

uFR Online log and access control mode v1.5

Table of contents

How to enable log mode?	3
How to enable access control mode?	4
Access control mode additional options	5
• Log mode without access control	6
• Log mode with access control	7
How to wire the access control board?	8
In-reader log format	9
In-reader whitelist/blacklist format	10
Log and access control mode flowchart	11
• Card read event	11
• Reader/Server synchronization (every 60 seconds)	12
HTTP(S) server request and response protocols	13
• Reader/Server synchronization protocol	16
PHP and MySQL server script	18
• MySQL database structure	18
• PHP script flowchart	24
Revision history	25

How to enable log mode?

1. Open uFR Online WEB configurator GUI and login.
2. Enable master mode (if already not enabled).

Working in master mode - Click to switch to slave mode

3. Enable log mode (only available if master mode is previously enabled)

Log mode enabled - Click to disable

Log server host:

Exclusive whitelist:

Edit

Show device log

Show server log

Download device log

Send device log

Download device blacklist

Select blacklist JSON file

Update blacklist from JSON file

Download device whitelist

Select whitelist JSON file

Update whitelist from JSON file

How to enable access control mode?

1. Open uFR Online WEB configurator GUI and login.
2. [Enable log mode](#).
3. Enable access control mode (only available if log mode is previously enabled).
4. Turn off uFR Online from power supply
5. Connect the Access control board.
6. Turn on uFR Online from power supply

Access control mode enabled - Click to disable

Relay pulse time (ms):

Relay pulse frequency (Hz):

Relay pulse power (%):

Relay active time (ms):

Output mode (0 - Access control board, 1 - Zero on UART1, 2 - Zero on UART2):

Access rights counter mode:

Block address:

Auth mode:

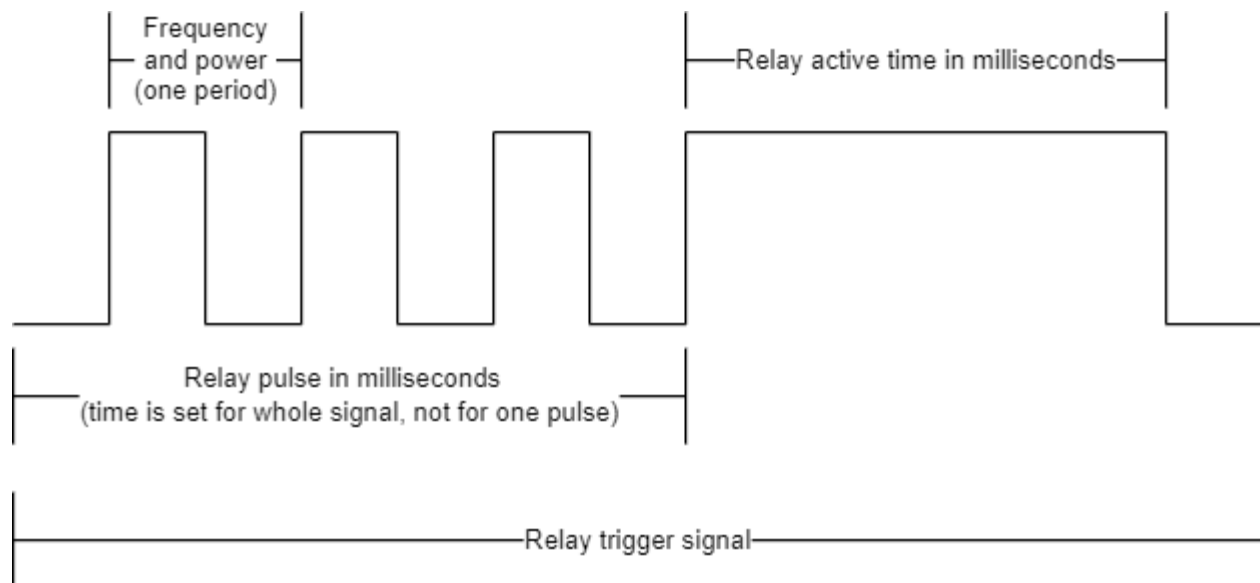
Key index:

Edit

*****Access control mode must be enabled before the access control board is connected.**

Access control mode additional options

- Relay pulse time: How many milliseconds relay outputs square wave pulse
- Relay pulse frequency: Square wave output frequency in Hz
- Relay pulse power: Square wave output power (duty cycle)
- Relay active time: How many milliseconds to stay output high after square wave pulse
- Output mode: 0 - Access control board, 1 - Zero on UART1, 2 - Zero on UART2
- Access rights counter mode: Only available if access control rights are used and the counter is set on the server. Define what function is used to decrement the counter in the card.
- Block address: Only available if access control rights are used and the counter is set on the server. Define block address where the counter is stored in the card.
- Auth mode: Only available if access control rights are used and the counter is set on the server. Define what authentication mode is used to authenticate the card block.
- Key index: Only available if access control rights are used and the counter is set on the server. Define reader key index.
- Key: Only available if access control rights are used and the counter is set on the server. Define provided key (only if provided key method is used).



Use cases

In this section will be described two main use case scenarios.

- Log mode without access control

Enable log mode and make sure that access control mode is disabled.

1. Navigate to the log mode section and click the Edit button.
2. [Enter the Log server host URL.](#)
3. Click the Save button.
4. Click on the Save and restart button.
5. Log mode is now ready to use.

The table below will describe which cards are allowed or denied based on blacklist or whitelist.

Scenario	Allowed/Denied
Blank both whitelist and blacklist	All cards are allowed
Whitelist blank and blacklist not blank	All cards except blacklisted are allowed
Whitelist not blank and blacklist blank	Only whitelisted cards are allowed
Both whitelist and blacklist not blank	Only whitelisted cards that are not blacklisted are allowed
Exclusive whitelist enabled	Only whitelisted cards that are not blacklisted are allowed (In pro mode, only whitelisted company cards are allowed except blacklisted)
If a card is allowed, the reader will beep once and the green light will be turned on. If a card is denied, the reader will not beep and the red light will be turned on.	

- Log mode with access control

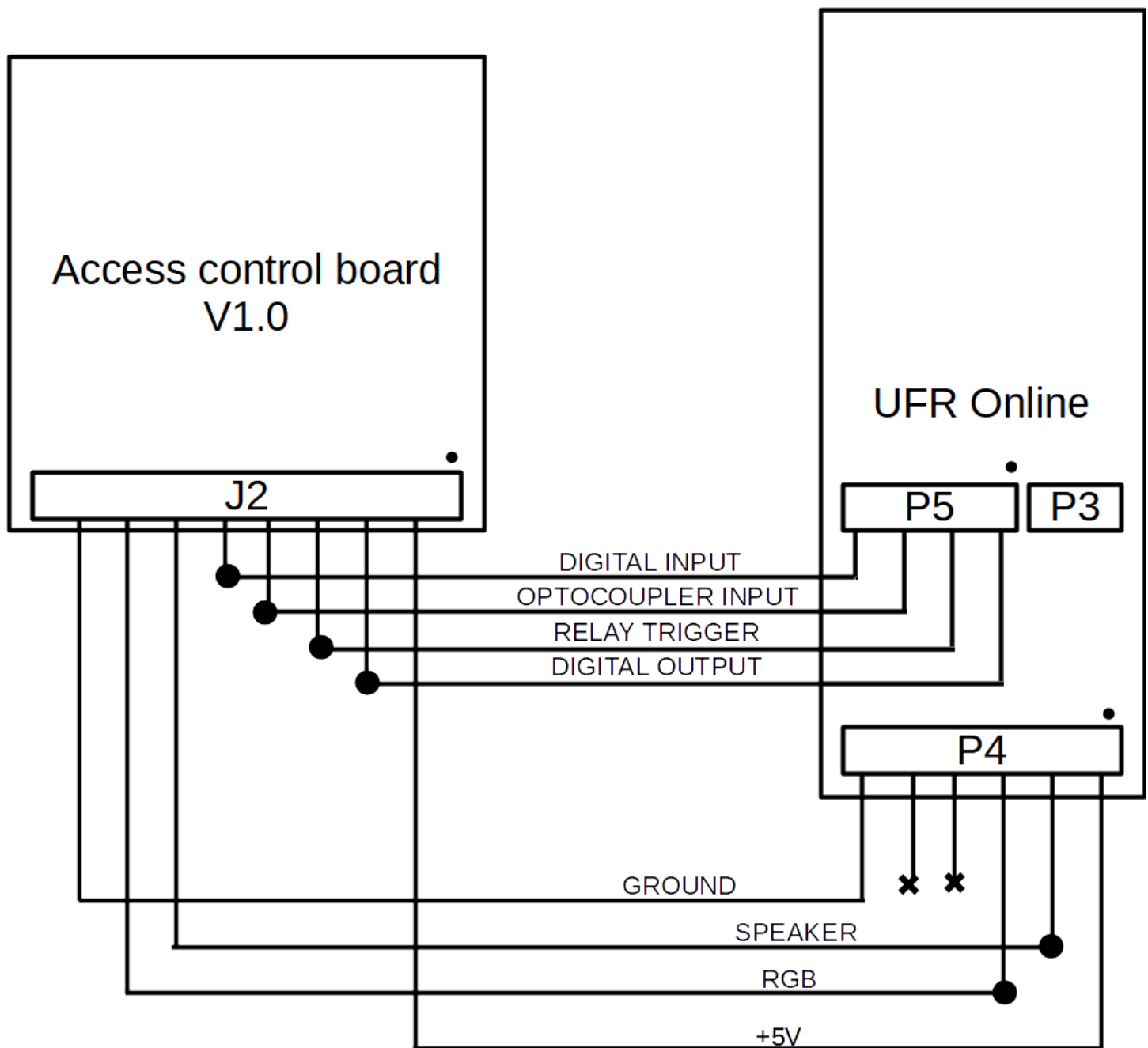
Enable log mode and make sure that access control mode is enabled.

