Sentinel Receiver and Decoder

SAR-100 Digital Repeater

Sentry Digital Receiver

PimaGuard Software

Central Monitoring Station Products

Installation and Configuration Guide

PIMA
FOR BETTER PROTECTION

Table of contents

Figure Index

Introduction

This guide will introduce you with four PIMA Electronic Systems products for the Central Monitoring Station (CMS):

- Sentry digital receiver unit
- Sentinel PCI-based receiver and decoder
- SAR-100 digital repeater unit
- PimaGuard software (©Windows)

1. Sentry

Sentry is an advanced digital standalone receiver. It supports telephone (PSTN), radio and Ethernet channels. Sentry can receive transmissions from up to 64,000 alarm systems, and relay them to the CMS's management software, via serial (RS-232) or network communication.

Sentry is controlled and monitored by PimaGuard.

1.1. Content of the product package

- The Sentry receiver
- Driver installation package[1]
- Radio cable with D-type connector (P/N 3411055)
- Four RJ-11 standard telephone cords (P/N 3411046)
- Crosslink, 9-pin, D-type serial cable (P/N 3411048)
- AC cord
- Battery cables with fuse holder

1.2. Features

- Up to four PSTN inputs
- Up to two Radio inputs
- Supports the IP Receiver
- Supports PSTN protocols PAF, NPAF, PID, CID, SIA, PULSE, and more.
- Supports Radio protocols PAF, NPAF, PID, MILCOLD, INTRAC2000, and more.
- Supports CMS management software SURGARD, FBI, ANDROMEDA, and more.
- Connection to the CMS's management software through COM and Ethernet
- Powered by AC power and backed up by a battery
- Can be remotely controlled and supported

[1] Requires a dedicated hardware. Refer to PIMA.

1.3. Components & Architecture

Figure 1. Sentry - front panel

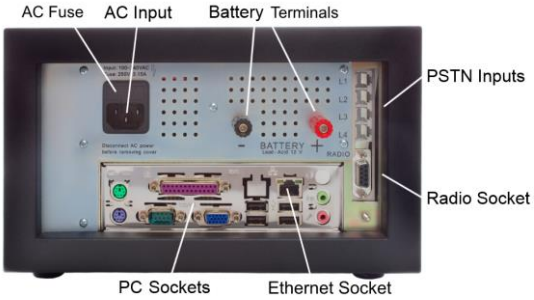


Figure 2. Sentry - back panel

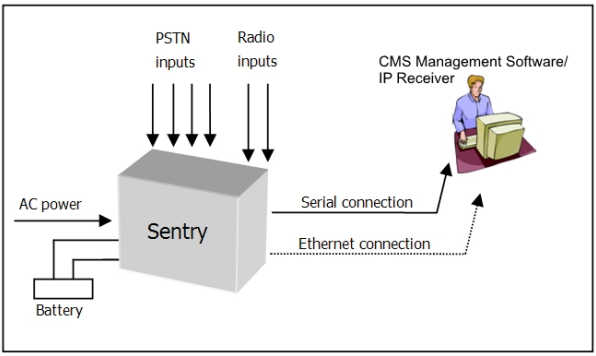


Figure 3. Sentry's mode of operation diagram

1.4. Safety instructions

- The Sentry must be connected to ground.
- To use a radio transceiver, connect the screw-nut on PimaGuard's back panel to solid ground with a thick conductor.

1.5. How to connect the Sentinel cards

1. Connect the telephone cords to the RJ-11 sockets (up to 4. Line #1 at the top).

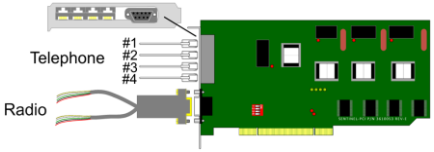


Figure 4. Sentinel connection diagram

2. Connect the radio cable to the Radio connector. Each Sentinel is supplied with a split cable, that has a 'D' type connector. You can connect up to 2 radio transceivers. To connect the radio, do the following:
   a) Connect the transceiver's wires to the Sentinel's cable according to the following table:

Sentinel	Radio
Red	PTT
White	DATA Out
Green	DATA In
Black	Volume[2]
Yellow	Shield (GND)

   b) Adjust the transceiver's output, as described in Appx A, on page 40.

Note

- *Recommended transceiver's output signal: 1 Vp-p (peak-to-peak)*
- *Turn off the transceiver's squelch control, so the reception signal will not be interrupted by the squelch filter.*

1.6. Installation

To install the Sentry, do the following:

1. Place the Sentry on a flat surface.
2. Connect telephone lines to the (RJ-11) sockets on the back panel.
3. Connect the supplied radio cable between the radio/s and the Sentry, according to the next table:

Wire	Sentry	Radio
Red	PTT	PTT
White	DATA Out	Audio Input
Green	DATA In	Audio Output

[2] Connect any unused radio wire to ground.

Wire	Sentry	Radio
Black	Volume	Volume control
Yellow	GND	GND

4. Make sure the ON/OFF switch on the front panel is turned off.
5. Connect the Sentry to power with the supplied AC cord.
6. Connect a 12V Lead-Acid backup battery (not supplied) to the binding posts on the back panel, as follows:
   a) Release the battery connection caps.
   b) Connect the supplied battery wires to the binding posts. Observe battery polarity.
   c) Secure the caps.
   d) Connect the "U" shape spade connectors on the wires to the battery.
7. Connect a monitor and click the Power button to turn on the Sentry.
8. Connect the Sentry to the CMS management software, with the crossbred RS-232 cable, or a network cable.

After connecting the Sentry to power, verify that:

1. The Power LED is on.
2. The AC Fault LED is off. If it is on, check the AC cord.
3. The Low Battery LED is off. If it is on, check that the battery is charged and is connected correctly.

1.6.1. Radio test[3]

1. Verify that the station number and frequency are configured correctly in the alarm systems that report to the Sentry.
2. Trigger various events and send them over the radio to the Sentry.
3. Verify that the events are received by the CMS in the *Monitor* view.

Tip: connect a 50Ω terminator instead of the radio antenna: transmitting with an antenna too close to the radio receiver may saturate it.

1.6.2. PSTN test

1. Verify that the PSTN protocol and the CMS phone number(s) are configured correctly in the alarm systems that report to the Sentry.
2. Trigger various events and send them over the phone to the Sentry.
3. Verify that the events are received by the CMS.

[3] See *Transceiver's settings and recommended specifications*, on page 41.

1.7. How to remotely access the Sentry via WAN

PimaGuard must have a static IP address (in LAN or WAN)

The Sentry is provided with the "UltraVNC" free[4] remote desktop application (www.uvnc.com). It is configured with the password "Sentry". To use it, do as follows:

1. On your router, forward port 5900 to the Sentry (see "Limited support notice" at the end of this guide).
2. On the remote computer, click the following address and download the latest version of the UltraVNC application: http://www.uvnc.com/downloads/ultravnc.html
3. Install the application and run the "Client Viewer".
4. Enter the Sentry's IP address (or URL, if you use DDNS service) where it is required, and connect to it.

