

PARADOX

IPC10

IP to CMS Converter



PARADOX IP REPORTING TO IPC10

Version 1.0

October 2nd, 2024

TABLE OF CONTENTS

1. Reporting configuration for EVOHD+ panel	4
1.1. Report codes configuration	4
1.2. Report Codes Format Configuration	5
1.3. Central Station Info Configuration	5
1.4. Reporting options	6
1.5. GPRS Service Provider Info	6
1.6. Event call direction (for backup landline reporting only)	7
2. Reporting configuration for MG/SP+ panels	8
2.1. Report codes configuration	8
2.2. Report codes format configuration	9
2.3. Central station info configuration	9
2.4. Reporting options	10
2.5. GPRS Service Provider Info	10
3. IPC10 Configuration	11
3.1. Initial Configuration Setup	11
3.1.1. Powering up the Receiver	11
3.1.2. Locating the Receiver's IP Address	11
3.1.3. Accessing the Web User Interface	12
3.1.4. Naming and Password Setup	12
3.2. IPC10 Web Interface/UI	13
3.3. Events	14
3.4. Accounts	15
3.5. Configuration	16
3.5.1. Receiver Users	16
3.5.2. Network configurations	17
3.5.3. CMS Configuration	18
3.5.4. Other Configuration	20
3.5.5. Receiver Events	20
3.6. About	21
4. Reporting to IPC10 Receiver (Internet Connection)	22
5. Reporting to IPC10 Receiver in closed networks (No Internet)	24
6. BabyWare Closed Network Connection	27
6.1. BabyWare MQTT Closed Network Connection Via IPC10	27
6.2. BabyWare IPC Server (closed network only)	28

Preface

This document explains Paradox IPC10 reporting in-depth and covers the following topics:

- Panel reporting configuration
- IPC10 configuration and operation
- BabyWare closed network connection

General presentation

The IPC10 receives signals from Paradox systems/accounts encoded with Paradox IP protocol, records them, converts them to known formats, and sends them to central monitoring station (CMS) software. The IPC10 is based on MQTT (Message Queuing Telemetry Transportation) technology that is continuously supervised, reliable, and fast. Reporting from the Panel to the CMS, the cycle is usually less than 100ms. Created for the modern CMS with a low footprint and minimal wire connections, it offers a high account capacity of up to 5,000, one cable connection, very low power consumption (6W), reliability, and redundancy with less than 5 minutes replacement time if needed to full operation.

The IPC10 includes backup batteries for up to 20 hours of operation and will work in a closed network without internet with supported versions of reporting devices (IP180, IP150+MQ, IP150MQTT, PCS265V8).

Protocols

MQTT protocol is used between our field communication devices (IP180, IP150+MQ, IP150MQTT, or PCS265V8) 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: SURGARD MLR2-DG, ADEMCO 685, and ADEMCO CID-TCP.

If the CMS software is compatible with one of these protocols, it can be integrated with our receivers.

IP reporting structure (Requirements):

For IP reporting, the following components are required:

- Field communication devices: IP180, IP150+MQ, IP150MQTT or PCS265V8 devices connected on the panel's serial port.
- Hardware receiver – IPC10 V1.02.000 and up.
- POE Switch or POE Injector.
- CMS automation software which is connected through Ethernet to IPC10. This software is not developed by Paradox and will communicate with our receiver through one of the following open-source protocols: SURGARD MLR2-DG, ADEMCO 685, or ADEMCO CID-TCP.

Note:

- IP180 and PCS265V8 devices can be configured for reporting up to four receivers, and IP150+MQ, IP150MQTT up to two receivers.
- If you are currently reporting to three receivers, once you upgrade to an IP150+/IP150 MQTT version, you will no longer be able to configure or report to three receivers.
- A mix of MQTT and TURN communication devices on the same panel is not supported.

1. REPORTING CONFIGURATION FOR EVOHD+ PANEL

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 the Contact ID report code format is used, then all events should be set as FF. Best practice: type "FF" in the main field 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.

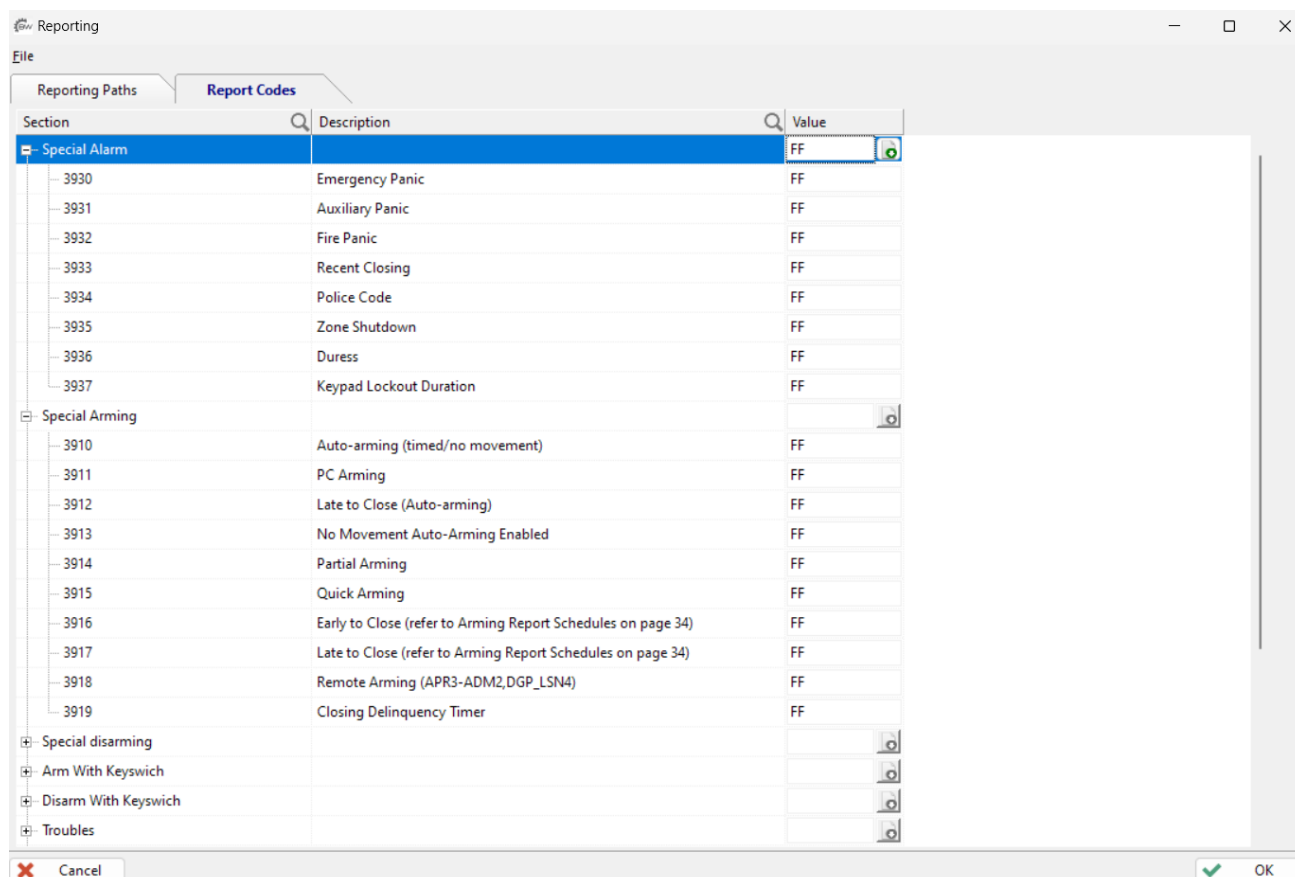


Fig. 1 Report Codes

1.2. REPORT CODES FORMAT CONFIGURATION

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

Report Code Format

Phone #1 / Receiver MAIN: ADEMCO CONTACT ID

Phone #2 / Receiver BACKUP: ADEMCO CONTACT ID

Phone #3 / Receiver PARALLEL: ADEMCO CONTACT ID

Phone #4: ADEMCO CONTACT ID

Reporting Options

Account # Transmission: By Area

Report zone restore: Bell Cut-Off

Delay Alarm Transmission: 000 sec.

Delay Power Failure Report: 030 min.

Power failure restore report delay: 030 min.

Auto Test Report Every

☒ Every: 000 days At 0:00

☐ Every hour on the minute: 0

☐ Every: 005 min. minutes when armed, 060 min. minutes when disarmed

☐ Every hour on the minute: 0

Every 000 min. minutes when armed

Every 000 min. minutes when disarmed

Reporting Options	Area 1	Area 2	Area 3	Area 4	Area 5	Area 6	Area 7	Area 8
Report System Disarming	Always	Always	Always	Always	Always	Always	Always	Always
Recent closing	000 sec	000 sec	000 sec	000 sec	000 sec	000 sec	000 sec	000 sec

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.

Up to four receivers can be configured for reporting (IP180, PCS265V8), and up to two receivers for IP150+MQ, IP150MQTT.

