uFR Online log and access control mode v1.2

Table of contents

How to enable log mode?

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

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

Digital Logic Ltd.

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):

70

Relay pulse frequency (Hz):

50

Relay pulse power (%):

50

Relay active time (ms):

1500

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
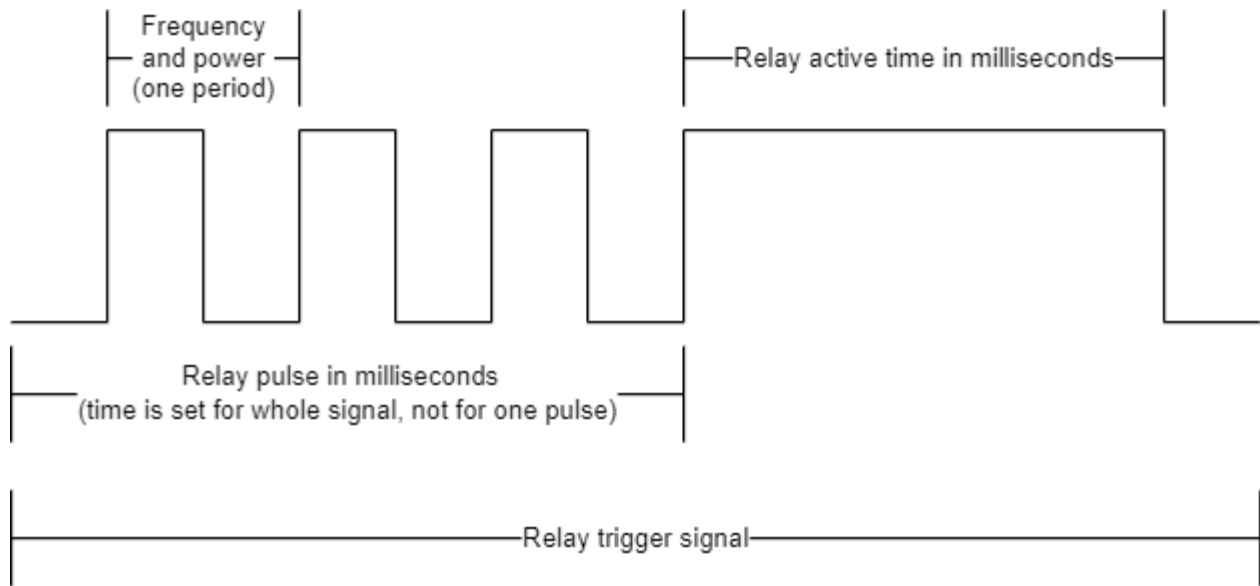
Use cases

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)
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. 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.	

