PARADOX IP REPORTING TO IPR512

Version 1.0

April 28th 2020

Created by: Victor Maciuca

Contents

Preface

This document will explain Paradox IPR512 reporting in depth and will cover the following topics:

- Panel reporting configuration
- IPR512 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. Hardware receiver – IPR512
3. Automation software which is connected through serial connection to IPR512. 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.

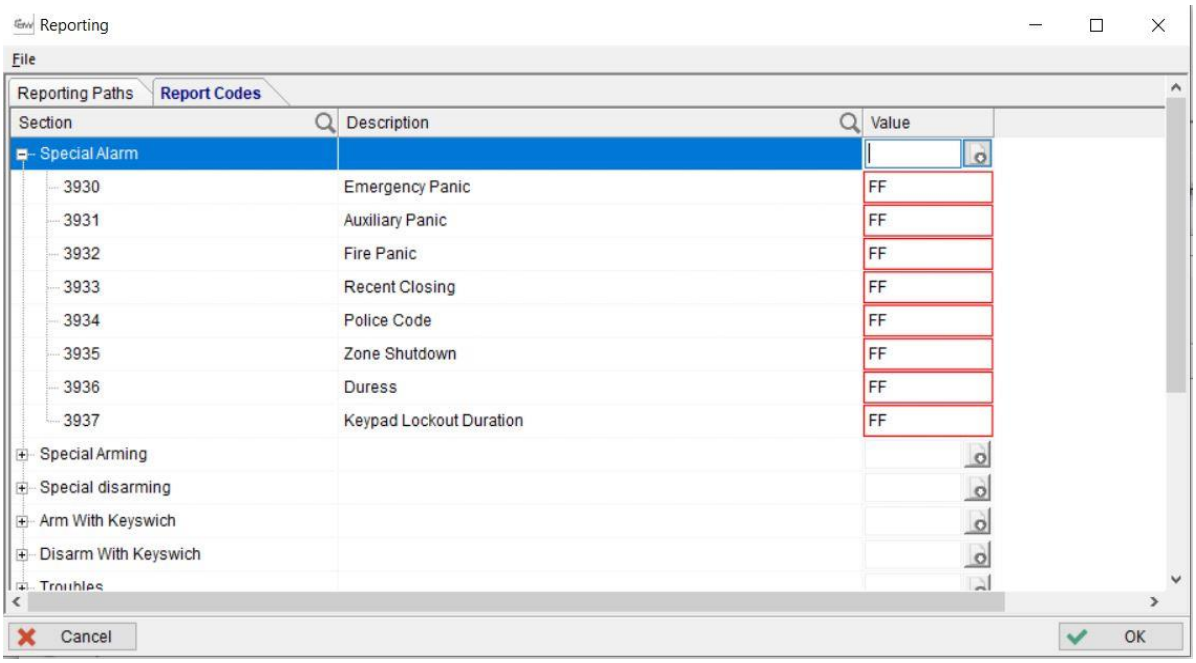


Fig. 1 Report Codes

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.

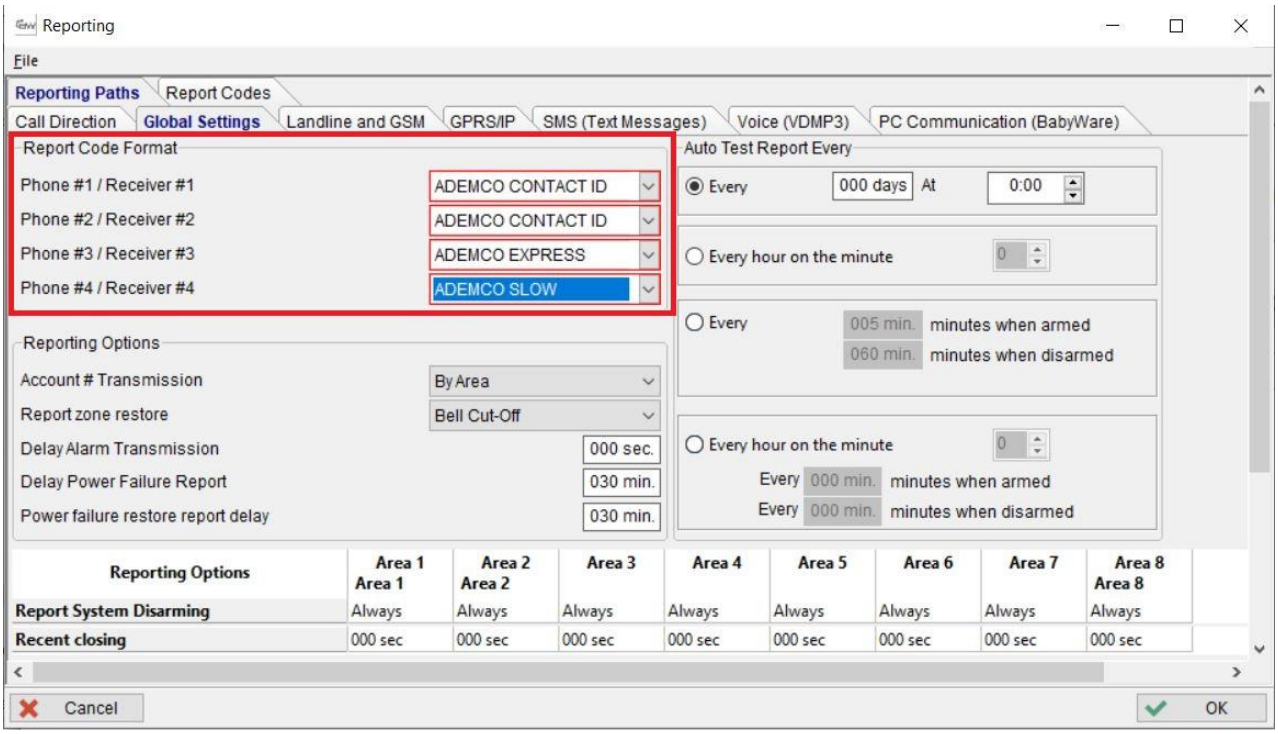


Fig. 2 Report Code Format

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 IPR512, WAN 1 IP and port are mandatory to be filled. If both WAN ports are used on IPR512, both IPs and ports will need to be filled in Babyware.
b) Receiver password - by default the IPR512's password is 123456. This password is used only in registration step, not for receiver management. It can be changed from receiver's web interface.
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.