Note: If you are currently reporting to three receivers, once you upgrade to an IP150+/IP150 MQTT version, you will no longer be able to configure or report to three receivers.

The following parameters should be programmed in the Central Station Info tab (Fig. 3):

- IPC10 Receiver's IP Address and Port.
- Receiver password – IP Password is NOT required when using an IPC10 receiver.
- Register button – after all receiver parameters are programmed and sent to the panel, click on the Register button.
- IP Profile – is used to set the security profile polling and supervision time of the communication module.
- Account Number - 4 digits hexadecimal account to identify the site.

The screenshot shows the 'Central Station Info' window in the Paradox software. Red arrows and boxes highlight specific features:

- IPC10 IP and PORT:** Points to the 'WAN1 IP Address' and 'WAN1 IP Port' fields.
- Security Profile:** Points to the 'IP Profile' dropdown menu.
- Register Button:** Points to the 'Register' buttons for each receiver.
- Registration Status:** Points to the 'COM 1' and 'COM 2' status columns.
- Account Number:** Points to the 'Main/Backup account #' field.

Receiver	WAN1 IP Address	WAN1 IP Port	IP Password (*)	IP Profile	Register	COM 1	COM 2
MAIN	82.76.223.153	5000	123456	04	Register	Registered	Registered
BACKUP	192.168.1.230	8883	123456		Register	Registration Error	Unregistered
PARALLEL	0.0.0.0	10000	123456		Register	Registration Error	Registration Error

Main/Backup account #: 1111

Also refer to the Account # Transmission feature in the Global Settings tab

(*) IP Password is not required when using an IPC10 receiver.

Fig. 3 Central Station Info

1.4. REPORTING OPTIONS

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

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

The 'Reporting Options' window shows the following settings:

- Reporting (GPRS/IP): ☒
- Dialer Channel: ☒ Dialer used as backup to GPRS/IP ☐ Dialer used in addition to GPRS/IP
- GPRS/IP Service Failure Options: Trouble Only

Fig. 4 Reporting options

1.5. GPRS SERVICE PROVIDER INFO

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

The 'GPRS Service Provider Info' window contains the following fields:

- Access Point Name (APN): Carrier'sAPN
- User Identification: Carrier'sUsername
- Password: Carrier'sPassword

Fig. 5 GPRS Service Provider Info

1.6. EVENT CALL DIRECTION (FOR BACKUP LANDLINE REPORTING ONLY)

Event groups can be programmed to dial up to four monitoring station telephone numbers with one used as a backup. Four event groups can be programmed to report to one or multiple monitoring station telephone numbers: Arm/Disarms, Alarm/Restore, Tamper/Restore, and Trouble/Restore (Fig. 6).

Reporting Paths | Report Codes

Call Direction | Global Settings | Landline and GSM | GPRS/IP | SMS (Text Messages) | Voice (VDMP3) | PC Communication (BabyWare)

Arming/disarming

Arm/Disarm Events	Area 1 Area 1	Area 2 Area 2	Area 3 Area 3	Area 4 Area 4	Area 5 Area 5	Area 6 Area 6	Area 7 Area 7	Area 8 Area 8
Phone #1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Phone #2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone #3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone #4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup on	Phone #4	None	None	None	None	None	None	None

Alarm Restore

Alarm/Restore	Area 1 Area 1	Area 2 Area 2	Area 3 Area 3	Area 4 Area 4	Area 5 Area 5	Area 6 Area 6	Area 7 Area 7	Area 8 Area 8
Phone #1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Phone #2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone #3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone #4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup on	None	None	None	None	None	None	None	None

Tamper Restore

Tamper Restore	Area 1 Area 1	Area 2 Area 2	Area 3 Area 3	Area 4 Area 4	Area 5 Area 5	Area 6 Area 6	Area 7 Area 7	Area 8 Area 8
Phone #1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Phone #2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone #3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Phone #4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup on	None	None	None	None	None	None	None	None

Trouble restore

Event	Phone #1	Phone #2	Phone #3	Phone #4	Backup on
Trouble/Restore All Areas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Phone #4
Special Report Codes All Areas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None

Cancel OK

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 the Contact ID report code format is used, then all events should be set as FF. Best practice: type "FF" in the main field 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.

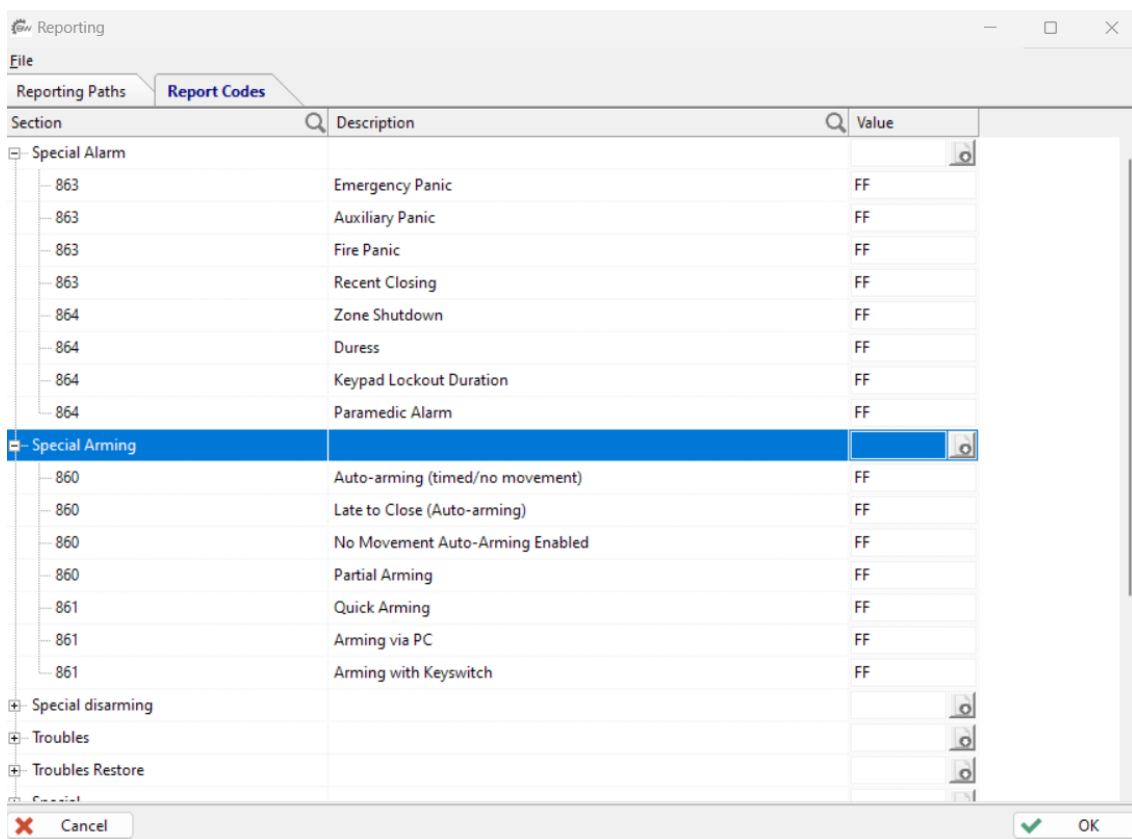


Fig. 7 Report Codes on MG/SP+ panels

2.2. REPORT CODES FORMAT CONFIGURATION

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

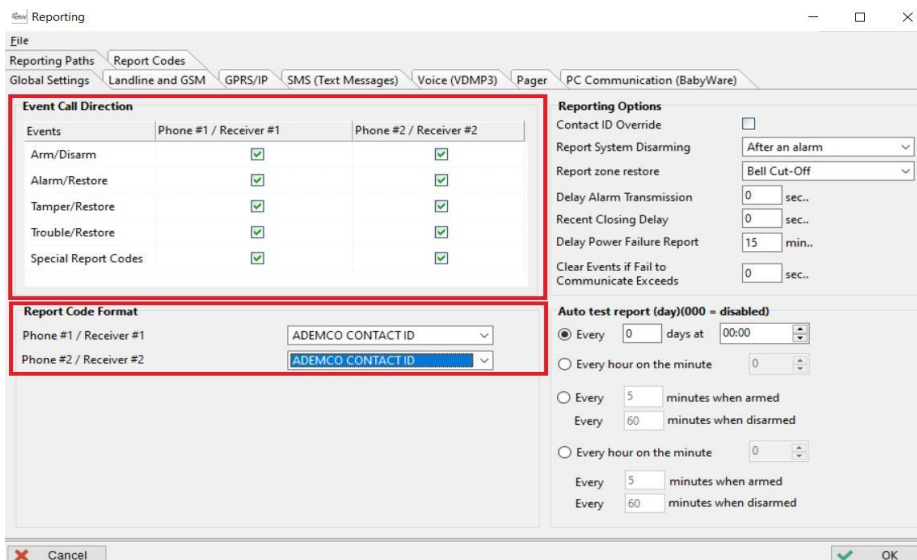


Fig. 8 Global settings

2.3. CENTRAL STATION INFO CONFIGURATION

Up to four receivers can be configured for reporting (IP180, PCS265V8), and up to two receivers for IP150+MQ, IP150MQTT.