1.8. Troubleshooting

In case of a malfunction, use the following table for troubleshooting. To shut down the Sentry, press the Power button briefly.

Fault	Troubleshooting
Low Battery LED illuminates	• Verify that the battery supplies 12V. If it does not, replace it or wait for recharging, if the battery had been discharged. • Check the battery cables. • Check the fuse on the battery's cable.
AC Fault LED is On	• Verify AC supply is OK. • Check the AC fuse on the back panel (see Figure 2, on page 5). • Check the AC cord.
Events are not received via the radio	• Check the radio cable. • Verify that the frequency of the transceiver and of the control panel transmitter's are the same. • Verify that the radio protocol of the Sentry and the control panel are the same. • Check for incoming transmissions noises in the transceiver.
Events are not received via the telephone	• Check the PSTN wires. • Verify that the telephone numbers in the control panel are correct. • Verify that the PSTN protocol of the Sentry and of the control panel are the same. • Call the IP Receiver and make sure it picks up the call.
The CMS software does not receive events	• Check the connection between the CMS's PC and PimaGuard. • Check the *Monitor* for errors, to make sure the output is configured properly.

[4] As of the time this guide is written, the application is free. Another application you can use is "TeamViewer".

1.9. Technical specifications

- Four PSTN lines
- Two radio inputs
- RS-232 port
- Four USB ports
- Power input: 90VAC~240VAC
- AC frequency range: 47 to 63 Hz
- Power consumption: 50W
- Network interface: 10/100MB Ethernet, TCP/IP, UDP
- Operating temperature: C0 -10 to +40
- Dimensions: 29.5/26.5/16.5 cm (L/W/H)
- Weight: ~5.150 Kg
- Optional backup battery: Lead-Acid, 12V, up to 20AH

2. SAR-100

2.1. Introduction

The SAR-100 is an advanced standalone repeater. Based on the Sentry (see the previous section), it is designed to expand the radio coverage of the CMS.

SAR-100 is capable of relaying radio transmissions from thousands intruder alarm systems to the Sentry. It is mounted inside a robust, waterproof metal case. It can hold an optional cellular modem and radio transceiver.

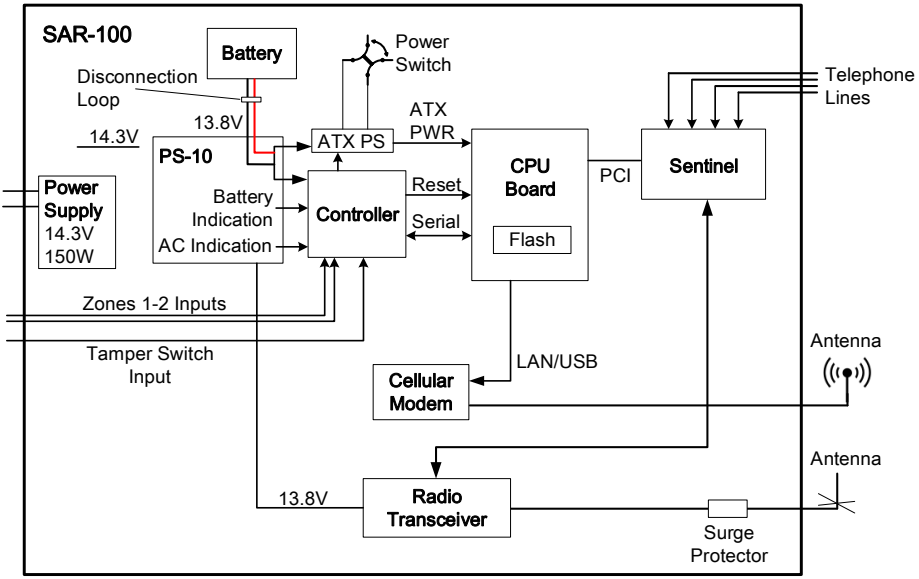


Figure 5. SAR-100 block diagram[5]

2.2. Content of the product package

- The SAR-100 repeater
- Radio cable with D-type connector (P/N 3411055)
- Spare fuse
- Plastic lockers key

2.3. Main features

- Radio events can be relayed to the following channels: Radio, Ethernet, PSTN and Cellular
- Full data-event capability by using PAF and PID PIMA protocols
- Up to 16 SAR-100 repeaters can be installed in a star topology, or unlimited number in chain.

[5] Cellular modem is optional and must be ordered separately

- Event log storage and display in case of disruption of communication, until renewal of link with the CMS.
- Self-supervision on: AC fault, low battery, and overheating.
- Bi-directional communication with the CMS in all channels ensures reliable reporting.
- Optional backup of the communication channels
- Remote firmware and software update
- Full remote desktop control
- Optional: 20Ah Backup Battery

2.4. Quick reference guide

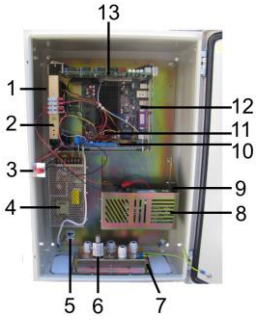


Figure 6. The SAR-100

1. Radio terminals
2. Mainboard power switch
3. Tamper switch
4. Power supply: the main power supply output voltage is 14.3VDC, 150W. The AC input is monitored at the main power supply output. AC fault may be caused by AC loss or fault in the power supply.
5. 220V input and fuse
6. Surge protector
7. Cables pass
8. Battery and radio bracket
9. Backup battery (not supplied)
10. Controller: monitors the zones, tamper switch, battery, mainboard PS and functionality. See the next section.
11. The PS-10 power supply charges the backup battery and supplies the power to the SAR-100, in case of AC fault. Also, it monitors for low battery and indicates on them to the CMS.
12. The mainboard is based on Intel ATOM-270 processor. The operating system of the SAR-100 is Windows XP© Embedded Home/Pro. The mainboard components are listed next.
13. The Sentinel digital receiver; see section 3.7, on page 21 for details

2.4.1. Other components

COM #3 port

This port is used for the communication between the controller and the mainboard.

Keyboard, mouse and display ports

These ports are used for maintenance.

Battery cut-off

This module protects the battery from a complete drain, in case of a prolonged power cut: when the battery reaches 7V, the cut-off module disconnects the battery.

Surge protector

The SP-1 protects the transceiver against lightning, entering through the antenna.

2.4.2. Controller

The controller does the following:

- Monitors the mainboard and resets it, in case of a fault.
- Monitors the local zones and tamper input
- Triggers reports on alarms, AC loss, and low battery, and restores them.

