



IDP Electronic ID Products LTD

6 Tushia st, Tel Aviv Israel | Tel: 972-3-5617395 | sales@idp.co.il | www.idpltd.com

Access Control Manual – Version 34



* See appendix B' - Wiring diagrams at the end of this manual.

Controller web interface

You can get to the controller interface by typing its IP address (or host name: <http://idp>) in the web browser, we recommend using a Google Chrome.
You can also get to the interface using your mobile phone as long as it is connected to the same network (supported only by IP address)

In order to change/find the IP address of the controller please see appendix A' on page 22 (**Connecting to the controller through the LAN**).

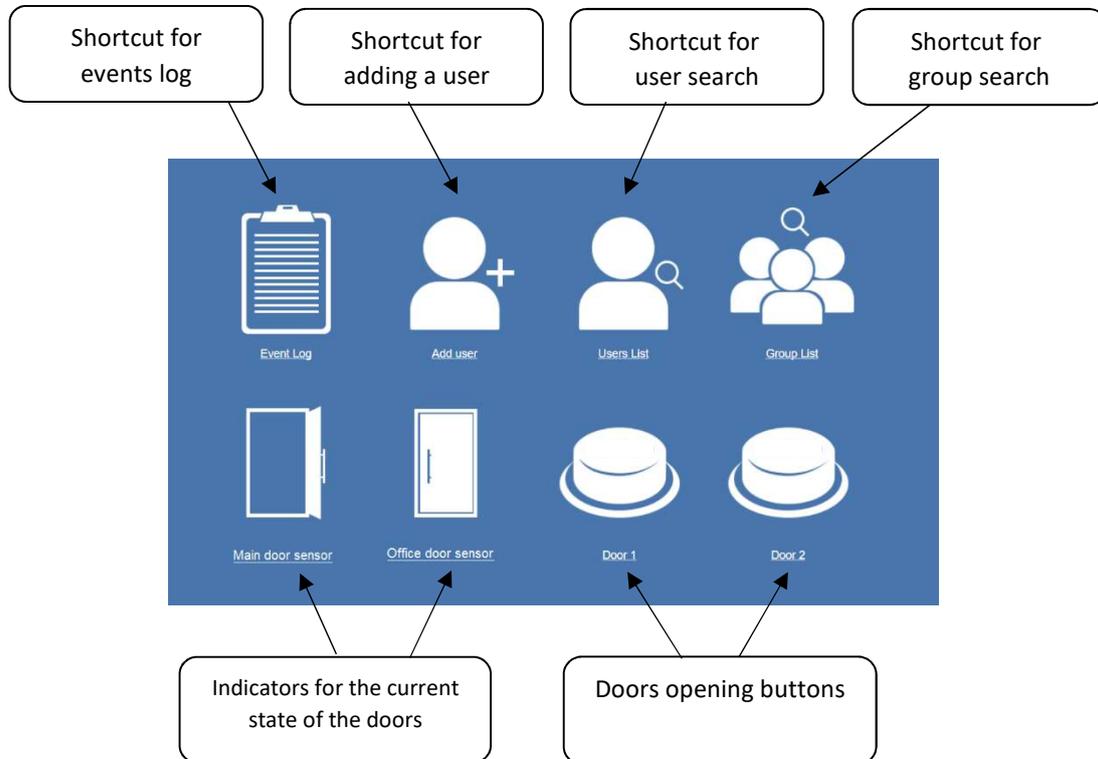
The default password in the Login page is blank.



Main Page

Menu> Main Page

In this quick access page you can see the main shortcuts, buttons and indicators. Here are some of the icons and buttons you may find here:



Sequence for setup a new access controller

The sequence for setup a new access controller is:

1. Setup the doors.
2. Associate the readers with those doors.
3. Add a group that the user will be part of (this is required even if it's a single user)
4. Add the user.

Doors setup

Menu> Access Control> Doors settings

Door 1	
Door name	
Button type	Normally open
Activation time (seconds)	5
Interlock	No
Interlock Delay	0
Door disturbed	0
Event door disturbed	No
Event door breached	Yes
Event physical button	No
Event html button	No
SAVE RELOAD	

1. Upper box- select the relevant door.
2. **Door name:** in this box you can change the door name.
3. **Button type:**
You can connect a push button to the controller in order to operate a relay.
For a button that closes a circle select: Normally Open
For a button that opens a circle select: Normally Close
4. **Activation time:** Relay time (for how long the door will be open).
5. **Interlock** – select if the door is a part of the interlock (when this door is open the other door will not open, and vice versa)
6. **Interlock Delay**– set a time interval between the first door closed until the second door will be able to open (in seconds)
7. **Door disturbed** – this option is used in cases that an alert is needed when a door is open for too long. You should write the number of seconds that if the door is opened more than this number, then an alert will be generated. In case that no alert is needed, you should write 0.
8. **Event door disturbed** – this parameter determines if an event will be added in the Events Log each time that there is a troubled door.
9. **Event door breached** – if the door opens without any approved tag was present the controller will make an event and opens a second relay.
10. **Push Button Event** - this parameter determines if an event will be added in the Events Log each time that a door will be open using a Push Button.
11. **Browser Button Event** - this parameter determines if an event will be added in the Events Log each time that a door will be open using a button in the browser.
12. **Save-** save the settings.

Readers settings

Menu> Access Control> Readers Settings

Reader 1

Reader action: Entrance

Selected Door: main entrance door

Passage to: Without

SAVE RELOAD

1. Upper box- select the reader you wish to set (based on the physical input in the controller that the reader is connected to)
2. **Reader's action**- select if the reader action is entrance or exit.
3. **Selected door**- select the door that the reader will control on.
4. **Switch To** – this option should be used in cases that we want to know the location of users (if they are inside or outside the office or in which floor they are at). You can choose the location that the user will be at when he enter the door.
5. **Save**- save the settings.

Users groups

Adding a group

Menu> Group List> Add group

Group List

Search

Add group

Download List

Upload List

Clear list

Group ID: 6

Group name: Plaster walls repair

Connected doors: 1,2,3,4

Start date: 11/08/2017

End date: 11/30/2017

Time	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00
Sunday											
Monday											
Tuesday											
Wednesday											
Thursday											
Friday											
Saturday											

SAVE RELOAD DUPLICATE A DAY

Group ID- is set automatically by the controller and is not configurable.