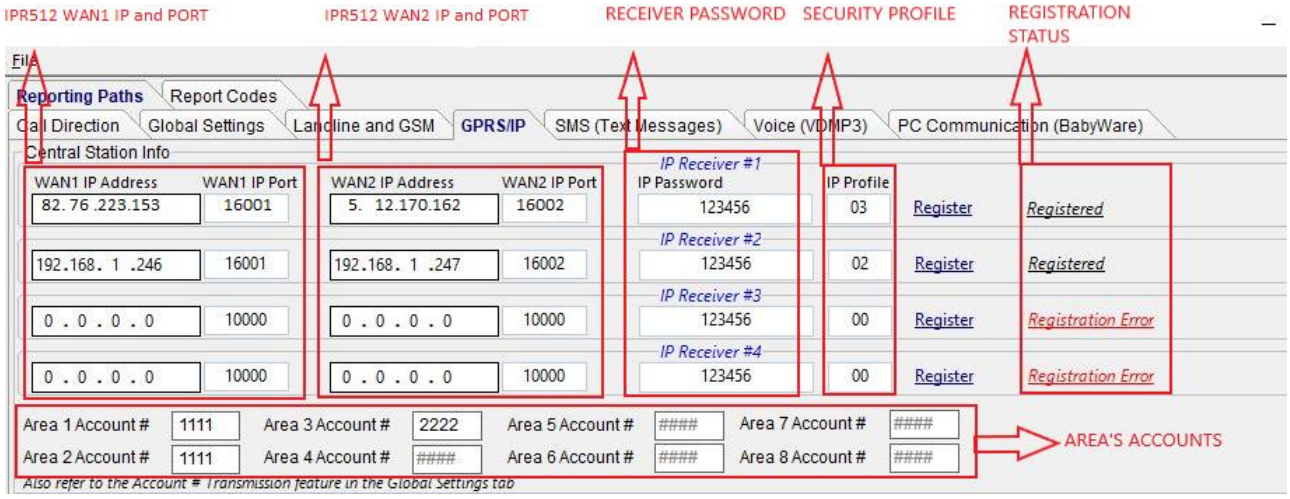


Fig. 3 Central station Info

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.

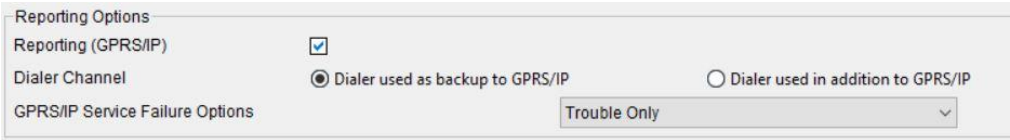


Fig. 4 Reporting options

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.

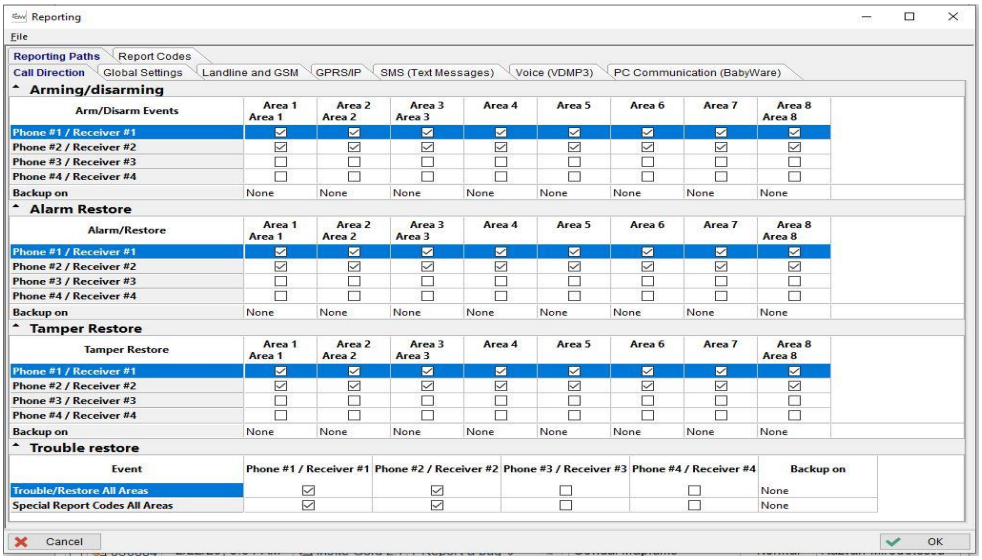


Fig. 6 Report call direction

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.

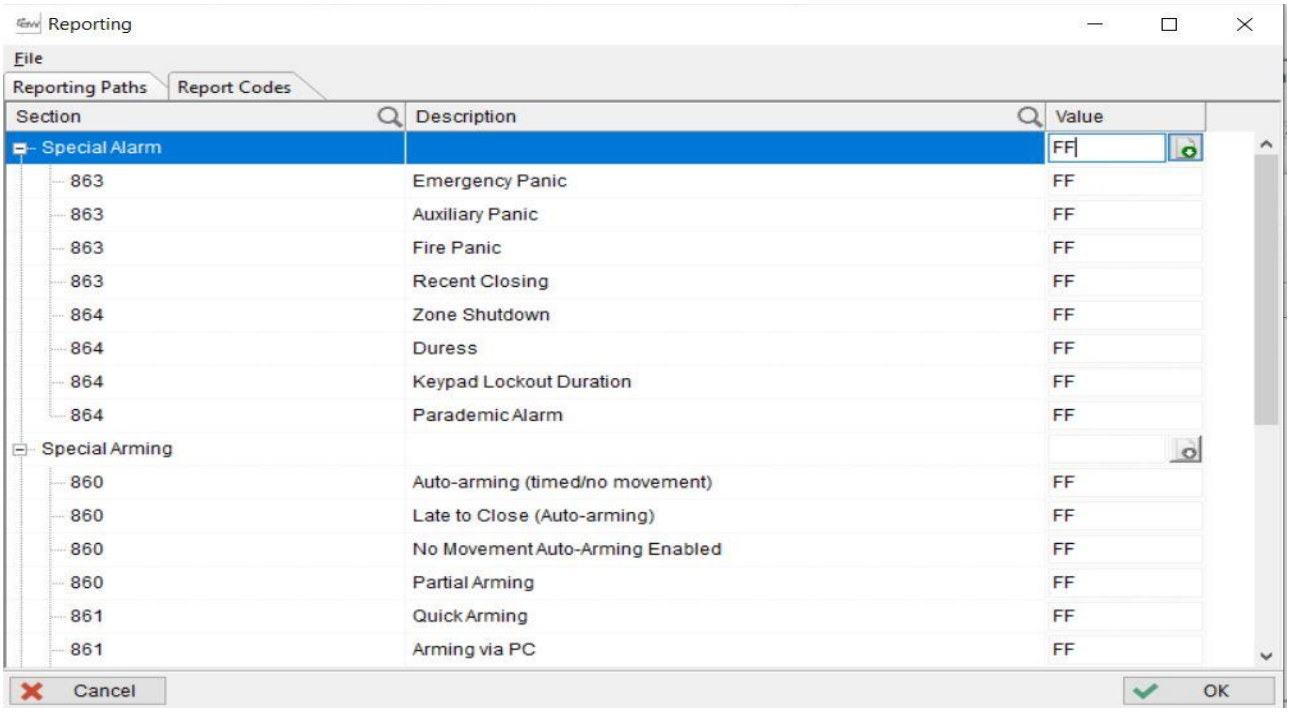


Fig. 7 Report Codes on MG/SP panels

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).

