

DP Door W4G / Door Master W4G

Mobile application and/or phone call based gate controller
with 4G/WIFI/Bluetooth connection

Controlling 2 independent gate/door/ramp

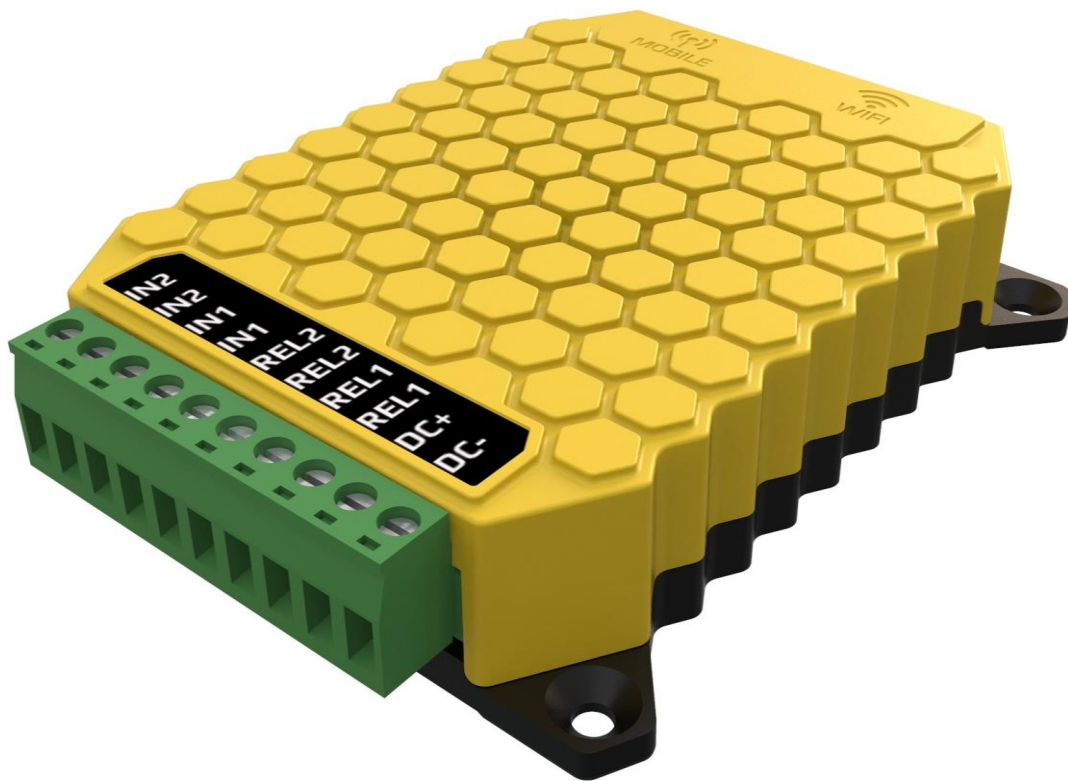


Table of contents

1	General information.....	3
1.1	Advantages.....	3
1.2	Operation	3
2	Appearance	4
3	Connection diagram.....	5
4	Settings.....	5
4.1	Mobile network connection settings	6
4.2	Setting the device WIFI connection using PC software.....	6
4.3	Setting up the WIFI connection with smartphone (alternative mode).....	7
4.4	Setting up control validity periods	8
4.5	Setting up additional features.....	8
4.5.1	Gate position monitoring.....	8
4.5.2	Alert if the gate is left open	9
4.5.3	Automatic opening hours.....	9
4.5.4	Change the timing of relay output	9
4.6	Gate control by caller phone number identification	10
4.6.1	Exportable/importable client list	10
4.7	Control with any caller ID.....	11
5	Status lights.....	11
6	Factory default settings	11
7	Setting up and using the mobile app	12
7.1	Application setup in first start.....	12
7.2	Application details and useful tips	13
8	Remote management, password protection and application restriction.....	14
8.1	Device password protection	15
8.2	Limiting mobile app users	15
9	Technical details.....	15
10	Content of the package	15

1 General information

Mobile application and/or phone call based remote gate controller with the following features:

- 4G Mobile data connection (LTE)
- 4G Voice calling capability (VoLTE)
- 2.4GHz WIFI connection
- Bluetooth connection for backup controller (in case the LTE and WIFI connection failed)
- Bluetooth connection for wireless open/close sensor
- 2 independent relay outputs for triggering the gate control (dry contacts)
- 2 contact inputs for wired open/close sensor (gate status monitoring)

The **Door Master 300 W4G** is an internet based remote controller which means, for using the smartphone application the Door Master 300 and the operating smartphone should also be connected to the internet. The Door Master 300 has a built in backup bluetooth connection (in case the internet connection failure) for operating the gates locally, this feature provides the devices perfect operating for the users. The connection and communication has a AES-128 encryption.

1.1 Advantages

- Handling up to 300 User, with caller ID and smartphone access rights assigned
- Managing and monitoring 2 separate gates
- Notifications for gate opening and closing with PUSH notifications
- Alarm can be set in case the gate is left open
- Automatic gate opening period can be set (e.g. M-F / 08h-17h)
- 2 types of opening sensor management (wired or wireless)
- The device can be managed remotely via the website
- User rights can be managed through the website
- Event list
- [Exportable/importable client list and editable by external application](#)

1.2 Operation

When dialing the phone number of the inserted SIM card or control the unit from the PULOWARE mobile app, it closes the output contact for 1 second (in default setting) and sends the dry contact signal to the connected "open/close" input of any gate drive controller. The product includes 2 relays for controlling 2 gates, dedicated at the application and assigned to the caller number at the caller ID recognition.