Group name- a group name is required.

Connected doors- choose the doors that the users will be able to use.

Start date / End date- between what dates the group have entry permit.

Timetable- group members can have specific times and days they can travel in the secured areas, i.e. Plaster walls repair team have approval to enter Mon-Sat between 1:00-6:00 only between 11/08/17-11/30/17.

Save- save the settings.

Reload- resets the window and the data of the settings.

Duplicate a day- enables to copy one of the days' definitions and duplicate it to the rest of the days.

Group search

Menu> Group List> Search

Group ID	Group name	Connected doors	Start date	End date	Edit
1	צוות א	1,2,3,4	01/01/2000	31/12/2099	

Search groups can be done by:

Group ID / Group name / Connected Doors / Start date / End date.

On the lower part of the page is a list of all the groups.

Delete a group- put a V next to the desired group and press Delete Selected.

Group ID	Group name	Connected doors	Start date	End date	Edit	
8	Executives	1,2,3,4	01/01/2000	31/12/2099		<input checked="" type="checkbox"/>
7	Managers	1,2,3,4	01/01/2000	31/12/2099		<input type="checkbox"/>
3	C	1,2,3,4	01/01/2000	31/12/2099		<input checked="" type="checkbox"/>
2	B	1,2,3,4	01/01/2000	31/12/2099		<input type="checkbox"/>
1	A	1,2,3,4	01/01/2000	31/12/2099		<input type="checkbox"/>

Note!

A group cannot be deleted as long as it has users connected to it.

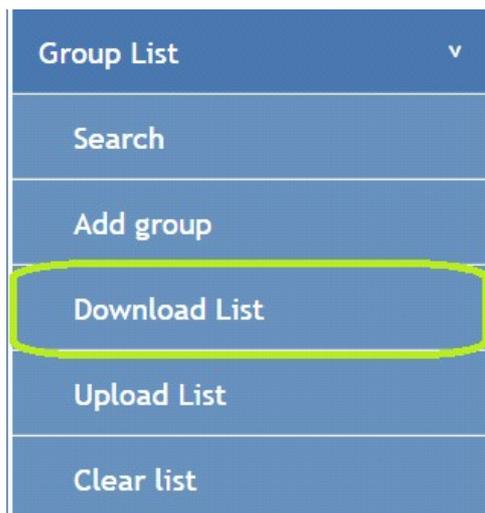
Edit a group- press the blue pencil icon next to the relevant group.

Group ID	Group name	Connected doors	Start date	End date	Edit	
3	C	1,2,3,4	01/01/2000	31/12/2099		
2	B	1,2,3,4	01/01/2000	31/12/2099		
1	A	1,2,3,4	01/01/2000	31/12/2099		

Backing up the groups

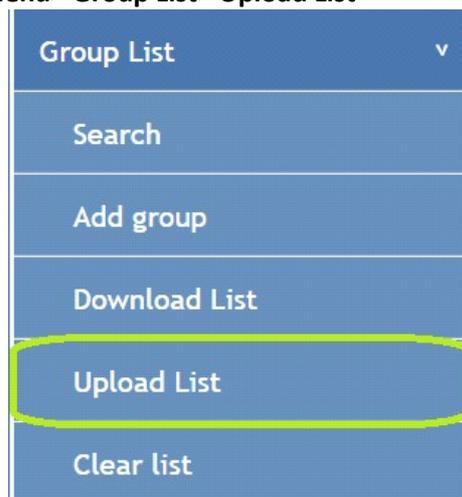
The backup will be downloaded as a csv file to the PC.

Menu> Group List> Download List



Uploading the file to the controller

Menu> Group List> Upload List

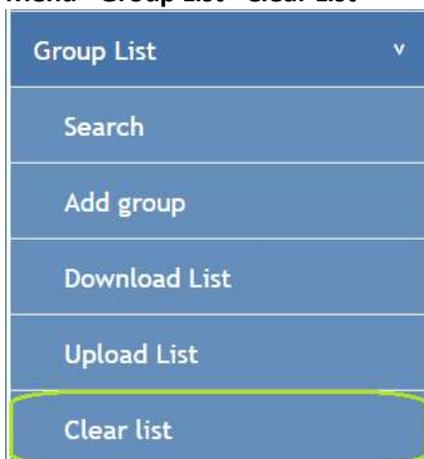


Attention!

This action will delete the current groups list and cannot be reverted.

Clearing the group list

Menu> Group List> Clear List



Attention!

This action will delete all of the groups.
The groups' lists cannot be restored after getting deleted.

Users list

After adding a group it is now possible to connect users to the group.

Adding a user

Menu> Users List> Add User

The image shows a web interface for adding a new user. On the left is a sidebar menu with options: Users List, Search, Add user (highlighted with a green box), Download List, Upload List, and Clear list. The main area is titled 'Add new user' and displays 'Last user tag: 831E85'. Below this is a form with the following fields: User name (text input), Tag number (text input with value 831E85), Pin code (text input), Group 1 (dropdown menu with 'Without' selected), Group 2 (dropdown menu with 'Without' selected), Status (dropdown menu with 'Active' selected), Entries (text input with value 10), and Location (dropdown menu with 'Without' selected). At the bottom of the form are two buttons: 'SAVE' and 'RELOAD'.

User name:

User name is mandatory

Tag number:

-If the tag number is known (normally it is unknown) it can be added manually.

- if purchased a desktop reader- connect it to the USB in your PC and put the mouse pointer in the **Tag number** box, then put the tag close to the reader and the tag number will appear in this box.

- In the case where the tag number is unknown and you did not purchase a desktop reader, you can use one of the system's readers for the purpose of recognizing the tag number:

1. Read the tag with one of the readers attached to the system. The tag number will be shown in the title Last User Tag and also in the
2. The tag number will be shown in the field Last User Tag and also in the Tag Number field.

PIN code:

When there is a numerical keyboard connected to the controller- type the personal PIN Code of the user in this box. Note that you cannot use the same PIN Code for more than one user.

The user can open the door using this pin code followed by a hashtag (#).