2.4.2.1. LEDs

The controller has three LEDs on the front panel:

Color	Label	Description
Green	RUN	The controller works OK
Red	MASTER DATA	Data exchange with the mainboard, via COM #3
Red	FAULT	• Single flash: AC fault • Two flashes: low battery • Three flashes: no response from the mainboard

2.4.2.2. Zone inputs

The controller has two zone inputs, which can be used to connect PIR detectors or magnetic switches. Note that these inputs are automatically bypassed for one hour when the SAR-100 box is opened, and are reconnected two minutes after closing the box, to allow the technician to leave the protected area.

2.4.3. Radio mode of operation

When the SAR-100 relays events via the radio, the SENTINEL encodes the events and the SAR-100 sends them to the CMS via the radio.

The SENTINEL triggers the radio via the PTT connection and sends the data to the transceiver's audio input.

2.4.4. Safety instructions

The SAR-100 must be connected to ground.

2.5. Installation

To install the SAR-100, follow the next steps.

1. Unpack the SAR-100, open the box and verify that all the components are secured, with no loose parts.
2. Mount the box on a wall (not plaster!) using the supplied 4 screws and wall anchors, or place it on a firm surface.
3. Insert the telephone and radio cables (and zone wires, if used) through the bottom pass and connect them.
4. Connect telephone cables to the telephone sockets.
5. Connect network cable (if in use) to the network socket.

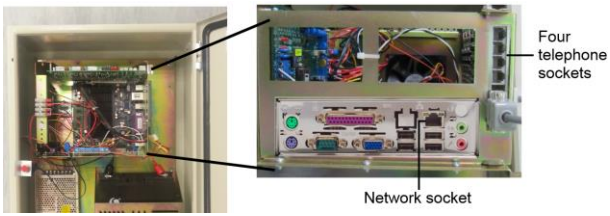


Figure 7. The mainboard sockets panel

6. Optional: connect peripherals to zone #1 and #2 inputs, in the terminal block.

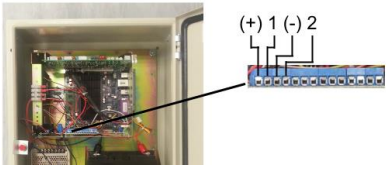


Figure 8. The controller's terminal block

7. Make sure the mainboard ON/OFF switch is switched OFF

Figure 9. Mainboard's ON/OFF switch

8. Insert the battery to its bracket and connect the cables
9. Insert the supplied 10A fuse to the fuse socket on the battery Red wire
10. If you use the radio, mount it on the front part of the battery bracket and connect its wires to the radio cable that is connected to the SENTINAL

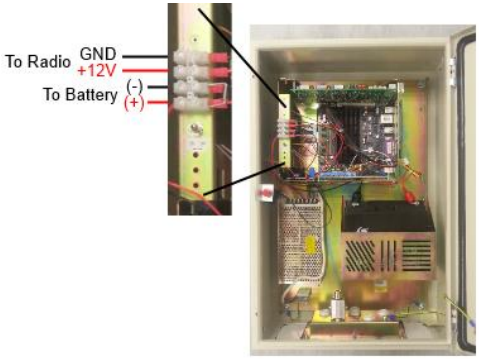


Figure 10. The terminal block

2.6. Connecting and running

1. Connect 220V wires to the AC connector. See Figure 6 and section 10, on page 11.
2. Connect a keyboard and a monitor to the mainboard panel.
3. Turn ON the mainboard's ON/OFF switch (see the image on the previous page).
4. Wait until the SAR-100 boots up and close the box.

2.6.1. Post installation tests

After completing installation, perform the following tests:

1. Open the SAR-100 box and verify that a tamper alarm and restore events are reported to the CMS. The SAR-100 account is the same as the PimaGuard one.
2. If in use, wait 2 minutes (a timeout after closing the box) and trigger zones #1 and #2. Verify that the CMS receives the Alarm and Restore events.
3. Disconnect AC power from the SAR-100, wait 30 sec. and connect it back. Verify that the CMS receives "AC Power" fault and restore events
4. Disconnect the battery, wait 30 sec. and reconnect it. Verify that the CMS receives "Low Battery" fault and restore events.

The following tests depend on the SAR-100 configuration:

5. Send various events to the repeater from a control panel, via the radio. Verify that the CMS receives all the events within a reasonable time via the repeater's main channel (e.g. network).

Tip: connect a 50Ω terminator instead of the radio antenna: transmitting with the antenna too close to the radio receiver may saturate it

6. If the repeater has a backup channel, disable the main channel (for example, by disconnecting the radio antenna) and verify that events are transmitted through the backup channel(s).
7. Reconnect any cable you have disconnected and close the box.

2.7. GSM communication

To report the SAR-100 transmissions via a cellular network, you need a cellular modem or router.

These should be installed inside the SAR-100 housing Install an antenna outside the SAR-100 housing.

2.8. How to access the SAR-100 via network

The SAR-100 must have a static IP address (LAN or WAN)

The SAR-100 is provided with the "UltraVNC" free[6] remote desktop application (www.uvnc.com).

[6] As of the time this guide is written, the application is free. Another free application you can use is "TeamViewer" (www.teamviewer.com).

It is configured with the password "Sentry". To use it:

1. Forward port 5900 to the PimaGuard PC (see "Limited support notice" at the end of this guide).
2. On the remote computer, browse to http://www.uvnc.com/downloads/ultravnc.html and download the UVNC application.
3. Install the application and run the "Client Viewer".
4. Enter the SAR-100 IP address (or URL if you use DDNS).

2.9. "SpeedFan" temperature monitor

The SAR-100 mainboard temperature can be monitored by the PimaGuard application, using a third party software, *SpeedFan*[7], that is installed on the repeater's PC.

To configure *SpeedFan* to report to PimaGuard on temperature changes, do the following:

1. Run *SpeedFan*.
2. Click *Configure*.
3. Click the *Events* tab.
4. Assign the following rules:
   a) To report on "Critical Temperature" (+65°C):
      1. Enter the command "C:\Program Files\Common Files\SIS\SIS.exe –t" .
      2. Set a minimum of 1 min. interval.
   b) To report on "Critical Temperature Restore":
      1. Enter the command "C:\Program Files\Common Files\SIS\SIS.exe –T".
      2. Set a minimum of 5 min. interval.

2.10. Technical specifications

- Supports common radio protocols such as PAF, NPAF, PID, Milcol-D, Intrac-2000
- Supports common telephone formats such as ContactID, 4x2 and SIA
- Supports Ethernet
- Housing protected by Tamper switch
- 2 monitored zone inputs
- Lightening protection
- Power input: 88VAC/176VAC~132VAC/264VAC
- 14.3VDC, 150W Power Supply
- Power consumption: 50W in idle, 150W when transmitting
- Antenna interface: N-type, female
- Network interface: 10/100MB Ethernet, TCP/IP, UDP
- Size & weight: W:40 x L:20 x H:60 cm, 17kg

[7] http://www.almico.com/speedfan.php

3. PimaGuard

PimaGuard is a versatile configuration management software, and a decoder. It is used for configuring the Sentinel modules.