In the case of call control, the unit recognizes the user's pre-set telephone number and, if it matches the set permissions, controls the set output relay. Since call control requires only the recognition of the caller number, the unit it will reject the call after the recognition of the telephone number, thus making the control cost-free.

The information of the gate status (which is OPEN or CLOSED) is displayed from the position of the opening sensor. When opened or closed, the unit can send a notification to users, giving a visual indication of the garage door status and the identification of who opened or closed the door.

2 Appearance



Explanation of symbols:

- 1 Connector for connection to gate controls

IN2/IN2	IN1/IN1	REL2/REL2	REL1/REL1	DC+	DC-
Opening sensor input for gate 2	Opening sensor input for gate 1	Pulse control relay for controlling of gate 2	Pulse control relay for controlling of gate 1	Positive voltage supply	Negative voltage supply

When inputs marked with same label are connected to each other, the status of that door will become closed. The output terminals labeled with same name are relay outlets, providing a dry contact to each other for one second after the control command is received. If required, the output pulse time (default 1sec) can be set or the relay switched to bistable mode, which means that each time a control command is sent, it only changes state and remains in that state until the next control command.

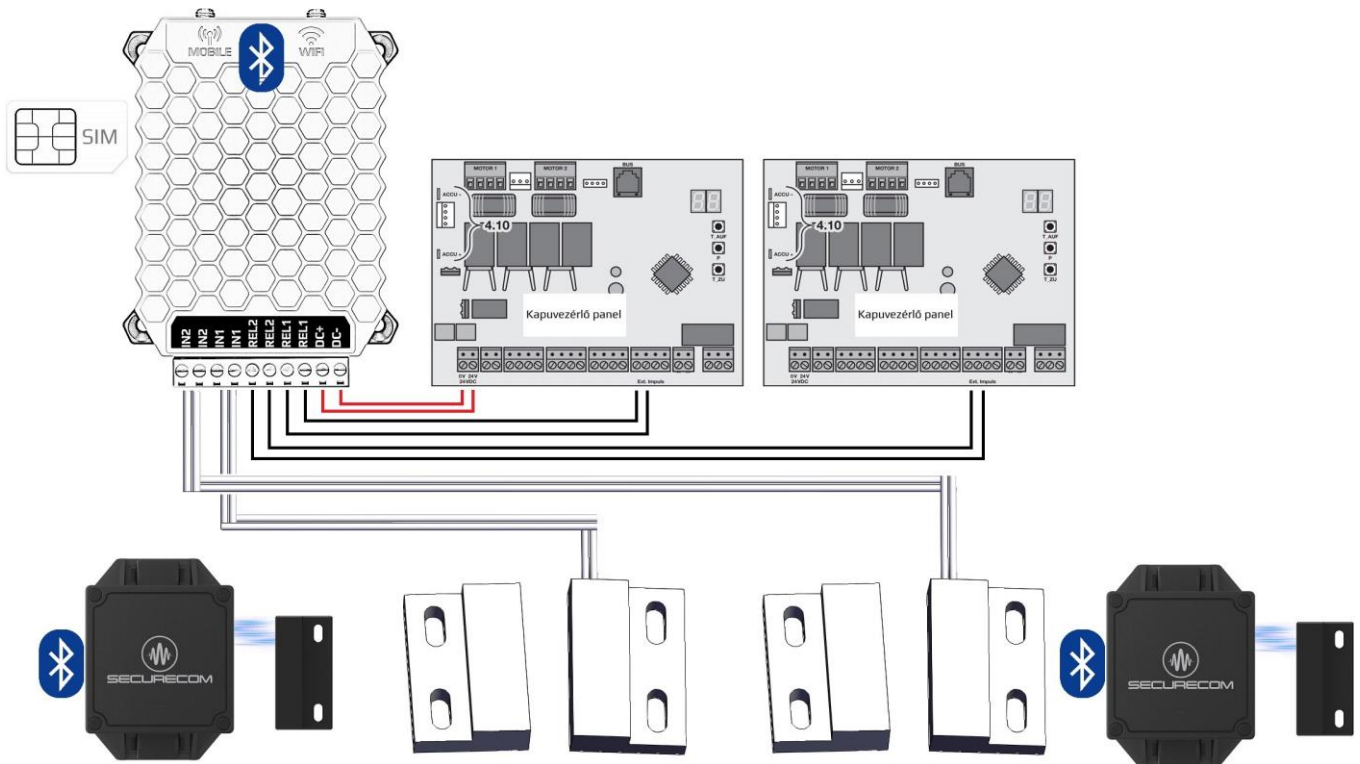
The supply voltage input is DC only with an operating range of 9-30VDC.

- 2 Mobil network antenna connector
- 3 WIFI network antenna connector
- 4 WIFI hot-spot and factory default button
- 5 Product identifier sticker

TYPE:	SERIAL No:	DEVICE ID:	QR code
Door Master 300 W4G	Production number	Device ID for mobile app and remote WEB access	Device identifier for adding the device to the smartphone

- 6 WIFI connection status LED
- 7 Serial port for diagnostics
- 8 USB mini B connector for computer configuration
- 9 Mobile network connection status LED
- 10 SIM card holder

3 Connection diagram



The figure shows the possible connection options for up to 2 different gate controllers. In this case, the unit is powered by only one of the gate controllers or from an external power supply. The relays trigger the opening or closing of the gate potential-free. Monitoring of the gate position (open or closed) can be done by wired or wireless SECURECOM DM-RF opening sensor.