Group 1:

Group 2:

Users must be connected to one or two groups.

Status:

Active – the user is active

Blocked – the user is not active.

Limited – the user can enter a limited number of times.

Master- a user that has no conditions of AntiPassBack Interlock or Schedule- he can come in or out any time he wants.

Entrances:

When there is a user with a Limited Status, this field will show the number of times that he can still enter. When the parameter will show 0, this user will not be able to enter anymore.

Location:

The location of the user will be shown (only if locations were predefined).

Search users

Menu > Users List > search

User name	Tag number	Pin code	Group 1	Group 2	Status	Location	Edit
מלי לוי	5CEE21	776667	מנקים		Active	בתוך המשרד	
טל יוספי	5CEDA3	45544	סטודנטים		Limited entrance	מחוץ למשרד	
עידן עטיה	82AA82	123456	מנהלים		Active	מחוץ למשרד	

Search can be done by:

User name / Tag number / PIN Code / user groups / user status or Location.

At the bottom of the screen you can see the Users List.

Delete a user- mark a V in the boxes next to the relevant users and press **Delete Selected**.

User name	Tag number	Pin code	Group 1	Group 2	Status	Edit
Jacob	AC542569	0	1	1	Free	<input checked="" type="checkbox"/>

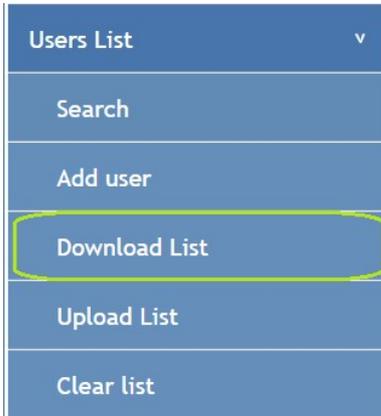
Editing a user- press the blue pencil icon next to the user you want to edit.

User name	Tag number	Pin code	Group 1	Group 2	Status	Edit
Jacob	AC542569	0	1	1	Free	<input checked="" type="checkbox"/>

Backing up the Users list

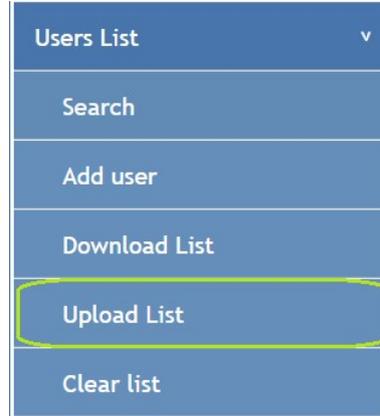
The backup will be downloaded as a csv file to the PC.

Menu> Users List> Download List



Uploading the file to the controller

Menu> Users List> Upload List



Note!

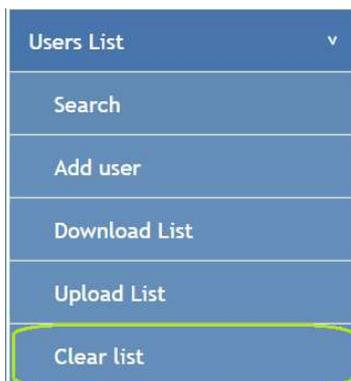
This action will run over the users lists which cannot be restored after getting deleted.

Deleting all the users

Menu> Users List> Clear list

Note!

This action will delete all the users' lists and it cannot be restored after getting deleted.



Event Log

Menu> event Log> Search

A screenshot of a menu with the following items: 'Event Log' (with a dropdown arrow), 'Search' (highlighted with a yellow box), 'Download List', and 'Clear list'.

The 'Search event' form includes the following fields: Name/Value (text input), Door (dropdown menu with 'All' selected), Event (dropdown menu with 'All' selected), Date (From) (text input with placeholder 'mm/dd/yyyy'), Time (From) (text input with placeholder '---:--:--'), Date (Until) (text input with placeholder 'mm/dd/yyyy'), and Time (Until) (text input with placeholder '---:--:--'). Below the form are 'SEARCH' and 'CLEAR' buttons.

The 'Event Log' table below the form displays the following data:

Name/Value	Door	Event	Date	Time
RFID: 000511	Gate	Entrance - Denied unknown	03/07/2019	13:46:02
Shimon	Gate	Entrance - Denied unknown	15/06/2019	17:00:00
Shimon	Gate	Entrance - Denied door	15/06/2019	16:00:00
Shimon	Gate	Exit - Denied interlock	15/06/2019	15:00:00
Shimon	Gate	Exit - Denied APB	15/06/2019	14:00:00

Below the table are 'TOP' and 'BOTTOM' buttons.

In the Event log you can see the recorded events.

i.e. who entered and when and who didn't get approval to enter and when.

The page is made of two parts:

- Events search table.
- Details of all the logs from the latest time to the oldest time.

Logs search table

In this page you can search using all or part of the boxes

Name- user name / **Value-** by "Value" is meant- when an unknown tag was swiped or an unknown code was put in and it is not possible to connect these to a user

Door- event search by door

Event - see event types:

Entrance:

Approved- The user got OK to enter.

Blocked User – the status of the user is defined as blocked.

Denied unknown- the tag or the code were unknown and thus there was no OK to enter.

Denied door- an approval wasn't granted as the user has no OK to enter through this door.

Denied date- an approval wasn't granted as the user has no OK to enter through at this date.

Denied time- an approval wasn't granted as the user has no OK to enter through at this time.

Denied APB(Anti Pass back)- an approval wasn't granted as the user is logged as Inside and didn't exit.

Denied interlock- an approval wasn't granted as one of the doors was Open.

Exit:

Approved- The user got OK to exit.

Denied unknown- an unknown code or tag presented and thus didn't get OK to exit.

Denied door- an approval wasn't granted as the user has no OK to exit through this door.

Denied date- an approval wasn't granted as the user has no OK to exit through at this date.

Denied time- an approval wasn't granted as the user has no OK to exit through at this time.

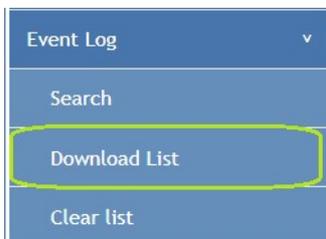
Denied APB(Anti Passback)- an approval wasn't granted as the user is logged as outside and didn't enter.