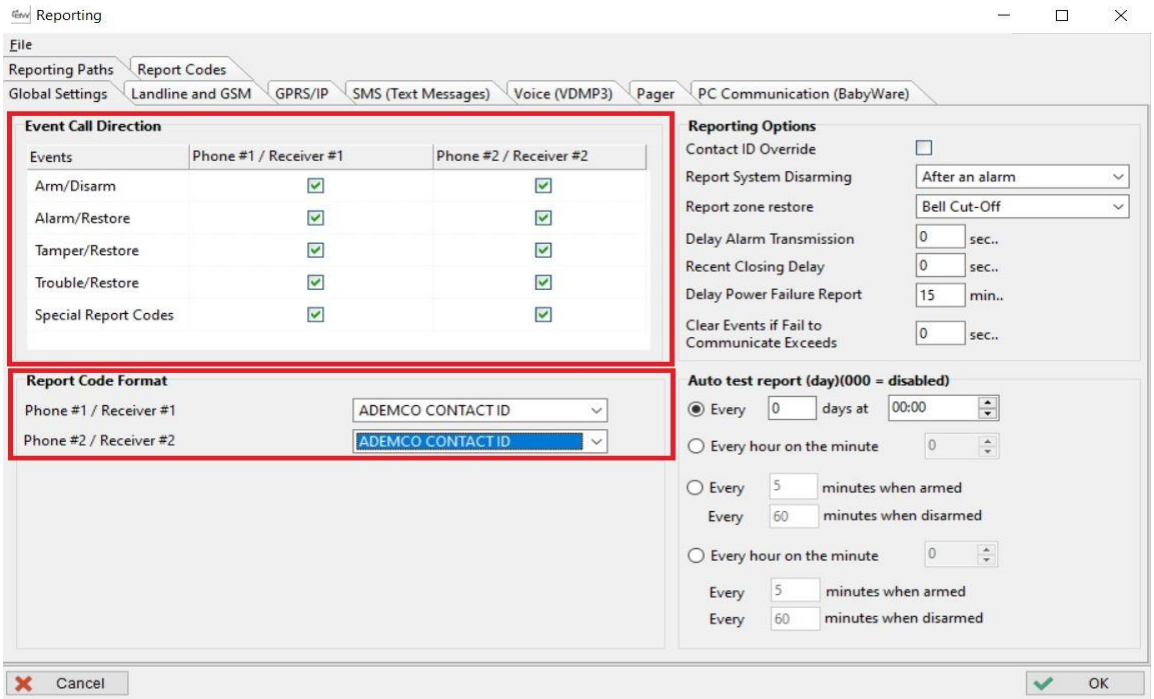


Fig. 8 Global settings

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:
   For IPR512, WAN 1 IP and port are mandatory to be filled. If both WAN ports are used on IPR512, both IPs and ports will need to be filled in Babyware.
b) Receiver password - by default the IPR512's password is 123456. This password is used only in registration step, not for receiver management. It can be changed from receiver's web interface.
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.

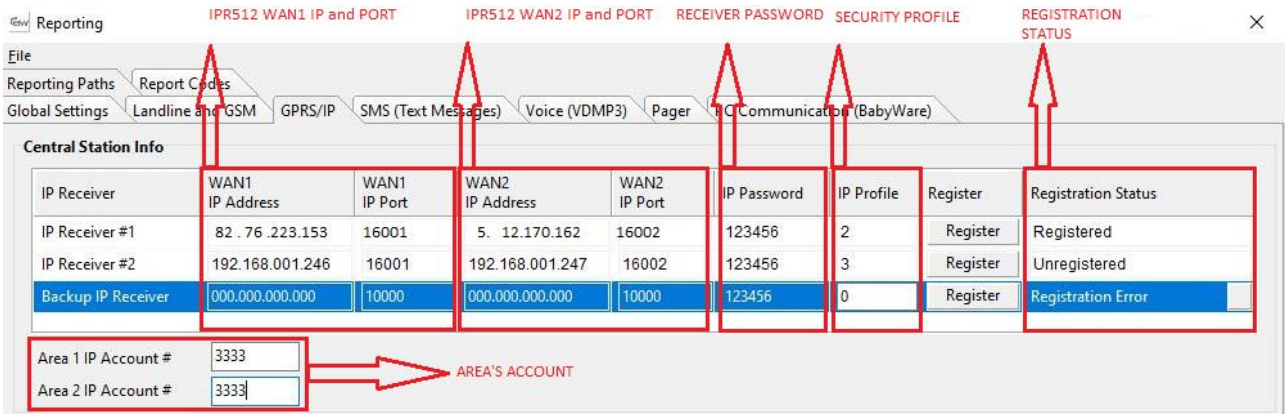


Fig. 9 Central station Info

2.4. Reporting options

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

f) 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.

g) 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)

h) 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.

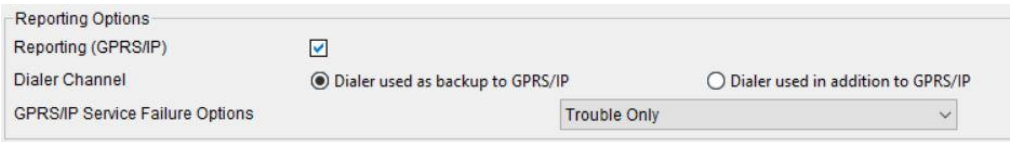


Fig. 10 Reporting options

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. IPR512 accounts and settings

Paradox IPR512 is a hardware receiver that can handle up to 1024 accounts. An account will contain an IP150/+ module, an PCS module or both modules (combo mode).

3.1. Web interface login

In order to access the web interface of the receiver, the LAN IP should be accessed in a web browser. The default IP of the LAN port of the receiver is 192.168.1.250. If the receiver is installed in a network with a different IP class, it can be changed from receiver's keypad. The receiver's LAN IP can be found with IP Exploring Tool found on our website.

By default, the user is "admin" and the password is "admin" (Fig. 12). The password can be changed after first web interface login and it's used only for receiver management not for account's registration. Starting with version 2.96, receiver's password cannot be recovered using the "Forgot user password" in the login screen. For receivers with firmware 2.96 and above kindly contact Paradox support team and the recover procedure will be provided.

Fig. 12 IPR512's web interface login

3.2. Receiver configuration

3.2.1. Network configuration

The LAN/WAN IPs and ports can be configured from the Interfaces Configuration tab. (Fig.13)

The IPR512 receiver has 3 RJ45 network interfaces:

1. LAN – HTTP web browser sessions are allowed on this interface
2. WAN1 – for receiving events – activated by default
3. WAN2 – for connecting another WAN from a different ISP for redundancy. By default, the receiver has activated only LAN and WAN1 interfaces. If WAN2 is used it should be activated also.