4 Settings

The device settings must be made on SecurecomConfigurator program, witch is downloadable from this link: <https://securecom.eu/dm300-w4g> . After downloading and running the program, connect the device to the computer through the USB port and click on connect.

SECURECOM Configurator v2.69

Type: Door Master 300 W4G
Firmware: v2.4.602
Device ID: 6628875cccf3d1fa

EN DE HU

LATEST EVENTS

MODULE STATUS		TIME PERMISSION SETTINGS		GATE CONTROL WITH CALLER IDENTIFICATION					
Mobile network:	E-UTRAN (4G) Yettel HU Yettel HU	Control period 1:	Edit...	<input type="checkbox"/>	Dusko	+36202538221	Always allowed	<input type="checkbox"/>	<input type="checkbox"/>
Network signal (%):	80%	Control period 2:	Edit...	<input type="checkbox"/>	Milan	+36306593974	Control period 1	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WIFI network:	TP-Link_9678	Control period 3:	Edit...						
WIFI signal:	51% [-65 dBm]	Control period 4:	Edit...						
Limit switch:	1 2	GATE 1 SETTINGS							
Outputs:	1 2	Gate position monitoring:	RF limit switch						
Supply voltage:	-	RF limit switch ID:	7161						
MODEM AND GPRS SETTINGS		Alert when gate was left open:	None						
PIN code:		Auto-open enabled:	No						
GPRS APN:	online	Auto-open time matrix:	Edit...						
User:		GATE 2 SETTINGS							
Password:		Gate position monitoring:	IN2 limit switch						
SMS forward number:		RF limit switch ID:							
		Alert when gate was left open:	None						
		Auto-open enabled:	No						
		Auto-open time matrix:	Edit...						

Setup starts by configuring the device's network connection. The device can be controlled either by a call or from an application, or both channels, so the device's connection must be configured as required.

- When using mobile call control, i.e. caller ID, there is no need to set up a mobile data network connection (APN), only the basic requirements for the SIM card which are described in the next section.
- When controlling from a mobile app, you need to configure either the mobile network connection or the WIFI connection, or you should configure both in parallel for near 100% availability.

4.1 Mobile network connection settings

To set up the connection to the mobile network, insert a suitable SIM card in the SIM card holder marked **10** on the side of the device (as indicated on the back). The SIM must fulfill with the following requirements:

- be able to make voice calls and the caller ID display should be active (in case of caller ID recognition)
- mobile data capable (if device is controlled by an application)
- APN connection details must be known
- the PIN of the card shall be known or PIN request disabled

If PIN code request is enabled on the card, you must enter the code in the PIN code field.

To establish a data connection, you must enter the Internet connection details provided by your service provider (usually there is no User and Password, only APN ID). Example for a prepaid Telekom SIM card:







MODEM AND GPRS SETTINGS	
PIN code:	
GPRS APN:	online
User:	
Password:	
SMS forward number:	

After the data is uploaded, the module reboots and connects to the network in about 30-100 seconds.

If successful, the status LED marked **9** will change from red to green flashing light. In case of a communication failure, the red indicator will continue to flash after 100 seconds, indicating a connection error. In the event of a fault, the exact description of the fault will be displayed in text in the LATEST EVENTS window.

4.2 Setting the device WIFI connection using PC software

When setting up WIFI network, only connect to 2.4GHz network for proper operation and should not be mixed with the 5GHz network

MODULE STATUS	
Mobile network:	E-UTRAN (4G) Yettel HU Yettel HU
Network signal (%):	80%
WIFI network:	TP-Link_9678 1. 
WIFI signal:	51% [-65 dBm]
Limit switch:	 
Outputs:	  
Supply voltage:	-



The screenshot shows a 'Wifi setup' window with the following elements:

- 1.** A gear icon next to the selected network name 'TP-Link_9678'.
- 2.** A 'Scan' button next to the 'Access point name' dropdown menu.
- 3.** A password input field containing 'xxxxxxx'.
- 4.** A 'Save' button at the bottom.

1. WIFI settings can be reached by clicking on the gear icon
2. By clicking on scan button it will list the available WIFI networks
3. Type in the WIFI networks password
4. By clicking on save button the device will connect to the network

If the WIFI network name (SSID) and the password are correct and the device can connect to the Internet, the LED will start flashing green. If the connection fails, the LED flashes red.

