PARADOX IP REPORTING TO IPRS7

Version 1.0

May 6th 2020
Created by: Victor Maciuca

Preface

This document will explain Paradox IPRS7 reporting in depth and will cover the following topics:

- Panel reporting configuration
- IPRS7 configuration and operation
- Receivers output configuration for CMS

General presentation

IP reporting to CMS was designed as a fast and reliable communication method, compared to the regular landline/GSM through DTMF reporting.

IP reporting structure

For IP reporting, the following components are required:

1. Field communication devices (IP150 or/and PCS devices) which are connected on the panel's serial port
2. Software receiver – IPR7
3. Automation software which is connected through serial connection or IP protocol (UDP) to IPRS7. This software is not developed by Paradox and will communicate with our receiver through one of the following open source protocols: ADEMCO 685, SURGARD MLR2-DG and RADIONICS 6500

Protocols

IPDOX protocol it's used between our field communication devices (IP150 or PCS) and our receivers. This is a proprietary protocol and due to security reasons, it cannot be shared for further integrations.

The protocols used on receivers' output are known protocols used in the physical security industry: ADEMCO 685, SURGARD MLR2-DG and RADIONICS 6500. Once the CMS software is compatible with one of these protocols, it can be integrated with our receivers.

1. Reporting configuration for EVO panels

1.1. Report codes configuration

Report codes can be programmed in Babyware, Panel programming -> Reporting -> Report Codes section. Reporting codes with 00 will not be transmitted and report codes with FF will be transmitted.

By default, all codes are 00 (no signal will be transmitted once the event occurs). These codes should be customized for each event.

If Contact ID report code format is used, then all events should be set as FF. Best practice: type “FF” in the main filed and press the extend button after. In this way all sub-fields will be automatically filled with FF code (Fig. 1). In this way the panel will follow a known Contact ID table for each report code.

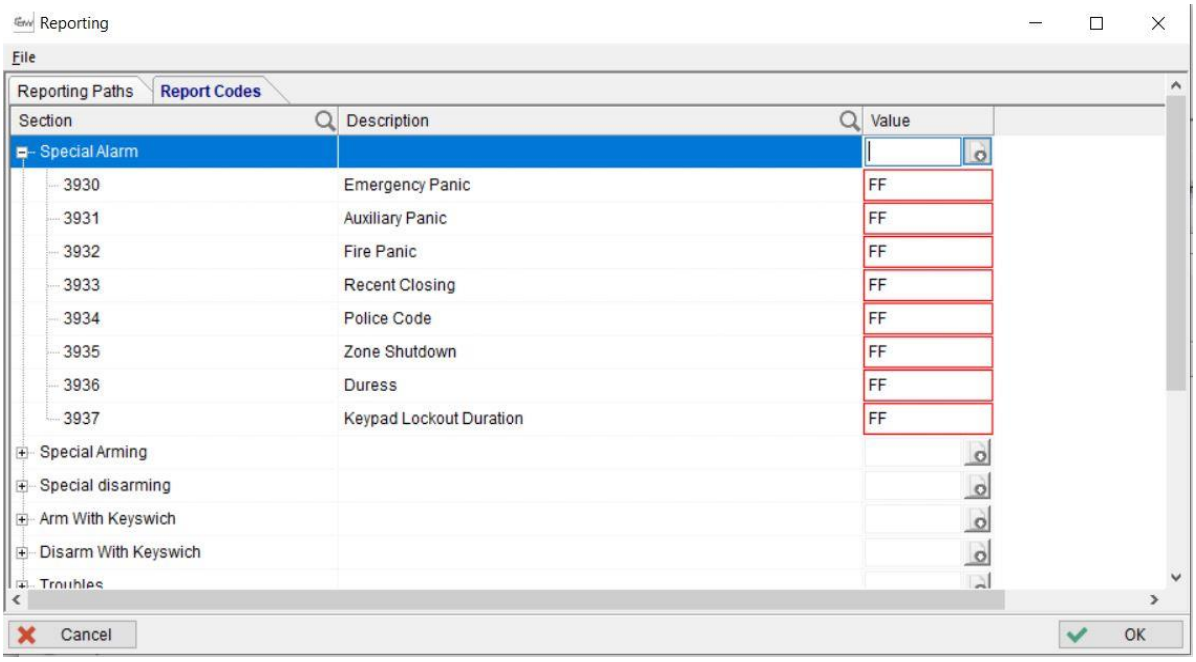


Fig. 1 Report Codes

1.2. Report codes format configuration

Report codes format can be configured in Panel programming -> Reporting -> Reporting paths -> Global Settings. The reporting codes format can be set for each receiver, from #1 to #4 (Fig. 2). Up to 4 receivers can be configured for reporting.

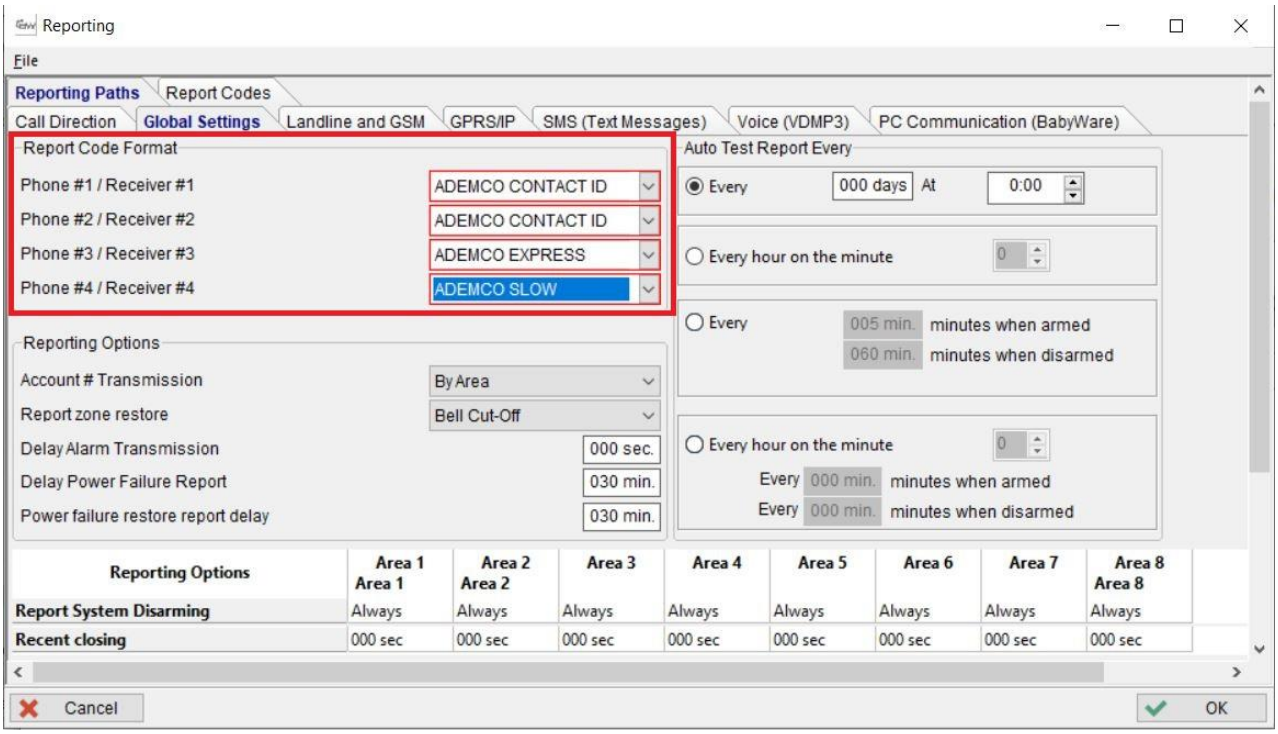


Fig. 2 Report Code Format

1.3. Central Station Info configuration

The receiver parameters need to be programmed in the Central Station Info section (Fig. 3) from the GPRS/IP tab. The following parameters should be programmed in Central station info tab:

a) Receiver's IP and port:
   For IPRS7, only WAN 1 IP and port needs to be filled. The second WAN and port are not used once an IPRS7 is used as receiver.
b) Receiver password - by default the IPRS7's password is 123456. This password is used only in registration step, not for receiver management. It can be changed from receiver's Setting tab – Input configuration.
c) Register button – after all receiver parameters are programed and sent to the panel, register button will be pressed.

d) IP Profile is used to set the security profile polling and supervision time of the communication module. More details can be found in receiver management chapters 3.

e) Area account is a 4 digits hexadecimal account used to identify the site or different areas of a system. All areas can be registered on the same account or different accounts for each area, if needed.

