ID Info 3000

Date: March 2025
Version: ID Info 3000

Please read and follow the installation instructions before operating the equipment, and keep the instructions for future reference or use after debugging.
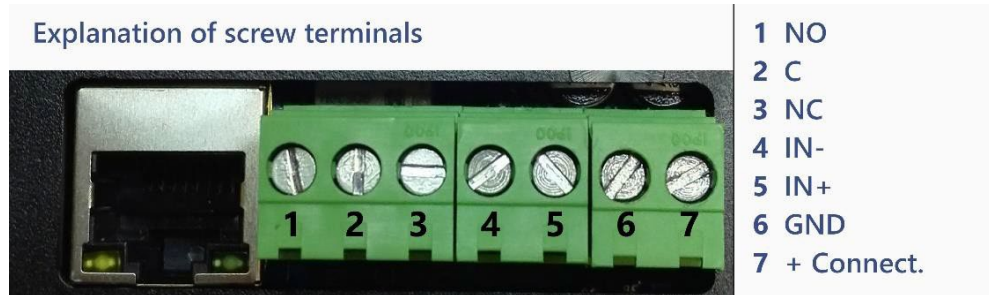
Contents

1. Quick User Guide

To start the device please follow these instructions:

1. To connect the device to the power grid, you have to connect a 9-23 V power supply to the screw terminals (6 and 7).

Nr.	clamp	Description
1	NO	Relay connection: normally open (connect ACS here)
2	C	Common (connect ACS here)
3	NC	Relay: normally closed
4 +5	IN- / IN+	Digital input: Detects if connection from IN- to IN+ is closed and then sends out an event.
6	GND	- 9-23 VDcV (340 mA) Power Supply
7	Positive connection	+ 9-23 VDcV (340 mA) Power Supply

2. Connect to the Ethernet and power on

3. The device starts automatically and after the boot sequence, the display shows for a short time the INFO Page (see image below).

4. Immediately after this, the HOME page appears, this indicates that the application is ready. As default settings, the device obtains its network settings from a DHCP server.

5. At any time it is possible to view the INFO Page clicking on the top right corner of the display.

6. Using the browser of a PC, Tablet or Smartphone that is connected to the same network as the device, you can manage the configuration pages that can be found at the link http://<ip_address>:4157.
    In this case type in the UR: http://192.168.0.66:4157

7. The password used on the web interface is the sum of the values of current year, month and day (e.g. Today 13/11/2020 the password is 13+11+2020 = 2044)

2. Webinterface

You can view and configure various information directly in the Webinterface

2.1 Home

Various parameters are displayed on the start screen.There you can also restart the reader and your application which is running on the device.
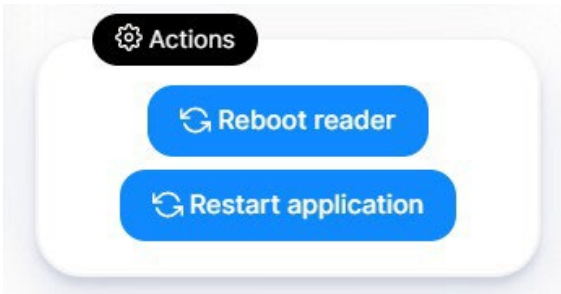
2.2 Ethernet Setup

2.2.1 Parameter of reader

Here you can setup the network configuration for the reader.

| Manual input | Get IP from DHCP |

2.2.2 Reference server parameters

Here you can adjust the network configuration of the server which is communicating with the reader and the Server timeout (SrvTOut)

2.3 Debug

2.3.1 Read Test

With virtual read test you can simulate a reading event of the reader and see what the server responds. With check user reading you can read cards with the reader and display the UID.

2.3.2 Test Commands

Here you can test specific parameters (Relay, Buzzer, Messages, Outcome Time) and send them as command to the device, like e.g. a special Marketing offer. The message will be shown as long as the outcome time is s

3. Software Integration

To connect the ID INFO 3000 with your software, you have to integrate it with your webserver. You can configure on which port the device listens to commands on the "reader parameter webpage".