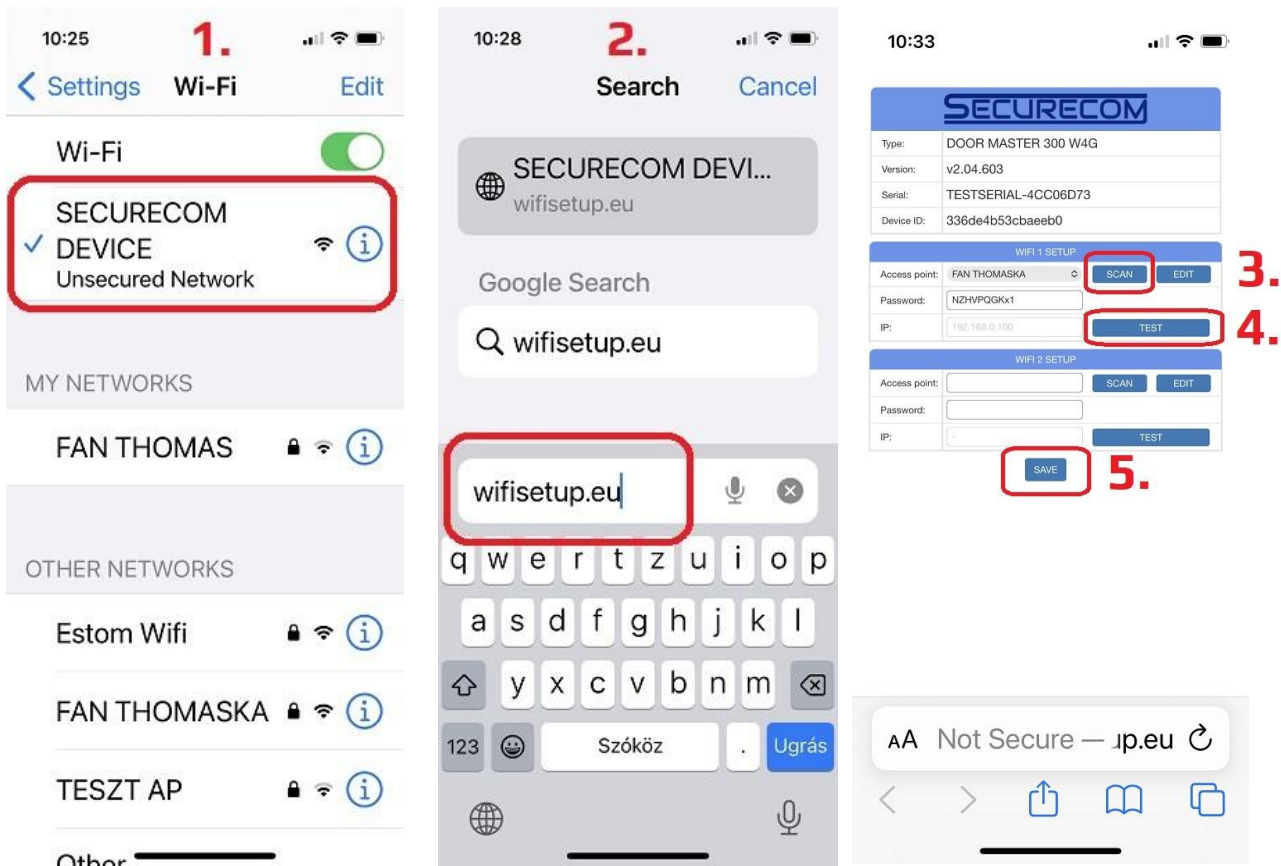
4.3 Setting up the WIFI connection with smartphone (alternative mode)

This method is used when it is not possible to configure the device with PC program. To make the configuration using smartphone, the unit's own WEB page must be accessed, which is enabled with a short press of the SET/RESET button 4. Then, the alternating flashing of the green/red light indicates the "HOTSPOT" mode, in which the unit broadcasts a dedicated WIFI network called **SECURECOM DEVICE** for the purpose of setting up its Internet connection. When a WIFI-enabled phone or computer is connected to this network, use a WEB browser to access the WEB page with the settings.

Accessing the unit's WEB site and steps to set up the connection

Press the SET/RESET button 4, the device entering the hot-spot mode and the status light will start flashing alternately green/red.

1. Find and connect to the SECURECOM DEVICE network in the WIFI networks on your smartphone.
IMPORTANT: turn off the mobile internet access from your phone during the setup, otherwise the web page of the unit will be replaced by the web site on internet.
2. After connecting to WIFI network, start the browser and open the web page: **wifisetup.eu**
That page is displayed by the Door Master 300 W4G and presents the available WIFI settings:



On the Door Master 300 W4G website, you can set up 2 different WIFI router connections by entering the network and password of your choice. The WIFI networks are back-up for each other, i.e. if the Internet connection on the WIFI1 network is lost, it will switch to WIFI2 and vice versa.

3. Press **SCAN** to list the available networks, select the appropriate network and enter the network password.
4. Press the **TEST** button to check if the connection was successful. If the password is correct, the device will receive an IP address. If it does not receive an address, either the password is incorrect or the connection has been interrupted.
5. Press **SAVE** to save the settings.

After that, the mobile internet access on the smartphone can be switched back on, and is even mandatory, as a mobile internet connection is a prerequisite for operating the app and control the device!

4.4 Setting up control validity periods

Different schedules, i.e. periods when user can control (logon), can be assigned to users. Control periods can be defined by creating schemas. There are a total of 6 different access rights schemes that can be assigned to each user. 2 are predefined (always allowed and always denied) and 4 can be edited individually. The system will execute control requests from a user within the selected periods and reject the command outside of these periods.

TIME PERMISSION SETTINGS	
Control period 1:	Edit...
Control period 2:	Edit...
Control period 3:	Edit...
Control period 4:	Edit...

	Hours																							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

[Save](#)

The green fields indicate the period with granted access, which can be changed by simply clicking on them with the mouse, i.e. the allowed hours can be switched on/off in the selected scheme. The defined time schemes can then be assigned to user phone numbers and mobile app IDs.

4.5 Setting up additional features

In addition to control by call or from the app, the unit can provide additional features that can be set up using the PC configurator or via the puloware.com website. The operation of these features requires the presence of a door open/close sensor, so it is imperative to install it!

4.5.1 Gate position monitoring

The position of the gate or gates can be monitored by installing a door open/close sensor, which can be wired (IN1 limit switch / IN2 limit switch) or wireless (RF limit switch). In the example below, the position of gate 2 is monitored with wired and gate 1 with wireless sensor.