3.1. Features

- Radio and Telephone channels configuration
- Cellular and Ethernet channels management and monitoring
- Various format modifications
- Log and Repeater configuration
- Debug mode
- Event filtering
- Users and permissions
- Multiple radio and telephone formats: NPAF/EPAF, CID, SIA, and many more.
- Automatic input channels testing - status is routinely reported to the CMS.
- Each PSTN channel supports up to four ACKs and eight formats per ACK
- Each Radio channel supports up to 32 formats
- Up to 16 communication channels with various switching options upon failure
- Each communication channel can be configured as Serial, TCP or UDP.
- Up to 8 different logs
- Bi-directional channel (repeater to CMS) saves airtime
- Advanced debugging and diagnostics
- Programmable timer for keeping up to 1000 events in the event buffer
- Optional Caller-ID/IP[8]
- High sensitivity radio signal
- Built-in scope utility for easy radio amplifier tuning
- Live monitoring of the last 1024 events

3.2. Repeaters

PimaGuard's build-in smart repeater utilizes bi-directional communication with the CMS software, for sending events efficiently. It requires no external software. The repeater is dual-mode and multi-channel - it can receive the event in one channel (e.g. radio) and relay it via various others.

The most common application of the repeater is radio-to-radio, with telephone or network as backup. The CMS should acknowledge each event sent by the repeater. If an ACK is not received, events are re-sent until acknowledged (the event buffer is limited by time or to 1000 events).

This process guarantees the following:

- Transmission time is very fast, as each transmission is consisted of two frames (contrary to transmission of 10 frames by the end-user's transmitter), thus saving airtime. While waiting for an ACK and retransmitting an event, new incoming events are stored in the buffer.
- Continuous, bi-directional monitoring allows communication failures identification.

[8] In supported countries

3.3. IP receiver

The IP receiver is an integrated IP signaling monitor, design to receive alarm and other messages (as TCP frames) from PIMA alarm systems, via network and GSM paths, and the SAT-N. All messages are encrypted using AES 128 bit encryption.

PimaGuard is offered in two versions: Basic and Premium.

- **Basic**

In the Basic version the IP receiver is used for receiving alarm and other messages from registered alarm systems via network, GSM and the SAT-N, and sending them to the CMS' software.

- **Premium**

In the Premium version the IP receiver monitors the registered alarm systems and protects against anti-substitution (the substitution of a valid control panel with a fraudulent one)/anti-replay (the interception and retransmission of authentic control panel messages, preventing an attack in which a valid data transmission is recorded and fraudulently repeated). The IP receiver accepts only valid data and only from registered accounts within a predefined, per-account interval.

3.4. Installation wizard

To install PimaGuard run the file *SIS Setup.exe* from the software's folder and follow the instructions. On Windows 7©, right-click the same file and click *Run as administrator*.

If the "Completing the setup wizard" window pops up, but the device driver software is still running, wait for it to finish before restarting the PC or PimaGuard will malfunction.

After restarting the computer, PimaGuard will run automatically and its icon will be placed in the tray bar. To open the software's window, right-click its icon on the taskbar and click "Show".

3.5. The menu bar

PimaGuard's window is divided into 2 panes: the navigation tree is displayed on the left, and the properties and values table on the right.

3.5.1. The File menu

The *File* menu includes the following commands:

Command	Description
Save	Save PimaGuard's current configuration
Export Configuration	Export the current configuration as a CSV file
Export IP Receiver Account	Export the IP receiver accounts as a CSV file
Upgrade/Restore Configuration	Allows upgrading PimaGuard, or restoring the configuration from a backup file.
Restore IP Receiver Account	Allows restoring the IP Receiver account file from a backup
Import IP Receiver Account	Allows importing accounts from an external file

3.5.2. The Edit menu

Use the Edit menu commands (Copy, Paste, Clear, and Discard Changes) anywhere in the software - formats, filters, ACKs and other parameters can be copied and pasted onto parameters of the same type.

3.5.3. The View menu

Command	Details
Status Bar	Show/hide the status bar at the bottom of the screen
List Grid	Show/hide the grid in the right pane
Tree Lines	Show/hide the tree lines in the left pane
Monitor	Select this option (press Ctrl+M) to show the event monitor on the lower right pane. For details about the monitor, see section 3.12.1, on page 34.

3.5.4. The Options menu

Command	Details
Start Test	Generate a test event ('00' in 4x2) on the main account (or a Repeater's account) and report the event in all the output paths.
Sentinels Slots Reset	Reset the Sentinel's PCI slots information. Note that reboot is required!
Fix IP Receiver Account	Rebuild the IP Receiver account file (ACCNT. Premium only).
Auto Logon	Allows automatic login to the PC

3.5.5. The Help menu

This menu includes the software's version under *About*.

3.5.6. The menu tree

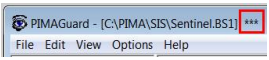
The menu tree is displayed on the left pane:

- Clicking an item in the tree displays its properties and values.
- Double-clicking an item opens its sub-menu (if there is one), or its configuration window.

3.5.7. Icons colors

Icons on the menus are green when active, and gray when inactive or at fault. The "Configuration Analyzer" menu has additional colors; see section 3.12.2, on page 35.

Three asterisks in the window header indicate that data was changed but not saved. Click File/Save and restart the PC for changes to take place.



3.6. General

3.6.1. Configuration

1. Double-click General on the menu tree.
2. Click Configuration. The properties are described in the next table. Double-click to change properties.

Property	Details
CMS Name	The Central Monitoring Station name
Note	User text
Created on	The date the installation file was created
Installed on	The date PimaGuard was installed
Last modified on	The date the installation file was modified
Last modified version	PimaGuard's version that created/modified the current configuration file
Configuration file	The configuration file (ACCNT) path
Account	Sentry's supervision account number (commonly, 8000). The supervision events (test) are routed according to the Routing table (see section 3.7.1.2, on page 22): Log, COM or Repeater. To disable the supervision, leave blank or enter zero.  • ***Make sure the account number is unique.*** • ***The account number cannot exceed FFFFFFFF. Note each format's restrictions.*** • ***The event buffer's time and size are programmable*** • ***The event buffer is limited to 1000 events per input***
Decoder ID	External decoder's ID for reporting via COM and Idle/ACK frames. Range: 0-99.
Router	The Routing table destination; see section 3.7.1.2, on page 22.
Event Timeout (min)	The event buffer's timeout (in minutes). Range: 0-255. When an event cannot be relayed to the selected routing destination, it is buffered for the time set here. When set to zero, the timeout is unlimited (subject to the machine's capability).
Beep Time (sec)	The time to sound a beep on errors (in seconds). Range: 0-999. To stop the beeping, click anyway on the screen or reset the error.
EN 50136-4	Enable/disable the EN Fire standard features (for East Europe/Russia)
Indicator Port	In use only on selected countries
Reminder Time (min)	An interval in minutes for resending fault events. Range: 0-1000. When the interval expires, the event will be re-sent via the Routing table output.
Run Delay (sec)	A delay in sec. before PimaGuard starts running. Range: 0-99. Useful when resources are needed to be loaded before the software runs. For example, network server location.
Interface	The software's interface language