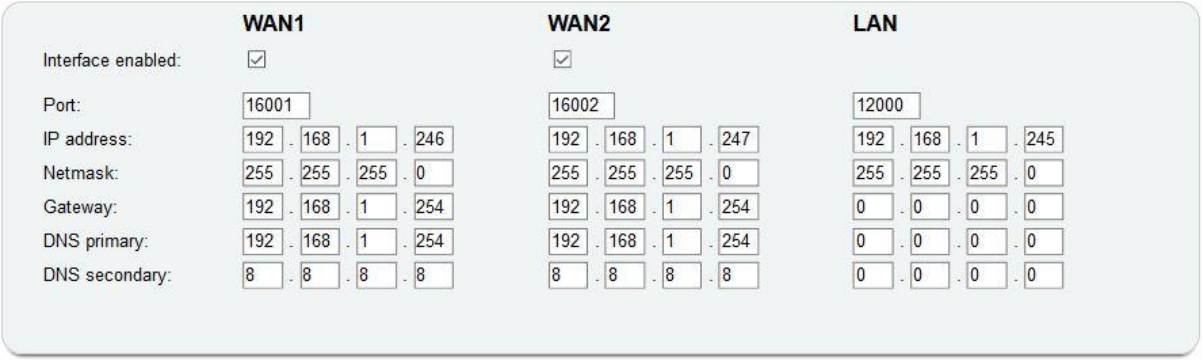


Fig. 13 IPR512's IP interfaces configuration tab

3.2.2. Output protocol

IPR512 receiver will not display the events received from communication devices on its interfaces. These events will be encapsulated in a known format and forwarded to central monitoring software (CMS).

The supported protocols are: ADEMCO 685, SURGARD MLR2-DG, and RADIONICS 6500. Communication with the 3rd party central monitoring software (CMS) will be done through serial connection on port COM1 of the receiver. The parameters should be set according to the protocol used and to the monitoring software requirements. (Fig. 14)

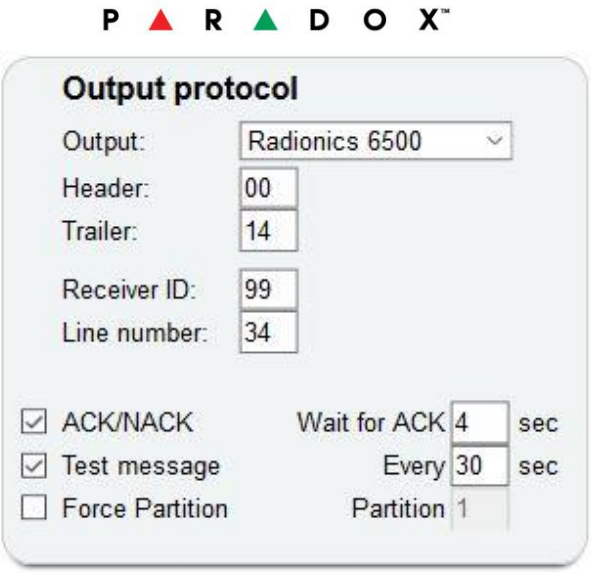


Fig. 14 Output protocol configuration

3.2.3. Serial ports configuration

The IPR512 has 2 serial ports that can be configured (Fig. 15):

- COM1 port (DB25 connector) is used to forward events to the central monitoring software
- COM2(DB9 connector) is used to connect a printer or a PC with an RS232 serial port, running software to view/print events in plain text format.

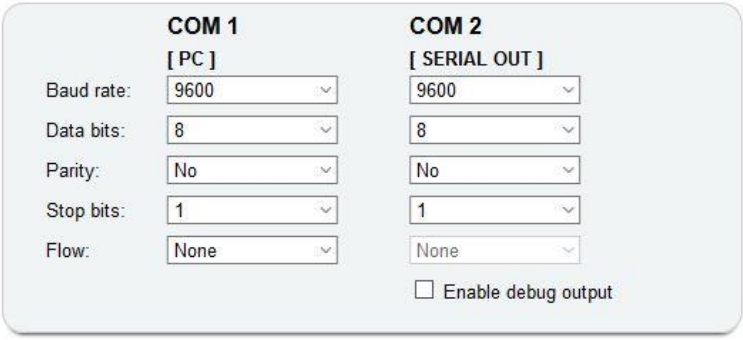


Fig. 15 Serial ports configuration

3.2.4. IPR512's other configuration

The following settings can be set on this tab (Fig.16)

a) Receiver password – password used for account registration. This password should be entered as well on the panel programming to register a module to the IPR512.
b) Polling website – by default is set to ipr512.paradoxmyhome.com and should be changed only when communicating in a closed network.

The polling interval can be set from 1 to 60 minutes and the attempts from 1 to 24. If the receiver will not be able to poll the website (for the number of attempts), it will report WAN1/2 Internet connection failure trouble.

c) Date and time – used to set receiver's date and time through an NTP server or manually.

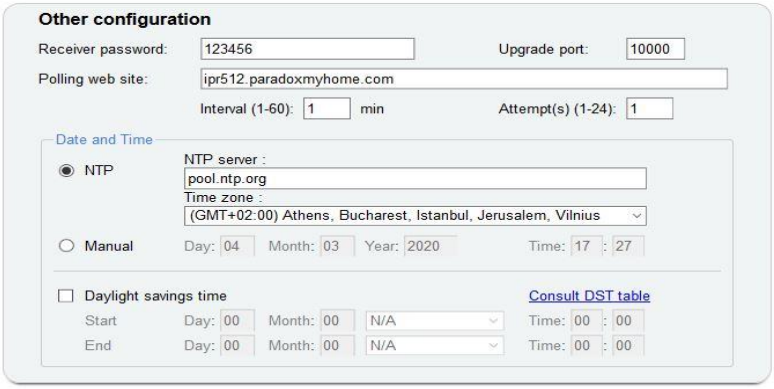
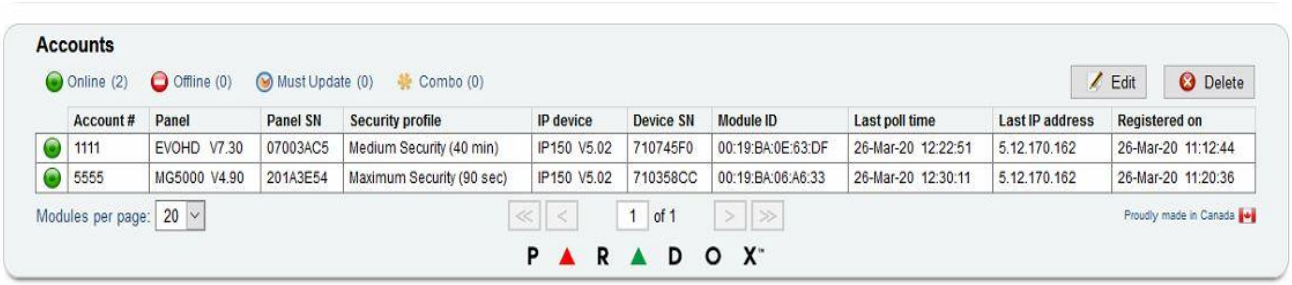


Fig. 16 – Other configuration

3.3. IPR512's accounts management

Up to 1024 accounts can be registered to an IPR512 receiver. An account can be created with an IP module, a PCS module or both (combo mode) (Fig.17). Once two modules (one PCS and one IP module) are installed in combo mode they will be registered under the same account.