Note: If you are currently reporting to three receivers, once you upgrade the IP150+/IP150 to MQTT firmware, you will no longer be able to configure or report to three receivers.

The receiver parameters need to be programmed in the Central Station Info section (Fig. 9) from the GPRS/IP tab.

The following parameters should be programmed in the Central Station info tab:

- IPC10 Receiver's IP Address and Port.
- Receiver password – IP Password is NOT required when using an IPC10 receiver.
- Register button – after all receiver parameters are programmed and sent to the panel, click on the Register button.
- IP Profile – is used to set the security profile polling and supervision time of the communication module.
- Account number – is a 4-digit hexadecimal account used to identify the site or different areas of a system. Both areas can be registered on the same account or different accounts for each area, if needed.

IPC10 IP and PORT

Security Profile

Register Button

Registration Status

IP Receiver	WAN1 IP Address	WAN1 IP Port	WAN2 IP Address	WAN2 IP Port	IP Password (*)	IP Profile	Register	Registration Status COM 1	Registration Status COM 2
IP Receiver #1	082.076.223.153	5000	000.000.000.000	10000	123456	4	Register	Registered	Registration Error
IP Receiver #2	192.168.001.232	8883	000.000.000.000	10000	123456	4	Register	Registered	Registration Error
Backup IP Receiver	000.000.000.000	10000	000.000.000.000	10000	123456	4	Register	Registration Error	Registration Error

(*) IP Password is not required when using an IPC10 receiver.

Area 1 IP Account # 2222

Area 2 IP Account # 2222

Account Number

Fig. 9 Central Station Info

2.4. REPORTING OPTIONS

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

- 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 the receiver.
- 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).
- 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 an audible alarm when the system is armed.

Reporting Options

Reporting (GPRS/IP) ☒

Dialer Channel Dialer used as backup to GPRS/IP

GPRS/IP Service Failure Options Trouble Only

Fig. 10 Reporting options

2.5. GPRS SERVICE PROVIDER INFO

If a PCS module is used for reporting, then the SIM card APN, username and password should be filled in, to be able to connect to the carrier's data network (Fig. 11). Access Point Name, Username and password credentials can be sent through SMS command as well.

GPRS Service Provider Info

Complete this section if you are using a PCS module for GPRS communication

Access Point Name (APN) 0/32

User Name 0/32

Password 0/32

Fig. 11 GPRS Service Provider

3. IPC10 CONFIGURATION

The IPC10 is designed to receive Ethernet IP Data from Paradox systems, convert them from Paradox encrypted IP protocol to CID format via MLR2-DG, Ademco 685, or Ademco CID-TCP protocols, and send them over Ethernet to the central monitoring station (CMS) software.

The IPC10 can be mounted on a 19" (48.3 cm) rack, using 1U of vertical space. Use appropriate mounting hardware to secure the unit to the rack.



Fig. 12 IPC10 Overview

3.1. INITIAL CONFIGURATION SETUP

3.1.1. Powering up the Receiver

Connect the Ethernet cable from the router with POE (max 8W consumption) to the Ethernet port located in front of the IPC10.

3.1.2. Locating the Receiver's IP Address

- **Using an IP Scanner:**

Search for the IP address of the IPC10 using a standard IP scanner. It will appear as IPC10-SERIALNUMBER. The serial number will be printed on the label of the IPC10 in the back.

- **Using Command Prompt:**

Open Command Prompt (CMD) on a Windows PC in the same network as the IPC10. Enter the following command: `arp -a | findstr receiver's Mac address` (printed on the label located on the back of the IPC10 unit).

Example: `arp -a | findstr e4-5f-01-33-4f-91`

The IP address of the IPC10 receiver should be displayed (Fig. 13).

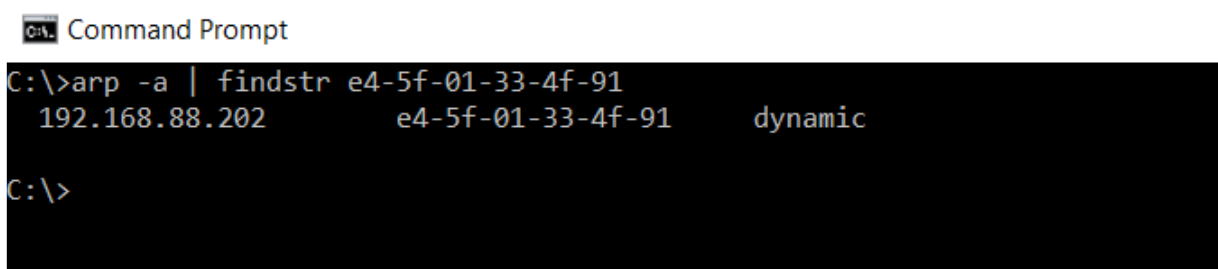


Fig. 13

3.1.3. Accessing the Web User Interface

Enter the IPC10 IP address you found in a web browser, followed by port 8080 to access the web user interface (e.g., <http://192.168.88.202:8080>). The UI page will appear on your browser (*Fig. 14*) The USER LED on the receiver will light up.

Fig. 14

3.1.4. Naming and Password Setup

The IPC default name is IPC10-Serial number. This will be used to identify the IPC10 physically in case you have more than one IPC10 on the network. We suggest printing the name and sticking it on the front of the receiver. When multiple IPC10s are installed, you can also locate it with the user LED that will be ON when logged in.

Enter a password of a minimum of six alphanumeric or symbols (case-sensitive) characters. Confirm the password.

Enter your email address. Confirm email address. Press the Verify Email button. A confirmation email with a code will be sent. Enter the code from email. Press Login.

If you forget your password, click the Forgot Password link on the Login screen, enter the Owner's email, a verification code will be sent. Enter the code from the email. Create a new password. Confirm password. Click Reset Password.

If you are on a closed network, skip the email verification by clicking on the checkbox.

3.2. IPC10 WEB INTERFACE/UI

To access the web interface of the receiver, the LAN IP and UI Web Port should be accessed in a web browser (*Fig. 15*).

The IPC10 name and password are configured in the initial [IPC10 Configuration Setup](#).

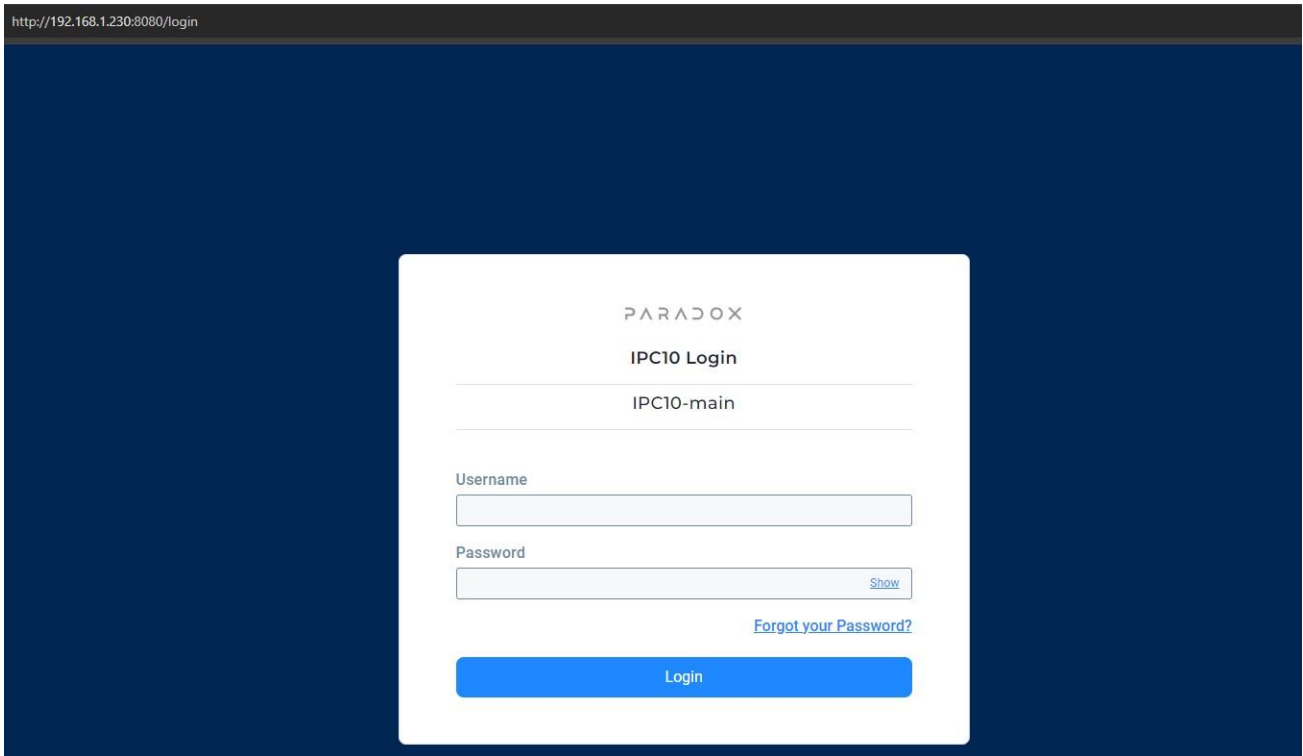


Fig. 15 IPC10 web interface login

The IPC10 web page provides access to the following four menu options:

Events – Allows to view account and converter-related events, which can be useful if CMS is down. Up to 20,000 events will be buffered based on a first-in, first-out basis.