Property	Details
Language	
Run on Startup	Enter the full path (and arguments, up to 16 rows) of programs that needs to run before PimaGuard starts running. PimaGuard will execute the programs one by one, with maximum 10 seconds timeout between each. "Run on startup" is executed after "Run delay" is (where relevant). This feature operates the same as the Windows "Run" command

3.6.2. Users

You can define up to eight PimaGuard users with separate passwords and permissions. When users are defined, every time the software starts up or restored from the tray[9], a password is required or PimaGuard will run but the interface will not open.

3.6.2.1. Permissions

1. On the menu tree, double-click General.
2. Click Users.
3. Double-click User X and enter a user Name.
4. Type a Password and re-enter it in the Confirm Password field.

Passwords are case-sensitive and up to nine characters long.

5. Check the permissions of the user; see the next table for details. The following permissions are automatically checked when checking any of the permissions:
   - Export the configuration settings
   - Modify accounts
   - View the monitor and filters

Permission	The user can…
View General menu	see if a format is active or inactive. The format's details remain hidden. This permission is automatically checked, when any other permission is, and cannot be disabled separately
Modify General menu	modify the General Configurations settings
Modify COM Formats	modify the Communication Formats
Modify Sentinels	modify the Sentinels settings, reset the cards' slots, view the Oscillograph, and update the firmware.
View Formats	view the Line and Radio formats settings
Modify Formats	modify the Line and Radio Formats, view the Repeaters' Channel Formats
Modify IP Rec. Config.	modify the IP Receiver's Configuration settings

[9] When PimaGuard has users defined and is idle for 10 min., it is minimized to the tray.

Permission	The user can…
Sync IP Rec. account	request to Sync with the IP Receiver's Accounts
Test IP Rec. account	test the IP Receiver's Accounts
Sync all accounts	sync all the IP Receiver's accounts
Modify IP Rec. Account	modify IP Receiver's Accounts (Edit/Add/Remove/Export/Import/Restore)
Modify COMs	modify filters, route, copy/paste
Modify Logs	modify filters, copy/paste
Modify Channels	modify Lines, Radios, and Repeater Channels
Modify Users	Manage all User Permissions

One user (minimum) must have all the permissions.

3.6.3. Serial port formats

Set PimaGuard's communication formats and structures. You can create up to 4 new serial and network formats (see section A, on page 45). The properties in this window are:

Property	Description
Format	Select the format from the drop-down list
ACK pattern	Set the pattern of the ACK signal
Idle pattern	Set the pattern of the Idle signal
Structure 1-4	• PAF/NPAF/EPAF, PID/CID, SIA, 4x2/RAW: select the input format. Only one selection can be made. The 4x2 format includes any format with up to 4 digit account numbers, and up to 2 hex digit events (e.g. PLS, DTMF, MILCOLD, INTRAC).
	• Special condition: conditions for a specific character range in the pattern
	• Event conversion: an option to convert incoming events using a predefined table or formula
	• Pattern: the current structure real pattern, using predefined symbols.

3.7. Sentinel Cards

3.7.1. Sentinel 1-4

1. Double-click on Sentinel X.
2. Double-click on *Inactive* in the right pane:
   a) IO Range: enter the minimum physical IO value of Sentinel 1; for example: 1C00, 3C00, 5C00. The maximum value is FF.
   b) Enter the Serial Number and ID for the Sentinels in use.

   For the changes to take effect, click "Sentinels Slots Reset" on the Options menu; see section 3.5.4, on page 18 for details.

3. Status: the faults status and description are displayed on the main window's right pane. Status 0000 is the Sentinel's fault code; see "Sentinel status" codes, on page 44.

3.7.1.1. Line 1-4

Every Sentinel can have up to 4 telephone line inputs, with up to 4 different ACKs, each in up to 8 formats. Only when you set an ACK, the next ACK can be set[10].

1. Double-click on Line X. The Line properties are:

Property	Description
Line	Activate/deactivate the telephone line input (if the line was enabled by PIMA)
Test time (Min)	Set an interval (in minutes) for PimaGuard to check for dialing tone. Range: 0-9999. Three tests are performed during every interval - if all three fail, an error event is generated. When set to zero, the dialing tone is not checked.
Caller ID	Report on data error will be sent with the Caller ID: if PimaGuard cannot resolve any event during an entire call session, it will send the internal fault event with the Caller ID to the Routing table outputs. See the Fault Codes appendix, on page 41.

2. In the main window, double-click on ACK X.
3. From the drop-down list, select the open ACK frequency.
4. First ACK Delay: if the first open ACK must be delayed, enter the delay in seventh (1/7) of a second. Range: 1-63 (minimum: 6). For example, for a 2 sec delay, enter "14".
5. ACK 1-2: Double-click and select the ACK and its delay.

3.7.1.2. Formats 1-8

The formats are displayed only after selecting the ACK.

1. Double-click on Format X. The format's properties are:

Property	Details
Format	Select the format from the drop-down list.
System (Hex)	The System is applicable for PIMA PID, PAF, NPAF, EPAF formats, and more. Note that in all PIMA formats the System must be an even number (00, 02, 04… FE).
Frame (DTMF and PLS)	Select the Frame from the drop-down list. Frame replaces System in the reports. Sentry will relay events in the above formats, only if they answer the frame definitions. For example, "4(3)x2+3x1 CS" in DTMF: • 4(3)x2 - events with 4 or 3 digit account number and 2 digit events • 3x1 - events with 3 digit account number and 1 digit events • CS - the events must have a checksum digit