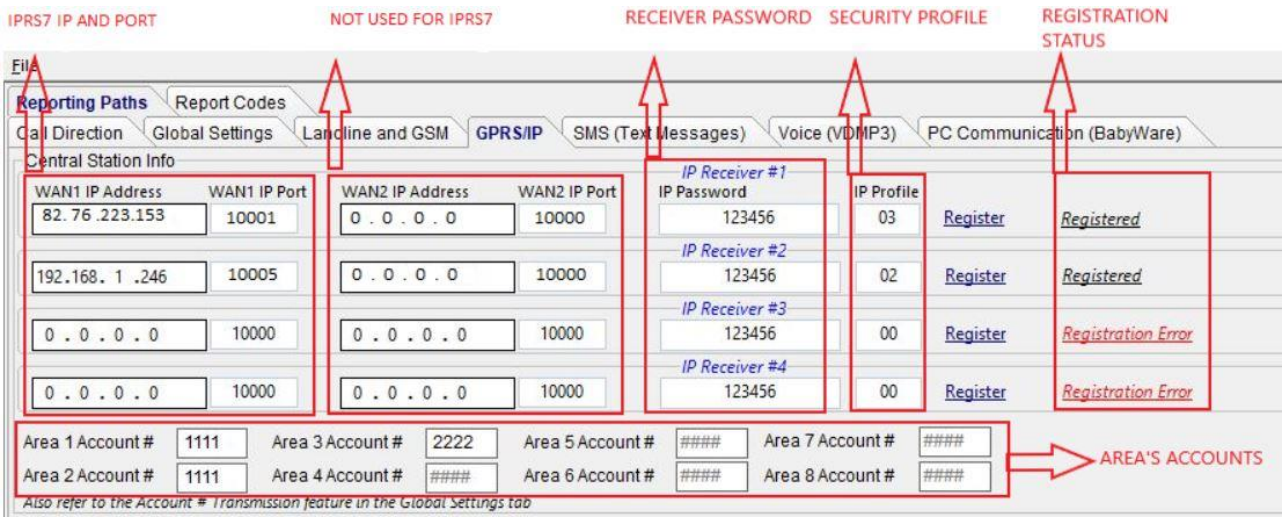


Fig. 3 Central station Info

1.4. Reporting options

The following reporting options (Fig.4) can be modified on panel programming:

a) Reporting (GPRS/IP) checkbox – this option is enabled by default. Once disabled, even if the reporting parameters are programmed there will be no signal sent to the receiver.

b) Dialer Channel - if dialer reporting is used also for the site, then dialer channel can be set as a backup to IP/GPRS reporting or in addition to the IP/GPRS reporting (same time)

c) GPRS/IP Service Failure – This option will set the behavior of the panel once the GPRS/IP service fails. The default option is Trouble Only. The option can be disabled or set as trouble when the system is disarmed and audible alarm when the system is armed.

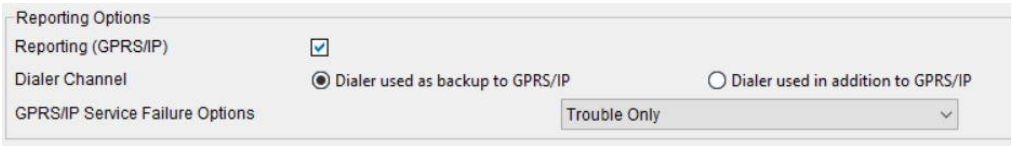


Fig. 4 Reporting options

1.5. GPRS Service Provider Info

If a PCS module (GPRS/3G/LTE communication) is used for reporting, then the SIM card APN, username and password should be filled, in order to be able to connect on carrier's data network (Fig. 5). Access Point Name, Username and password credentials can be sent through SMS commands as well.

Fig. 5 GPRS Service Provider Info

1.6. Event call direction

There are 4 event types which needs to be programmed to be reported to one or multiple receivers: Arming/Disarming, Alarm/Restore, Tamper/Restore and Trouble/Restore. (Fig. 6)

For example, Arming/Disarming can be programmed to report to Receiver 1 and Tamper to report to Receiver 2.

Troubles can be programmed to have backup on another receiver.

A maximum of 4 IP receivers can be programmed for EVO panels. By default, the panel is programmed to report only to first receiver. If more than one receiver is programmed, like the case from point 1.3, then the event call direction should be programmed as well as for the second receiver.

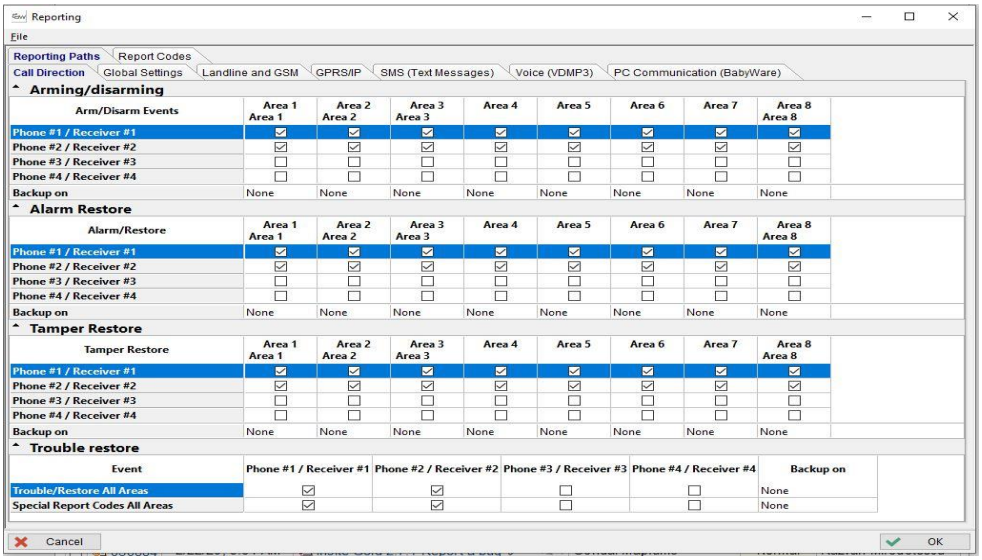


Fig. 6 Report call direction

2. Reporting configuration for MG/SP panels

2.1. Report codes configuration

Report codes can be programmed in Babyware, Panel programming -> Reporting -> Report Codes section. Reporting codes with 00 will not be transmitted and report codes with FF will be transmitted.

By default, all codes are 00 (no signal will be transmitted once the event occurs). These codes should be customized for each event.

If Contact ID report code format is used, then all events should be set as FF. Best practice: type "FF" in the main filed and press the extend button after. In this way all sub-fields will be automatically filled with FF code (Fig. 7). In this way the panel will follow a known Contact ID table for each report code.

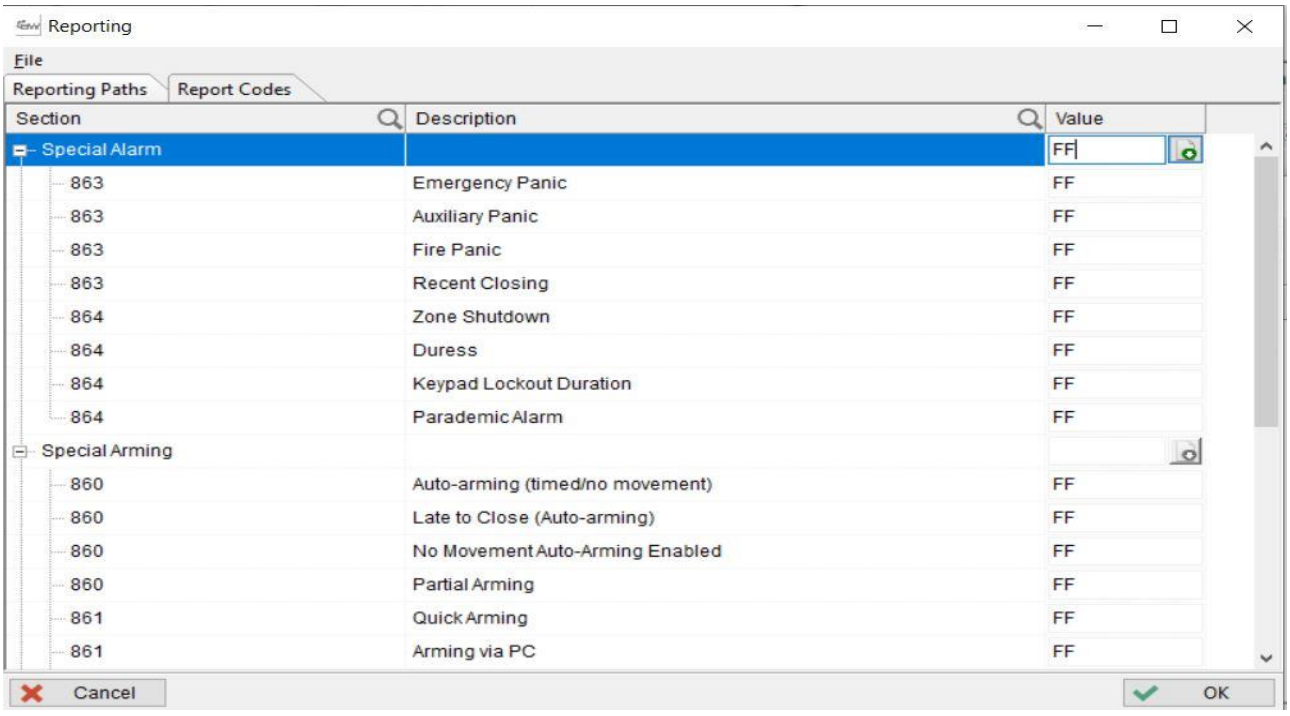


Fig. 7 Report Codes on MG/SP panels

2.2. Report codes format configuration

Report codes format can be configured in Panel programming -> Reporting -> Reporting paths -> Global Settings. The reporting codes format can be set for each receiver, maximum 2receivers can be configured for reporting. (Fig. 8).

