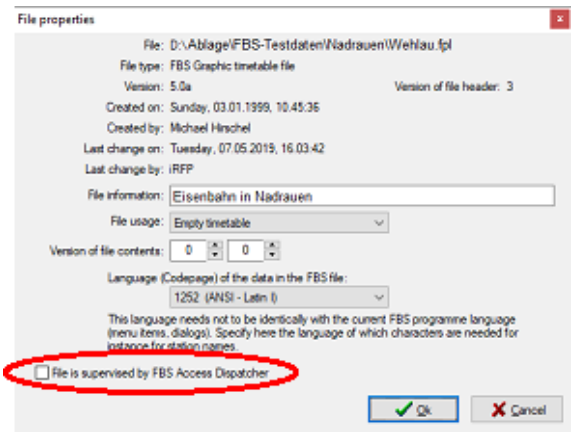
Regardless of the workstations setup, only FBS files (networks) that have been set up (marked) for this purpose are monitored by access control. Networks without corresponding identification behave like previous FBS files.

Switching the access control identifier on and off is done with the FBS dispatcher (not the access dispatcher, but the *FBSDispatcher.exe* program included in every FBS installation for managing FBS files)..

In the FBS Dispatcher, highlight one or more FBS-FPL or -NET files (*.fpl, *.ntz) that should be subject to access control on the shared network drive. Right-click and select *Properties*.



Check the box *File is supervised by FBS Access Dispatcher* and click Ok.



Turn on access control for the following FBS files:

For **FBS FPL files** (*.fpl), if you want to work on graphic timetables at several places in the network at the same time. It is recommended to always include all FPL files of a network in the access control system.

For **FBS-NETZ files** (*.ntz), if several users create or edit net objects in the same net file.

If each user is assigned a net file, but all net files share the same FPL files, you do not need to include the net files in the access control. However, you must include at least the FPL files that are used by more than one net file. Again, it is recommended to include all FPL files.

1.4. Working with Access Control (for Users)

In FBD files that are subject to access control, a "traffic light" is visible. The traffic light signals the read/write permission and is the only "difference" and "contact" to the access control visible for the user.

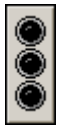
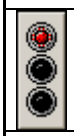
- **Red** traffic light:  no write permission is available. Nevertheless, certain work can be executed in this state and, in some cases, windows can be opened in which changes to the files are possible (e.g., display settings). A red traffic light does not exclude the right to edit, but only means that (currently) no right to save is available. In case of doubt, the user should decide how far he will (temporarily) change certain settings, knowing that they cannot be saved. It would be conceivable, for example, to temporarily change sheet sizes and other view settings to create a printout or a PDF file or to create a temporary circulation plan to determine the required number of vehicles.
- In FBS iPLAN networks there is a **traffic light for the network** (visible in the network main window at the bottom right in the object list) and another traffic light in each graphic timetable. The network traffic light controls the creation of new network objects and the modification of the network topology. Temporary graphic timetables (by map or train run) can also be created when the net traffic light shows red.
- The **traffic lights of graphic timetables** "block" the routes that are part of the respective graphic timetable. In this way, several users can work simultaneously in the graphic timetables of a network that contain different routes. However, the complete route is always used as soon as it is used by a graphic timetable even for a short piece - not only the piece visible in the graphic timetable.
- Some operations in the main network view **affect all graphic timetables**. These operations can only be performed if write permission is available for all graphic timetables. The write permission for all graphic timetables can best be obtained with the right mouse button in the route list (top right). Such operations are e.g., changing the general timetable data (calendar), the stops for all routes and the train numbers within train overview.
- The traffic light can be operated either by a simple left-click or by explicitly selecting a menu item with the right mouse button. Generally, only one following colour is possible for each state of the traffic light, so that a left click is sufficient.
- If the mouse cursor is hovered over the traffic light in its yellow state, a notification window with further information is displayed

- Generally, the following rules apply:
  - **When write permission right is granted** (traffic light changes from yellow to green), the relevant FBD files are reloaded, i.e., the visible file contents may change. This means that changes are adopted, the previous owner of the write permission may have executed.
  - **When the write permission is passed on** (traffic light changes from green to red), any changes made are saved. This ensures that the next holder of the write permission takes these changes into account and does not overwrite them.
  - Write permission has to be **given back at the exact same traffic light** the user got it from. If there are several traffic lights for the same file (same route opened in several graphic timetables), the write permission is only released again when the last of these traffic lights has been switched to red. The file is not saved until write permission has been given back at the last traffic light.
  - **Closing a window with a traffic light** (graphic timetable or network window) implicitly leads to giving up write permission of this traffic light - if it was still

green. However, it is not recommended to close windows with a green traffic light. Rather, the traffic light should always be manually switched to red (write permission active) beforehand, so it is possible to react to any save confirmation requests.

- A traffic light **can be green immediately when the window is opened**. This is always the case if write permission for all concerning files was already available (through other traffic lights). Even these traffic lights - where write permission right was not explicitly picked up - must be switched back to red manually werden.

2. Possible Signal Colours and their Meanings

	State	Meaning	Left-Click leads to
	No server connection	The FBS access dispatcher cannot be contacted; same state as *no write permission available.*	- - -
	No write permission, only read access	Files cannot be saved. Only reading is possible[1].	Requesting write permission for this client
	Write permission requested (by this computer)	See above; *if cursor is hovered over traffic light, notification window with current write permission holder will be displayed*	Withdrawing write permission request
	Write permission ready to collect	Write permission has been assigned to this client. When collecting, files are reloaded to apply any changes made by the previous write permission holder.	Collecting write permission
	Write permission ready to collect and requested by another client	See above; In the meantime, write permission was requested by another client	Collecting write permission
	Write permission valid	Changes can be made and saved	Giving away write permission
	Write permission valid and requested by another client	See above; write permission was requested by another computer. *if cursor is hovered over traffic light, notification window shows who requested it*	Giving away write permission

[1] If changes are (consciously) made while the traffic light is red, they will not be lost spontaneously, but only when the file is closed or when the write permission is collected.