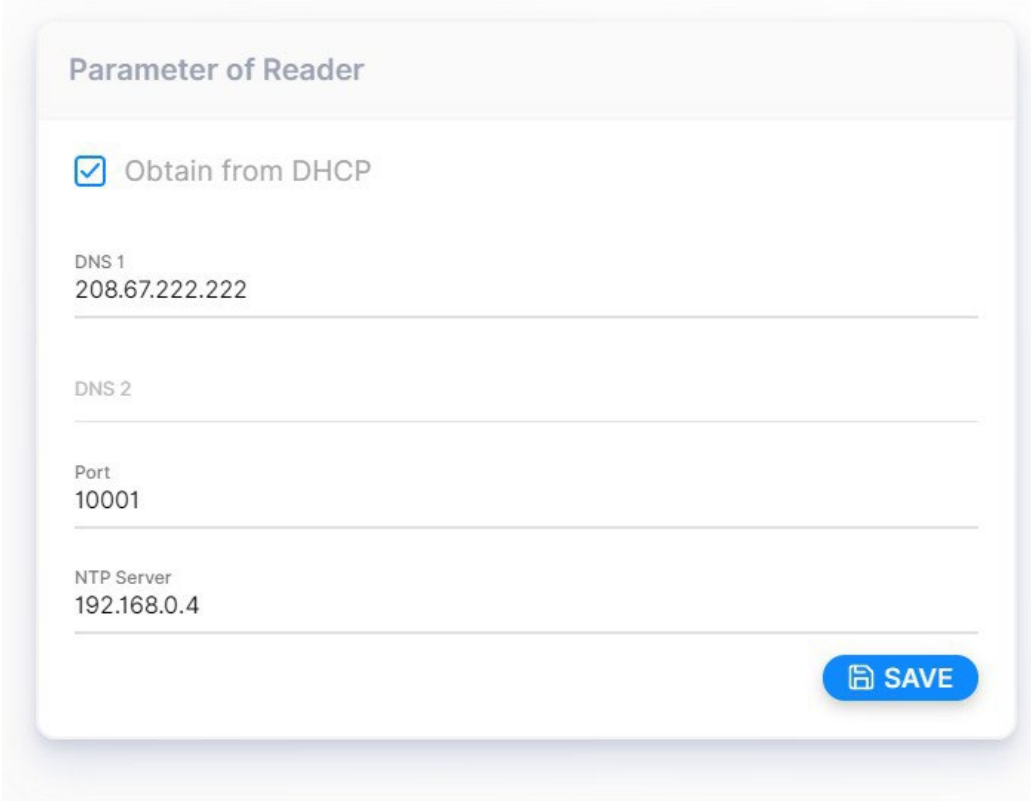## 3.1 Operating Logic

The ID INFO 3000 terminal is equipped with an internal web server and an integrated browser that allows to show standard html pages on the internal display.

The terminal operating mode is as follows:

After the reading of a badge, the terminal sends the information to a server through the GET of a specific page with the parameters relating to the event and expects a json in response containing the parameters of the actions to be performed. The server IP and the http event URL can be set from the setup pages under item 'Reference server parameters. (see Chapter 2.2.2)

At any time it is possible to send commands to the terminal by calling the page at this link http://<ip- terminal>:4157/kughi/set? followed by one or more command parameters.

3.2 Send commands to terminal

In order to send commands to the device you can use the following link:

http://<ip- terminal>:4157/kughi/set?LedR=<LedRED>&LedG=<LedGREEN>&LedB=<LedBLU>&LedT=<LedTimeout>&RelT =<ReleTimeout>&RelS=<ReleScale>&BuzT=<BuzzerTimeout>&BrwURL=<BrowserURL>&HfAnt=<AntennaHF>

Note: all parameters are optional

Value	Value range	Description
<LedRED>	0-255	Brightness of red LED
<LedGREEN>	0-255	Brightness of green LED
<LedBLU>	0-255	Brightness of blue LED
<LedTimeout>	0-999 tenths of a second	How long the LED will light up
<ReleTimeout>	0-9999 seconds, 0= disable,9999 enable forever, 9901 toggle status, 9902-9998 keep status unchanged	How long the relay will toggle
<ReleScale>	Scale 0-100 hundredths of seconds to be used for Rele Timeout unit. if omitted equal to 100 (1 second)	Can shorten the relay timeout
<BuzzerTimeout>	0..999 tenths of a second, 0 disable, > 900 keep unchanged	How long the buzzer will beep
<BrowserURL>	https://www.google.de/	URL of the page to be displayed by the internal browser
<AntennaHF>	True/false	enable/disable the reading function of the HF Antenna

3.2.1 Examples of commands for the URL field in browser

We have some examples for the communication with the server included in the PHP file" develop.php", which is contained in the SDK package. Please have a look into it.