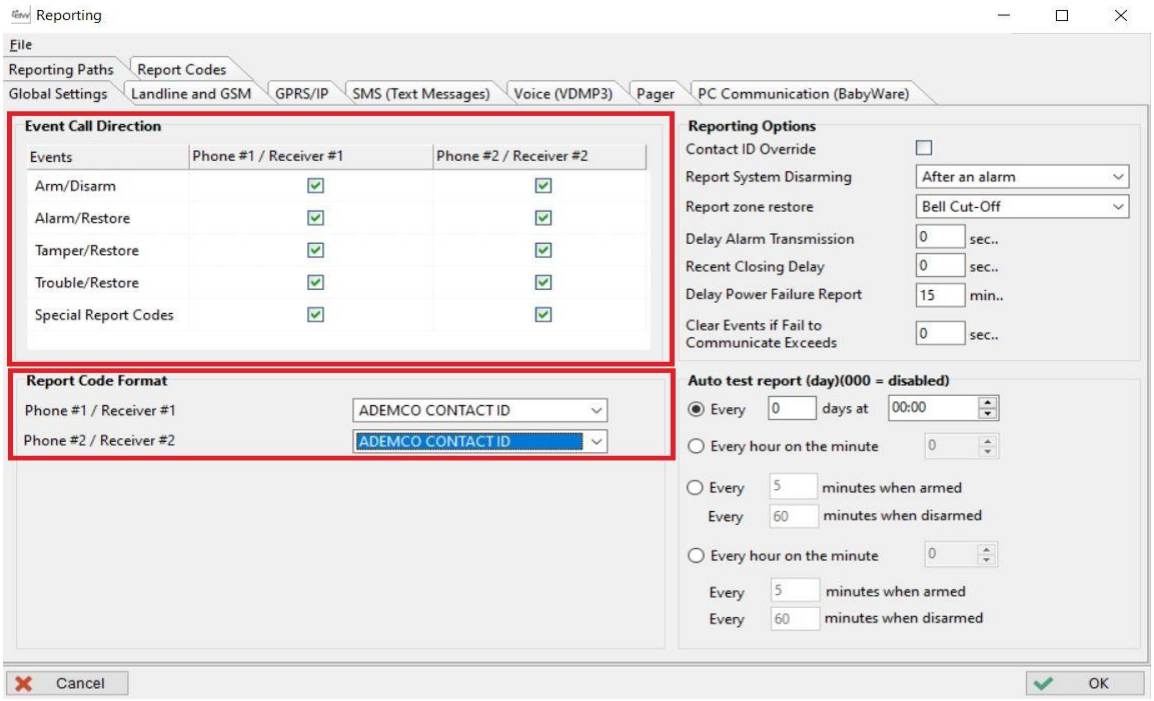


Fig. 8 Global settings

2.3. Central station info configuration

The receiver parameters need to be programmed in the Central Station Info section (Fig. 3) from the GPRS/IP tab. The following parameters should be programmed in Central station info tab:

a) Receiver's IP and port:
b) For IPRS7, only WAN 1 IP and port needs to be filled. The second WAN and port are not used once an IPRS7 is used as receiver.
c) Receiver password - by default the IPRS7's password is 123456. This password is used only in registration step, not for receiver management. It can be changed from receiver's Setting tab – Input configuration.
d) Register button – after all receiver parameters are programed and sent to the panel, register button will be pressed.

e) IP Profile is used to set the security profile polling and supervision time of the communication module. More details can be found in receiver management chapters 3.

f) Area account is a 4 digits hexadecimal account used to identify the site or different areas of a system. All areas can be registered on the same account or different accounts for each area, if needed.

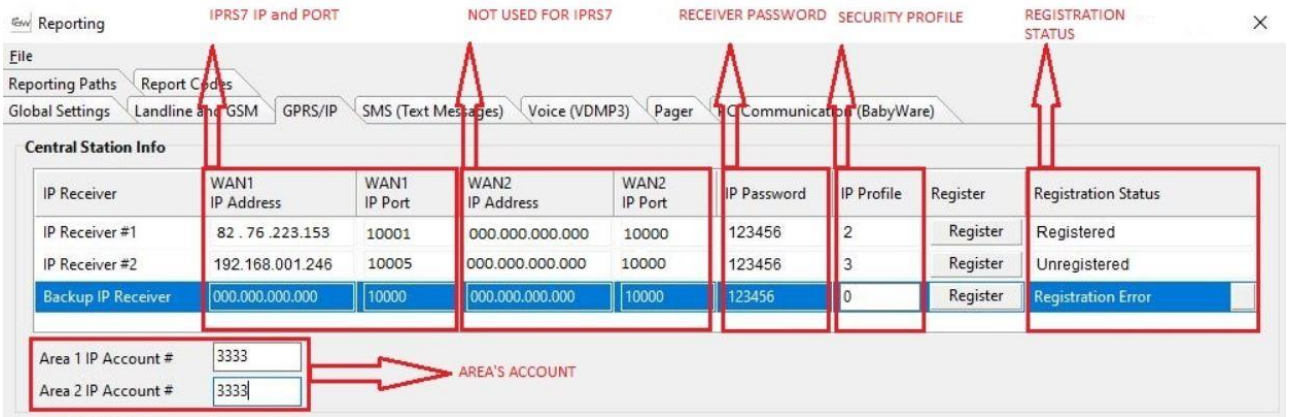


Fig. 9 Central station Info

2.4. Reporting options

Following reporting options (Fig. 10) can be modified on panel programming:

g) Reporting (GPRS/IP) checkbox – this option is enabled by default. Once disabled, even if the reporting parameters are programmed there will be no signals sent to receiver.

h) Diale Channel - if dialer reporting is used also for the site, then dialer channel can be set as a backup to IP/GPRS reporting or in addition to the IP/GPRS reporting (same time)

i) GPRS/IP Service Failure – This option will set the behavior of the panel once the GPRS/IP service fails. The default option is Trouble Only. The option can be disabled or set as trouble when the system is disarmed and audible alarm when the system is armed.

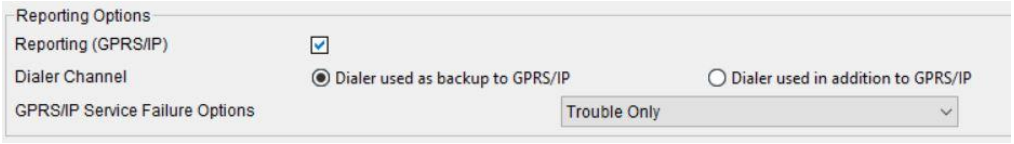


Fig. 10 Reporting options

2.5. GPRS Service Provider Info

If a PCS module (GPRS/3G/LTE communication) is used for reporting, then the SIM card APN, username and password should be filled, in order to be able to connect on carrier's data network (Fig. 11). APN, Username and password credentials can be sent through SMS commands as well.

Fig. 11 GPRS Service Provider Info

3. IPRS7's accounts and settings management

The IPRS7 is a software receiver which is running on Windows (only) based computers. It is designed to emulate the IPR512 IP/GPRS receiver directly from a computer without the need for a hardware receiver.

3.1. Input configuration

The Input configuration (Fig. 12) is used to set parameters used for communication with field devices. The following parameters needs to be set in this tab:

- receiver password (used in the registration step on panel side)
- network configuration – IP and port
- GSM/GPRS modem configuration if SMS reporting is used as a backup to the GPRS reporting. The IPRS7 will check all available network interface cards (NICs) of the PC and the operator will need to select the proper interface (IP). If the IPRS7 is used in an Internet-based network, the IP port should be forwarded in the router configuration.

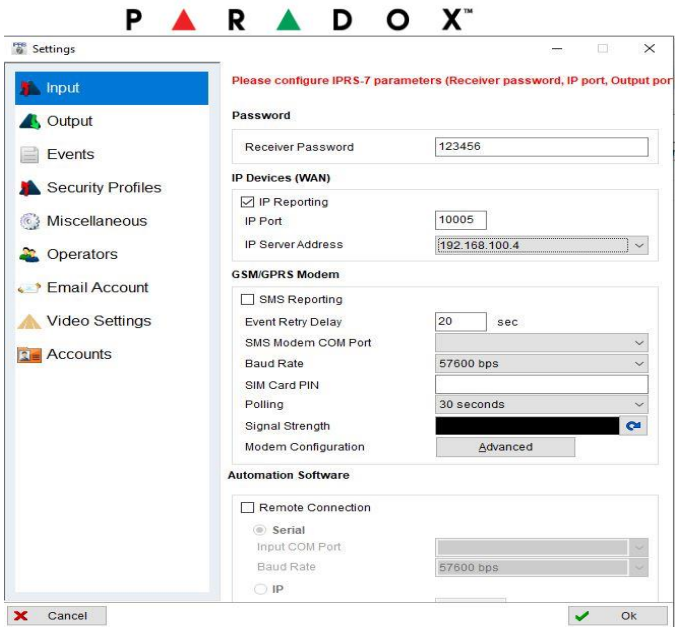


Fig. 12 IPRS7 input settings

3.2. Output configuration

The output configuration (Fig. 12) will allow communication with the automation software (CMS). IPRS7 supports serial connection as well as IP connection:

1. Serial connection – the PC should have installed a serial (RS-232) card which will be linked with another PC which runs the automation software (CMS).
2. IP connection - the IPRS7 will open a port to communicate with through IP with the automation software (CMS).

3.2.1. Configuration of the IPR512 output for IP connection:

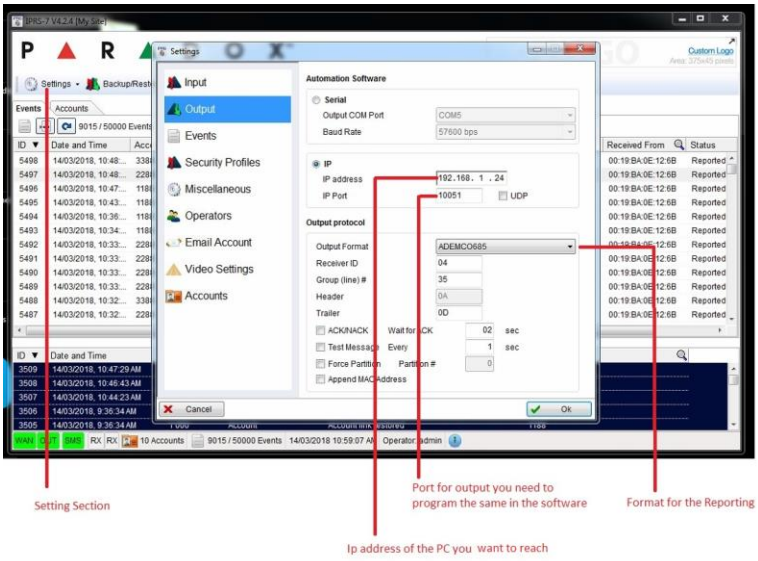


Fig.12 IPRS7 output configuration

1- Click on settings
2- Click on Output
3- Program the IP address (this is the address of the PC you want to reach)
4- Program the IP port (this is the port for the application you want to reach)
5- Select to output format to ADEMCO685, SURGARD MLR2-DG or RADIONICS 6500.