Accounts – Allows to view or suspend from CMS reporting accounts.

Configuration – This section facilitates users management, setup of network parameters and necessary fields (IP address, port, time, CMS configuration, etc.).

About – Provides IPC10 information and security profiles.

3.3. EVENTS

The Events tab displays the information related to events received from the accounts, such as date and time, account number, event CID number, description, panel serial numbers, reporting device, device type/connection, and zone/user (Fig. 16). This page includes an option to export the events data to an Excel file.

The columns for IPC10 received time, Account#, Event CID#, Panel S/N, and Reporting Device S/N can be sorted in ascending or descending order. The refresh time (7, 15, or 20 seconds) can be modified and will be kept while the session is active.

IPC10 received time	Panel event time	Account#	Event CID#	Description	Panel S/N	Reporting Device S/N	Device Type/Connection	Area	Zone/User
28-Mar-2024 11:19:58	26-Apr-2024 06:20:23	1234	E 144	Sensor tamper	07010867	S16ZSEX6	IP (ETH)	1	9
28-Mar-2024 11:19:56	26-Apr-2024 06:20:22	1234	E 144	Sensor tamper	07010867	S16ZSEX6	IP (ETH)	1	1
28-Mar-2024 11:19:30	26-Apr-2024 06:19:55	1234	R 144	Sensor tamper	07010867	S16ZSEX6	IP (ETH)	1	9
28-Mar-2024 11:19:28	26-Apr-2024 06:19:53	1234	R 144	Sensor tamper	07010867	S16ZSEX6	IP (ETH)	1	1
28-Mar-2024 11:19:26	26-Apr-2024 06:19:51	1234	E 144	Sensor tamper	07010867	S16ZSEX6	IP (ETH)	1	9
28-Mar-2024 11:19:23	26-Apr-2024 06:19:48	1234	E 144	Sensor tamper	07010867	S16ZSEX6	IP (ETH)	1	1
28-Mar-2024 11:18:17	28-Mar-2024 11:17:42	8000	E 110	Fire	29303ED8	S172061CF9	IP (ETH)	1	1
28-Mar-2024 11:18:02	28-Mar-2024 11:17:27	7777	E 401	Open/Close by User	310A93CA	S172058B317	IP (ETH)	2	1
28-Mar-2024 11:18:01	28-Mar-2024 11:17:26	7777	E 406	Cancel	310A93CA	S172058B317	IP (ETH)	2	1
28-Mar-2024 11:17:59	28-Mar-2024 11:17:25	7777	E 401	Open/Close by User	310A93CA	S172058B317	IP (ETH)	1	1
28-Mar-2024 11:17:58	28-Mar-2024 11:17:24	7777	E 406	Cancel	310A93CA	S172058B317	IP (ETH)	1	1
28-Mar-2024 11:17:49	28-Mar-2024 11:17:13	feff	E 100	Medical	28204827	S1720617CA	IP (ETH)	2	0
28-Mar-2024 11:17:48	28-Mar-2024 11:17:12	feff	E 100	Medical	28204827	S1720617CA	IP (ETH)	1	0
28-Mar-2024 11:17:44	28-Mar-2024 11:16:24	0333	E 401	Open/Close by User	2A02EEBA	S172053EDA	IP (ETH)	2	1
28-Mar-2024 11:17:42	28-Mar-2024 11:16:23	0333	E 406	Cancel	2A02EEBA	S172053EDA	IP (ETH)	2	1
28-Mar-2024 11:17:41	28-Mar-2024 11:16:21	0333	E 406	Cancel	2A02EEBA	S172053EDA	IP (ETH)	1	1
28-Mar-2024 11:14:04	28-Mar-2024 11:13:23	0555	R 144	Sensor tamper	21000179	S17205ACBC	IP (ETH)	1	1
28-Mar-2024 11:14:00	28-Mar-2024 11:13:20	0555	E 144	Sensor tamper	21000179	S17205ACBC	IP (ETH)	1	1
28-Mar-2024 11:08:18	28-Mar-2024 11:07:57	8999	E 602	Periodic test report	0860204B	S17205B30C	IP (ETH)	0	0

Fig. 16 IPC10 Events tab

The green top message "CMS online for" indicates that the connection has been established with the CMS software receiver, and the counter (is informative) indicates how long the connection has been maintained. The counter resets whenever the connection is lost and re-established with the CMS, or if any receiver settings are changed.

The "Panel event time" displays the actual Panel time (programmed in the Panel), while the "IPC10 received time" displays the receiver time (it will follow the date and time configured in the Other Configuration section of the Configuration tab). The receiver time is also displayed in the top right corner.

The receiver Time Zone should be properly adjusted to suit the country's Time Zone.

Note 1: Events in Green are already sent to the CMS. Events in black are buffered, in case the CMS does not provide ACK. If no ACK, a message in red will appear in the UI.

Note 2: Events will be erased on the power cycle, events are kept in memory during firmware upgrades.

Priority queue feature: any alarm reported bumps up to the top of the reporting queue to be reported first.

3.4. ACCOUNTS

The Accounts tab allows you to view the status of the system's accounts (Fig. 17) and also provides the possibility to suspend accounts from reporting to CMS (if unpaid as an example).

Offline accounts over 30 days will be deleted from the account list automatically. They will register if they become online.

Account	Profile	Status	Suspend	Panel S/N	Panel Version	Reporting Device S/N	Reporting Device Version	MAC Address
6666	04	ONLINE		05080071	7.80.003	S172053C17 (IP)	6.15.000	00:19:ba:1a:5a:38
0908	04	OFFLINE		086024C0	1.08.001	S13PYJGF (IP)	1.00.015	fc:b4:67:b8:ba:58
9199	03	ONLINE		086024BE	1.08.001	710519E5 (IP)	6.02.024	00:19:ba:0b:37:4f
0905	04	ONLINE		0700AF2F	7.70.018	S172053C66 (IP)	6.15.000	00:19:ba:1a:5a:87
2222	04	OFFLINE		0700CB6F	7.70.018	S13E7NFR (IP)	1.00.015	b0:b2:1c:f3:84:c4
2222	04	OFFLINE		0700CB6F	7.70.018	S13E7NFR (PCS)	8.00.073	00:19:ba:1a:c9:9f
3131	04	OFFLINE		2A20182D	1.30.001	S17D115D05 (PCS)	8.00.073	00:19:ba:1a:c9:9f
f0f0	02	ONLINE		29128C5E	7.17.000	71062225 (IP)	6.02.024	00:19:ba:0c:a5:37
5145	04	OFFLINE		2130D856	1.28.001	S172053C6D (IP)	6.15.000	00:19:ba:1a:5a:8e
8991	01	OFFLINE		0700683E	7.70.018	S13E7NFR (IP)	6.02.027	00:19:ba:08:35:e7

Fig. 17 IPC10 Accounts tab

To suspend an Account: Click on the 3-dot menu option (left of account) and select suspend account if desired. Suspended accounts will no longer send events to CMS, to unsuspend. Click again on the 3 dots and select unsuspend.

Online	Number of accounts or devices online. The online accounts can be viewed by pressing the ONLINE (green) button.
Offline	Number of accounts or devices offline. The offline accounts can be viewed by pressing the OFFLINE (red) button.
Suspend	Number of accounts or devices suspended. Press on the 3 dots on the left of the account to suspend and repeat to restore. The suspended accounts can be viewed by pressing the SUSPENDED (purple) button.
Waiting	This status will be displayed within five minutes after a reboot of the receiver displaying the accounts/devices waiting for a restore connection. After five minutes, all should be ONLINE and all devices/accounts that have not been restored will have an OFFLINE status and reported to CMS as OFFLINE and the button will be grayed out.

Note: The Search functionality is available only for panel S/N, reporting device S/N or account #.

3.5. CONFIGURATION

The Configuration tab is used to program the IPC10, and provides access to the following options:

3.5.1. Receiver Users

Allows the management of users for the IPC10 receiver. Up to 25 users may be added to the IPC10.

Configuration

CMS online for 15 days 12:05:09 2024-07-26 14:24:52

Receiver Users 4 / 10 ADD USER + Save Changes

ID	Username	First name	Last name	Permissions	Password
1	ealves@paradox.com			Owner	*****
2	jsmith@gmail.com	John	Smith	Master	*****
-	kbrown@gmail.com	Kate	Brown	View only	*****
-	mwaters@gmail.com	Michael	Waters	View only	*****

IPC10 offer three levels of users:

Owner: Has full rights in the receiver and can create or delete masters and users. Only the owner can have an email address to be used, as forgot password restore email address.