GATE 1 SETTINGS		GATE 2 SETTINGS	
Gate position monitoring:	RF limit switch	Gate position monitoring:	IN2 limit switch
RF limit switch ID:	7161	RF limit switch ID:	
Alert when gate was left open:	None	Alert when gate was left open:	None
Auto-open enabled:	No	Auto-open enabled:	No
Auto-open time matrix:	Edit...	Auto-open time matrix:	Edit...

- When the limit switch **IN1** or **IN2** is selected, the device monitors the closed or open position of the gate by means of a magnetic opening sensor connected to the **LIMIT SWITCH** input.
- When the RF limit switch is selected, the unit waits for signals from the **SECURECOM DM-RF** auxiliary radio opening detector.

After selecting the RF limit switch option, the 4-digit identifier of the RF transmitter must be entered, as shown in the picture. The Door Master 300 W4G unit will then detect the status information sent by the opening sensor. By installing any of the opening sensors, the door status will be visible through the application and when opening or closing, the unit can send a message in push notification if the user requests it.

4.5.2 Alert if the gate is left open

Warning notification will be send in case the gate is left opened for longer time than set. During the automatic open mode this signal is disabled. The alarm notification can be turned on/off remotely for any user.

GATE 2 SETTINGS	
Gate position monitoring:	RF limit switch
RF limit switch ID:	6d2f
Alert when gate was left open:	None
Auto-open enabled:	None
Auto-open time matrix:	2 mins 5 mins 10 mins 20 mins 30 mins 1 hour

4.5.3 Automatic opening hours

The function performs the scheduled opening of gates or barriers. Once enabled, you can set the hours at which the gate should be kept open continuously. During the selected periods (marked in green), the unit keeps the relay output continuously active, avoiding automatic reclosing of the gates. In case the gate would ignore the continuous control of the relay and would lock back, a programmable timer can be used to disable the drive power during the opening periods (e.g. Finder 80010240).

GATE 2 SETTINGS	
Gate position monitoring:	RF limit switch
RF limit switch ID:	6d2f
Alert when gate was left open:	None
Auto-open enabled:	Yes
Auto-open time matrix:	Edit...

	Hours																							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday																								
Tuesday																								
Wednesday																								
Thursday																								
Friday																								
Saturday																								
Sunday																								

Save

The green squares indicate the selected period when the gate should be kept open. The selected hours can be changed by clicking on the desired square.

4.5.4 Change the timing of relay output

The output relays switch a short-circuit pulse of 1 second in case of control (in default setting). If the application requires, the switching time and the nature of the control can be changed. To change the settings, click the gear icon at the end of the OUTPUTS field in the MODULE STATUS window. In bistable mode, the relay does not operate pulse by pulse, but changes state every time it is switched.

MODULE STATUS	
Data connection:	E-UTRAN (4G) Telekom HU Telekom HU
Network signal (%):	67 %
WIFI network:	FAN THOMASKA
WIFI signal:	
Limit switch:	1 2
Outputs:	1 2
Supply voltage:	-

Control duration	
Output 1:	Monostable 1 sec(s)
Output 2:	Monostable 1 sec(s)
	Bistable
	Monostable

SAVE

4.6 Gate control by caller phone number identification

This function matches the incoming caller ID with the phone numbers in the predefined user list. If found in the list and eligible for entry (e.g. valid entry period) it controls the corresponding output relay of the unit. The device can recognize up to 300 caller IDs, with their register of privileges, which data editing is locally restricted.

When installed at the gate site, a maximum of 20 caller numbers can be registered in the device, and the more other users can be registered and administered via the pulware.com website. As all settings of the product can be managed remotely, it is strongly recommended that only the Internet network connection is configured during installation. Once connected to the Internet, all user needs can be set remotely with maximum convenience.

Name	Phone number	Time	Relay 1	Relay 2
User 1	+3630111111111	Control period 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User 2	+3620222222222	Always allowed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User 3	+3620333333333	Control period 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User 4	+3620444444444	Always allowed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User 5	+3620555555555	Always allowed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User 6	+3630666666666	Control period 3	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User 7	+3630777777777	Always allowed	<input type="checkbox"/>	<input checked="" type="checkbox"/>

After pressing **+ ADD PHONE NUMBER**, a new field appears at the bottom of the list, where you can enter the user's name, phone number, access authorization time, and the relay of controllable gate number 1 and/or 2. After any modification, the data must be saved to the device using the **SAVE PHONE NUMBER LIST** button, to make the change valid.

To delete any users, drag the mouse to the right of the list next to the scroll bar, where a red x appears. Click on this to delete the user from the list. Saving the modified list to the device is also required here as mentioned above.

4.6.1 Exportable/importable client list

It is now possible to easily manage the modification of caller numbers and privileges by editing them with an external program. The format is .csv extension which can be used with various programs (e.g. MS Excel) can be easily edited. Customer list phone numbers can be exported from the unit or the edited file can be imported into the unit memory. This method makes it easy to manage an access area with access from multiple directions and through multiple gates, as it allows you to easily and conveniently synchronize the privileges in the devices.

The feature is only available from the pulware.com website, not with on-site USB configuration!

Pressing EXPORT button will create a **PhoneNumbers.csv** file in which the user data in the unit's memory and the associated privileges will be saved in the following format.