3.2.2. Configuration of the automation software

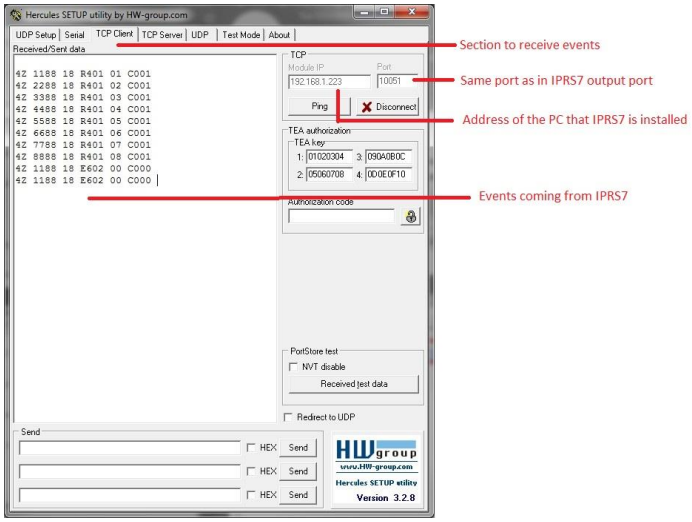


Fig. 13 CMS configuration for IP reporting

1- Open Hercules software
2- Click on TCP client
3- Program the IP address of the PC that the IPRS7 is installed
4- Program the same port that you have configured in the IPRS7

3.3. Events configuration

In the Events tab (Fig. 14) are two main categories of events which can be customized on IPRS7.

The first category is related to accounts (account supervision loss/restore and account registration/deletion).

The second category is related to receiver internal events. All these events could be configured per the CMS recommendations. Receiver events will be reported on a specific account which should be configured in the same page.

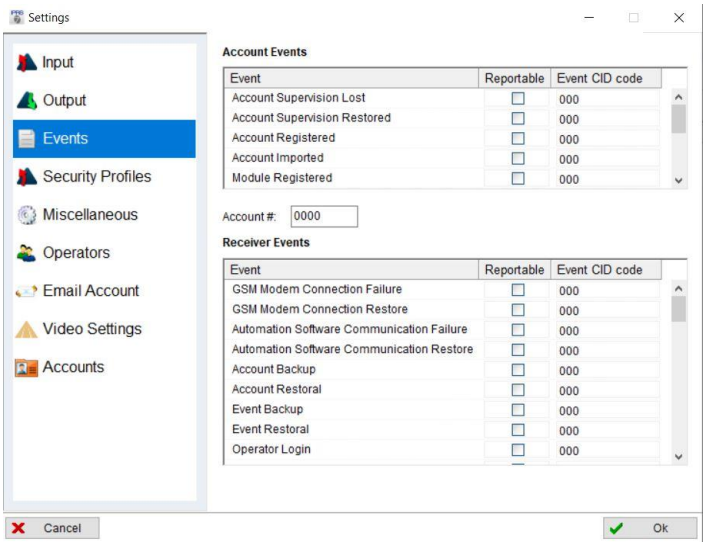


Fig. 14 Events tab

3.4. Security profiles

The IP reporting devices send a presence message to the receiver at intervals defined by the module polling time. If the receiver does not receive any presence messages within the receiver supervision time, the receiver can report a supervision loss of the account. There are five security profiles by default with specific polling times and supervision times. These security profiles can be modified using the Show Advanced option.

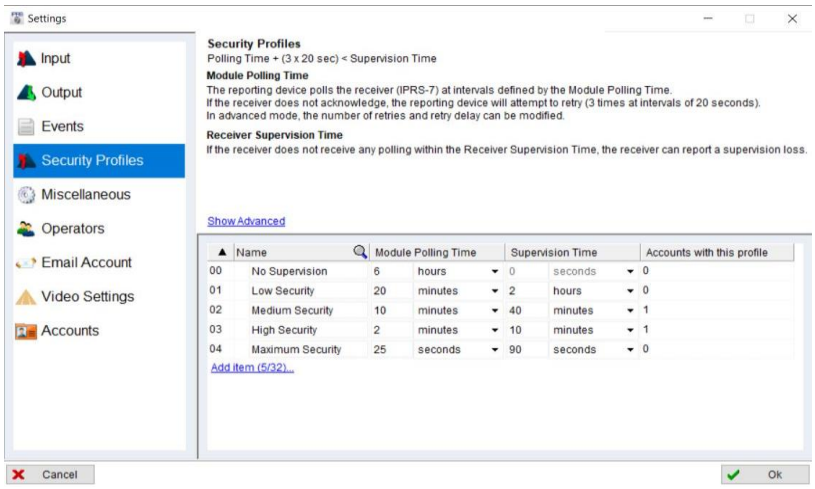


Fig. 15 IPRS7 Security Profiles

3.5. Miscellaneous

In this tab, the site name, custom logo and session expiry time can be set.

There are options to activate the logging mechanism of the receiver: log file size, log file lifetime and logs folder. These should be activated if something goes wrong with the receiver and logs are requested by Paradox Support Team in order to be investigated by the R&D.

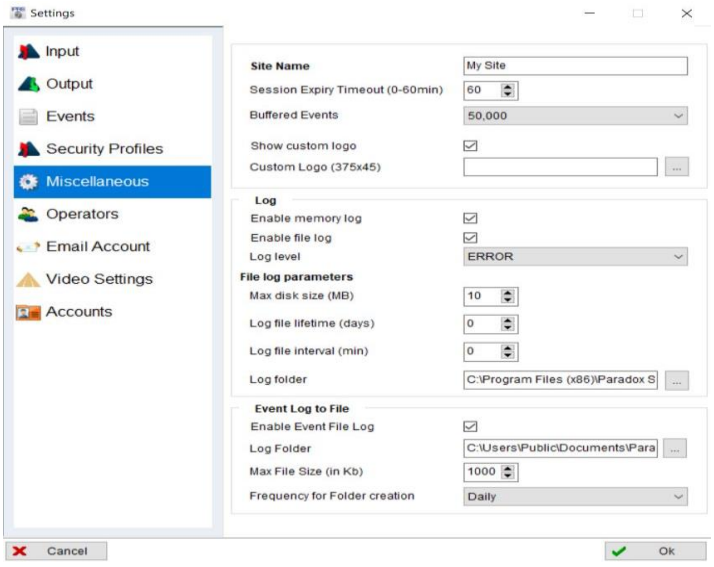


Fig. 16 Miscellaneous

3.6. Operators

Up to 256 operators could be added for IPRS7 login. It's recommended to add an email address for each operator for password recovery purposes. In case that a password is forgotten, the operator has the option to receive the password over email once the fields from chapter 3.7 are properly configured.

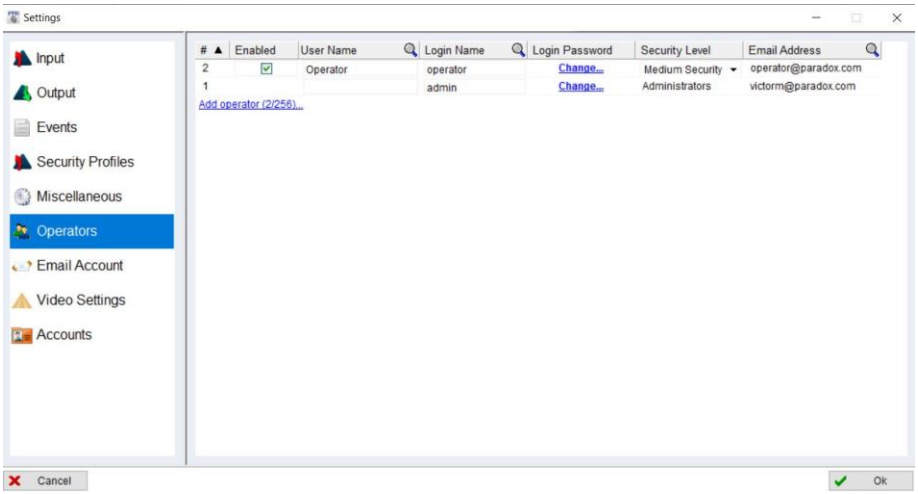


Fig. 17 Operators

3.7. Email account

In this section an email account can be set to recover an operator's password. Once the email is properly configured, by pressing the Forgot password button in the login dialog box, the password will be received on the email address added for each operator.

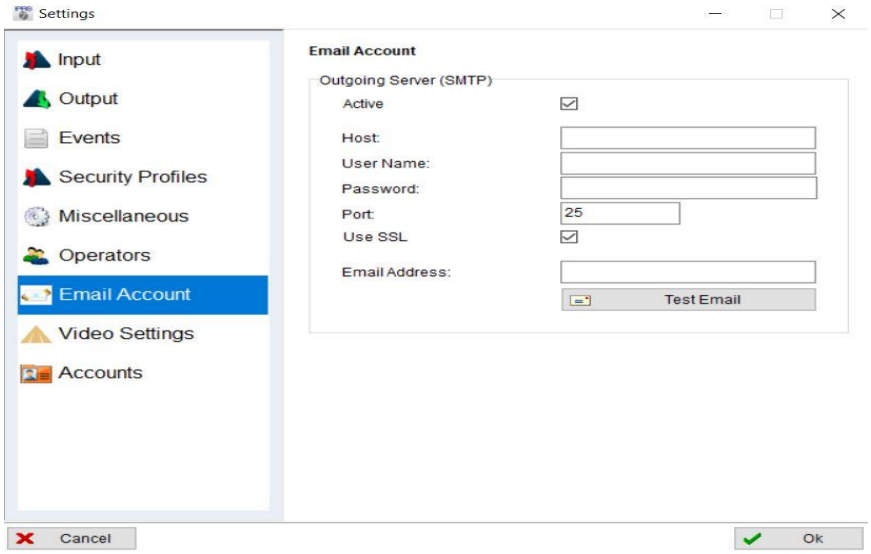


Fig. 18 Email account

3.8. Video settings

Video settings were used for HD77 camera integration. It's not used anymore for current cameras. Latest 4.1.6 version does not support HD78/88 camera integration.