How to wire the access control board?
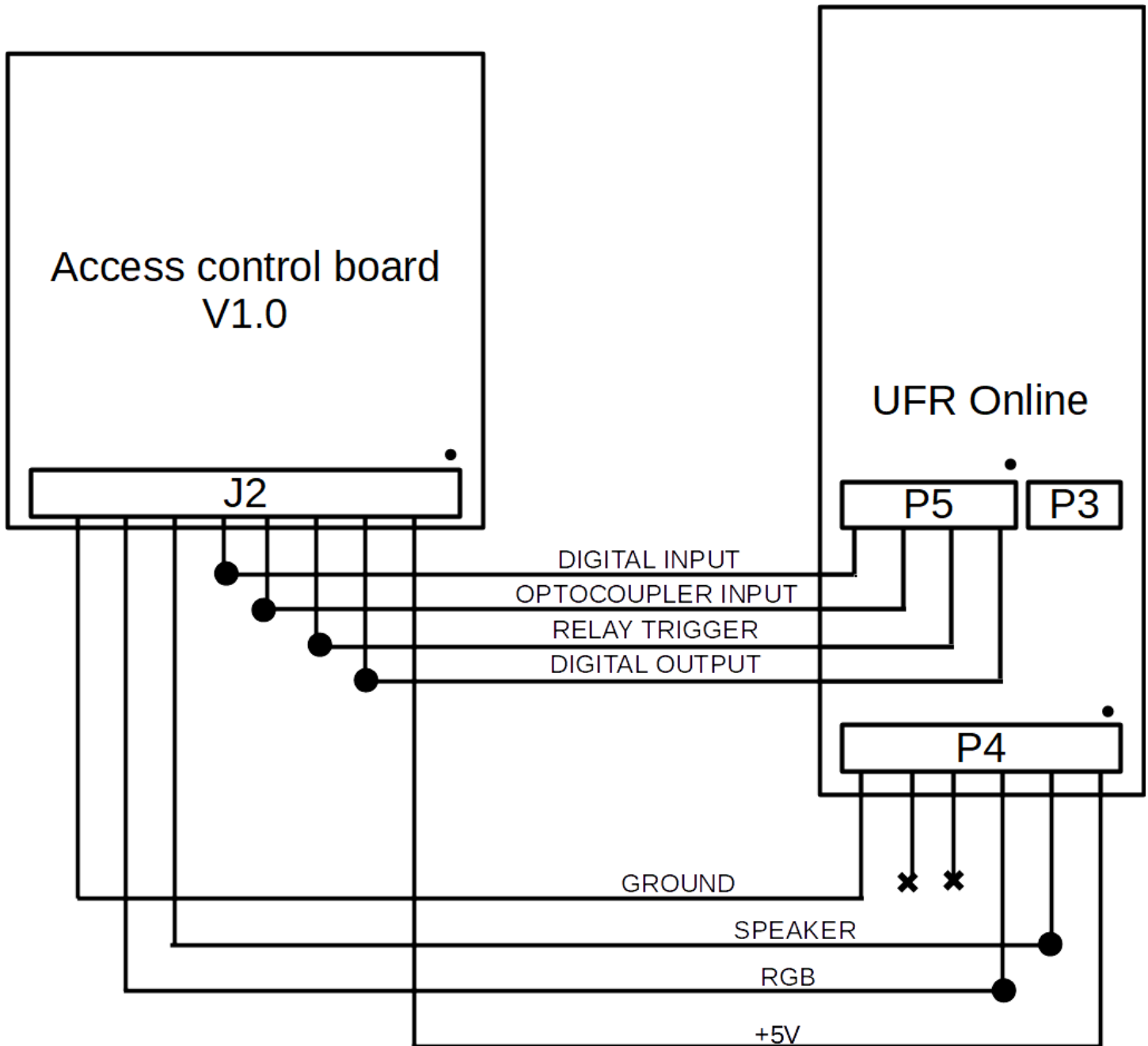
There is also a premade cable for connecting uFR Online and Access control board.

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	Always 0, reserved for future use
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

In-reader whitelist/blacklist format

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

Example of whitelist stored in uFR Online reader:

```
{
    "whitelist":["11223344", "AABBCCDD"],
    "timestamp":1660492955
}
```

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:

```
{
    "blacklist":["11223344", "AABBCCDD"],
    "timestamp":1660492955
}
```