1. Navigate to the log mode section and click the Edit button.
2. Enter the Log server host URL.
3. Click the Save button.
4. Click on the Save and restart button.
5. Log mode with access control is now ready to use.

The table below will describe which cards are allowed or denied based on blacklist or whitelist.

Scenario	Allowed/Denied
Blank both whitelist and blacklist	All cards are denied (In pro mode, all company cards are allowed)
Whitelist blank and blacklist not blank	All cards are denied (In pro mode, all company cards are allowed except blacklisted)
Whitelist not blank and blacklist blank	Only whitelisted cards are allowed (In pro mode, all company cards are allowed except blacklisted)
Both whitelist and blacklist not blank	Only whitelisted cards that are not blacklisted are allowed (In pro mode, all company cards are allowed except blacklisted)
Exclusive whitelist enabled	Only whitelisted cards that are not blacklisted are allowed (In pro mode, only whitelisted company cards are allowed except blacklisted)
<p>If a card is allowed, the reader will beep once and the green light will be turned on. Also, the access control board will trigger a relay, beep once and turn on the external LED ring.</p> <p>If a card is denied, the reader will not beep and the red light will be turned on. Also, the access control board will turn on the external LED ring.</p>	

How to wire the access control board?



There is also a premade cable for connecting uFR Online and Access control board.

NOTE: Access control mode must be enabled before the control board is connected, otherwise beeper will be enabled all the time.

In-reader log format

All log events are stored in human-readable JSON format.

Example of log stored in uFR Online reader:

```
{
  "log": [
    {
      "id": 1,
      "uid": "11223344",
      "time": "2022-08-15 06:56:02",
      "delta": 16,
      "type": 0,
      "reader": 1,
      "status": 0
    },
    {
      "id": 2,
      "uid": "AABBCCDD",
      "time": "2022-08-15 06:56:04",
      "delta": 18,
      "type": 0,
      "reader": 1,
      "status": 2
    }
  ]
}
```

JSON key/node name	Description
log	Main parent node that contains log events
id	Unique auto-increment log event id
uid	Card unique ID
pid	Personal ID .Only available in Pro mode
time	Log event date/time in UTC format
delta	Time difference between two log events
type	Type of card defined on server. Default is 1
state	Always 0. Reserved for future uses.
reader	1 if the internal reader has read card or 2 if external
status	0 - Allowed card 1 - Denied card 2 - Whitelisted card 3 - Blacklisted card 4 - Pro mode company card allowed 5 - Pro mode company card denied 6 - Allowed based on access control rights

In-reader whitelist/blacklist format

Whitelist and blacklist are stored in human-readable JSON format.