[10] Subject to your package

Property	Details
Flag (Hex)	Do not set the Flag unless asked by PIMA support Flag is the waiting time between frames in the same call session. The value set here (in hex) is multiplied by 35.8ms. For example: if the flag is set to FF Sentry will wait up to 9.15± sec. for the second frame. In PLS or ELL formats, the flag is multiplied by 143.2ms.[11]
Close ACK	Do not set, unless asked by PIMA support! This is the closing ACK's frequency, for control panels that require it.
PIMA Pattern	PIMA alarm systems' Format Structure. Format, System, Flag and Close ACK are the absolute definitions - verify them even if PIMA format is invalid
Convert	There are two Convert buttons: • Click the upper button to convert the Format, System/Frame and Close ACK (and the format's ACK) values, to Pima format's station number • Click the lower button to convert from PIMA Control Panels format to the above formats.
All-account prefix	You can enter any number to be added uniformly to all incoming account numbers. For example: if you enter 1500, and a account number is 500, Sentry will report with the account number of 1500+500=2000. Use this feature to distinguish between accounts from different sources, which use the same account numbers.
Decoder ID	Do not set Decoder ID unless asked by PIMA support Relevant for specific software outputs. Range: 0-99, decimal
Filter Type	See Filters, on page 37.
Routing table	A table of the Line routing options, for events that are received in the selected format. There are many possible combinations to route the events to Logs, COMs and Repeaters. The optional numbers 1-16 refer to the routing destination - for example Log #7, Repeater #8, and so on. The options are: • COM: the events will be routed to the respective COM (up to 8). Note that the COM must be in "Software" mode. • Log: the events will be logged in the respective log file (up to 4) • Repeater: the events will be routed to the respective logical repeater (up to 16). The repeater must be in Out mode. • Format: you must type the Format's number in which the events will be sent to the repeater, out of the 32 optional repeater formats (see section 3.11.1.2,on page 34)

Do not leave an inactive format between two active ones.

[11] Max. flag time in PLS/ELL: 5.5± sec.

3.7.1.3. Example

ACK 1	1400(Hz)
Format 1	NPAF P=173 133 Route to: Comm 0005 Log 01 Repeater 0018
Format 2	PLS P=1 193 4(3)x2+3x1 CS Route to: Log 01
Format 3	SIA S=00 F=00 Account: 100 - 500,0 - 0,List: 0 Add to Account: 10000 Route to: Comm 01C2 Log 01
Format 4	CID P=0 198 Decoder ID: 69 Route to: Comm 0001
Format 5	Inactive

Format 1 (NPAF)

- P: PIMA format pattern
- 173 133: Low/High byte
- Routing table: incoming events will be routed to COMs #1 and #3 (0x0005=0b0101), to Log #1 (0x01) and to Repeaters #4 and #5 (0x0018=0b11000).

Format 2 (PLS)

- 4(3)x2+3x1 CS: the structure; see section A, on page 45 for details.

Format 3 (SIA)

- S: System
- F: Flag
- 00: 0x00. In this example, the System and Flag are displayed because the format is programmed with a non-SIA open ACK, and does not match PIMA format pattern.
- Account: 100-500, 0-0, List 0: the filter definitions; see Filters, on page 37.
- Add to Account: 10000: see the previous sub-section for details.
- Routing table: the reports will be routed to COMs #2, #7, #8 and #1 (0x01C2=0b111000010), and to log #1 (0x01).

Format 4 (CID)

- Decoder ID: Format related data
- Routing table: the events will be routed to COM #1 (0x0001=0b0001).

3.7.2. Radio 1-2

Each Sentinel has up to 2 radio channels, each supports up to 32 formats.

1. Double-click Radio X on the menu tree. The properties in this window are:

Property	Details
Channel	Set to Active/Inactive (if the channel was enabled by PIMA)
Test Time (min)	If no valid data is received during this interval in minutes, a fault report is generated. Range: 0-9999. 0: test reports are disabled.
Transmit delay (50 mSec)	Do not set this delay unless asked by PIMA support! Add a delay in milliseconds before transmitting. Range: 0-255. The value entered is multiplied by 50. The delay should desynchronize two output repeaters that had become synchronized.
Filter time	A timeout in sec. for sending unique events. Repeating events from the same account will be filtered. Range: 5-600. Default: 180
Warm-Up Time	Do not set the this timer unless asked by PIMA support!

Property	Details
	The value entered here is in milliseconds and is multiplied by 50. This feature is for output repeaters only.

- ***Do not leave an inactive format between two active ones.***
- ***Do not assign DESK with other formats with the same ACK.***

3.7.2.1. Formats

See section 3.7.1.2, on page 22 for details.

3.7.2.2. Filters

See Filters, on page 37.

3.8. IP Receiver

The IP Receiver has Basic and Premium modes. The Premium mode includes account supervision and anti-substitution detection; see more details in section 3.8.2, on page 26.

3.8.1. Configuration

1. Double-click IP Receiver on the menu tree.
2. Double-click Configuration.

3.8.1.1. Basic type

The Basic type properties are:

Property	Details
Type	The type is set by PIMA
Port	Enter the listening port
Encryption key (Hex)	Enter the 64 Hex characters (0-F) encryption key.
Caller IP	Use this feature for reporting on data errors: if PimaGuard cannot resolve any event during an entire TCP session, it will send the internal fault event with the Caller IP to the outputs according to the Routing table; see Appx B, on page 41.
Image folder path	Not in use
All-account prefix	See section 3.7.1.2, on page 22.
Decoder ID	
Routing table	
Filter Type	See Filters, on page 37.

3.8.1.2. Premium type

The Configuration window of the Premium mode is the same as in the Basic mode, except that all properties are enabled.

Property	Details
Accounts file path	The default path to PimaGuard's accounts file is the installation folder.  ***If the account file is located on a network, verify its access privileges and path. If the folder becomes inaccessible, a fault report is generated.***
Offline accounts alert	The percentage of offline modules (mobile or network), that if reached, a fault report is sent to the outputs according to the Routing table. This feature helps verifying mobile and network routing faults. The percentage for both channels is the same, but evaluated and reported separately. When the number of offline modules drops back under 30%, a Restore report is generated. 0: disabled
Fault report interval (min)	An interval in minutes for reporting on the 791-795 events. Range: 0-1000. 0: disabled
Sync (791)	A control panel was synced (registered) with PimaGuard. 0: default 791
Sync 1 loss (792)	A sync loss with a control panel. 0: default 792
Offline account (793)	An input module (cellular or net4pro) that did report during the entire Sync loss timeout. 0: default 793
Unregistered account (794)	An event from an unregistered control panel was received. The event will be routed and followed by a 794 event. 0: default 794
Sync 2 loss (795)	A report on a control panel's module that reported the same frame several times. This may indicate on a panel's fault or communication error 0: default 795
Auto Configuration (796)	A report on a control panel that has been configured by the IP receiver.
Default Encryption Key (797	A report on a control panel that uses the IP receiver's default encryption key, and not a modified one.

3.8.2. Accounts Auto-config

This feature allows you to download some system codes and parameters when the client is registering its ***FORCE*** alarm system at the CMS. All the parameters are optional, except the Remote or Technician codes that allow the connection.

Property	Details
Remote code	The security code for connecting to the ***FORCE*** alarm system
Technician code	The ***FORCE***'s technician code
Module list folder	Enter a path to the folder where the auto-config module list is saved. The list is saved as an XML file. Refer to the next section for details.