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
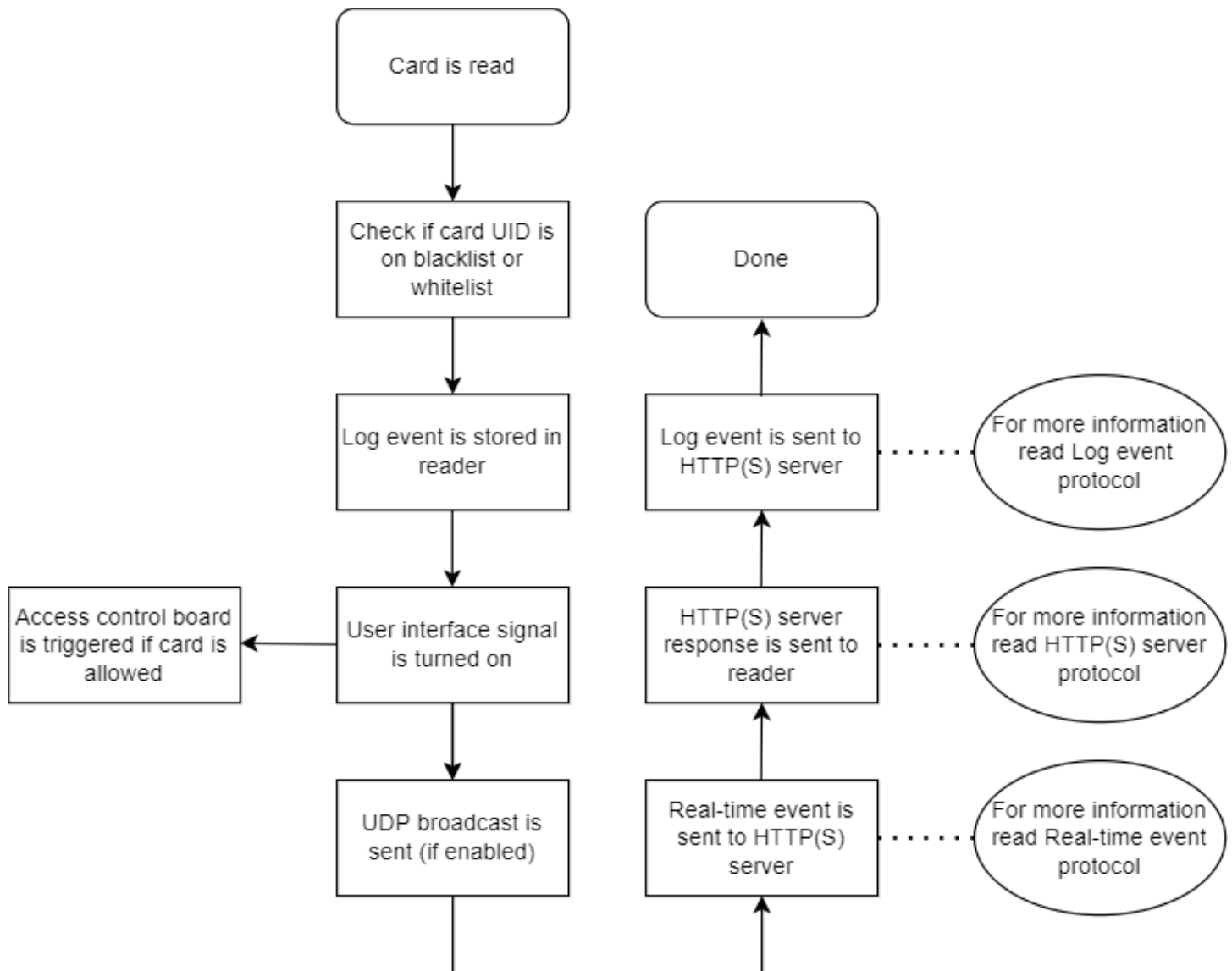
- Reader/Server synchronization (every 60 seconds)

```
┌─────────────────────┐
│  Reader sent HTTP(S) │
│  request to server   │
└─────────────────────┘
          │
          ▼
┌─────────────────────┐          ╭───────────────────╮
│  HTTP(S) server     │ · · · · ·│  For more information│
│  response is sent to │          │  read HTTP(S) server │
│  reader             │          │  protocol           │
└─────────────────────┘          ╰───────────────────╯
          │
          ▼
┌─────────────────────┐          ╭───────────────────╮
│  Log event is sent to│ · · · · ·│  For more information│
│  HTTP(S) server if   │          │  read Log event     │
│  needed             │          │  protocol           │
└─────────────────────┘          ╰───────────────────╯
          │
          ▼
┌─────────────────────┐
│       Done          │
└─────────────────────┘
```
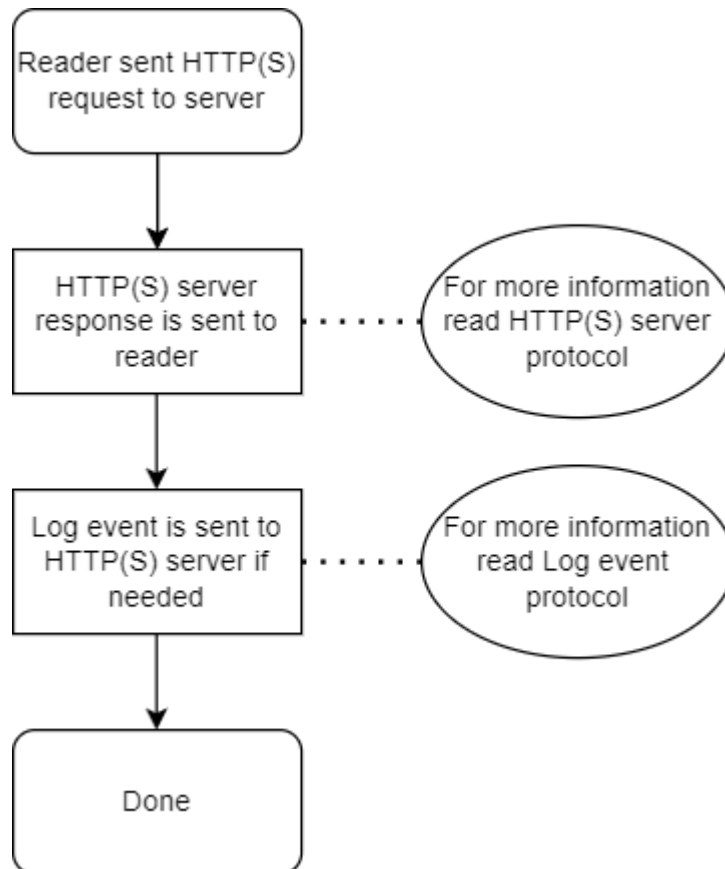
HTTP(S) server request and response protocols