On first power up or after reset to default, (or if you upgrade from previous versions), Owner is required to enter username, email address and confirm email address. A verification email will be sent verification code, once code entered, this email will be used to recover owner password. For log in, Owner needs username and his password.

Master: Has the same rights as the Owner, except for the ability to add, edit or delete users.

User: Users have view-only rights for the events list and accounts.

3.5.2. Network configurations

Allows to configure the IPC10 receiver network parameters (Fig. 18).

Network Configurations Save Changes

WAN

DHCP ☒

UI Web Port

Reporting Device Port

IP Address · · ·

Netmask · · ·

Gateway · · ·

DNS Primary · · ·

DNS Secondary · · ·

Fig. 18 Network configurations

DHCP

DHCP is selected by default. The IP address will be assigned by the router.

STATIC IP ADDRESS must be programmed at the CMS router by the IT manager based on the MAC address of the IPC10 that can be found on the About page.

Note 1: After configuring a static IP address, press the “Save Changes” button and reload the page using the new IP address.

Note 2: If a wrong IP address is saved, you can restore the DHCP status by pressing momentarily (up to 3 sec.) on the DHCP/Reset button.

UI Web Port

The default port is set to 8080 and can be changed if needed. Defines the port number assigned for Web User Interface access. Port numbers can be between 1 to 65535.

Note: After configuring the Port number, press the “Save Changes” button and reload the page using the new Port number.

Reporting Devices

The default MQTT Port access is 8883 (not configurable) and **MUST** be open on the router and ISP. The proper port forwarding configuration should be set from the public port to port 8883 on the receiver.

IP Address

Defines the local IPC10 receiver network address set up by the CMS IT manager. The IP address programmed at the reporting device’s end is forwarded internally at the CMS to the local IP address of the receiver.

The remaining fields should be assigned by the DHCP (network, gateway, DNS, primary, and secondary) or programmed manually if the DHCP is off.

Note: If the IPC10 is NOT in the same network as the communication modules (IP180, IP150+MQ, IP150MQTT, PCS265V8), the receiver’s Reporting Device Port (8883) must be forwarded.

3.5.3. CMS Configuration

Allows to configure the CMS Output protocol, IP, Port, and other CMS-related parameters (*Fig. 19*).

The IPC10 will connect to CMS software via local Ethernet and supports Sur-Gard MLR2-DG, Ademco 685, or Ademco CID-TCP formats.

The parameters should be set according to the protocol used and to the monitoring software requirements (*Fig. 20*)

Fig. 19 IPC10 CMS Configuration

Fig. 20 CMS Software Connection Configuration (CMS UI)

Security Protocol – The protocol used by the IPC10 Converter to the CMS software. Supported protocols are MLR2-DG (default), Ademco CID-TCP, and Ademco 685.

IP – Defines the IP address assigned to the CMS Software (IP address of the CMS host PC)

Port – Defines the port number assigned to CMS Software. Port numbers can be between 1 to 65535 (needs to be forwarded if the IPC10 and CMS Software are not in the same network).

Receiver ID – Defines the unique ID assigned to the IPC10. The Receiver ID can be between 0 and FF for Sur-Gard MLR2 and 0 to F for Ademco 685 and Ademco CID-TCP.

Group ID – Allows to assign the converter to a group ID in the central station setup. Can be between 0 to FFF for Sur-Gard MLR2 and 0 to F for Ademco 685 and Ademco CID-TCP.

Wait ACK/NACK – Defines the interval in seconds (1 to 15 seconds, default 3 seconds) which the IPC10 will wait for an acknowledgment from the CMS software, before sending the next event. If no ACK/NACK is received the IPC10 will retry sending the same event.

Link Test – Defines the interval in seconds (15 to 240 seconds, default is 30 seconds) at which the link test is sent to the CMS software (0 = disable).

Test Network – This allows you to test the communication between the IPC10 receiver and the CMS software. Once the test is complete, a Testing CMS Network window will be displayed indicating the results of the test.

Two-Stage Authentication – Defines if two-stage authentication is Enabled or Disabled.

CMS Tag – The default is set to 0. Add custom CMS tag if needed (1 or 2 Hex characters).

Additional Field – Additional information can be added to the event transmitted to the CMS like panel SN, device SN, or MAC address (default is set to none).

Below is an example of the IPC10 event code explanation for MLR2-DG and Ademco protocols (*Fig. 21*).

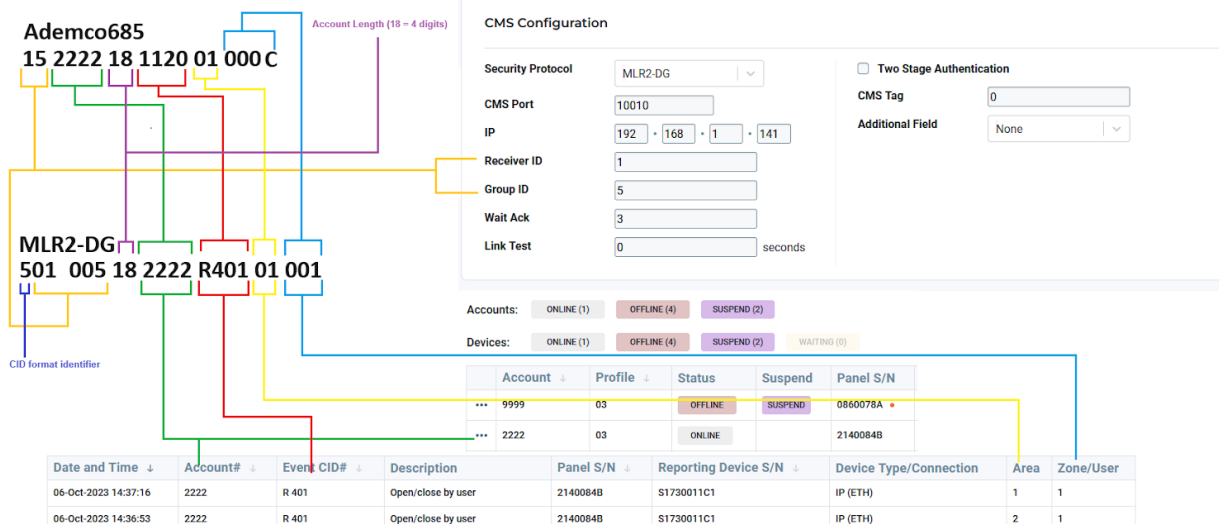


Fig. 21

Example of IPC10 receiver custom event:

MLR2-DG: 5015 180001E711100000

5 - protocol format

015 - Receiver ID (1) and group ID (5) – can be set in IPC10

18 - Token used to identify the message as contact ID

0001 - IPC10 account# – can be set in receiver settings

E711- Receiver custom event code - Web login event – can be set in IPC10

00 - Area - no area – receiver event

000 - User - no area – receiver event

Ademco: 15 0001 18 1711 00 000 C

15 - Receiver ID (1) and group ID (5) – can be set in IPC10

0001 - IPC10 account# – can be set in receiver settings

18 - Token used to identify the message as contact ID

1711 - Receiver event code - Web login event – can be set in IPC10 (1 - Event, 3 – Restore)

00 - Area - no area – receiver event

000 - User - no area – receiver event

E – Checksum

3.5.4. Other Configuration

IPC10 receiver Date and Time, NTP server, and Time Zone related configuration (Fig. 22).

Other Configuration

Date and Time

NTP

NTP Server: time.windows.com

Alternative NTP Server: 1.pool.ntp.org

Timezone: Europe/Bucharest

Set clock Save Changes

Fig. 22

Primary NTP – Main NTP server to use for the IPC10 database and time (functions only with the internet).

Alternate NTP – Alternative NTP as a backup of the primary NTP server (functions only with the internet).

Time Zone – Select the time zone to match the IPC10 location.

Set Clock – In closed networks, in rare cases, the clock might need adjustments with the set time button. When the internet is available, time will be adjusted automatically.

3.5.5. Receiver Events

Internal events of IPC10 reported to CMS, can be customized by CMS (Fig. 23).

Note: All changes will revert to default if the IPC10 is reset.

Receiver Events SN 100000002628c1446

Receiver Settings: Account# 0001 Reporting format: CID

Events description	Report CID
Web login	711
IPC10 power up	730
Account database reached 75%	700
Account database is full	0
Good Will account disconnect from CMS	710
Auto delete account offline	720
New account connected to IPC10	705

Save Changes

Fig. 23

In addition to the customizable receiver event codes, the IPC10 receiver also transmits the following events to the CMS software (cannot be modified):

Lost panel (E552) / Restore panel (R552) – If the panel is not communicating with the IP device, it will be displayed as Panel Lost in the Suspend column, and code E552 will be reported to the CMS. When restored, code R552 will be reported. Not listed in the events of the receiver.

IP unit lost (E551) / IP unit online restore (R551) – If the IP Communicator is not polling to the IPC10, it will be displayed as OFFLINE in the Status column, and code E551 will be reported to CMS. When restored, code R551 will be reported. Listed in the events of the receiver.