Name	Phone number	WIEGAND codes	Control rights	Relay 1	Relay 2
Administrator	06301234567		1	1	1
USER1	+36301234567		C1	1	0
USER2	+36201234567		C2	0	1
USER3	+36701234567		C3	1	0
USER4	+36901234567		C4	1	1
USER5	003600000000		0	0	0
USER123	0049125615452		1	0	0

This table can be further edited or extended with an external program according to the template, where the parameters for the column names can be specified as follows.

Name	User name, any character can be entered here without restriction
Phone number	User's phone number, where any number and the + character are accepted
Control rights	Set entry periods, according to the chapter 4.4 0= Always disallowed C1= Control period 1 C2= Control period 2 C3= Control period 3 C4= Control period 4 1= Always allowed
Relay 1	0= not allowed / 1= allowed
Relay 2	0= not allowed / 1= allowed

The edited table can be added to the settings using the IMPORT button, and then downloaded to the device's memory using the Download settings icon. 

4.7 Control with any caller ID

Selecting this function removes the restriction to control the output relays only for incoming caller IDs from pre-recorded and authorized telephone numbers. With this option, it is possible to control the unit from any number which, when controlled, will activate both outputs simultaneously.

GATE CONTROL WITH CALLER IDENTIFICATION					
<input checked="" type="checkbox"/> Control with any phone call					
	Name	Phone number	Period permission	Relay 1	Relay 2
<input type="checkbox"/>	User1	06201234567	Always allowed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	User2	06307654321	Always allowed	<input checked="" type="checkbox"/>	<input type="checkbox"/>

5 Status lights

The status indicators **6** and **9** provide the following status information.

	Mobile network status 9	WIFI network status 6
Constant RED	APN or SIM missing	No network settings
Blinking RED	Connection in progress, but after 120 seconds: incorrect setting	Faulty settings
Blinking GREEN	Normal operation	Normal operation
GREEN/RED changing	-	WIFI setup ("HOTSPOT" mode)

More detailed status information is available in the MODULE STATUS panel and in the LATEST EVENTS window of the SecurecomConfigurator.exe program.

6 Factory default settings


All settings can be deleted from the device and all existing connections to user phone apps can be terminated, according to the factory default setting. This operation can only be made if the device is in normal operating mode which means its connected to the server and at least one LED is blinking green.

To reset the device to factory default, press and hold the SET/RESET **4** button for 30 seconds while the LED **6** starts flashing red/green, indicating that the erase procedure is in progress. Hold on the button until constant red light - this means that the reset procedure is finished.

Caution: after defaulting the device all setting are permanently erased!