Denied interlock- an approval wasn't granted as one of the doors was Open.

Date/time From/until- the search can be limited to specific dates and times.

Download list

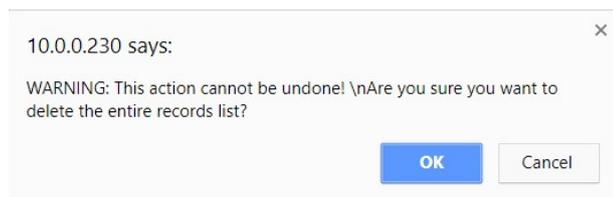
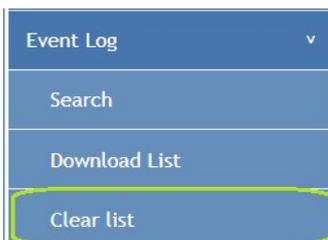
Menu> event Log> Download list



The events log will be downloaded to the PC as a file.

Clear the log List

Menu> event Log> Clear list



The events log list will be deleted from the controller's memory.

Note!

After deleting the list cannot be restored.

Last Events

Configuration of the Access Control

Menu> Last Events

The Last Events page shows the last 10 events (you can decrease the number of events that will be shown under **Access Control > General Settings**).

You can see a different color indication for each of the following events:

Green – approved event

Orange – unapproved event (for example: unapproved user that tried to enter)

Red – unusual event (for example: troubled door)

You can press the user name in order to edit the user details or to press on an unidentified card number in order to add it as a new user in the system.

The screenshot shows a 'Last events' page with a blue header and a grid of 10 event cards. Each card contains the following information: a colored bar at the top, a name or value, door name, event type, state, date, and time. The events are as follows:

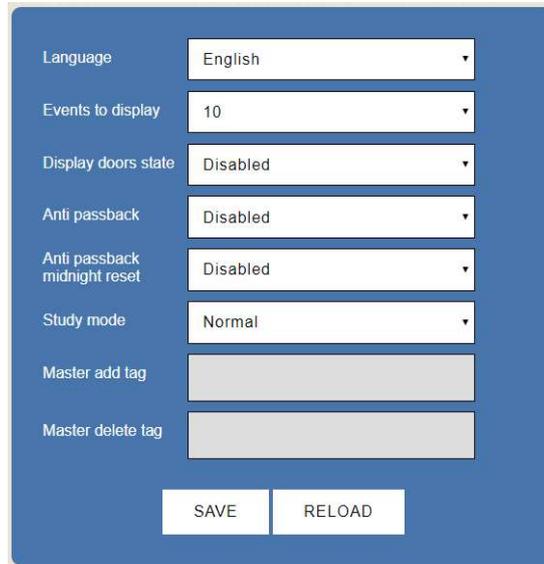
Color	Name/Value	Door	Event	State	Date	Time
Green	דלת מסך	main entrance door	Virtual Button	Approved	07/06/2018	13:18:51
Green	עידן עטיה	main entrance door	Entrance	Approved	07/06/2018	13:17:18
Orange	831E85	main entrance door	Entrance	Denied unknown	07/06/2018	13:17:14
Red	נול יוספי	main entrance door	Entrance	Denied date	07/06/2018	13:17:03
Red	מלי לוי	main entrance door	Entrance	Denied time	07/06/2018	13:16:43
Orange	6CEE21	main entrance door	Entrance	Denied unknown	07/06/2018	13:16:13
Orange	6CEDA3	main entrance door	Entrance	Denied unknown	07/06/2018	13:14:53
Green	עידן עטיה	main entrance door	Entrance	Approved	07/06/2018	13:14:40
Orange	831E85	main entrance door	Entrance	Denied unknown	07/06/2018	13:14:23
Orange	82AA82	main entrance door	Entrance	Denied unknown	07/06/2018	13:13:15

Entrances remained: 9

Other Access Control settings

setting the access control

Menu> Access Control> General Settings



Language	English
Events to display	10
Display doors state	Disabled
Anti passback	Disabled
Anti passback midnight reset	Disabled
Study mode	Normal
Master add tag	
Master delete tag	

SAVE RELOAD

Language

Select between Hebrew and English.

Events to display

Choose how many event will be shown on "Last events" page.

Display doors state

Enabling this will show the status of the doors in the main page.

If there is a magnet that checks the door status it is recommended to select **Enable** status.

If there is no magnet that checks the door status it is recommended to select **Disable** status- in order to prevent confusions.

Anti Passback

The user cannot enter again or exit again as long as he didn't present his tag at the opposite reader.

i.e. When a user enters together with another person without showing his tag- he will not be able to exit until he shows his tag in the entrance, or when a person left the place without presenting his tag at the exit he will not be able to re-enter until he presents his tag at the exit.

Anti Passback Midnight Reset

Resetting the AntiPassBack at midnight will give OK to enter to those who left the secured area without presenting the tag, i.e. when the gates were fully opened at night for fast exit.

Study mode

Normal – Add users from this web interface.

Master's tag – you can set two masters tags in the next boxes for the ability to add users without the user interface, after you will present the master add tag in the reader, the controller will add all of the next tags that will be presented to the reader until you will present the master add tag again, the users will be add as master users.

Auto – if you choose this option all the tags that will present to the reader will be add automatically as master users and the controller will open the door.

Set the date and time

Settings> Date and Time

Settings	▼
General settings	
Network settings	
Date and Time	
Set Password	
System update	

Synchronize time	Time server ▼
Time server IP	24.56.178.140
Time zone	+2 ▼
Daylight saving time	Israel ▼
Date (dd/mm/yyyy)	11/13/2017
Time (hh:mm:ss)	09:49:44 AM

SAVE RELOAD

Synchronizing the time:

Setting the date and time automatically can be done by synchronizing through the cellular network or by an internet time server.

Time server:

This option is recommended when there is an access to the internet.

Cellular network:

If the controller have a cellular modem of IDP it can be defined synchronize the date and time from the cellular network.

The controller has to be connected to a cellular network.