Example of whitelist stored in uFR Online reader:

<pre>{ "whitelist":["11223344", "AABBCCDD"], "timestamp":1660492955 }</pre>	
JSON key/node name	Description
whitelist	Node that contains whitelisted uids in comma separated format
timestamp	Current stored whitelist timestamp

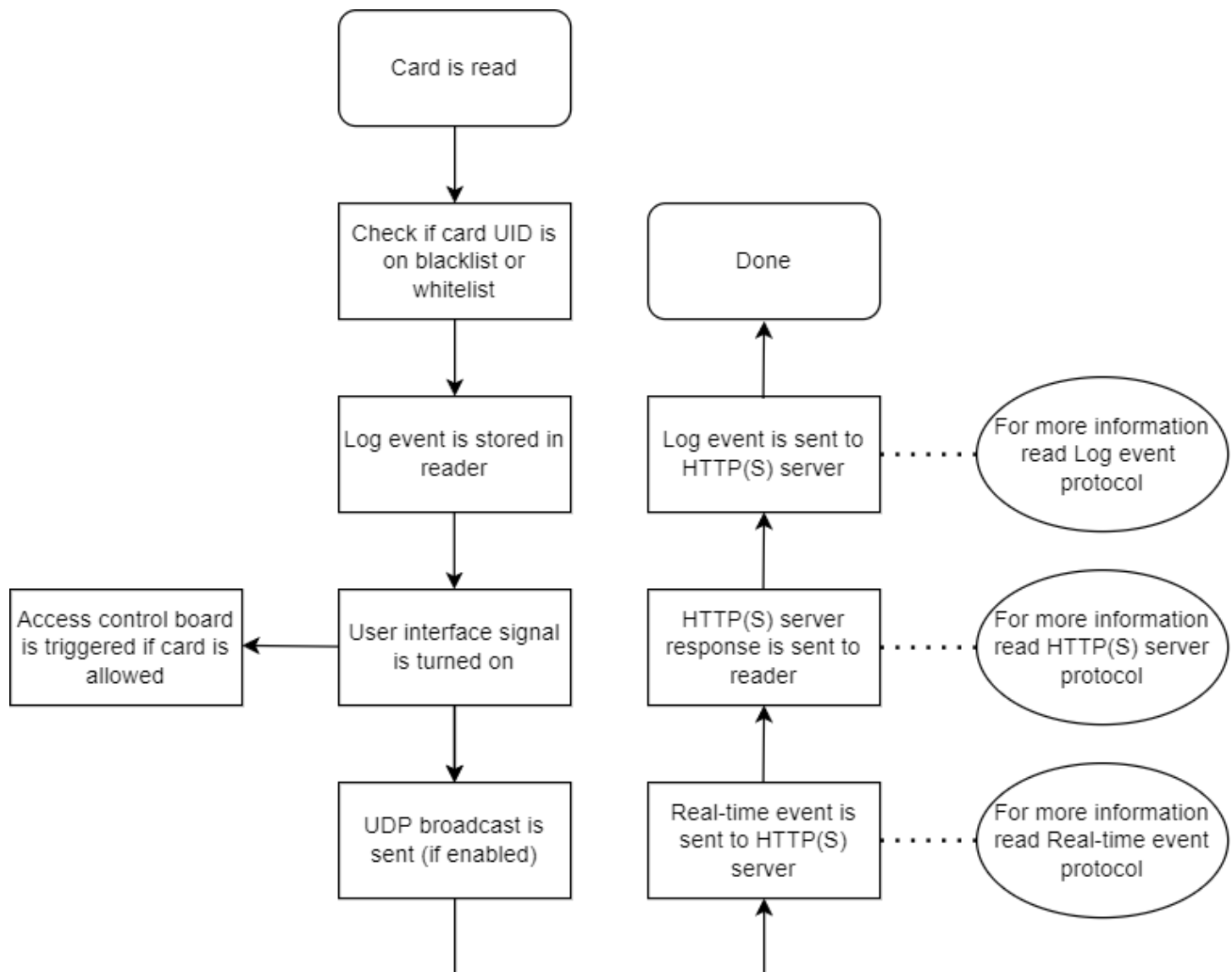
Example of blacklist stored in uFR Online reader:

<pre>{ "blacklist":["11223344", "AABBCCDD"], "timestamp":1660492955 }</pre>	
JSON key/node name	Description
blacklist	Node that contains blacklisted uids in comma separated format
timestamp	Current stored blacklist timestamp

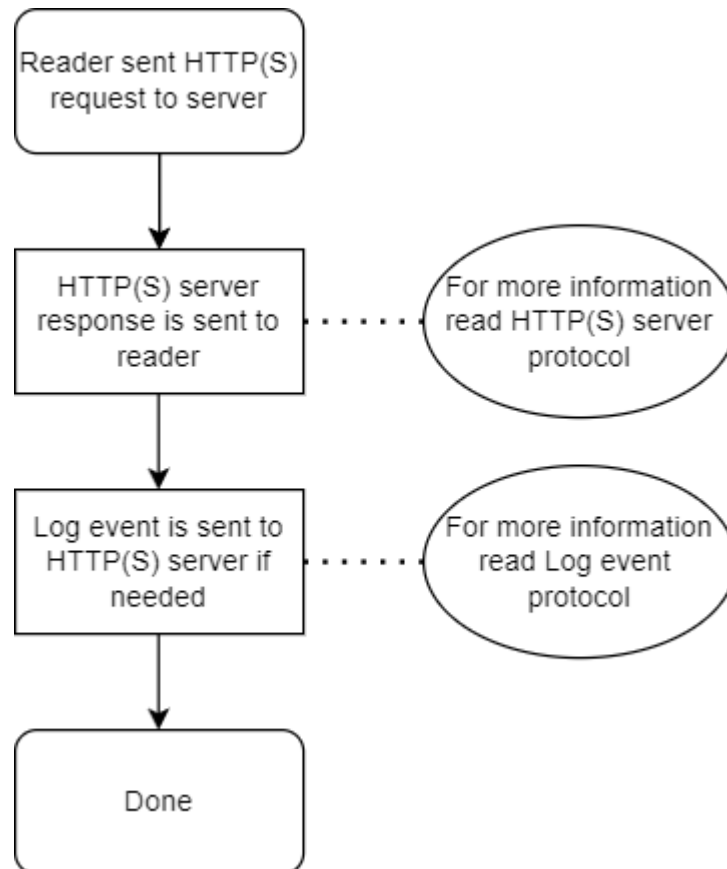
Log and access control mode flowchart

There are two main events in log and access control mode.

- Card read event



- Reader/Server synchronization (every 60 seconds)



HTTP(S) server request and response protocols

- Real-time event protocol

Real-time events are sent to the server in human-readable JSON format.

Example of real-time event request from reader to server:

Reader HTTP(S) request to server	
<pre>{ "rte": [{ "id":83,"pid":10,"uid":"AABBCCDD","time":"2022-08-16 07:45:01","delta":89349,"type":0,"state":0,"reader":1,"status":1 }], "whitelist_timestamp":1660492955, "blacklist_timestamp":1660492955, "types_timestamp":1660492955, "rights_timestamp":1660492955 }</pre>	
JSON key/node name	Description
rte	Parent node that contains real-time event
For more information about rte child node read in-reader log format	
whitelist_timestamp	Current in-reader stored whitelist timestamp
blacklist_timestamp	Current in-reader stored blacklist timestamp
types_timestamp	Current in-reader stored card types list timestamp
rights_timestamp	Current in-reader stored access control rules list timestamp
Readers serial numbers, IP address and firmware versions are sent in HTTP POST header as "OSN", "SN1" and "SN2", "IP", "FW", "FW1", "FW2"	