PCS offline (E554) / PCS online (R554) – PCS offline and restore code. Listed in the events of the receiver.

Time /Local time zone change (E625) – When the receiver's time zone or clock is adjusted, code E625 will be reported to CMS.

IPC10 power failure (E314/R314) – When the receiver's power source is disconnected.

At the bottom of the Configuration page, Generate Logs and Restore Factory Default buttons can be found:

Generate Logs – creates a log file that will be saved in the default download folder set in the browser.

Restore Factory Default – resets the IPC10 to factory defaults.

3.6. ABOUT

The About tab provides access to IPC10 receiver system details, including firmware version, last upgrade timestamp, receiver production date (Birthdate), Serial number, MAC address, System Metrics, and firmware upgrade (Fig. 24)

Receiver Info

VERSION	LAST UPGRADE	BIRTHDATE	ACCOUNTS USED
IPC10 version 1.1.7	02-Sep-2024 10:00:17	N/A	10 of 5000
Serial #	MAC Address:		
10000000c08c86e3	d8:3a:dd:3a:df:cb		

System Metrics

LOAD AVERAGE LAST MINUTE	LOAD AVERAGE LAST 5 MINUTES	LOAD AVERAGE LAST 15 MINUTES	CURRENT RUNNING PROCESSES
0%	0%	0%	1

Fig. 24

It also displays the **Security Profiles** (Fig. 25) that provide the supervised time of the monitored accounts.

Security Profiles

IP Module

ID/Devices	Supervision
1	1200 seconds
2	600 seconds
3	300 seconds
4	90 seconds

PCS Module

ID/Devices	Supervision
1	1260 seconds
2	840 seconds
3	420 seconds

Fig. 25

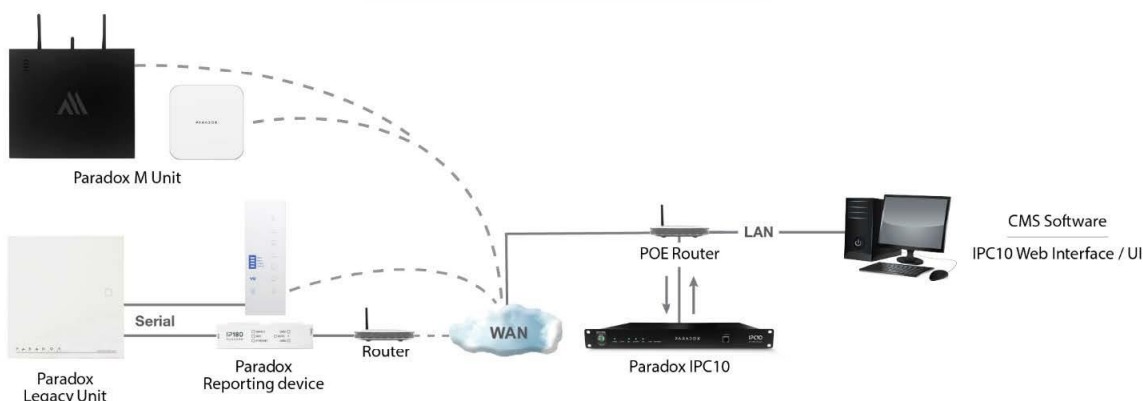
The reporting module (IP/PCS) sends a presence message to the receiver at intervals defined on the module polling time. If the IPC10 does not receive a presence message within the configured supervision time, the receiver will report a supervision loss of the monitoring station's automation software.

The IPC10 can handle up to 5,000 accounts using profile 01, and up to 3500 accounts using profile 04 or any combination.

The ID (e.g. 2) of the polling profile needs to be added as an IP profile (e.g. 02) in BabyWare or in section programming.

Help us to improve: The owner can select this option upon first-time login or in the about page by owner or masters. Only statistics like the number of accounts, processor load, and average load are sent periodically. No specific data of any kind is sent about the device. This will help us to monitor the performance and capabilities of the IPC10 in the future.

4. REPORTING TO IPC10 RECEIVER (INTERNET CONNECTION)



For IP reporting (internet connection), the following components are required for connection/configuration:

- IPC10 v1.02.000 (and up)
- BabyWare v5.6.52 (and up)
- IP150+MQ, IP150MQTT, IP180, PCS265 V8 devices connected on the panel's serial port.

In the example below, three IPC10 receivers are installed on the same network (*Fig. 26*).

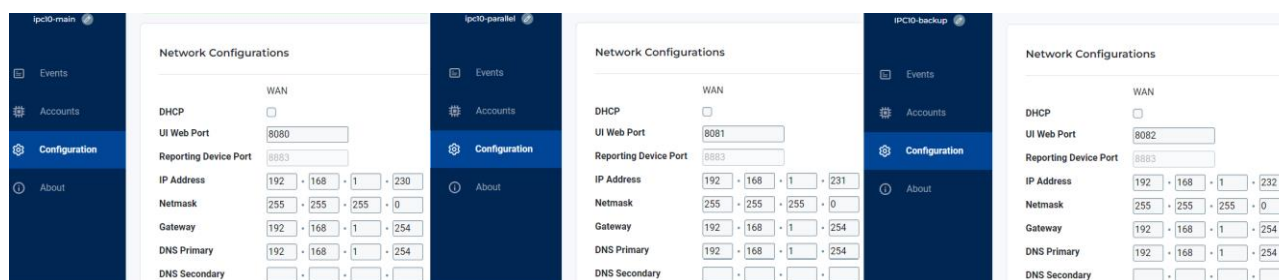


Fig. 26

Local Network Registration

To register an account (communication devices) on all three receivers on the same network, the Central Station Info panel parameters should be programmed as shown in (*Fig. 27*).

Receiver	WAN1 IP Address	WAN1 IP Port	IP Password (*)	IP Profile	Register	COM 1	COM 2
MAIN	192.168.1.230	8883	123456	04	Register	Registered	Registered
BACKUP	192.168.1.232	8883	123456		Register	Registration Error	Unregistered
PARALLEL	192.168.1.231	8883	123456		Register	Registration Error	Unregistered

Main/Backup account # 1111

Also refer to the Account # Transmission feature in the Global Settings tab

(*) IP Password is not required when using an IPC10 receiver.

Fig. 27

External Network Registration

To register an account (communication devices) on all three receivers from outside the network (Public IP), the Central Station Info panel parameters should be programmed as shown in (Fig. 28).

The reporting device port (8883) must also be forwarded on the router to be accessible from outside the network, as shown in (Fig. 29).

The screenshot shows the 'Reporting' window with the 'GPRS/IP' tab selected. The 'Central Station Info' section contains a table for configuring three receivers: MAIN, BACKUP, and PARALLEL. Each receiver has fields for WAN1 IP Address, WAN1 IP Port, IP Password (*), IP Profile, and buttons for Register, COM 1 status, and COM 2 status. The MAIN receiver is registered, while BACKUP and PARALLEL show 'Registration Error'. A 'Main/Backup account #' field is set to 1111. A note at the bottom states: '(*) IP Password is not required when using an IPC10 receiver.'

Receiver	WAN1 IP Address	WAN1 IP Port	IP Password (*)	IP Profile	Register	COM 1	COM 2
MAIN	82.76.223.153	5000	123456	04	Register	Registered	Unregistered
BACKUP	82.76.223.153	5002	123456		Register	Registration Error	Unregistered
PARALLEL	82.76.223.153	5001	123456		Register	Registration Error	Unregistered

Main/Backup account # 1111

Also refer to the Account # Transmission feature in the Global Settings tab

(*) IP Password is not required when using an IPC10 receiver.

Fig. 28

Current Port Forwarding Table:

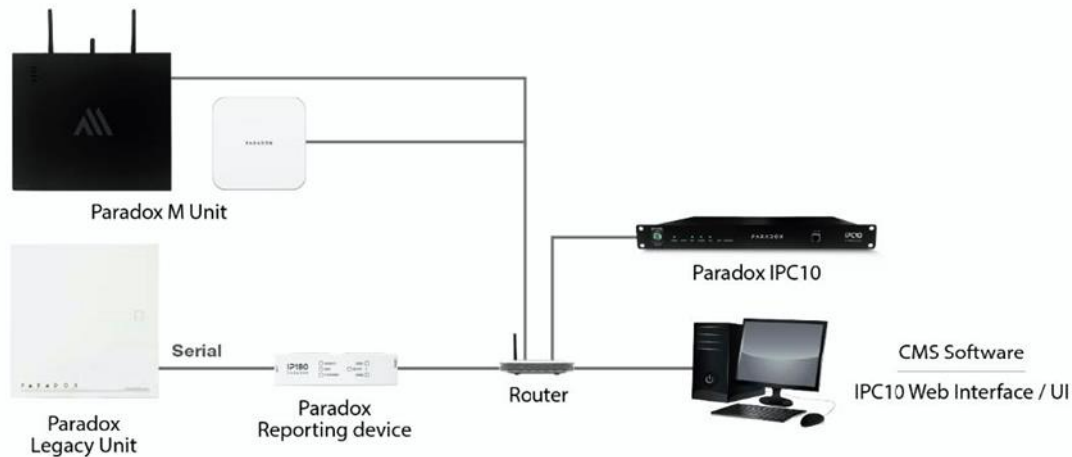
Local IP Address	Protocol	Int Port	Ext Port	Comment	Select
192.168.1.230	TCP+UDP	8883	5000	IPC10-S-Primary	<input type="checkbox"/>
192.168.1.231	TCP+UDP	8883	5001	IPC10-S-Parallel	<input type="checkbox"/>
192.168.1.232	TCP+UDP	8883	5002	IPC10-S-Backup	<input type="checkbox"/>

Fig. 29

Notes:

- IP180 and PCS265V8 devices can be configured for reporting up to four receivers, and IP150+MQ/IP150MQTT up to two receivers.
- If you are currently reporting to three receivers, once you upgrade to MQTT version, you will no longer be able to configure or report to three receivers.
- A mix of MQTT and TURN communication devices on the same panel is not supported.