Off:

This is used for manual update of the date and time.

Time server IP:

In the case where the controller has access to the internet it is recommended to synchronize against IP address 77.235.14.49

Time zone:

For Israel choose +2

For other areas in the world use time zone map to find the relevant time zone.

Daylight saving time:

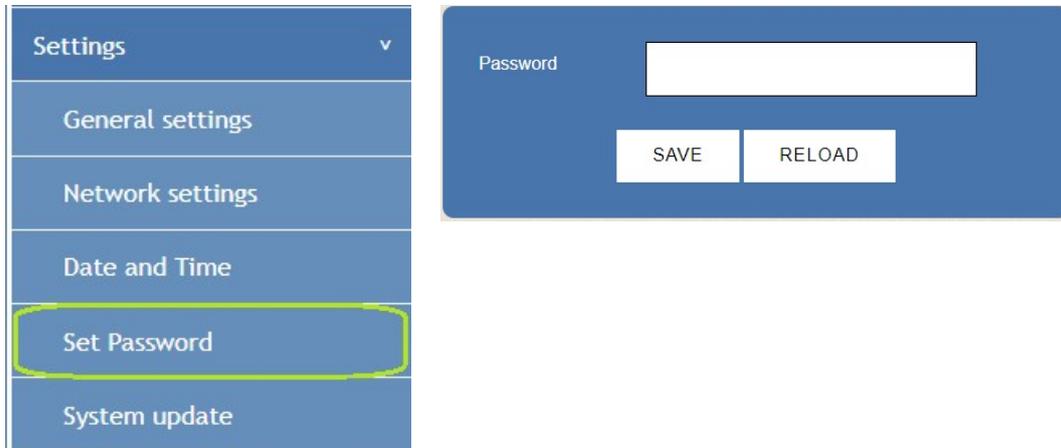
Select if a DST is on or off, and also choose if the time will be adjusted to Israel, Europe or USA

Note!

If the controller has no connection to the internet there might be a deviation of up to 60 minutes per 1 year.

Set password for the controller web page

Menu> Settings> Set password



You might want to change the password for the login to the web page.

After setting the password make sure to press **Save**- to save the password.

In order to cancel the password leave the field empty and press save.

Resetting the password

in order to reset the password to its default value- (empty) you can press the physical button marked with the letter **M** for 30 seconds, when there is a Beep the password is in its default value.

The **M** button is on the front of the controller on its right side- the lower button of the two.



Network settings

Menu> Settings> Network settings

DHCP	Limited
Host name	
IP-address	10.0.0.200
Gateway IP	10.0.0.138
Subnet mask	255.255.255.0
Local Port	1001
Primary DNS	8.8.8.8
Secondary DNS	4.2.2.1

SAVE RELOAD

This page is for the setting of the network definitions.

DHCP Disabled - Static IP address, selection of the IP address is made by the user only. The address doesn't change.

DHCP Enabled - Dynamic IP address, selection of the IP address is made by the DHCP server. The address can change according to different changes in the network.

DHCP Limited (Default) - When the controller re-boot, he have his latest IP address in memory, He sends a DHCP request, receiving in return a new address, gateway and a netmask.

If his current address match the subnet which was supply by the DHCP server, the controller will stay with his current address leaving him in a 'static' mode.

If his current address doesn't match the subnet, the controller will take the address which was suggested by the DHCP server.

See appendix A' **connecting to the controller through the LAN.**

Save the new definitions.

Weekly operation board

Menu> Weekly operation board

Action/Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Activate Time 1	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Deactivate Time 1	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Activate Time 2	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Deactivate Time 2	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Activate Time 3	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Deactivate Time 3	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Activate Time 4	00:00	00:00	00:00	00:00	00:00	00:00	00:00
Deactivate Time 4	00:00	00:00	00:00	00:00	00:00	00:00	00:00

In this time table you can set for each door the time that it will stays open, in this period of time the controller will not save event data in his memory for that door.

System update

Menu> Settings> System Update

Settings ▾

- General settings
- Network settings
- Date and Time
- Set Password
- System update**

Choose File No file chosen

SAVE CLEAR

Warning:
The following action overwrites the existing data in flash memory and then performs a software update. Please complete a full backup before the update, and then follow the guidelines of IDP company. Update not according to instructions, may cause irreversible damage to the controller!

Note!

Do not attempt to do this action without contact us.

When you get an update for the controller keep it locally- use only English letters for the path and the name of the file, as the update will not be able to take place otherwise.

Browse> select the file> **Save**

Important!!!

This action deletes ALL the data stored in the controller- it is recommended to back the definitions and the database and after the update is complete to upload them.

For the backup press Download list- note that there are three different lists and all three should be backed up.

Group List> Download List> Save

Users List> Download List> Save

Event log> Download list> Save

After the update is complete you can upload the files:

Group List> Upload List> Browse to the required file> Save

Users List> Upload List> Browse to the required file> Save

It is impossible to upload the event log back to the controller.

Remotely reboot the controller

Menu> Reboot



Press Reboot> Ok

The controller will make a reboot without the need to be next to it.

Logout

Menu> Logout



Will do an orderly exit.

Trouble Shooter

Note- after solving the problem, if the controller is still not working well go over the trouble shooter again from the beginning. If after that there is still a fault contact IDP support for finding the solution to it.

Trouble: you can't find the controller in an HTML page.

1. Green and Red LEDs flashing and there was one beep sound when the controller was turning On?

Yes- go to step 2

No- go to step 4

2. An orange LED is On?

Yes- go to step 3

No- go to step 5

3. The IP address of the controller is at the same addresses range of the LAN it is connected to?

In order to check and change the IP of the controller see appendix **A' Connecting to the controller through the LAN**

4. The controller is connected to a working 12VDC power supply?

Yes- contact IDP support

No- please connect a correct and working power supply.

5. The controller connected to a working network cable that on the other end is connected to the LAN?

Yes- go to step 6

No- please connect a working network cable and make sure it is connected well on both sides, also make sure the other network peripherals are working, i.e. switch etc.

6. firewall or antivirus might be blocking your controller.

This step has to be done by a professional PC technician or IT personnel.

Steps to take:

Are there any routers (bridges, firewalls, proxies) between your PC and the Device Server?