Server HTTP(S) response to reader

```
{
  "last_id":79,
  "time":1660636893,
  "blacklist":["AABBCCDD"],
  "blacklist_timestamp":1660636882,
  "whitelist":["11223344"],
  "whitelist_timestamp":1660636882,
  "update_fw":["2.8.2", "5.0.71", "5.0.70"],
  "rights":[{"right":1,"rules":[0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]},
  "rights_uids":[{"right":1,"list":["55667788"]}],
  "rights_timestamp":1670926613
}
```

JSON key/node name	Description
last_id	Last log event id that is stored on the server. Reader will send all log events that have ID larger than last_id
time	Optional. If server timestamp is sent, reader will sync internal RTC time with server time
blacklist	Optional. If a server blacklist is sent, the reader will replace the current stored blacklist with a newly received one.
blacklist_timestamp	This parameter is mandatory if a blacklist is sent . the reader will replace the current stored blacklist_timestamp with a newly received one.
whitelist	Optional. If a server whitelist is sent, the reader will replace the current stored whitelist with a newly received one.
blacklist_timestamp	This parameter is mandatory if a whitelist is sent . the reader will replace the current stored whitelist_timestamp with a newly received one.
update_fw	This parameter is optional. It contains requests to update in reader firmwares. If this parameter is sent, the reader will trigger the firmware update procedure. First element of the array contains uFR Online firmware, second contains the UART1 reader and the



	third contains the UART2 reader. If the array element is an empty string, update will not be triggered.
rights	Optional. If a server access rights is sent, the reader will replace the current stored rights with a newly received one. The rights parameter contains an array of rights (as a right) defined in the database. Array elements must have two parameters (right and rules). Right is a unique number of rule and rule is numeric representation of columns defined in the database.
rights_uid	This parameter is mandatory if a rights is sent . the reader will replace the current stored list of uids with a newly received one. If a server access rights uids is sent, the reader will replace the current stored rights with a newly received one. The rights_uid parameter contains an array of uids defined in the database. Array elements must have two parameters (right and list). Right is a unique number of rule and the list contains a list of uids defined by this rule..

- Log event protocol

Log events are sent to the server in human-readable JSON format.

Example of real-time event request from reader to server:

Reader HTTP(S) request to server	
<pre>{ "log": [{ "id":83,"pid":10,"uid":"AABBCCDD","time":"2022-08-16 07:45:01","delta":89349,"type":0,"state":0,"reader":1,"status":1, "id":84,"pid":10,"uid":"AABBCCDD","time":"2022-08-16 07:45:01","delta":89349,"type":0,"state":0,"reader":1,"status":1 }] }</pre>	
JSON key/node name	Description
log	Parent node that contains array of log events
For more information about log child node read in-reader log format	

Log event is sent every time when the "last_id" parameter is received from the server (Real-time event response or reader/server synchronization response).

- Reader/Server synchronization protocol

Log events are sent to the server in human-readable JSON format.

Example of real-time event request from reader to server:

Reader HTTP(S) request to server	
<pre>{ "whitelist_timestamp":1660492955, "blacklist_timestamp":1660492955, "types_timestamp":1660492955, "rights_timestamp":1660492955 }</pre>	
JSON key/node name	Description
blacklist_timestamp	Current in-reader blacklist timestamp
whitelist_timestamp	Current in-reader whitelist timestamp



types_timestamp	Current in-reader stored card types list timestamp
rights_timestamp	Current in-reader stored access control rules list timestamp

PHP and MySQL server script

There are prebuilt PHP and MySQL scripts that can be hosted to the server. It is made to easily implement the server-side part of log and access mode. It can handle real-time events, log events and reader- server synchronization requests.

- MySQL database structure

"events" table	
Column name	Column description
id	Unique log event id
uid	Card UID
pid	Personal id. Can be used to identify same user with multiple card UIDs
time	Event timestamp
delta	Time difference between two events
type	Type of card
state	Always 0, reserved for future uses
status	Event status
osn	uFR Online serial number
sn1	Internal connected uFR NFC reader serial number
sn2	External connected uFR NFC reader serial number
reader	1- If the card is read by an internal reader 2- If the card is read by an external reader
rte	1 - If the event is Real-time 2 - If the event is Log