The edit option will allow to change the security profile of the account. Delete option will remove the account from the list. If there is no need to restore the deleted account in future, it should be removed from View/Restore deleted modules as well, otherwise the account number will not be available to be used again.



Account #	Panel	Panel SN	Security profile	IP device	Device SN	Module ID	Last poll time	Last IP address	Registered on
1111	EVOHD V7.30	07003AC5	Medium Security (40 min)	IP150 V5.02	710745F0	00:19:BA:0E:63:DF	26-Mar-20 12:22:51	5.12.170.162	26-Mar-20 11:12:44
5555	MG5000 V4.90	201A3E54	Maximum Security (90 sec)	IP150 V5.02	710358CC	00:19:BA:06:A6:33	26-Mar-20 12:30:11	5.12.170.162	26-Mar-20 11:20:36

Fig. 17 IPR512's accounts management

3.4. Security profiles

There are five security profiles by default with specific polling times and supervision times. These security profiles can be modified using the Edit button or other profiles can be added using Add button (Fig. 18).

The reporting module (IP150/PCS) sends a presence message to the receiver at intervals defined on the module polling time. If the receiver does not receive any presence messages within the receiver supervision time, the receiver will report a supervision loss of the account.

The ID of the polling profile needs to be added as the IP profile in Babyware or in section programming.

Security profiles

The IP reporting device sends 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.

Add | Edit | Delete

ID	Name	Module polling time	Receiver supervision time	Modules using this profile
00	No Supervision	6 hours	Not supervised	0 modules
01	Low Security	20 minutes	2 hours	0 modules
02	Medium Security	10 minutes	40 minutes	1 modules
03	High Security	2 minutes	10 minutes	0 modules
04	Maximum Security	25 seconds	90 seconds	1 modules
05	Custom profile	15 minutes	50 minutes	0 modules

Fig. 18 Security profiles

3.5. Events configuration

There are two main categories of events which can be customized on the receiver side (Fig. 19):

- Account events - account supervision loss/restore and account registration/deletion can be signaled
- Receiver events - these events should be configured per the CMS recommendations. Receiver events will be reported on a specific account which should be configured in the same page.

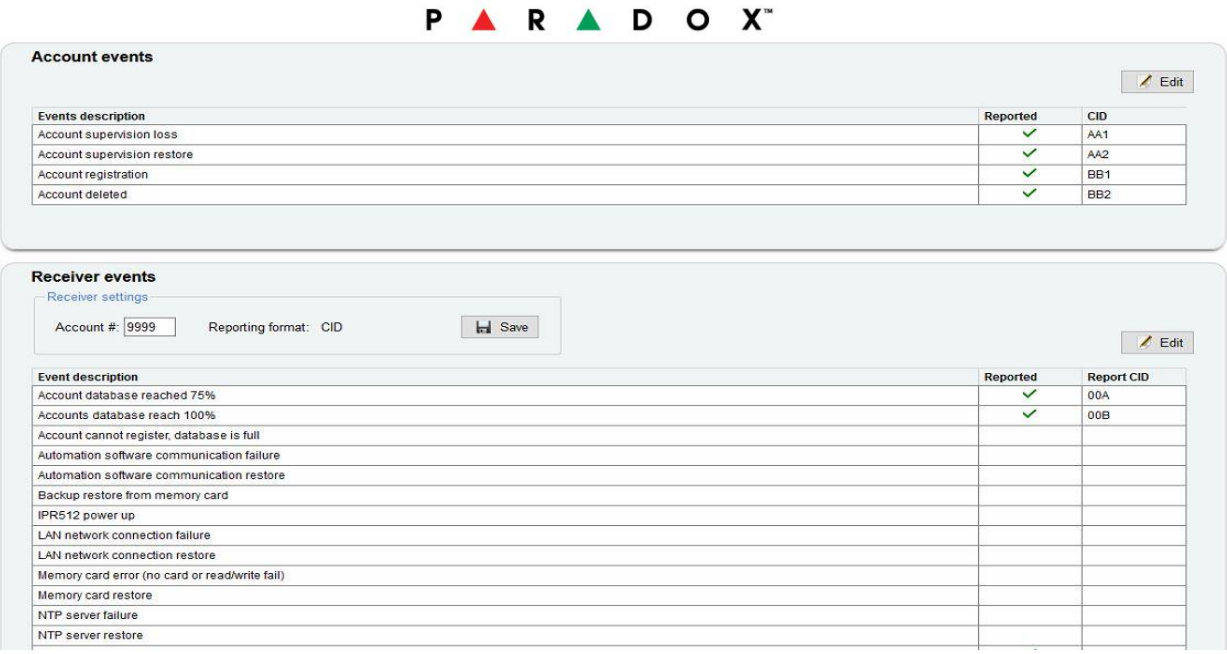


Fig. 19 Event configuration

3.6. Receiver status

Receiver status tab it's used for troubleshooting and important settings as backup or clear database. (Fig. 20)

The receiver information status shows the serial number, the MAC address of the network interfaces, firmware and hardware versions.

Additional actions can be done as follows:

- Export system logs - when requested by Paradox Support Team for investigation
- Export accounts - in .csv format
- Backup on SD Card - backup accounts and settings of the SD card
- Clear database - will remove all accounts in the receiver
- Restore to factory default - will restore the factory setting – including deletion of all accounts registered

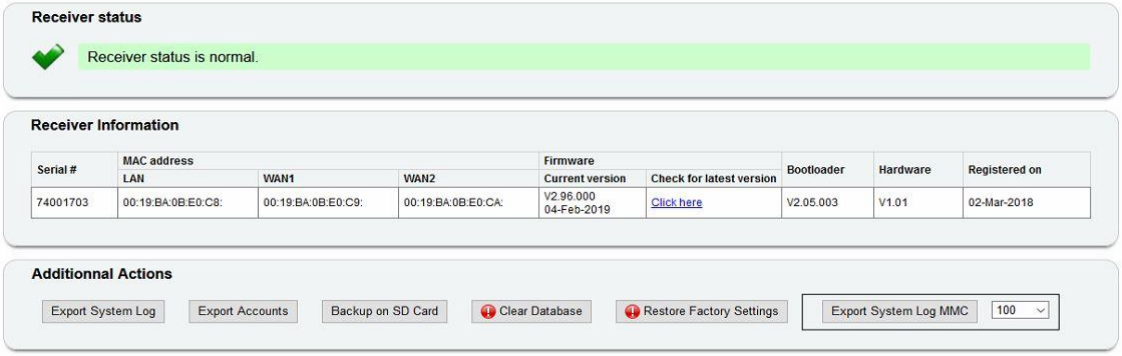


Fig. 20 Receiver status

3.7. Search engine

IPR512 has a built-in search engine (Fig. 21) which is helpful for account management. The operator can search by a single account, an account range (e.g. From 1000 to 1010) or by a specific account or by a module ID (MAC address e.g. Module ID = 0019ba0e63df).