If your device has for example the IP: 192.168.10.199

toggle relay for 1 second
http://192.168.10.199:4157/kughi/set?RelT=1

show google page
http://192.168.10.199:4157/kughi/set?BrwURL=https://www.google.de

set Led Red to 200 (80% of its brightness) for 100 tenths
http://192.168.10.199:4157/kughi/set?LedR=200&LedG=0&LedB=0&LedT=100

set Led Green to 255 (100% of its brightness) for 100 tenths of a second and the buzzer for the same time
http://192.168.10.199:4157/kughi/set?LedR=0&LedG=255&LedB=0&LedT=100&BuzT=100

set Buzzer on for 5 seconds
http://192.168.10.199:4157/kughi/set?BuzT=500

3.3 Event

In case of reading or other event (e.g. input status change or similar, read UID) the terminal sends the data relating to the event to the server in the form of parameters of a GET to the page specified in the setup as query string to the webserver. The parameters differ according to the type of event and are included among those listed below.

Note: DeviceID UID uniquely assigned OTP to the terminal, or his MAC Address

To read a block of a Mifare tag you have to …

1. Enable reading of UID tag Mifare 13.56 MHz in the HF setup page
2. Choose Key A or B
3. Authenticate with the chosen key
4. Insert the block number
5. Block password

ActionType	Value	"Valuerange" or <variable>	Description
"IN"	InputPostion InputState InputName	<number> "0" or "1" <description>	<number> "0" or "1 <description>
"BATT"	0-9999	<millivolts>	Battery Voltage
"A" = fast badge presentation "B"= when a badge is kept longer than a setup parameter "C"= badge removed	TagType TagUID TagBlock Antenna HFType HFSize	"HF" <tag code> <if set> "SX" | "CX" | "DX" "U" "1" "4" "B" "I" "D" "S" "D" "T" "I"	HF Tag UID of Tag If set on HF-webpage of device SX=Left CX=Center DX=Right ultralight or emulations Mifare 1k Mifare 4k ISO 14443_B ISO 15693_3 (I code SLI) ISO 14443_4 (Desfire) Single 4 bytes UID Double 7 bytes UID Triple 10 bytes UID I Code 8 Bytes UID

3.3.1 Examples of commands for the URL field in browser

Example: read Mifare 1K tag on left antenna side

QueryString:
?ActionType=A&Antenna=SX&DeviceID=F8DC7A330534&HFSize=S&HFType=1&TagType=HF&TagUI D=6B28C874

Explanation:

Device with the mac address F8DC7A330534 read a HF Tag Mifare 1K with 4byte UID 6B28C874 on the left antenna side

Example: removed a HF-tag on right antenna side

QueryString:
?ActionType=C&Antenna=CX&DeviceID=F8DC7A330BA0&TagType=HF&TagUID=3E37F9AC&

> **Explanation:**
>
> On the device with the mac address F8DC7A330BA0 read a HF Tag with the UID 3E37F9AC on was removed the middle antennaside.

Example: read Mifare 1k tag and readout blocks

QueryString:
?ActionType=A&Antenna=DX&DeviceID=F8DC7A330534&HFSize=S&HFType=1&TagBlock=000000000000000000000012345678 9&TagType=HF&TagUID=2EE49A89

> **Explanation:**
>
> Device with the mac address F8DC7A330534 read a HF Tag Mifare 1K with 4byte UID 2EE49A89 on the right antenna side which has this value 00000000000000000000000123456789 in the chosen block.

Input Status change (closed)

QueryString:
ActionType=IN&DeviceID=F8DC7Axxxxxx&InputName=EXT_INPUT&InputPosition=0&InputS tate=0&

> **Explanation:**
>
> Device detected the closing of the contacts IN+ and IN-

Input Status change (opened)

QueryString:
ActionType=IN&DeviceID=F8DC7Axxxxxx&InputName=EXT_INPUT&InputPosition=0&InputS tate=1&

> **Explanation:**
>
> Device detected the closing of the contacts IN+ and IN-

3.4 Server answer

In response to this GET, the terminal expects from the server, within SrvTOut seconds, a json formatted as described below:

Note: You can set SrvTOut seconds in the web interface on the ethernet setup, it's called server timeout.

[

{"Target":"Led", "Colore":{"Red":<LedR>,"Green":<LedG>,"Blue":<LedB>},"Timeout":<LedT>},
{"Target":"Rele","Timeout":<RelT>,"Scale":<RelS>},
{"Target":"Buzzer","Timeout":<BuzT>},
{"Target":"Browser","URL":<BrwURL>},
{"Target":"Display","Timeout":<DisT>,"nIcon":<NPag>,"Row1":<Triga1>,"Row2":<Triga2>,"Row3":< Triga3>},

]

Where each element of the array is optional (for example, you can control only the LEDs, only the relay or only the browser or a combination of them.)

Note   "Target":"Browser" and "Target":"Display" must not be used at the same time.