3.8.2.1. Auto-config account list

Double-click on *Auto-config account list* on the right pane. In the pop-up window enter the main account number and communication path (Cellular/Ethernet) for each control panel that is about to connect to PimaGuard for registration. Press *Add* to ass the account. Press *Next* to add another account.

If you don't enter a file path in the auto-config window, the Auto-config folder will be located on the PimaGuard's folder.

3.8.3. Accounts (Premium only)

1. Click on *Accounts*. The properties in the right pane are described below.

Property	Value
Sync all accounts	See section 3.8.3.1.
Number of accounts	The total number of the IP Receiver accounts
Offline - cellular modules	Modules that have not sent any valid report during the Idle timeout (event 793)
Offline - Ethernet modules	
Sync loss - cellular modules	Modules that are not synced (event 792 or 795)
Sync loss - Ethernet modules	
Waiting for sync - cellular modules	Modules that are set to be synced in the *Account* window (event 791)
Waiting for sync - Ethernet modules	
Modules under test	Accounts under Test mode (receiving encrypted and non-encrypted events)

2. Double-click on *Accounts* to open the accounts window. Each account can have up to 16 accounts/partitions. 'Account 1' (that is, partition #1) will serve as the main account number. The properties are described in the following table.

Property	Details
Search	Enter the Account number to display it
Cellular/Ethernet Statuses	Check the modules connection status and IP address. If the module is at fault, the *Waiting For Sync* and *Modules under test* timeouts will be displayed.
Previous/Next	Scroll between the accounts
Sync	Click this button to sync the anti-substitution counter with the control panel. The control panel is expected to send an event no. 791. The event can be sent within a period of 4 hours. Click the button again to cancel the action. For example, to register or sync the anti-substitution counter of the ***FORCE*** alarm system, the user must enter the User menu and browse to *Communication → CMS Registration* and press *CMS X*.

Syncing a control panel may significantly impact security aspects of PimaGuard. Use it cautiously!

Property	Details
Test	Click this button to allow PimaGuard to accept unencrypted frames from the current control panel. The timeout for this action is 4 hours. Click again to cancel the test.
Cellular/Ethernet	Check the module/s in use.
Idle timeout (sec)	If no valid report is received from any of the account's modules during the Idle timeout, a 793 event is reported to the CMS. Range (sec): 0-65535. 0: idle supervision is disabled
Override Sync	When checking this option PimaGuard ignores the 792 and 795 events, and accepts not synced events.

If 'Idle Timeout' is disabled while 'Override Sync' is enabled, it may significantly impact security aspects of PimaGuard and the control panels. Do it cautiously, only when reception or network faults occur.

Separate sync	A separate sync trace
Account 1 (Main)	The control panel's main account number. The number should be unique. When any other account becomes loss, this account is used for reporting. Accounts range: hex, 1-FFFFFFFF
Account 2-16	Additional accounts for partitions. The accounts must be set in ascending order, consecutively.
Clear All	Click to clear all the fields in the window.
Modify	Click to save any modification.
Delete	Delete the current account.
Close	Close the window without saving (if the account was modified).

3.8.3.1. Sync all accounts

This feature allows the CMS to sync the anti-substitution counter of all the registered accounts within 4 hours. Each account will be synced while communicating with the IP receiver.

An example for using this feature is when importing a new account file, or if the account file was inaccessible for a period of time, causing all accounts to become unsynchronized.

If an account was already in a Lost Sync state when force sync was executed, PimaGuard will send a Restore event after receiving the first event from it.

Double-click *Sync all accounts* to start the process; double-click it again to stop it.

Use the "Sync all accounts" only when many accounts become un-synced at the same time. This feature significantly reduces security aspects of PimaGuard!

3.9. Communications

PimaGuard offers up to 16 optional COMs, or communication configurations.

1. Double-click Communications, on the menu tree.
2. Double-click COM X. The COM window properties are described in the following table.

Property	Details
Type	Select the communication path - Serial, TCP, or UDP.
Mode	Select between Software, Repeater or External: • Software: the events will be routed to the CMS's software • Repeater: the events will be routed to an IN or OUT logic Repeater • External: the events will be routed from an external decoder
Format	Select the format in which the events will be routed to the CMS.
Error Switching	Select a backup path; see the next section.
ACK Timeout	Set the timeout. Range: 0-65535. 0: Disabled • Software: ACK waiting time (in sec) for each frame • External : disabled (0) - PimaGuard will send an ACK frame, immediately when receiving an event frame.
Idle Timeout	Range: 0-65535. 0: Disabled • Software: if no event is received within this timeout (in sec), an Idle frame is sent to the CMS. • External: an Idle or any other frame is expect within this timeout.  *The Idle timeout must be longer than the ACK timeout.*
Idle ACK	Software and External modes Idle ACK pattern. The ACK will be expected or sent upon idle (according to COM's Mode).
Port and IP/URL	TCP and UDP parameters.  ***Do not set the Port and IP/URL parameters in External IN and Repeater IN modes.***

3.9.1. Software mode

3.9.1.1. Error switching (Backup path)

Set a backup path to the CMS. The COM must be in Software mode, and must be defined with any Active ACK for Faults, Idle and Restore. Press OK when done.

Example

COM 1 and COM 2 are set in Software mode:

- COM 1: On Error Switch To: COM 2, ACK Timeout: 3, Idle Timeout: 30, Idle ACK: Active

- COM 2: On Error Switch To: Inactive

If COM 1 stops receiving ACKs for event or idle frames, the events are routed to COM 2 and a fault report is sent via that COM.

PimaGuard will keep checking COM 1 for Idle ACKs once every 30 sec. Routing to COM 1 will be restored when ACKs are received again. However, the event buffer is not automatically set back to COM 1. To do so, set COM 2 On Error Switch To: COM 1 and ACK Timeout to "3". When COM 2 becomes faulty, the event buffer will be routed back to COM 1. This looping is required.

If a report is routed to both COM 1 and COM 2, and these are set in a loop, it will be sent to both COMs. If one COM is faulty, a duplicate event will be sent.

3.9.1.2. Output filters

1. Double click Output Filter X on the properties table. Each COM in Software mode can have 2 output filters (logic association not required) for filtering the same events ,when received from multiple sources. An output filter is based on the next points:
    - Unique account ID (including the prefix, if in use)
    - Equivalents of events, regardless of the format (PAF, NPAF, CID, etc.)
    - Filter and package average timeout
2. Double-click an Output filter. The properties are described in the following table.