3.9. Accounts

Accounts tab (Fig. 19) allows a few advanced settings for sites registered to the IPRS7: set remote access parameters to allow operators to arm/disarm sites or to control PGMs.

Also, in this section a security level can be assigned to each account. Based on these security levels, operators with higher or lower access level will be able to connect only to the assigned sites. Remote connections are not supported on EVO panels version 7.10 and above or for MG series ECO S029 and S030.

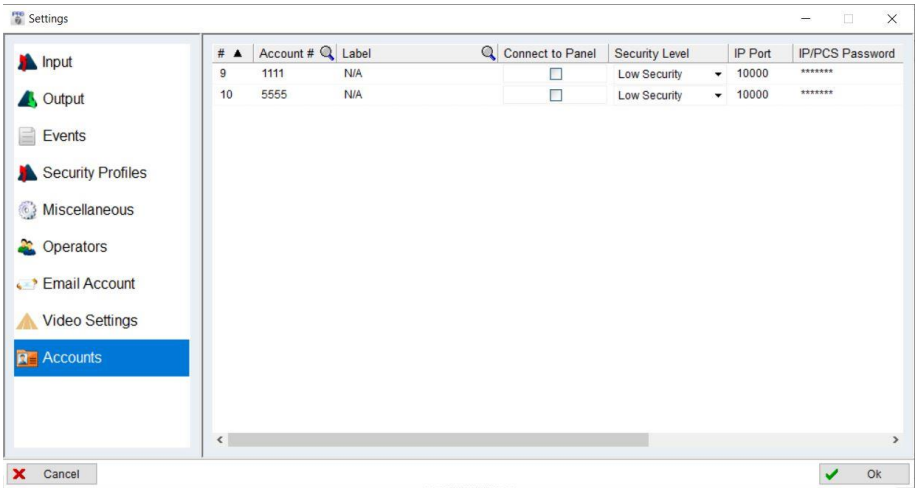
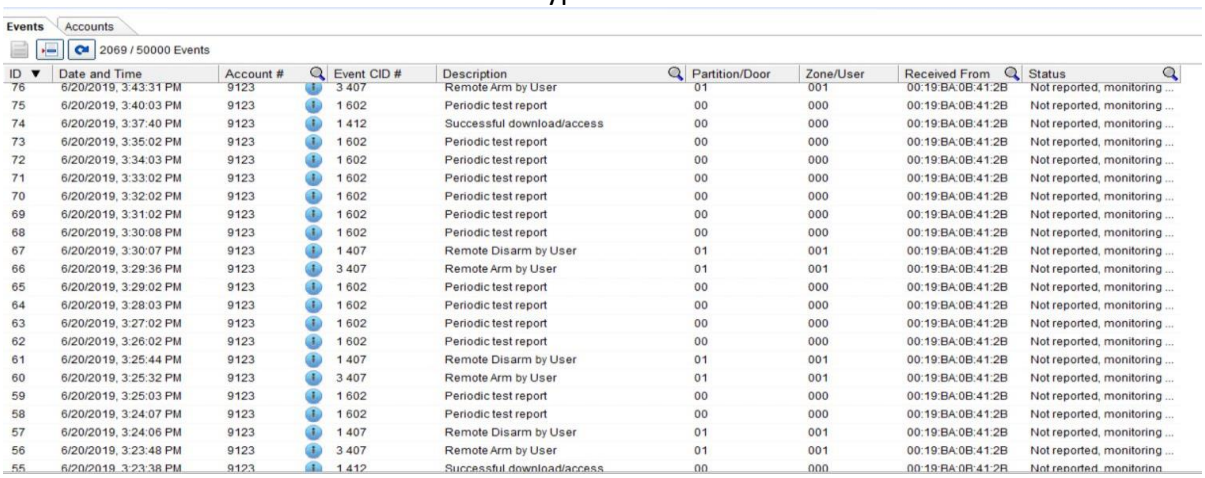


Fig. 19 Accounts tab

3.10. IPRS7 events main window

The main screen of the IPRS7 is organized in two tabs, Events and Accounts.

Events tab (Fig. 20) is used to monitor each event transmitted by the communication modules to the IPRS7. The Event list is mostly used for troubleshooting, in order to find out if the events are properly transmitted to the receiver. Event list CANNOT replace the functionalities of a dedicated CMS software. It does not contain features to customize the events by type or to generate audible alarms in case of an alarm type.



ID	Date and Time	Account #	Event CID #	Description	Partition/Door	Zone/User	Received From	Status
76	6/20/2019, 3:43:31 PM	9123	3 407	Remote Arm by User	01	001	00:19:BA:0B:41:2B	Not reported, monitoring ...
75	6/20/2019, 3:40:03 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
74	6/20/2019, 3:37:40 PM	9123	1 412	Successful download/access	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
73	6/20/2019, 3:35:02 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
72	6/20/2019, 3:34:03 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
71	6/20/2019, 3:33:02 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
70	6/20/2019, 3:32:02 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
69	6/20/2019, 3:31:02 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
68	6/20/2019, 3:30:08 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
67	6/20/2019, 3:30:07 PM	9123	1 407	Remote Disarm by User	01	001	00:19:BA:0B:41:2B	Not reported, monitoring ...
66	6/20/2019, 3:29:36 PM	9123	3 407	Remote Arm by User	01	001	00:19:BA:0B:41:2B	Not reported, monitoring ...
65	6/20/2019, 3:29:02 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
64	6/20/2019, 3:28:03 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
63	6/20/2019, 3:27:02 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
62	6/20/2019, 3:26:02 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
61	6/20/2019, 3:25:44 PM	9123	1 407	Remote Disarm by User	01	001	00:19:BA:0B:41:2B	Not reported, monitoring ...
60	6/20/2019, 3:25:32 PM	9123	3 407	Remote Arm by User	01	001	00:19:BA:0B:41:2B	Not reported, monitoring ...
59	6/20/2019, 3:25:03 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
58	6/20/2019, 3:24:07 PM	9123	1 602	Periodic test report	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...
57	6/20/2019, 3:24:06 PM	9123	1 407	Remote Disarm by User	01	001	00:19:BA:0B:41:2B	Not reported, monitoring ...
56	6/20/2019, 3:23:48 PM	9123	3 407	Remote Arm by User	01	001	00:19:BA:0B:41:2B	Not reported, monitoring ...
55	6/20/2019, 3:23:38 PM	9123	1 412	Successful download/access	00	000	00:19:BA:0B:41:2B	Not reported, monitoring ...

Fig. 20 Event page

3.11. IPRS7 Accounts main window

Accounts window (Fig. 21) will display all sites registered to the IPRS7. In this page the operator will be able to modify the Security profile for accounts or to add labels to accounts. Also, in this page there are details about panels or communication devices. Accounts can be deleted

from the same page, by selecting the account -> right click -> Delete account. In order to be used for future installation the account should be deleted also from Backup/Restore -> Recycle bin.

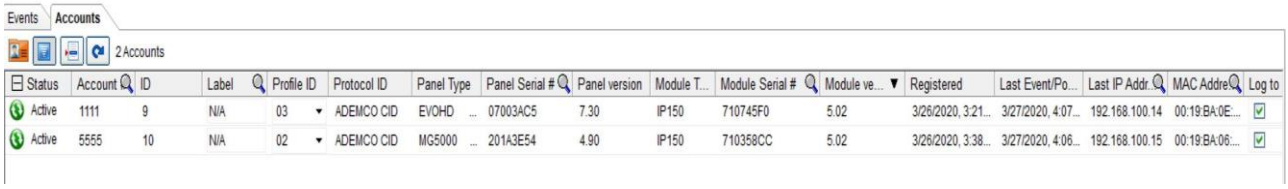


Fig. 21 Accounts page

4. Backup/restore procedures for Paradox receivers

4.1. Backup/restore for IPRS7 receiver

There are two methods to backup accounts and events for the IPRS7.

4.1.1. Automatic backup option

IPRS7 should be set to backup the accounts and events automatically. This option can be configured in Backup/Restore menu -> Backup menu.

For accounts, a filename prefix and destination path can be set.

For events, a filename prefix and destination path and the automatic backup interval can be set.

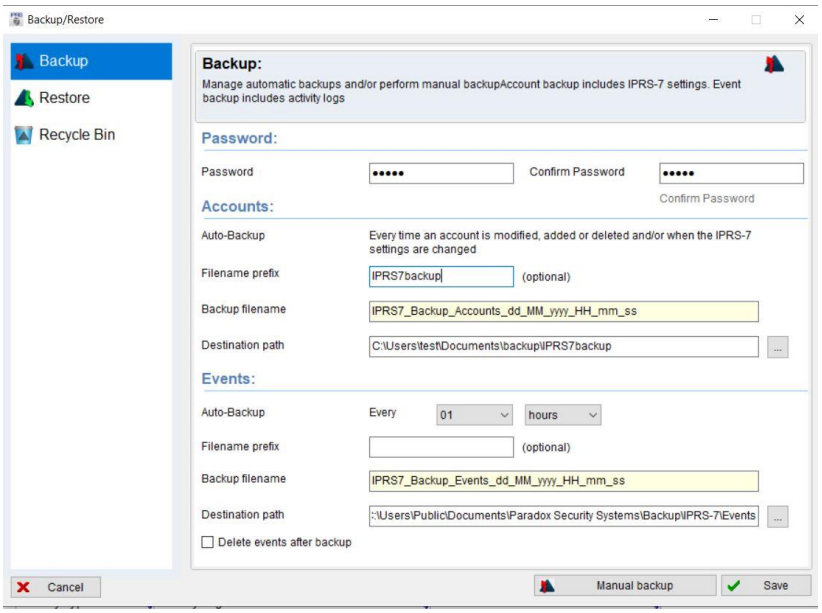


Fig. 22 Automatic backup

4.1.2. Manual backup option

IPRS7 support also manual backup that can be found in the Backup/Restore menu. A manual backup for accounts and events is recommended when a receiver migration is scheduled. In this way the operator will be sure that all details will be migrated to the new IPRS7.