        For ID Info 3000 type terminals it is recommended to use the "Target":"Display" command

Parameter	Value	Description
<LedRED>	0-255	Brightness of red LED
<LedGREEN>	0-255	Brightness of green LED
<LedBLU>	0-255	Brightness of blue LED
<LedT>	0-999 tenths of a second	How long the led will light up
<RelT>	0-9999 seconds,0= disable,9999 enable forever, 9901 toggle status, 9902-9998 keep status unchanged	How long the relay will toggle
<ReleScale>	Scale 0..100 hundredths of seconds to be used for Rele Timeout unit. if omitted equal to 100 (1 second)	Can shorten the relay timeout
<BuzT>	0..999 tenths of a second, 0 disable, > 900 keep unchanged	How long the buzzer will beep
<BrwURL>	/	URL of the page to be displayed by the internal browser
<AntennaHF>	True/false	enable/disable the reading function of the HF Antenna
<DisT>	Time in seconds	Represent the display of the page before returning to the home

<NPag>	2 character string value	2-character string indicating the page to be displayed
	00	No Icon - [Not used]
	01	Home (mode: Light / Dark)
	02	Access denied (Line 1 - Line 3 is not displayed)
	03	Access allowed
	04	PinCode keyboard - [Not used]
	05	Access allowed with warning
	06-90	reserved for future developments
	91	No Network Connection ,displayed over icon
	92	Server Timeout
	93	Lan network not detected
	94	Info page
	95	SlideShow1
	<Triga1>	20-character string indicating the first part of the message that can be displayed on the screen of the device
	<Triga2>	20-character string for the the second part
	<Triga3>	20-character string for the the third part

3.5 Example for server answer

Example: Led will light up in green and blue | rele toggle | buzzer noise | show weppage | show a message

[

{"Target":"Led", "Colore":{Green":100,"Blue":100},"Timeout":5},
{"Target":"Rele","Timeout":2},
{"Target":"Buzzer","Timeout":2},
{"Target":"Browser","URL": https://www.google.de},
{"Target":"Display","Timeout":10,"nIcon":03,"Row1":NOVEMBER OFFER,"Row2":50% on Smoothies, "Row3":Your FitClub Team},

]

Explanation:

- Led light up in green and blue for 5 seconds.
- Toggle relay for 2 seconds.
- Toggle buzzer for 2 seconds.
- Show web page https://www.google.de (web page of Google)
- Access allowed and Show message: "NOVEMBER OFFER. 50% on Smoothies. Your FitClub Team" for 10 seconds

3.6 Example of a full communication from terminal to server

Here you can see how the communication between server and terminal is established.

Device send event via GET as querry string to server :

?ActionType=A&Antenna=SX&DeviceID=F8DC7A330534&HFSize=S&HFType=1&TagType=HF&TagUI D=6B28C874

Server checks for validation of UID in a database

In this step the server should check if the UID which came from the device is contained in a sql database and then gets the corresponding user of this UID and parse it to a variable which should be send to the device. You can see an example for this in the PHP file which is also contained in this SDK.

```php
// ES
$valid=false;
var UID;
var User;

if (isset($_GET["TagUID"]) {
    $_GET["TagUID"] = UID ;

}
$servername = "localhost";
$username = "username";
$password = "password";
$dbname = "dbname";

?>
try{
    $conn = new PDO("mysql:host=testserver;dbname=Userdatabase", admin, test123);
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    $q = $conn->prepare("SELECT `User` FROM `Userdatabase` WHERE `UID` = "UID");
    $q->bindValue(':User', $User, PDO::PARAM_INT);
    $valid=true;
    $q->execute();

    }
    catch(PDOException $e)
{
    echo  $e->getMessage();
}
```

Adjusting the json script based on the boolean value "valid" and show user from database in information text:

```
[
  {
    "Target":"Led",
    "Colore":
    {
      "Red":<?= $valid ? 0 : 200 ?>,
      "Green":<?= $valid ? 200 : 0 ?>,
      "Blue":0
    },
    "Timeout":500
  },
  {
    "Target":"Rele",
    "Timeout":<?= $valid ? 2 : 9959 ?>
  },
  {
    "Target":"Buzzer",
    "Timeout":30
  },
  {
    "Target": "Display",
    "Timeout":50,
    "nIcon": <?php echo($valid ? '3' : '2') ?>,
    "Row1": "Hello " <?php echo($User) ?>,
    "Row2": "Welcome to our Club !",
    "Row3": "Your Fit Club Team"
  }
]
```

IF UID IS CONTAINED IN THE DATABASE:

In json format It would be:

[

{"Target":"Led", "Colore":{"Red":0,"Green":200,"Blue":0},"Timeout":500},
{"Target":"Rele","Timeout":2},
{"Target":"Buzzer","Timeout":30},
{"Target":"Display","Timeout":50,"nIcon":3,"Row1": Hello "User","Row2": Welcome to our CLUB,"Row3":Your Fit Club Team},

]

IF UID IS NOT CONTAINED IN THE DATABASE:

In json format It would be:

[

{"Target":"Led", "Colore":{"Red":200,"Green":0,"Blue":0},"Timeout":500},
{"Target":"Rele","Timeout":9959},
{"Target":"Buzzer","Timeout":30},
{"Target":"Display","Timeout":<50>,"nIcon":2},

]

3.7 Tips

On the INFO page, tapping on the IP address you can display a QR-Code with a quick link to the management pages.

Still on the INFO page, by clicking on the lower left corner you can access the HARDWARE TEST, from which it is possible to test the ration of the LEDs, the relay, the buzzer and the reading of the rfid tags.
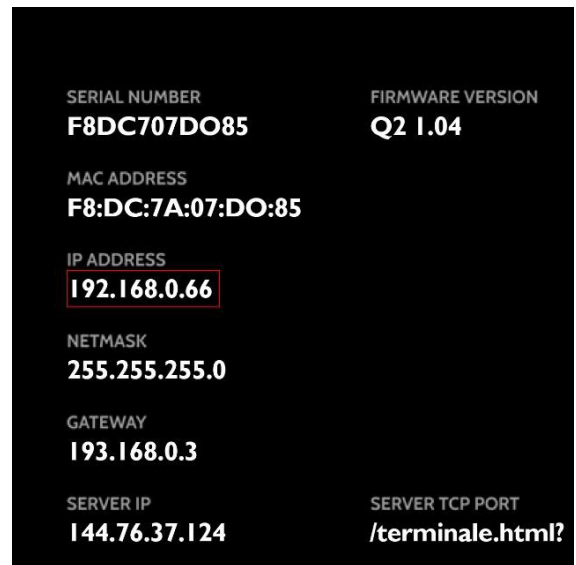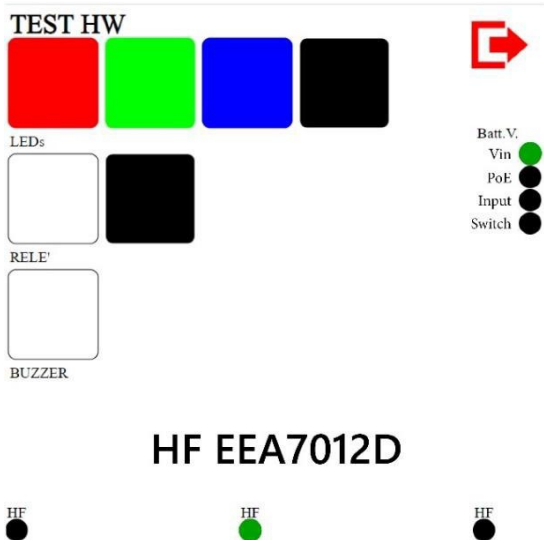

3.8 Change background image

You can access to the O.S. via SSH (port 22) login as: root, without password (this is the configuration for OEM version).

You can also use SFTP (port 22), e.g. from windows using WinSCP (https://winscp.net/eng/index.php)

The web inteface is on: /mnt/storage/terminale/wwwpages/setup_ENG

The background images are on:

ID Info 3000: /mnt/storage/terminale/wwwpages/Q2_img
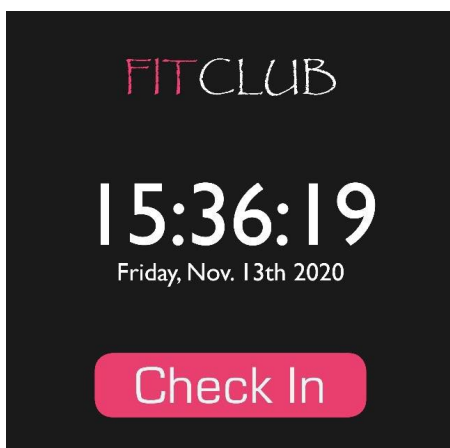
Exemplary Dark Mode

Exemplary Bright Mode

4. Customer Service

We are very happy to help you in the future when you encounter problems or product defects, if the use or operation is not clear, please timely contact the after-sales service staff.

Warranty Card

(Warranty: 3 years)

Order Date:	Product Name:	Product Model:
Customer Country:	Company Name:	Email:
Fault descriptions with photo/video:		