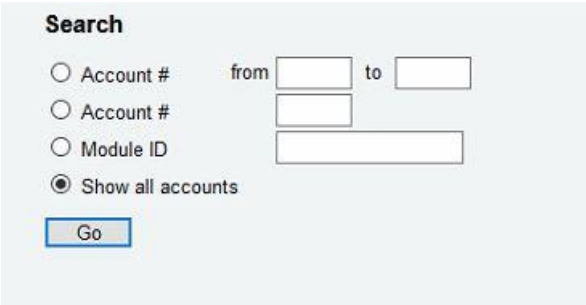


Fig. 21 Search engine

4. Backup/restore procedures for Paradox IPR512 recevier

4.1. Backup/restore for IPR512 receiver

It is possible to backup and restore data from old to new IPR512. To achieve that on NEW IPR512 please enter Backup menu -> Enter password (admin default) -> Restore data from memory card. Based on backup file size this might take some time to finish. Once done the IPR512 will reboot.

Please note that network configuration should be imported as well, however please double check WAN configuration to be the same with old IPR512 otherwise the reporting modules will fail to reach IPR512. It should not be necessary to register again the modules.

Please be advised that along with accounts and network setup, also the IPR512 password will be imported from backup file.

4.2. Backup from IPR512 and restore to IPRS7

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

Versions used:
IPR512 2.90.005 or above
IPRS7 4.11.1 or above -> beta version

Procedure:

1. Please connect with a browser to IPR512 web interface and make a manual backup (Backup on SD Card button below – Fig. 22) of data to SD Card (please make sure that SD Card is inserted into IPR512). This will ensure that latest IPR512 database is exported to SD Card.

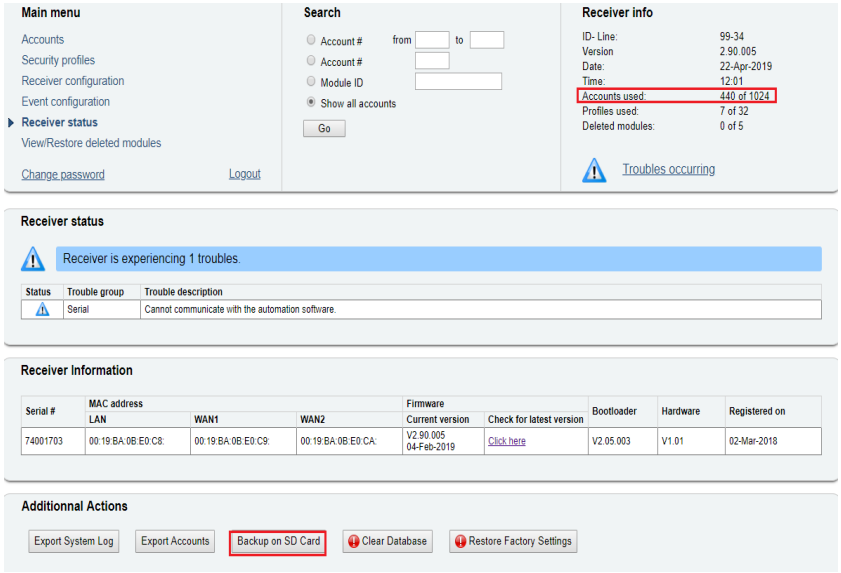


Fig. 22 Backup on SD Card

2. Please remove the SD card from IPR512 and insert it into a PC with IPRS7 installed. From IPRS7 interface, press Recycle Bin and select Convert IPR512 SD Card option (Fig. 23).

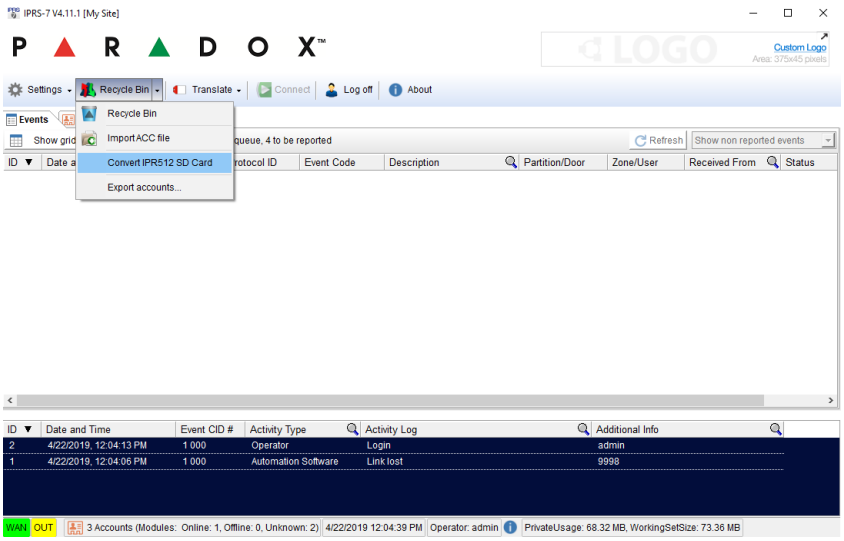


Fig. 23 Convert IPR512 SD Card

3. Paradox IPR512 DB conversion tool will appear (Fig. 24). Click on Import from SD Card button. This will list all valid backups available on SD card. Select the latest backup (shown with bold in the list). Once the backup is selected, please click Save to ACC File button. This should generate an ACC file that needs to save locally on PC.