"readers" table	
Column name	Column description
osn	uFR Online serial number
descriptor	uFR Online reader descriptor. Default is empty
sn2	External connected uFR NFC reader serial number
whitelist_on_server	Timestamp of last modified whitelist on server. Automatically updated by user_after_update trigger
whitelist_in_reader	Timestamp of whitelist stored in reader. Automatically updated by HTTP POST sent by reader
blacklist_on_server	Timestamp of last modified blacklist on server. Automatically updated by user_after_update trigger
blacklist_in_reader	Timestamp of blacklist stored in reader. Automatically updated by HTTP POST sent by reader
types_on_server	Timestamp of last modified card types on server. Automatically updated by user_after_update trigger
types_in_reader	Timestamp of types stored in reader. Automatically updated by HTTP POST sent by reader
rights_on_server	Timestamp of last modified access rights on server. Automatically updated by user_after_update trigger
rights_in_reader	Timestamp of access rights stored in reader. Automatically updated by HTTP POST sent by reader
last_seen	Timestamp of last HTTP request sent by reader.



ip	Timestamp of blacklist stored in reader. Automatically updated by HTTP POST sent by reader
online_firmware	Current uFR Online firmware version. Automatically updated by HTTP POST sent by reader
reader1_firmware	Current uFR on UART1 firmware version. Automatically updated by HTTP POST sent by reader
reader2_firmware	Current uFR on UART2 firmware version. Automatically updated by HTTP POST sent by reader
requested_online_firmware	If this field is populated and is different from online_firmware, update request will be sent to the reader
requested_reader1_firmware	If this field is populated and is different from reader1_firmware, update request will be sent to the reader
requested_reader2_firmware	If this field is populated and is different from reader2_firmware, update request will be sent to the reader
New readers are automatically added on every reader event. For example if a new reader is connected to the network and Log mode host URL is setted, the new reader will be dynamically added the first time when an event is sent. **Do not add readers manually	

"users" table	
Column name	Column description
uid	Card unique ID
pid	Personal ID. Can be used to identify same user with multiple card UUIDs
type	Type of card. Must be defined in the card_types table.
description	User description. Can be used eg. to set first and last name.
image	Binary formatted user image
access_right	Access control rule. Must be defined in the card_types table and serial number must be set to ACCESS_RIGHT.
*ON123456	Example of uFR Online reader with serial number ON123456. This field is used to whitelist, blacklist or access control rule current user on this reader
*ON654321	Example of uFR Online reader with serial number ON654321. This field is used to whitelist, blacklist or access control rule current user on this reader
<p>New readers are automatically added on every reader event. For example if a new reader is connected to the network and Log mode host URL is setted, the new reader will be dynamically added the first time when an event is sent as a new column. If a new reader is added.</p> <p>*Example readers. **Do not add readers manually.</p>	