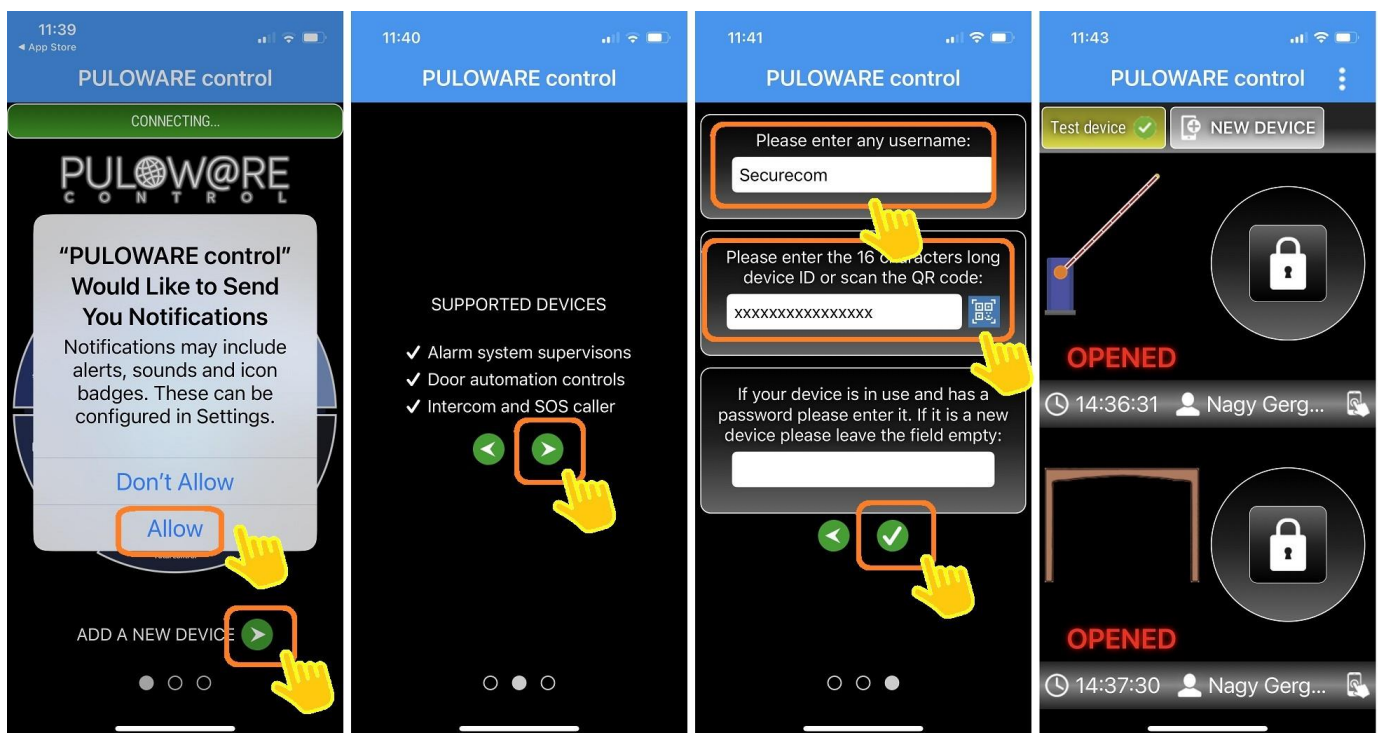
7 Setting up and using the mobile app



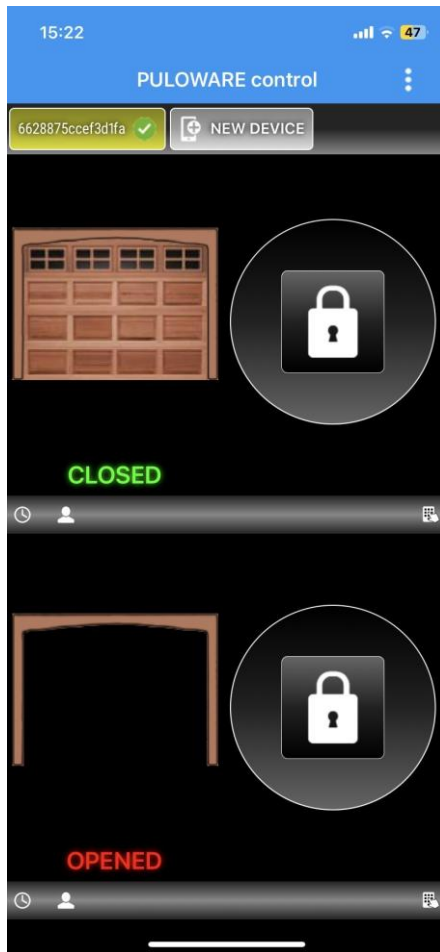
The PULOWARE  is a free application which can be downloaded to any smartphone, based on the phones platform (**Google Play** or **App Store**). Start the application and follow the next steps.

7.1 Application setup in first start

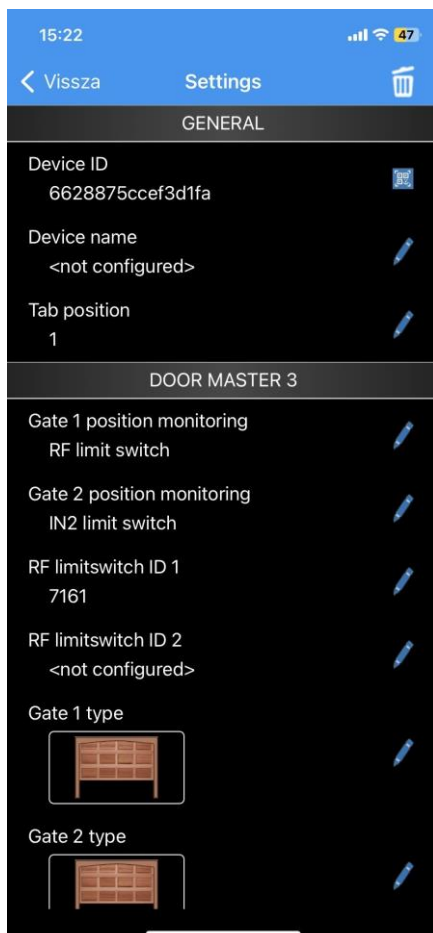
1. Allow the pop up window
2. Press the green arrow icon to move to the next page
3. Press again the green arrow icon to move to the next page
4. Enter any username that would identify your phone (you)
5. Enter the 16 character long Device ID. This number can be found on the sticker placed at the back of the device, or on the quick start in the box. You can enter the number manually or scan the QR code to enter it. For that, you must tap the blue icon with form of a QR code to open the reader and after that present the Device ID QR to the smartphone camera. Finally, enter the device password. By default, there is no password for devices so leave the password field empty when a new device is assigned. A device password can be added, changed or deleted on the **puloware.com** web site, after the device is added to the users account. If a password was once assigned to a device, it can not be added to any account or smartphone app without that password.
6. Press the green checkmark icon to add the device to your smartphone.



7.2 Application details and useful tips



- ➔ Main menu: Operator, Events, Setting
- ➔ Device list, other PULOWARE compatible devices
Drag/scroll the screen horizontally to view additional tools can be selected
- ➔ Gate 1 position (open/closed) and control push button which must be pressed and held down (2 seconds) until the circular status indicator rotates and the control starts
- ➔ Time and user name of the latest gate controlled by relay 1
- ➔ Gate 2 position (open/closed) and control push button which must be pressed and held down (2 seconds) until the circular status indicator rotates and the control starts
- ➔ Time and user name of the latest gate controlled by relay 2



- ➔ Bin icon to delete the device from the App
- ➔ Unique ID of the gate opener + QR code (touch the icon to display)
- ➔ The name of the device (changing this affects all users)
- ➔ The order in the main screen toolbar
- ➔ Selecting the opening sensor for gate 1 (none, IN1 wired, RF wireless)
- ➔ Selecting the opening sensor for gate 2 (none, IN2 wired, RF wireless)
- ➔ Identifier of the RF wireless open/close sensor for gate 1
- ➔ Identifier of the RF wireless open/close sensor for gate 2
- ➔ Selection of gate type 1 (sliding, opening, etc.)
- ➔ Selection of the type of gate 2 (sliding, opening, etc.)