5. REPORTING TO IPC10 RECEIVER IN CLOSED NETWORKS (NO INTERNET)



For IP reporting in closed networks (no internet), the following components are required for connection/configuration:

- IPC10 v1.02.000 (and up)
- BabyWare v5.6.52 (and up)
- IP150+MQ V6.15.000 (and up)
- IP150MQTT V6.50.000 (and up)
- IP180 V1.00.015 (and up)
- Closed network environment (without internet connection).

To configure reporting, first, please make sure that the network on which the IPC10 and communication devices (IP150+MQ, IP150MQTT, IP180) are located, does not have an internet connection and Swan is disabled on the modules.

To access the web configuration page of the IP150+MQ/IP150MQTT/IP180, and configure the network parameters, please follow the below steps:

1. Please make sure that the IP150+MQ/IP150MQTT/IP180 devices are not connected to the internet.
2. Download IP Exploring Tools (V1.66) from our website (Software & Apps section). Use the IP Exploring Tools, or the BabyWare scan feature when selecting Static IP connection type, to find the IP of the IP150+MQ, IP150MQTT and IP180 modules.
Note: IP Exploring Tools (V1.66) only supports IP150+MQ/IP150MQTT and is not compatible with IP180.
3. Enter the IP address of the module in a web browser.
4. Enter the Installer PC Code of the panel (same as the PC Password in BabyWare, default 0000).
5. Disable Swan from the web interface and change the network parameters (disable DHCP), if required (Fig. 30).

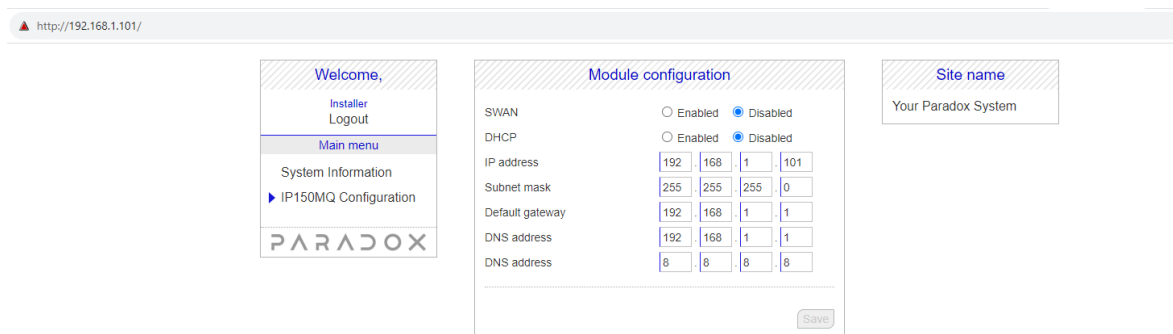


Fig. 30

In the example below, the IPC10 receiver (Fig. 31) is installed in a closed network environment alongside an IP150+MQ module.

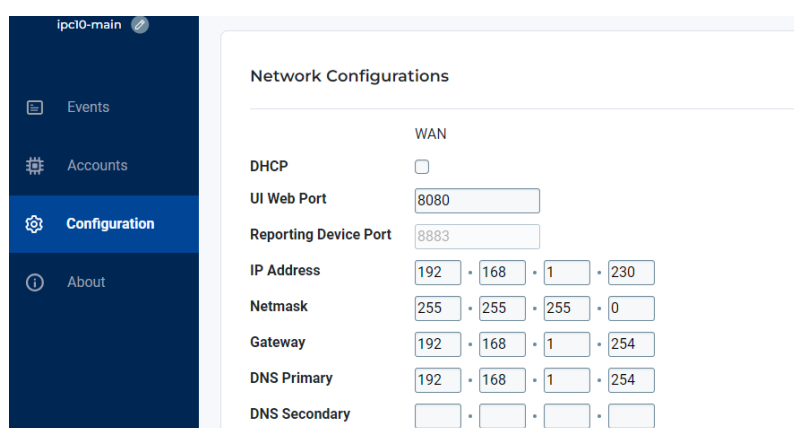


Fig. 31

After the IP150+MQ module SWAN option has been disabled, to configure reporting parameters, enter panel programming via BabyWare (Serial COM Port connection with 307USB interface).

The reporting parameters can also be configured using the keypad programming in the relevant panel sections (please refer to IP/GPRS Reporting Programming in the panel programming guide).

Enter the CMS account number, IP address(es) of the receiver(s), port, and security profiles (2-digit number), that indicate the supervision time (Fig. 32)

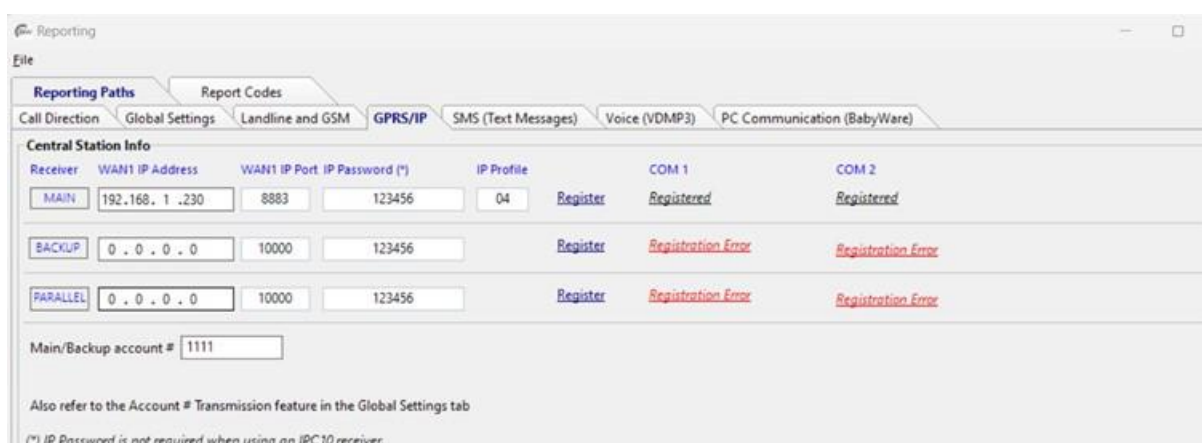
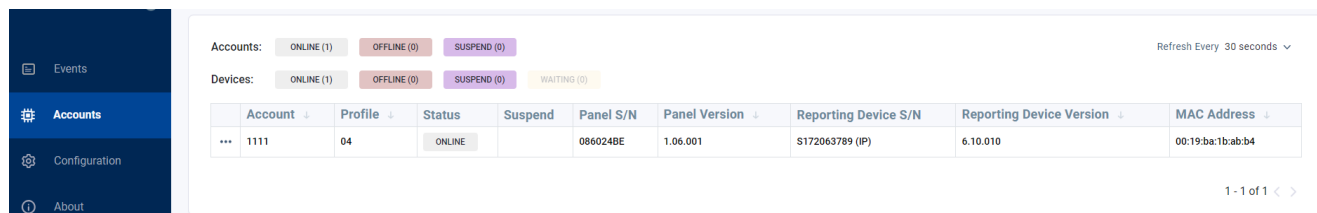


Fig. 32

Once the receiver parameters are configured and transferred to the panel, press the Register button. The account will be registered to the IPC10 receiver and will be Online in the receiver's Accounts tab (*Fig. 33*).



The screenshot shows the Paradox Accounts tab. At the top, there are status counts: Accounts (ONLINE: 1, OFFLINE: 0, SUSPEND: 0) and Devices (ONLINE: 1, OFFLINE: 0, SUSPEND: 0, WAITING: 0). A 'Refresh Every 30 seconds' dropdown is on the right. Below this is a table with the following data:

Account	Profile	Status	Suspend	Panel S/N	Panel Version	Reporting Device S/N	Reporting Device Version	MAC Address
1111	04	ONLINE		086024BE	1.06.001	S172063789 (IP)	6.10.010	00:19:ba:1b:ab:b4

At the bottom right of the table, it says '1 - 1 of 1' with navigation arrows.