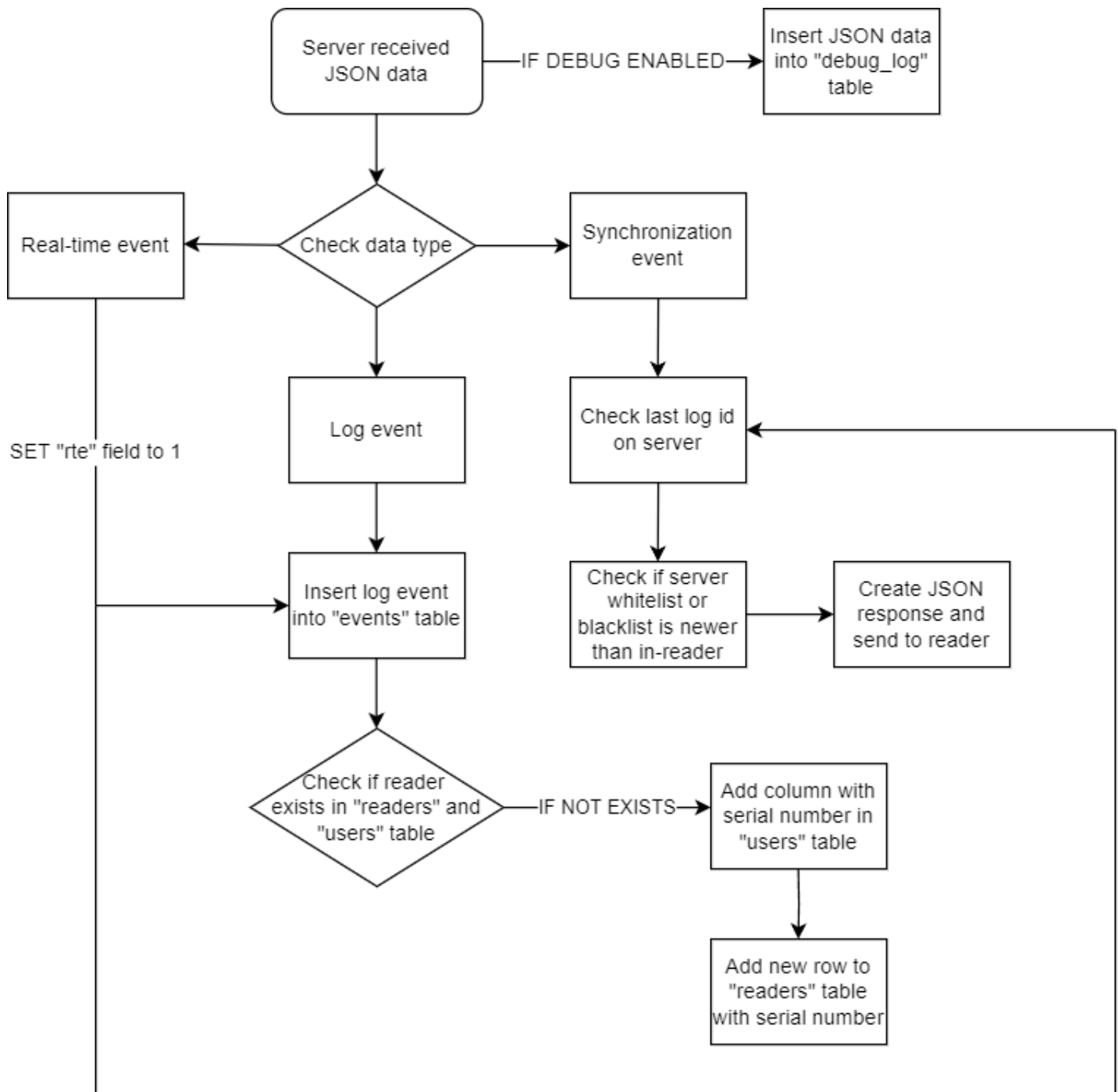
"card_types" table	
Column name	Column description
type	Unique card type id. Type 1 is reserved.
description	Card type description.
color	Hexadecimal representation of color (eg. 00FFFF for blue). Reader will blink for 5s if a card with defined type is checked on the reader.

"access_rights" table	
Column name	Column description
rights	Right id. Multiple rights with same id are allowed
begin_date	Date/Time when rule is starting to be valid
end_date	Date/Time when rule is not valid anymore
monday_begin	Time of day when rule is starting to be valid
monday_end	Time of day when rule is not valid anymore
.....
sunday_begin	Time of day when rule is starting to be valid
sunday_end	Time of day when rule is not valid anymore
timeout	If the timeout is set to a value greater than 0 card will not be allowed to pass for a number of seconds defined by timeout. For example, if the timeout is set to 60, the same card can be passed only one time in a minute.
counter	If the counter is set to a value greater than 0, counter option set in WEB frontend will be used to decrement card counter by this value.



"debug_log" table	
Column name	Column description
id	Unique debug id
osn	uFR Online serial number
log	Raw POST data sent from reader to server or from server to reader
time	Current server timestamp
direction	FROM_SERVER - HTTP server response FROM_READER - HTTP reader request
Debug log table is populating only if "DEBUG" flag is set enabled in PHP script	

- PHP script flowchart



Revision history

Date	Version	Comment
2022-08-15	1.0	Base document
2022-08-30	1.1	CID renamed to PID
2022-10-05	1.2	Reader table and headers updated
2022-10-24	1.3	Access control module beeper note
2022-10-25	1.4	Firmware update request description
2022-12-13	1.5	Card types and access control rules added