The DS Manager can work in two different network modes as defined by the selection in the Access Mode drop-down:

Auto-discovery mode that finds all the Device Servers in the local network segment automatically

Address books mode that is not limited to a local network segment but you have to specify each IP-address manually

Notice, that auto-discovery only works for a local network segment. If there are any routers or bridges between your PC and the Device Server in question then the DS Manager won't be able to find this Device Server automatically. This is because so-called broadcast packets used to find the Device Servers cannot penetrate routers and bridges. In this case you need to specify the address of the Device Server manually:

First, make sure that the IP-address of the Device Server is set correctly

Next, select Device Servers from the Address Book in the Access Mode drop-down box

Press the *Add* button, input the IP-address of your Device Server (input a comment if you wish) and press OK

The DS Manager will refresh the data in the list and you will see the IP-address you've just entered

The icon next to the Device Server should appear in solid blue. If the icon is gray then the Device Server at specified IP-address could not be found!

If you have done all of the above correctly but you are still unable to "see" the Device Server in the DS Manager or Connection Wizard then the problem may be with your router (bridge, firewall, proxy):

You may have to specify the "IP forwarding" i.e. setup your router to pass the network traffic addressed to your Device Server to the network segment where your Device Server resides

If there are "port restrictions" set on your router then you need to make sure that TCP and UDP traffic is allowed for port 1001 (this is the default data port of your Device Server; it is programmable so if you've changed it then you need to open a matching port number on your router). In addition, you need to enable UDP traffic on port 65535 (this is a fixed command port that is used to program the Device Server). Both data and command ports must be accessible!

Finally, you must set the router to pass "pings" (ICMP protocol)

7. The PC that the controller is connected to has another network card or a VPN, like cellular or Wi-Fi dongle or internal card?

Yes- go to step 8

No- contact IDP support

8. Network prioritization- This step has to be done by a professional PC technician or IT personnel.

If your computer have multiple active network interfaces (Ethernet, WiFi, VPN, etc.), then sometimes windows will force the auto-discovery packet to only be sent out of the first interface in the list.

For DS Manager, you will reassign the "default" interface to the one that the Tibbo device is connected to, please follow the instructions below:

1. Open Command Prompt and type: route print - you will see a list of active routes, the last column displaying their "metric". Lower metric routes are preferred over higher ones.

2. Open the Network Adapter Properties (Control Panel > Network and Internet > Network Connections > right-click on adapter and choose Properties)

3. Open the properties of Internet Protocol Version 4 (TCP/IPv4).

4. Click on Advanced.

5. Un-tick "Automatic Metric" and set the interface metric to a number.

6. Hit OK until you close the Network Adapter properties.

7. Repeat steps 2-6 for your other network adapter(s) choosing different metrics.

Remember lower metrics are preferred over higher ones.

Check the new metrics in Command Prompt by typing: route print

For Device Explorer, it is easier, click on "settings". Inside it you have the option to select which interface you wish to send the packet out of and also which protocol to use to communicate with the devices.

Appendix A'

Connecting to the controller through the LAN

1. Connect the controller to the LAN using a Networking cable and supply it with 12VDC from your adapter.
2. The first thing you will note is that the orange LED will turn on, this indicates that a network communication is available.
3. If you have DHCP server on your network (your router is normally the DHCP server) then the controller will get its IP address from that. In case your network mask is **10.0.0.xxx**, the controller address will be **10.0.0.200**
4. If you are using Win7/8/10 PC, open your browser and type into the address bar: <http://idp> you should now see the login screen. (You may change the host name, under Settings → Network settings)
5. If you don't have DHCP available, or your controller is connected directly to your computer, you will need to manually change the address to the correct network range by downloading the DS manager software from the following address:

For 32bit PC: <http://idp.co.il/vault/files/tdst-5-09-10-x86.zip>

For 64bit PC: <http://idp.co.il/vault/files/tdst-5-09-10-x64.zip>

Start> All Programs> Tibbo <Tibbo Device Server Toolkit <DS Manager

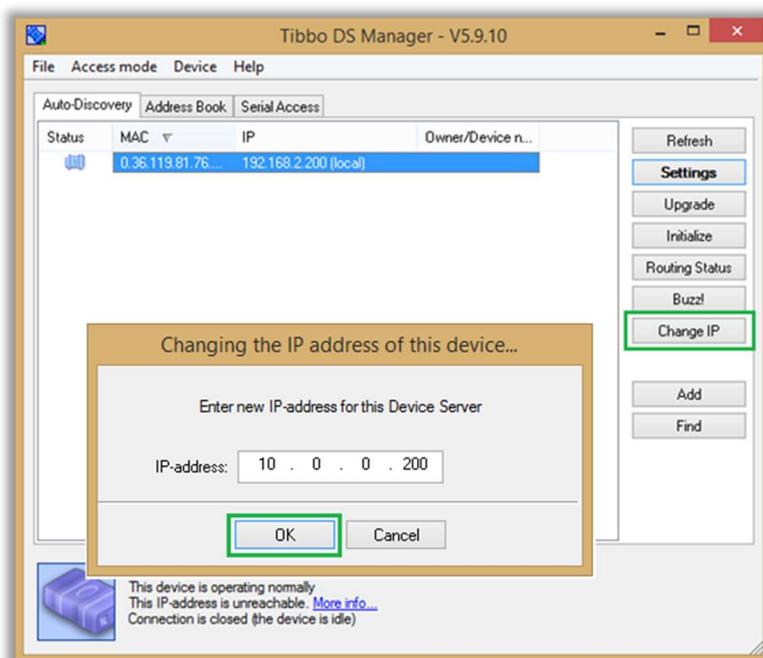
After the DS Manager is up a list of all of IDP controllers will appear.

Make sure the address of the controller is in the addresses range of your LAN.