- 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

```
{
"rte": [{
      "id":83,pid":10,uid":"AABBCCDD","time":"2022-08-16 07:45:01","delta":89349,"type":0,"reader":1,"status":1
}],
"whitelist_timestamp":1660492955,
"blacklist_timestamp":1660492955
}
```

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
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
}
```

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.

- ## 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

```
{
"log": [{
     "id":83,pid":10,uid":"AABBCCDD","time":"2022-08-16 07:45:01","delta":89349,"type":0,"reader":1,"status":1,
     "id":84,pid":10,uid":"AABBCCDD","time":"2022-08-16 07:45:01","delta":89349,"type":0,"reader":1,"status":1
}]}
```

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

```
{
     "whitelist_timestamp":1660636882,
     "blacklist_timestamp":1660636882
}
```

JSON key/node name	Description
blacklist_timestamp	Current in-reader blacklist timestamp
whitelist_timestamp	Current in-reader whitelist 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	Always 0, reserved for future use
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**
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**
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 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 UIDs
description	User description. Can be used eg. to set first and last name.
image	Binary formatted user image
*ON123456	Example of uFR Online reader with serial number ON123456. This field is used to whitelist or blacklist current user on this reader
*ON654321	Example of uFR Online reader with serial number ON654321. This field is used to whitelist or blacklist current user on this 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 first time when an event is sent as new column. If a new reader is added. ***Example readers. **Do not add readers manually.**	

"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	

Digital Logic Ltd.

- PHP script flowchart

A flowchart describing the PHP script logic:

- **Server received JSON data** → IF DEBUG ENABLED → **Insert JSON data into "debug_log" table**
- **Server received JSON data** → **Check data type**
  - → **Real-time event** → SET "rte" field to 1 → **Insert log event into "events" table**
  - → **Log event** → **Insert log event into "events" table**
  - → **Synchronization event** → **Check last log id on server** → **Check if server whitelist or blacklist is newer than in-reader** → **Create JSON response and send to reader**
- **Insert log event into "events" table** → **Check if reader exists in "readers" and "users" table** → IF NOT EXISTS → **Add column with serial number in "users" table** → **Add new row to "readers" table with serial number** → (loops back to Check last log id on server)

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