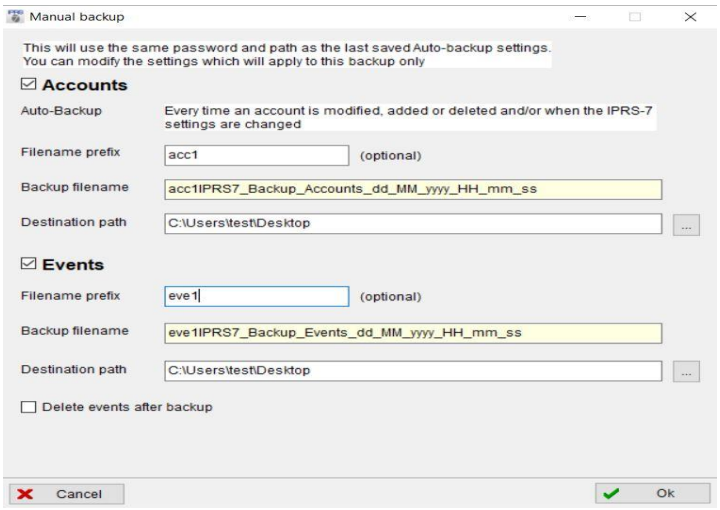


Fig. 23 Manual backup

4.1.3. Restore option

In order to restore accounts and events on a new IPRS7 (in case that the first receiver fails) the user should access Backup/Restore menu -> Restore tab (Fig. 24).

Here, the accounts and backup files will need to be imported. It doesn't matter how the backup was done (automatic mechanism or manually), the backup files will be uploaded in the same way.

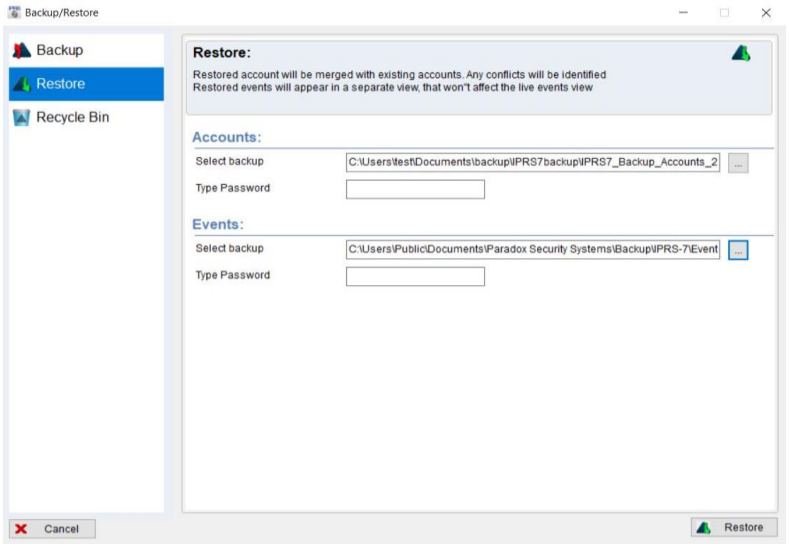


Fig. 24 Restore option

4.2. Backup from IPRS7 and restore to IPR512

This chapter will explain the steps that need to be followed in order to import IPRS7 accounts to IPR512 receiver.

Versions used:

IPR512 2.96.000
IPRS7 4.1.6 or above

IPR512 DB Conversion tool

In order to be able to convert accounts from IPRS7 to IPR512 below software should be downloaded and run as administrator on the machine where IPRS7 is installed:

https://drive.google.com/open?id=1Wf4Oh6LeSokWDx9j05_ZSw0WCEdWfYkt

Basic requirements

1. NEW SD card (It is preferred NOT TO use SD cards with previous IPR512 backups)
2. IPR512 V2.96
3. IPRS7 installed and operating (Not a specific version is required)
4. PC where the user has full admin rights is required to run DBIPR512convert.exe

Extracting IPR512 DB Conversion tool

1. Create a Folder to extract DBIPR512converter.zip
2. Extract the zip file in the folder created
3. The following information should be available in the folder

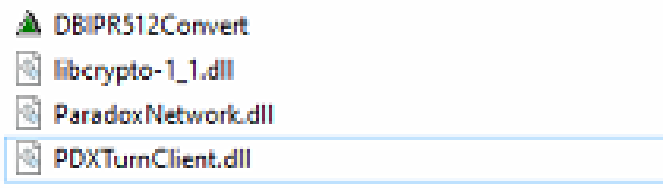


Fig. 25 IPR512 DB Conversion tool folder

General software view

The following options form the tool will be available:

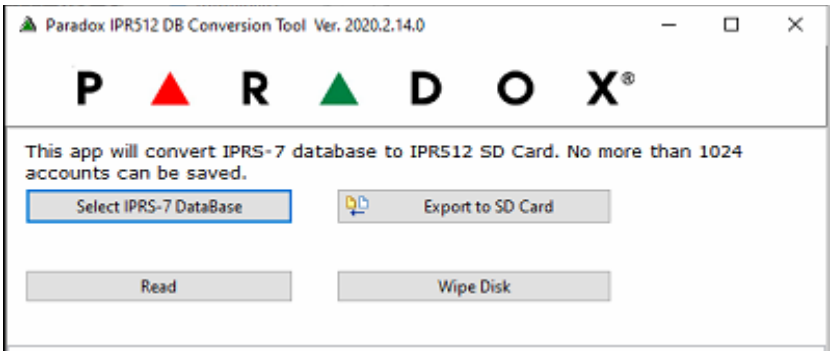


Fig. 26 IPR512 DB conversion tool - software view

- **Select IPRS-7 DataBase** option: allows you to select the database folder to convert to IPR512
- **Export to SD Card** option: Only available when you select a valid IPRS-7 DataBase
- **Read** option: It is used to read the content of an SD card for R&D analysis in case of an error (please refer to the end of document for additional information)
- **Wipe Disk** option: It is used to wipe out the information of an SD card. It is recommended to use it specially if you have an Access Denied Error with an SD card. The time this process takes varies depending on the size of the card. (4GB cards takes 5-10 min, 32 GB cards takes about 30 min)

WIPE DISK Option:

1. Select the File DBIPR512Convert tool and run as administrator
2. The tool will show the following option

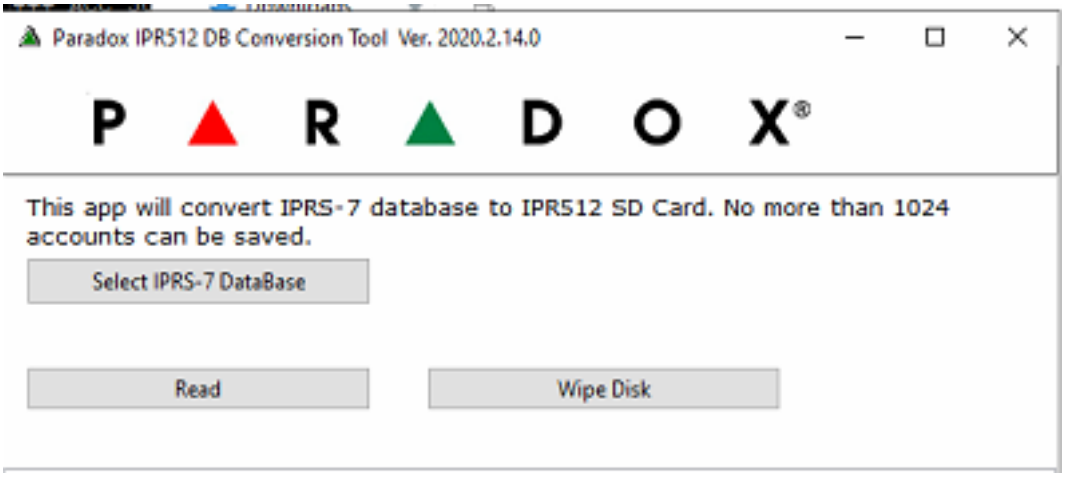


Fig. 27 DBIPR512Convert tool – first opening

3. Select Wipe Disk Option and the following menu will appear

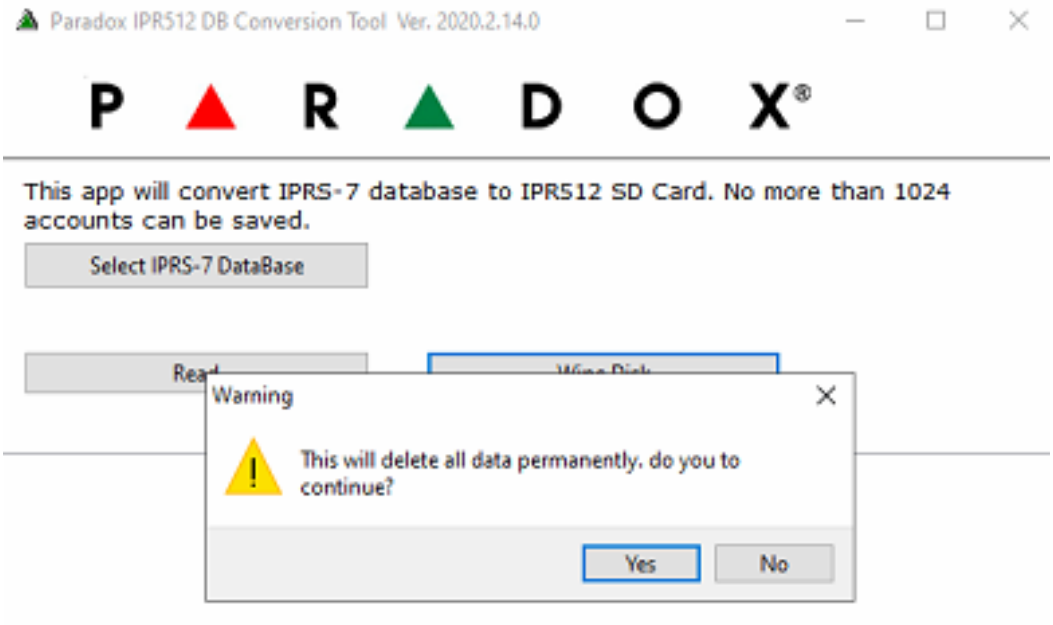


Fig. 28 Wipe disk

4. Click Yes. If a message with an error appears, please click OK and repeat the process

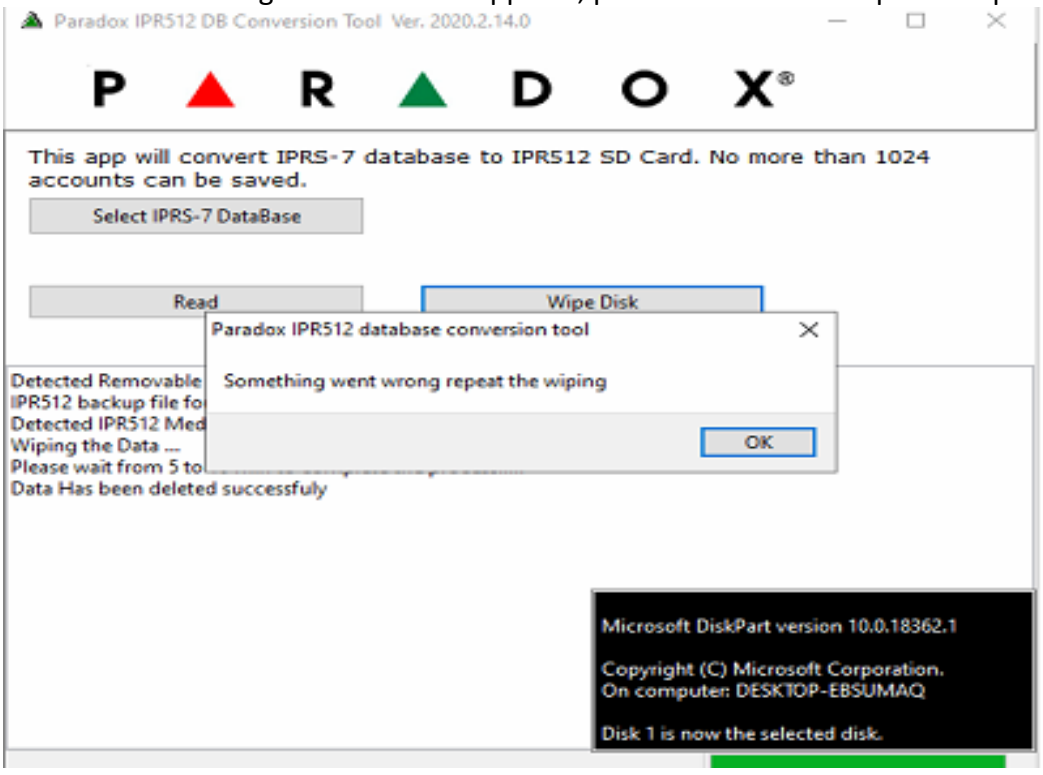


Fig. 29 Error after Wipe Disk is selected

5. The below message will appear indicating an approximate time for the process to complete.

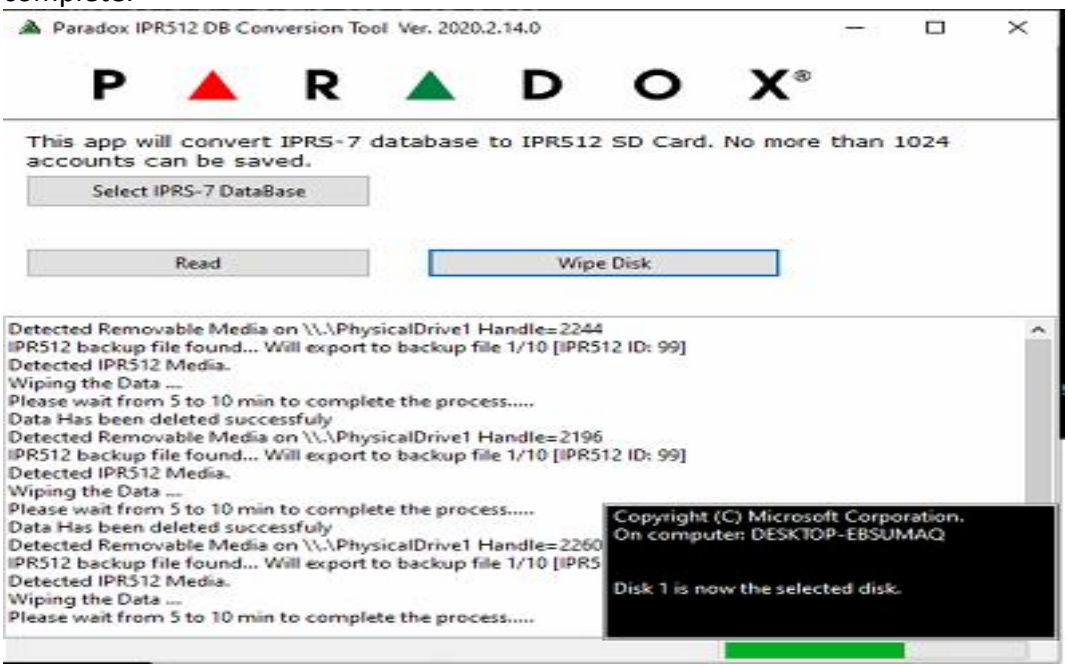


Fig. 30 Wipe disk progress

6. In case there is a message on the top of the window not responding please let the process continue until the end.
7. There will be a prompt message indicating the process is completed and you will be asked to remove the SD card.

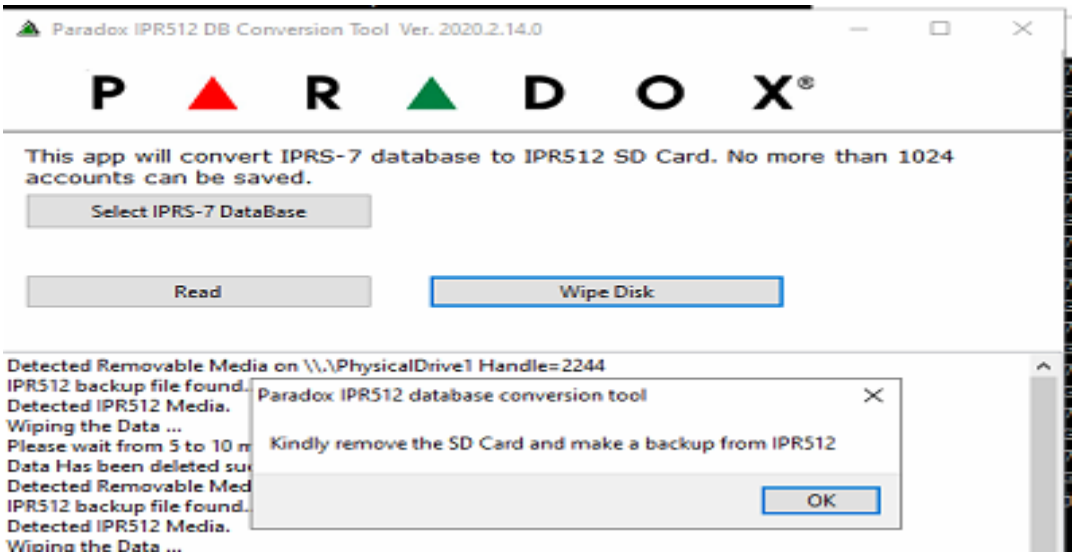


Fig. 31 Wipe disk process completed

8. At this point please remove the SD card and click OK
9. After doing the above process please follow the instructions below to convert the database from an IPRS-7 to IPR512

Database transfer from IPRS7 to IPR512

10. Insert the SD card in the slot of the IPR512
11. Create a backup from the IPR512 (default password: admin)
12. Remove the SD card from IPR512 and insert it in the PC where the IPRS7 and IPR512 DB Conversion Tool are running.
13. Close and exit the IPRS-7 session
14. Run as administrator the tool "DBIPR512 convert tool"
15. Select the option “select IPRS-7 Database”