 Grayed icon - The address of the controller is out of the addresses range of the LAN

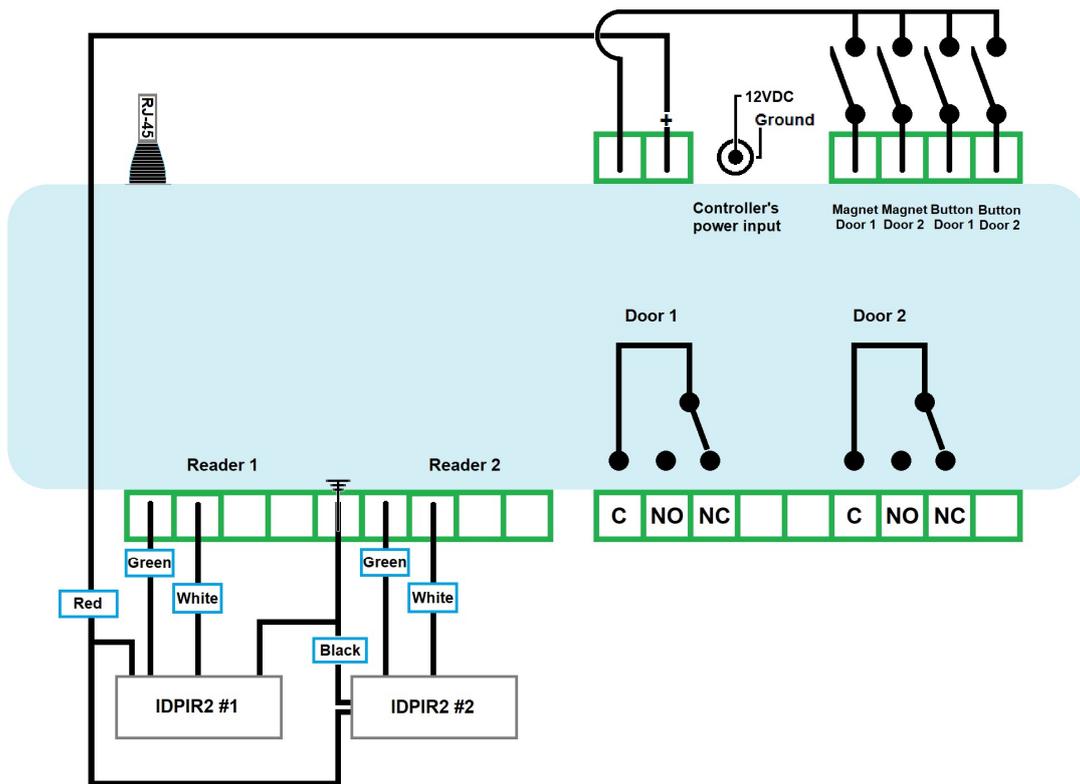
 Blue icon - The address of the controller is inside the addresses range of the LAN

To put the controller IP address inside the LAN address range: mark the device by one click on the list in DS Manager and press Change IP button.



Appendix B' - wiring diagrams

IDPIR Readers wiring

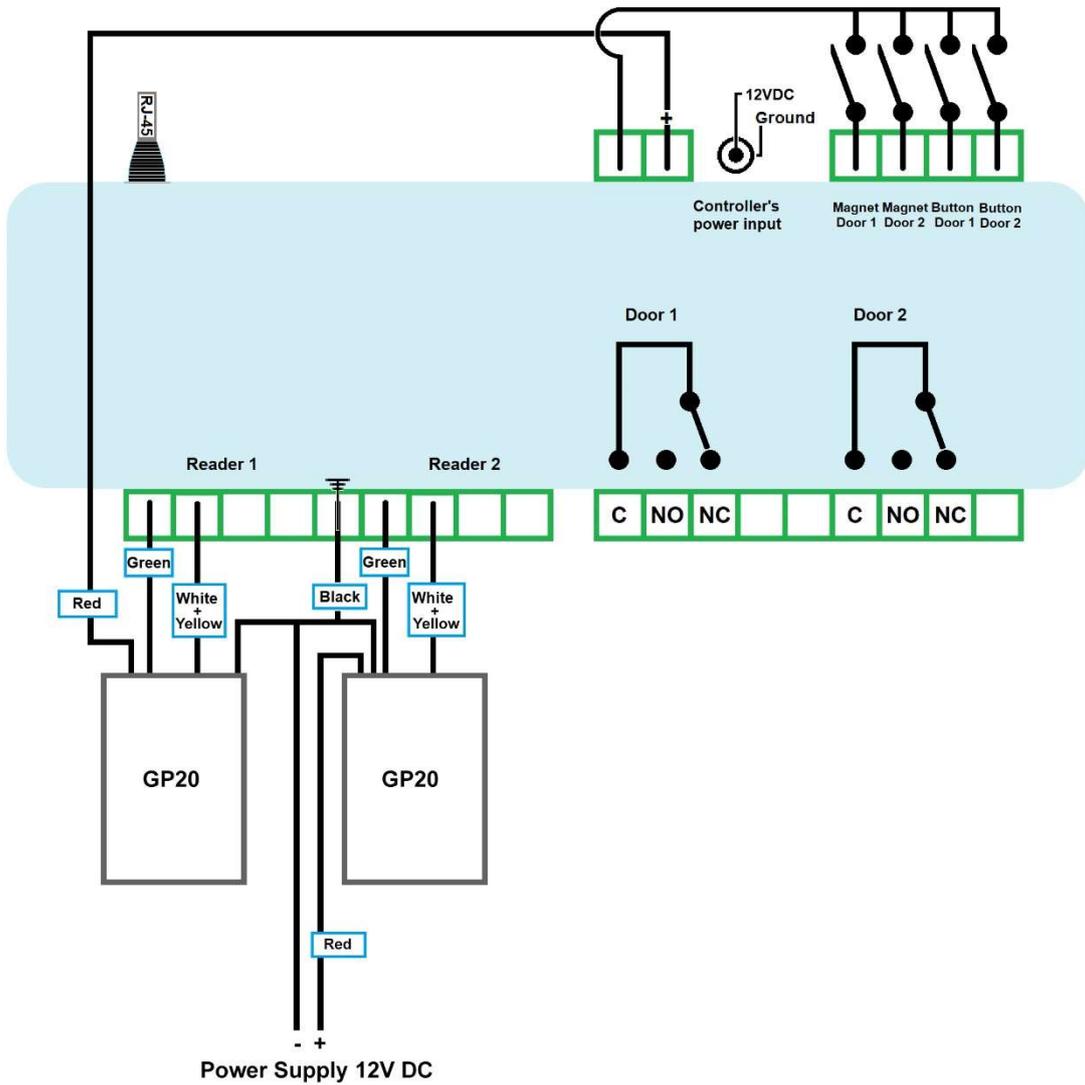


*Power can be supplied via banana socket or the green socket next to it

*An IDPIR2 reader can indicate when a door is opened by a built in beep and/or an internal LED.

to do this connect the brown wire(indicating by LED) and/or the yellow wire(indicating by beep) to the NO contact in the relay, it is important that if the minus (-) that goes to the lock will be the one that is connected to the relay's output like in the next diagram.