Fig. 33

Notes:

- Up to two receivers can be used to report with the IP150+MQ/IP150MQTT. If you are currently reporting to three receivers, once you upgrade to MQTT firmware, you will no longer be able to configure or report to three receivers.
- Up to four receivers can be used to report with the IP180.
- Wi-Fi is not available and operational when the IP180 is in a closed network installation.
- Sending emails is not supported in closed networks (custom SMTP not supported).

After the reporting configuration is finalized (panel registered), a panel connection with BabyWare can be established, by choosing the “MQTT Close Network Connection Via IPC10” connection type.

There is also the possibility to connect BabyWare to the IPC10, to import all the panels connected in a closed network (IPC10 Server feature).

The procedures are detailed in the next chapter ([6. BabyWare Closed Network Connection](#)).

6. BABYWARE CLOSED NETWORK CONNECTION

This procedure will explain how to connect to the panel using MQTT Closed Network Connection Via IPC10 and IPC10 Server feature.

For this type of connection, the IPC10 and communication devices must not be connected to the internet.

Swan needs to be disabled on the communication module (IP150+MQ, IP150MQTT, and IP180), from the web interface.

The account (panel) needs to be first registered to the IPC10.

6.1. BABYWARE MQTT CLOSED NETWORK CONNECTION VIA IPC10

This connection type is used for connecting to a single panel, in a closed network, via IPC10.

After the registration is successful (keypad programming or BabyWare serial connection) a panel connection with BabyWare can be established, by choosing the “MQTT Closed Network Connection Via IPC10” connection type (*Fig. 34*)

Settings

Connection Advanced Encryption Alarm System Label

Select a connection type

- ☐ Panel S/N
Use if the comm. module is connected to Swan
- ☐ Site ID and Email address
Use if a Swan site is created on the system
- ☐ Site Token
Use if a Swan site is created on the system
- ☐ Static IP
- ☐ Serial
COM Port
- ☐ GPRS/Static
SIM card with Static IP
- ☐ GPRS/Private Network Call back
- ☐ Modem
- ☒ MQTT Close Network Connection via IPC10

IPC10 IP Address: 192.168.1.230

IPC10 Port: 8883

Panel SN: 086024BE

Important

In order to connect with Babyware in closed network (using the above settings), it is required to first register an account via keypad or serial (USB307) programming, to the IPC10 receiver that will be used for the Babyware connection.

☒ Automatically upload panel changes to Babyware upon connection

☒ Programming changes

Cancel OK

Fig. 34

After the IPC10 IP address, Port, and Panel SN fields are filled, press OK and connect to the panel.

6.2. BABYWARE IPC SERVER (CLOSED NETWORK ONLY)

This feature is used for importing all panels reporting to an IPC10, in a closed network.

To add the panels registered to an IPC10, click on the "IPC Server" button at the top panel (Fig. 35).

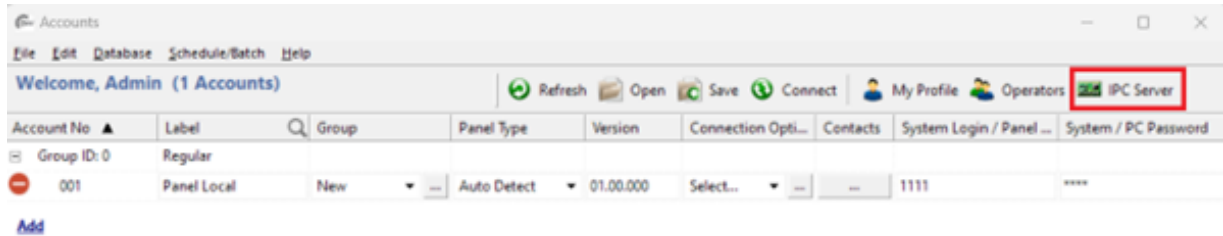


Fig. 35

A window will open, requiring entering the following details (Fig. 36):

- Label: Indicates a name for this IPC Server
- IP: IPC10 local IP address
- Port: IPC10 connection port.
- Scan Panels: Clicking on it will connect to the IPC10, as a Server, and load the list of panels connected to it. This list will be displayed in the "Panel List" grid where the Panel ID and PC Password can be filled in.

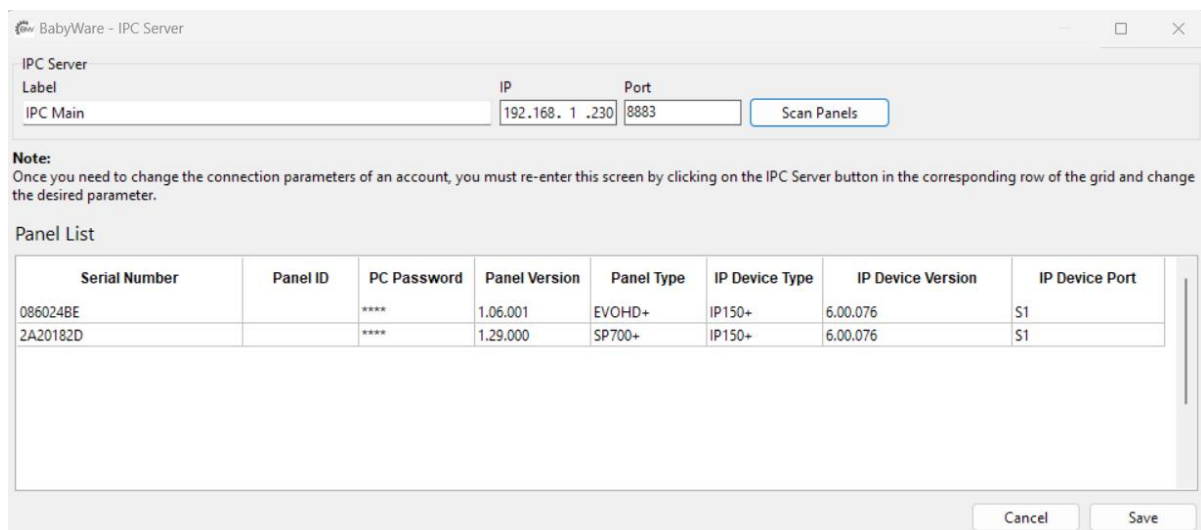


Fig. 36

Once the list of panels has been loaded, click on the "Save" button. This will create an account for each panel listed (*Fig. 37*).

IPC Server

Label: IPC Main IP: 192.168.1.230 Port: 8883 **Scan Panels**

Note:
Once you need to change the connection parameters of an account, you must re-enter this screen by clicking on the IPC Server button in the corresponding row of the grid and change the desired parameter.

Panel List

Serial Number	Panel ID	PC Password	Panel Version	Panel Type	IP Device Type	IP Device Version	IP Device Port
086024BE		****	1.06.001	EVOHD+	IP150+	6.00.076	S1
2A20182D		****	1.29.000	SP700+	IP150+	6.00.076	S1

Cancel **Save**

Fig. 37

For each registered IPC10, a grouping will be created in the Accounts form (*Fig. 38*).

Note: The Label defined on the previous screen will be the name of the grouping. If this label has not been defined, the information displayed will be the IP and Port of the IPC.

To change any data related to an existing IPC10 group, simply click on the IPC Server button on the Account Group Line.

The IPC Server window will open with all the data loaded, giving you the option of editing the list of Panels or changing the IP, Port, and Label of the IPC10.

If any changes have been made, simply click on "Save".

Accounts

File Edit Database Schedule/Batch Help

Welcome, Admin (2 Accounts) Refresh Open Save Connect My Profile Operators IPC Server

Account No	Label	Group	Panel Type	Version	Connection Opti...	Contacts	System Login / Panel ...	System / PC Passwor
Group ID: 0	Regular							
001	Panel Local	New	Auto Detect	01.00.000	Select...	...	1111	****
Group ID: 8	IPC Main							
0017	Panel 086024BE	New	Auto Detect	01.00.000	IPC10 Local	...	1111	****
0018	Panel 2A20182D	New	Auto Detect	01.00.000	IPC10 Local	...	1111	****

Add

Fig. 38

Note:

Trying to delete the IPC10 panel account via the regular ways will prompt the below message (*Fig. 39*)
Deleting the IPC10 group will delete the group and all the associated panels.

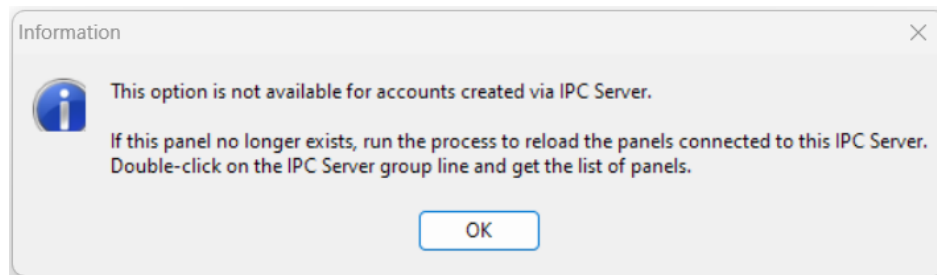


Fig. 39