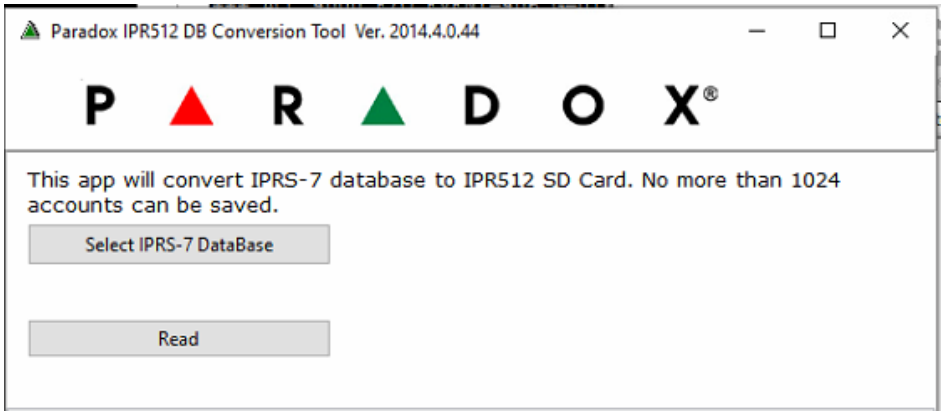


Fig. 32 Selecting IPRS7 database

16. Browse and select the folder Data under users/public/public documents/Paradox Security Systems/ IPRS7/ {949f…}/data

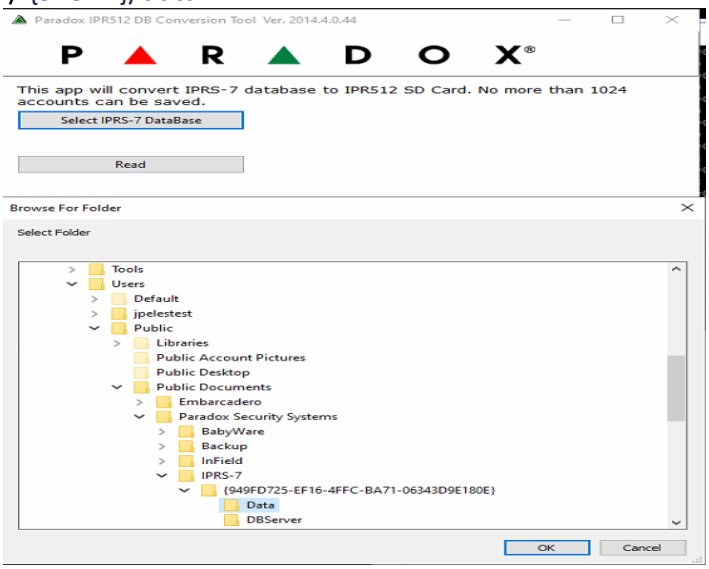


Fig. 33 IPRS7 database path

17. Click OK
18. Select the option of export to SD card

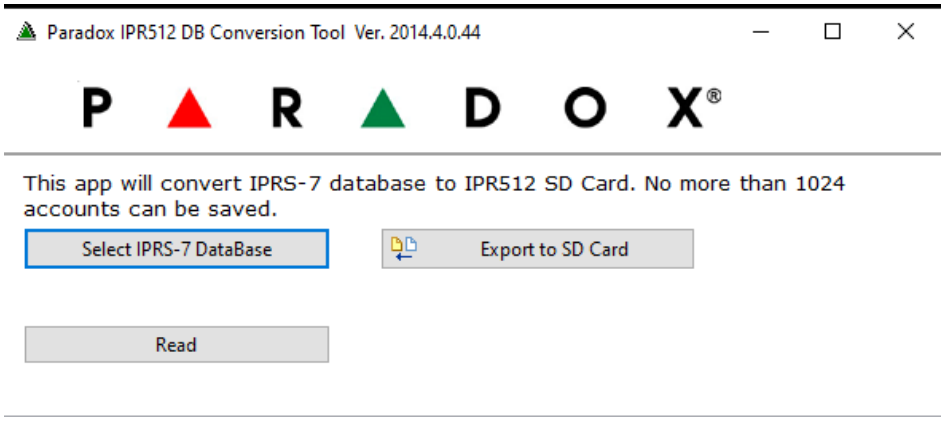


Fig. 34 Exporting IPRS7 database to SD card

19. If there are accounts that need to be removed or added please select those accounts to be added and deselect the ones not desired

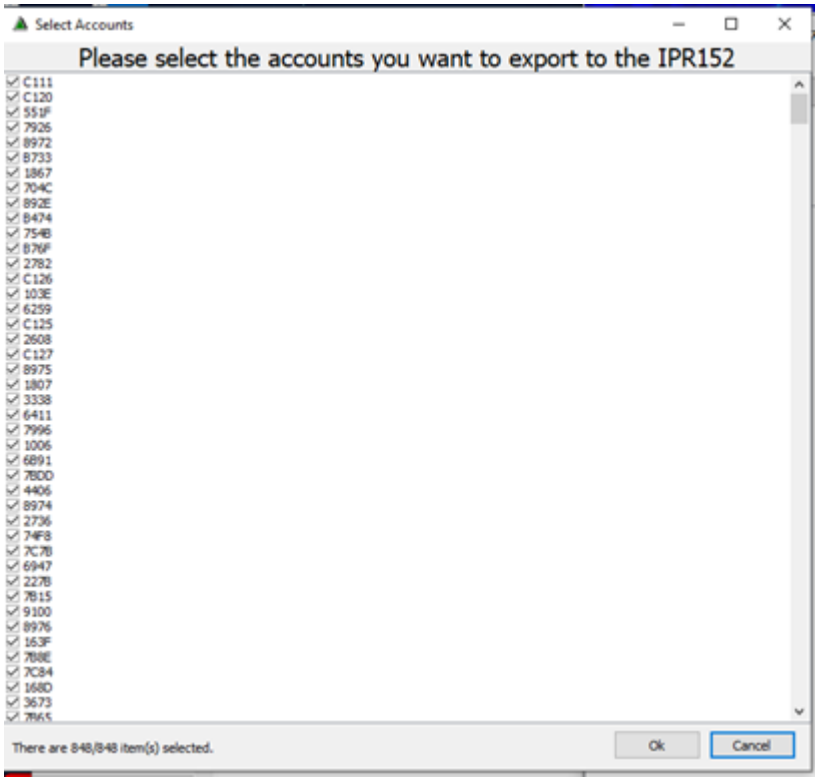


Fig. 35 IPRS7 database management

20. Message below should appear (media update successful)

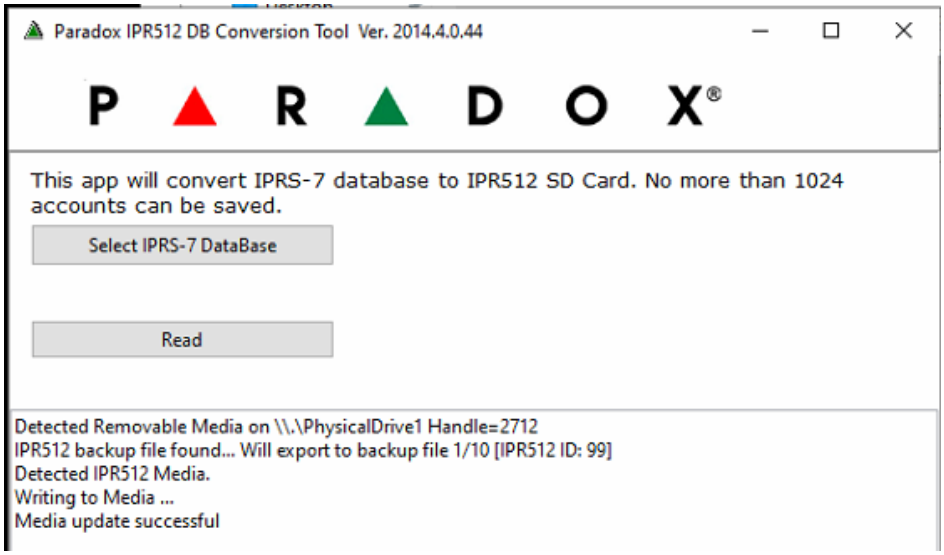


Fig. 36 Exporting progress

21. After the backup is being generated please remove the SD card from the PC
22. Insert the SD card in the IPR512 slot
23. Select the backup menu option from the IPR512 LED screen an restore the backup (Only one backup will be available)
24. In the LED screen should be seen the amount of accounts generated and should match the accounts you wanted to restore from the backup in your IPRS-7

READ Option - used for R&D analysis in case of an error

1. Select the File DBIPR512Convert tool and run as administrator
2. The tool will show the following option

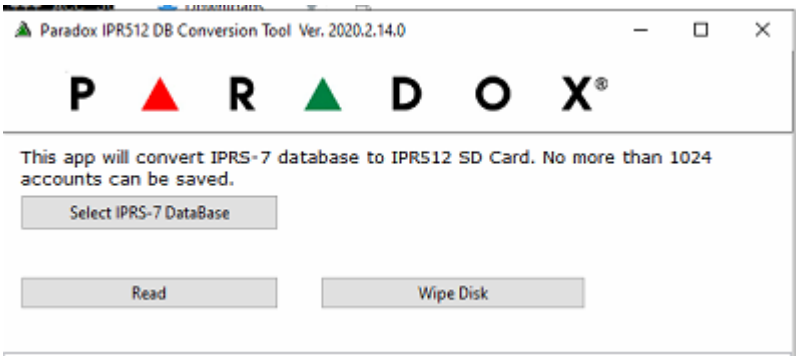


Fig. 37 Read option

3. Select Read Option and the following menu will appear

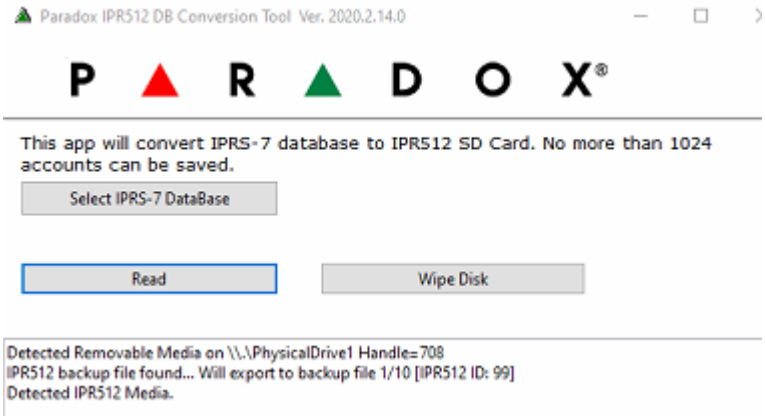


Fig. 38 Read progress

4. You will be asked to save the file, please select a folder where you want to save the file.

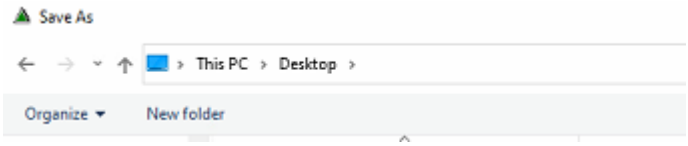


Fig. 39 SD card image saving location

5. Send the file to the Paradox contact which was asking for the file