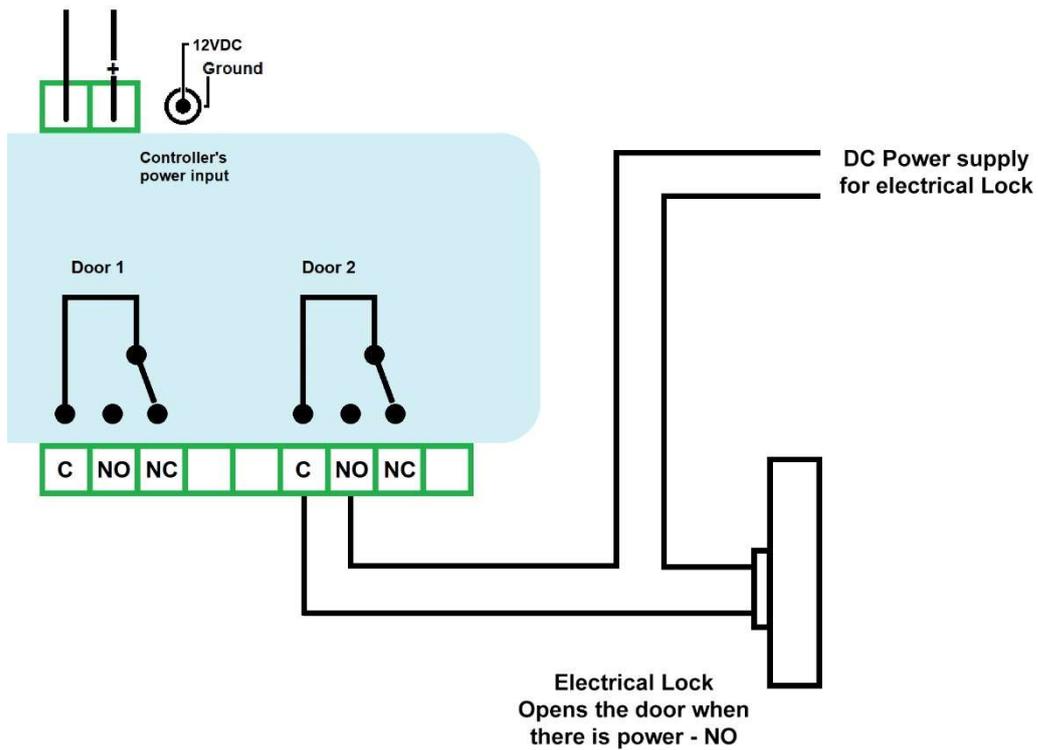
GP20 Readers wiring



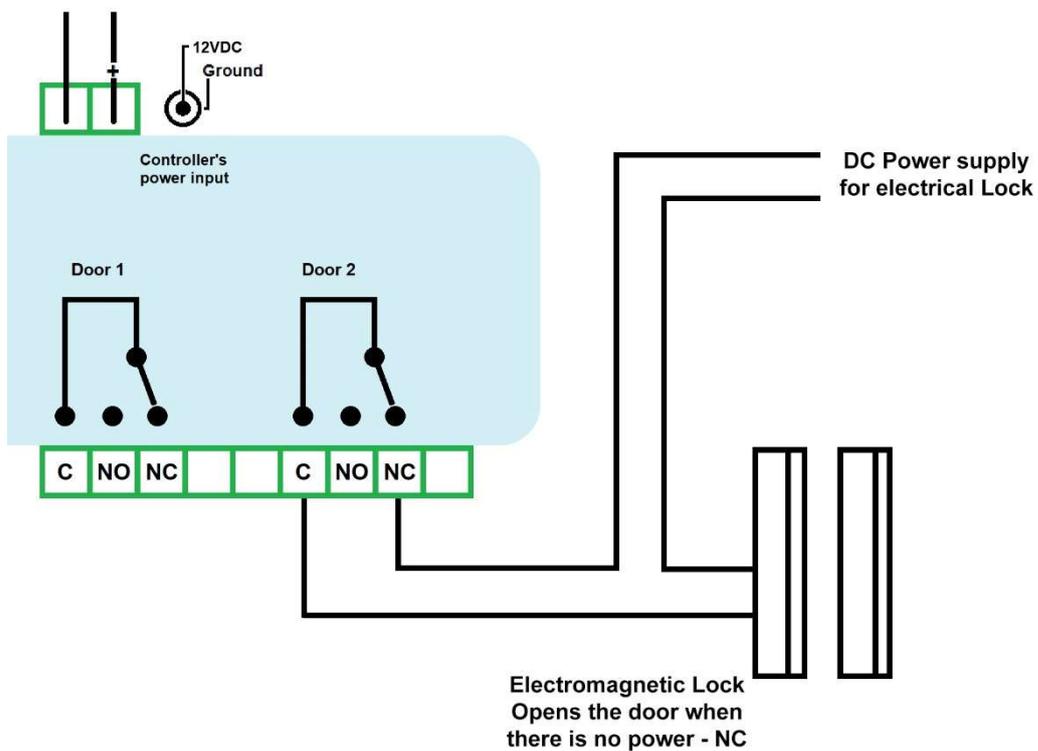
*You will need to connect two power supplies – one for the controller + GP20 #1 and second power supply for the GP20 #2.

You need to connect both of the power supplies ground together like in the diagram.

2. Wiring – Electrical lock



3. Wiring – Electromagnetic lock



Controls and buttons on the controller

The controller has 2 buttons on its right side and 3 LEDs on its left side