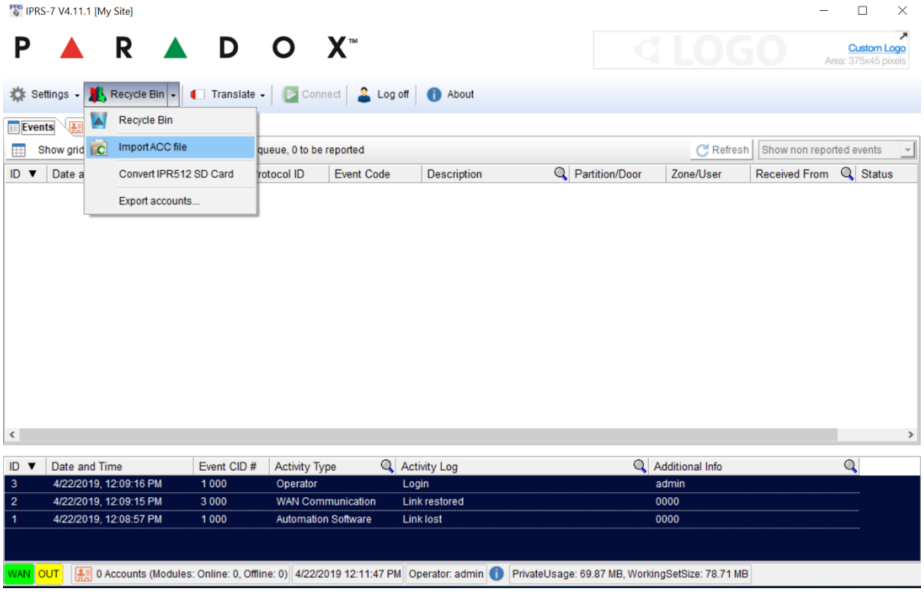


Fig. 24 IPR512 DB conversion tool

4. From IPRS7 please select Import ACC file (Fig. 25) and select the ACC file exported at previous step

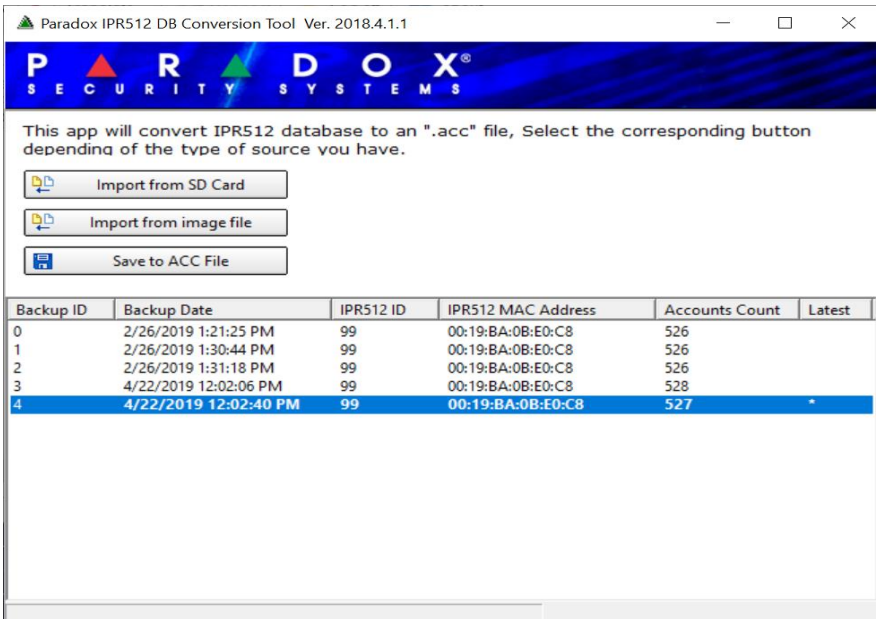


Fig. 25 – Import ACC file

5. Once the importing process is completed, please click Refresh button in IPRS7 to show imported accounts.

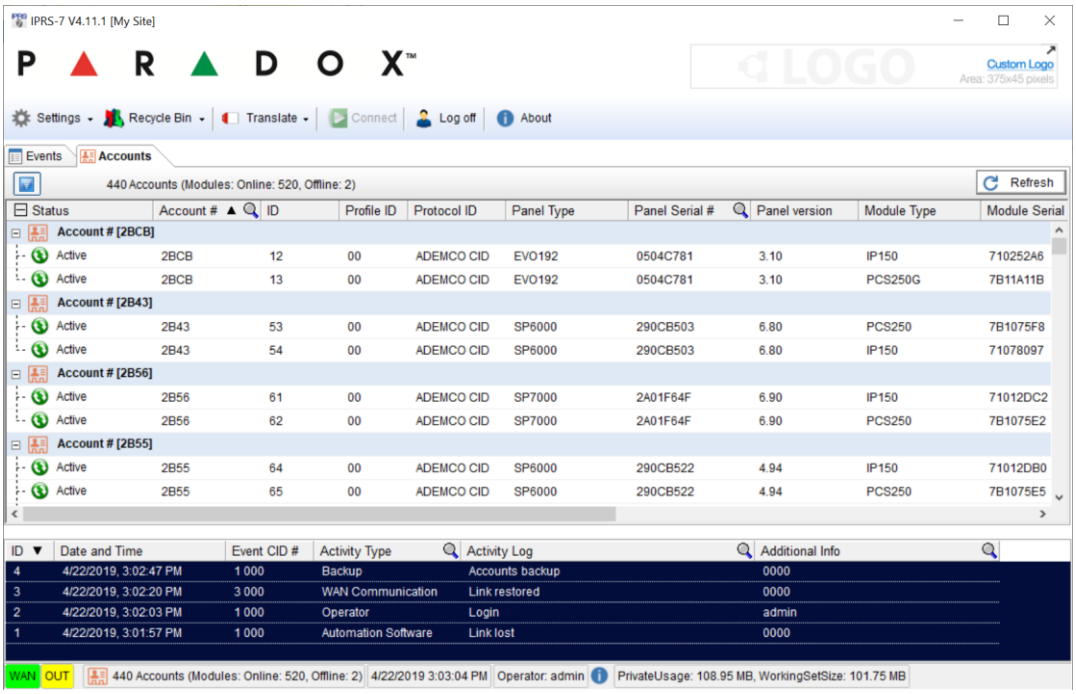


Fig. 27 Imported accounts

5. IPR512 network requirements

We found that in practice and in some monitoring stations the IPR512 unit is not running on isolated networks and the IPR512 has to handle other messages broadcasted in the network that might not be of interest.

This is making the unit to process unnecessary packets and therefore consuming processing resources, at some point causing the unit to reboot.

To cope with that Paradox is STRONGLY recommending isolating the network physically and if not possible then to create VLAN with distinct subnets for each IPR512 WAN and LAN ports. The protocols that needs port forward are: LAN TCP only and WAN UDP only.

Please check following diagrams with details that need to be implemented to isolate the network, using VLANs (Fig. 28) or using routers (Fig. 29).