8 Remote management, password protection and application restriction

All the advanced features of the Door Master 300 W4G are available via the IoT cloud-based server, accessible via www.puloware.com, but registration is required to use the website. Once registered, the device ID of the communicator must be added to the account to manage it. After logging in, the website looks like this:

The screenshot displays the Securecom web interface. At the top, it shows the account name 'c@c.hu', a 'LOGOUT' button, and the operator name. The main content is divided into several sections:

- DEVICES:** A list on the left showing 'DEMO SINGULAR WIFI', 'DEMO DOOR MASTER 3', and 'Test device' with their respective IDs and status icons. Below this is a summary table:

Number of devices:	1
Online devices:	1
Offline devices:	0

 A '+ ADD DEVICE' button is located below the summary.
- SECURECOM:** A central header for the selected device, showing 'TYPE: DOOR MASTER 300 W4G', 'FIRMWARE: v2.4.603', 'NAME: Test device', and 'Output mode: Negative impulse (1 sec)'. It includes several status icons.
- MODULE STATUS:** A section showing connection details: 'Data connection: E-UTRAN (4G) Telekom HU Telekom HU', 'Network signal (%): 67%', 'WIFI network: FAN', 'WIFI signal' (with a bar chart), 'Limit switch: 1 2', 'Outputs: 1 2', and 'Supply voltage: -'.
- MODEM AND GPRS SETTINGS:** A section with fields for 'PIN code', 'APN', 'User', 'Password', and 'SMS forward number'.
- TIME PERMISSION SETTINGS:** A table for defining control periods:

Control period 1:	Edit...
Control period 2:	Edit...
Control period 3:	Edit...
Control period 4:	Edit...
- GATE 1 SETTINGS:** Settings for the first gate, including 'Gate position monitoring: RF limit switch', 'RF limit switch ID: 6d2f', 'Alert when gate was left open: 10 mins', 'Auto-open enabled: Yes', and 'Auto-open time matrix: Edit...'.
- GATE 2 SETTINGS:** Settings for the second gate, including 'Gate position monitoring: RF limit switch', 'RF limit switch ID', 'Alert when gate was left open: None', 'Auto-open enabled: No', and 'Auto-open time matrix: Edit...'.
- GATE CONTROL SETTINGS:** A table for defining user permissions:

Name	Phone number	Time	Relay 1	Relay 2
User 1	+3630111111111	Control period 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User 2	+3620222222222	Always allowed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
- EVENT LIST:** A table showing a history of events:

Date/time	Event	CID	MS1	MS2
2023.06.04 13:14:22	Setup changed			
2023.06.02 13:11:20	Device restored			
2023.06.02 09:53:32	Device lost			
2023.06.01 13:45:13	Setup changed			
2023.06.01 13:44:51	Setup changed			
2023.06.01 13:01:35	Setup changed			
2023.05.31 15:46:49	Setup changed			
2023.05.31 14:38:32	Gate 1 opened			
2023.05.31 14:38:25	Gate 1 closed			
- MOBILE APP SETTINGS:** A yellow header section.
- MOBILE APP USERS:** A table showing app user details:

Phone	User	Last seen	APP enable	APP full access	APP push enable	Control period
iPhone	Securecom	2023.06.04 12:23:39	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Always allowed

The **DEVICES** bar on the left contains a list of the IDs already attached to the account, which for new registrations is obviously still empty. Below that, the **+ ADD DEVICE** button can be used to add new devices.

Adding device is performed by entering the Device ID, which is a 16-digit number and letter sequence that can be read off the back of the unit or from the mobile app installation guide. The password field on the new device should be left blank!



Then, by selecting (clicking on) the desired device from the list of already recorded identifiers, the product specific information will be displayed on the right side, which corresponds to the status information and configuration options displayed in Securecom Configurator software

8.1 Device password protection

By default, adding the device are not protected with a password. For increased security, a password can be set by clicking on the padlock icon in the administration window with the SECURECOM label. Once the password has been set, new users will can not add the device to their phone or Puloware account without this password. In case of forgotten password, it can be removed only by resetting to Factory Default! In this case all settings are deleted, and the device is removed from all phones and Puloware accounts!

8.2 Limiting mobile app users

By default, the PULOWARE application provides full access to all features of the registered devices, available to all users. If it is necessary to restrict or disable certain user functions, or to permanently delete a user, this can be made on the Puloware server page, at the **MOBILE APP USERS** table.

MOBILE APP USERS							
Phone	User	Last seen	APP enable	APP full access	APP push enable	Time matrix	
 M2101K7BNY	BaDphone	2023.05.22 16:36:40	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Always allowed	▼
 iPhone	Securecom	2023.05.22 16:34:36	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Control period 1	▼

You can restrict the user from controlling by deselecting the first checkbox. . The user will see the opening/closing when opening the application, but will no longer be able to send commands. With the second checkbox, the access to device setup and event list is inhibited. With the third checkbox you can control if the PUSH notifications are sent to that user. To remove a device from some phone, the mouse must be dragged to the end of the selected line and the delete icon will appear. Clicking on it removes the user (smartphone) from the list, and also deletes the device from the app on that smartphone.

9 Technical details

Supply voltage	9-24V DC
Maximum current consumption	500mA
Operating frequency	WIFI: 2.4 GHz, LTE (4G): B1/B3/B5/B7/B8/B20/B38/B40/B41
Relay load capacity	max. 2A @ max. 60V
Operating temperature	-40...+85°C
Dimensions	75x120x25mm
Environmental protection	IP40 (outdoor installation in protective box required)

10 Content of the package

- Door Master 300 W4G remote control device
- Antenna 2pcs (WIFI and 4G)
- Open/close sensor 1pc (reed relay + magnet + screws)
- USB cable
- Warranty ticket