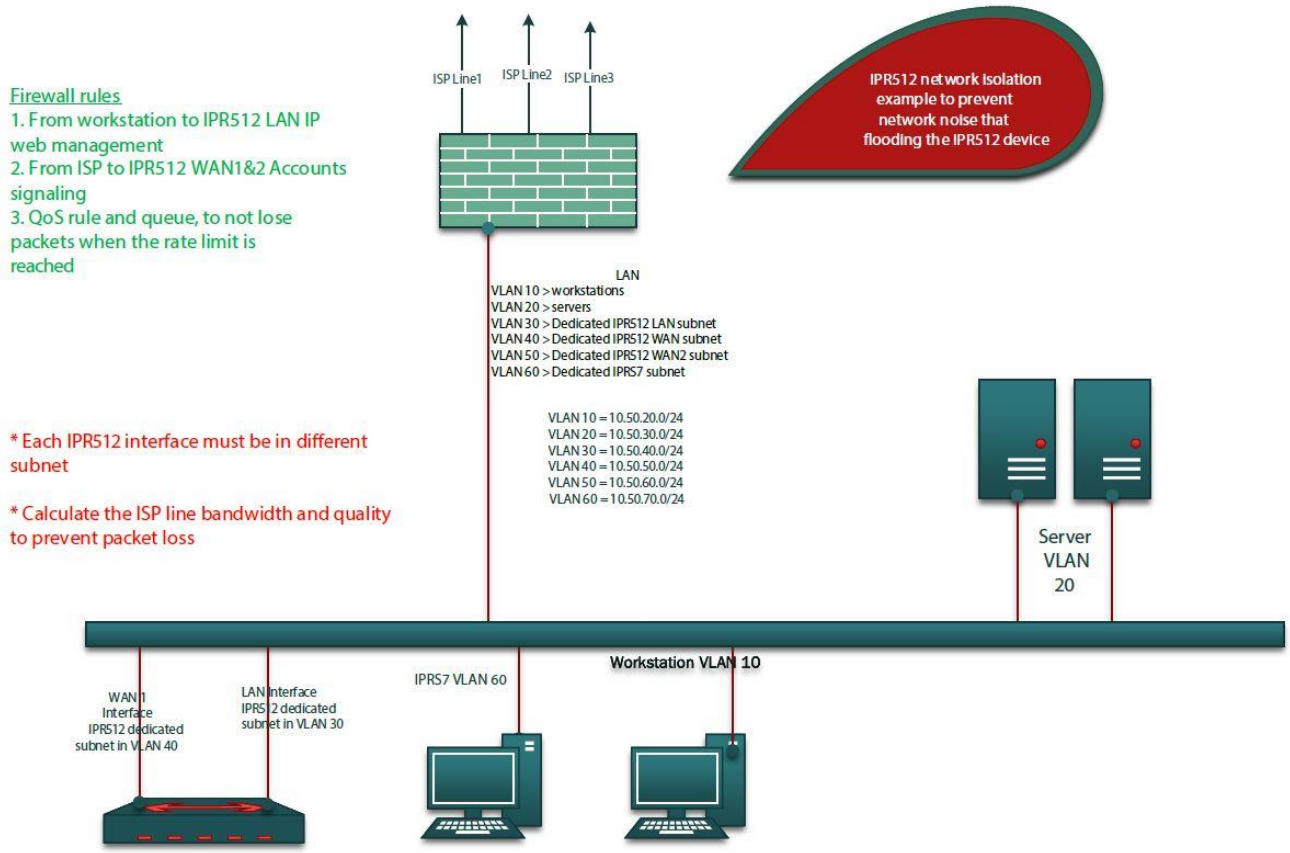


Fig. 28 Network isolation using VLANs

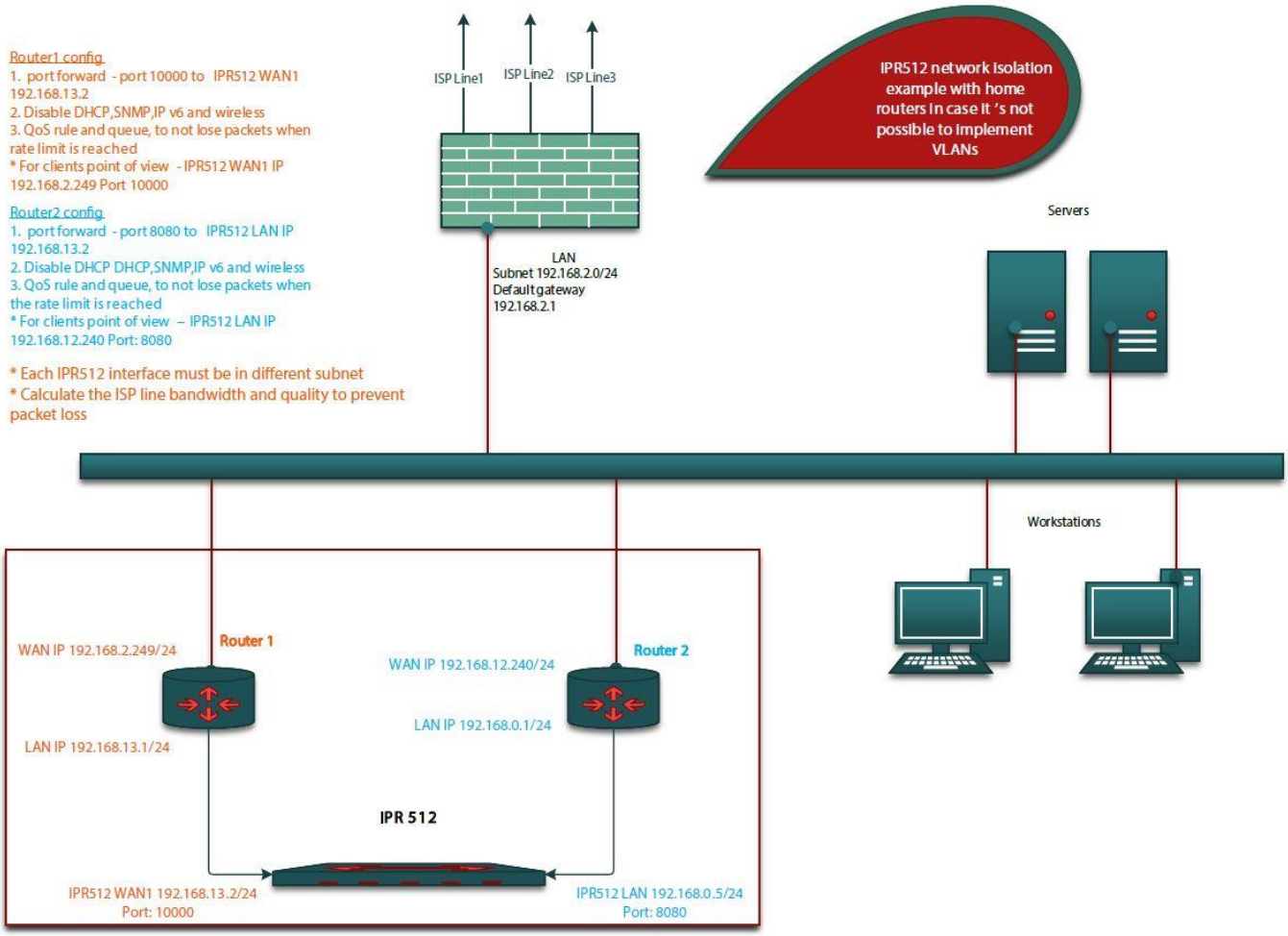


Fig. 29 Network isolation using routers