Property	Details
Filter time (sec)	The total time for relaying all the events to the output channel. Time must be less or equal to the *Event Timeout* (see page 19).
Package Time (sec)	The estimated time for receiving an average amount of events from all channels. Must be less or equal to the *Filter time*.
Input 1-4 Channel	Select at least 2 input channels to be filtered.
Format	PimaGuard only Line and Radio formats. Check the formats to apply the filter. The formats are taken from the Sentinels' properties; see section 3.7.1, on page 21.
4x2 to CID table path	The path to the Event conversion table (txt file). The table can be used under the following conditions: • One of the formats is 4x2, OR • All the formats are 4x2, but need some conversions. If only 4x2 formats are selected and all the events have the same event code on all channels, the table is useless. You can create text file with a conversion table in it with the following structure: [4x2] 00=3602000 01=3130001 …. FF=3601000

Example

PAF, CID and PID are filtered in three different input channels. The following should be set:

- Buffer Timeout (on General > Configuration): 30 minutes.

- Input 1 - Sentinel 1 Radio 1: PAF, NPAF and PID (in this order).
- Input 2 - Repeater 2 Channel 1, and Input 3 - Repeater 3 Channel 1: PID, PAF, NPAF and 4x2 (in this order).

Account X is transmitting a sequence of events via the Radio, each is received in three input channels at the same time: Alarm in Zone 9 (JW), Burglary Alarm in Zone 10 (JX), and AC Fault (RK).

Example:

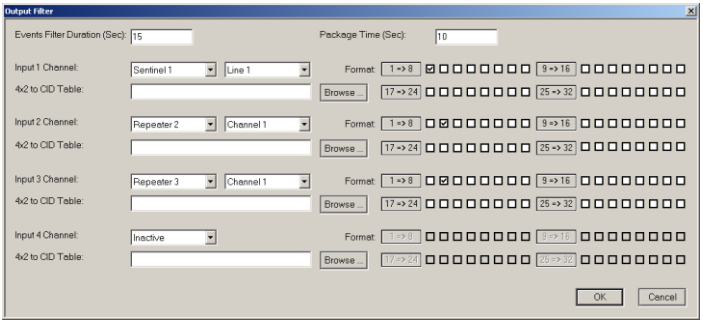


Figure 11. Output filters example

The following diagram demonstrates the filtering process (estimation only):

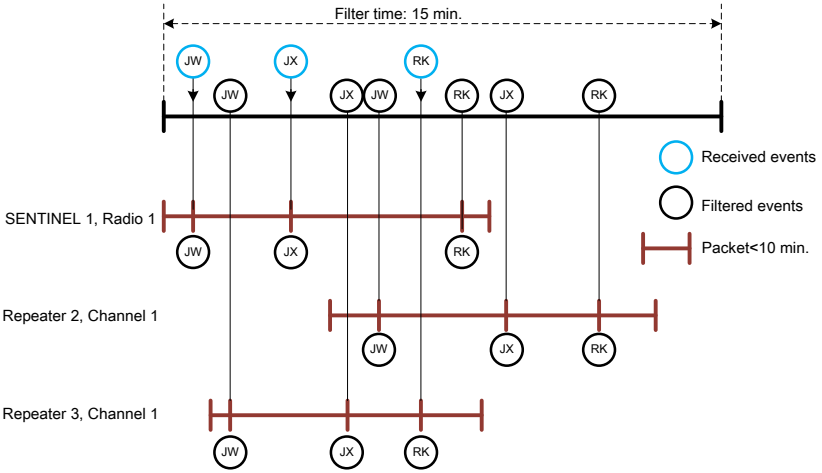


Figure 12. Output filters timeline example

- *PAF, NPAF, SIA and other fixed formats have special conversion tables for the same event codes, if the filter is required for 2 different formats.*
- *Test events are not filtered.*
- *In PID and CID, partitioning is ignored by the filter.*

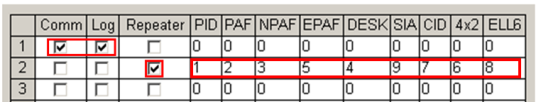
3.9.2. External mode

When *External mode* is selected, double-click on *Routing table* on the right pane. Using this table you set the routing the Line/Radio formats.

External decoder inputs can be set in multiple frame formats. Routing to repeaters requires to select to which format to convert the events.

3.9.2.1. Example

In the following example, events from external decoders will be routed to COM 1, Log 1, and Repeater 2. In addition, PID events will be routed to the repeater's Format 1, PAF events to the repeater's Format 2, NPAF to Format 3, and so on.



	Comm	Log	Repeater	PID	PAF	NPAF	EPAF	DESK	SIA	CID	4x2	ELL6
1	☑	☑	☐	0	0	0	0	0	0	0	0	0
2	☐	☐	☑	1	2	3	5	4	9	7	6	8
3	☐	☐	☐	0	0	0	0	0	0	0	0	0

Figure 13. External Router Window Example

- ***When you select a Repeater as an output, the routing of <u>all the formats</u> in the table must be set, even if the repeater does not use all of them.***
- ***Consult PIMA support before routing to Repeaters in External mode.***

3.10. Logs

Set Sentry's event log files.

1. Double-click on *Logs*.
2. Double-click on *Log X*
3. Click *Browse* and point to the location of the log files folder. If a log file does not exist yet, type the full path to the folder, with the name of the file and "log" as extension, and Sentry will create the file. Optionally, you can create two filters for each log.

3.10.1. Log file size

The size of a Log file can be up to 200 Mb, depending on the available disk space. When the size reaches 200 Mb, the file name is changed to "Filename.log.old" and a new "Filename.log" file is created. In this way the 2 files can reach up to 400 Mb together.

When the "Filename.log" file reaches 200 Mb for the second time (and onwards), it writes over the "Filename.log.old" file, so you have to backup the log files once every few months

3.11. Repeaters

Repeaters and Formats can only be programmed by PIMA. Only the Channels can be modified by the users

A repeater can receive events from any alarm system, and relay them to the CMS in any medium - radio, network or telephone. A repeater can be part of a chain, but have a separate log.

Up to 16 repeaters can be set in Sentry, each can be entirely separated logical repeater.

To set the repeaters' channels, do the following:

1. Double-click on Repeaters.
2. Double-click on Repeater X. A repeater can be defined with up to 4 channels: a channel can be any medium defined in Sentry, and have up to 32 formats, and different Keepalive and supervision accounts.
3. Double-click on Channel X. The properties of the Channels window are:

Property	Details
Channel	The physical channel
Station Phone Number	Set the destination phone number (that is, Sentry's Repeater IN), when the SENTINEL is in Line mode and the repeater is set as Out
Test Time	Set the interval in min. for the channel's supervision. Range: 0-9999 0: disable supervision • In Repeater OUT: life signal is sent (with the account no.) if no other event was sent during Test Time • In Repeater IN: if no event is received during Test Time, a fault event is sent (see the Fault Codes appendix, on page 41)
Account	Set the account no. for PimaGuard life signals and fault reports. If repeater OUT is in use and Sentry's fault account is routed to this repeater's channel, the account no. will be replaced with the channel's account no. See the next section for limitations.  ***Make sure the account no. is unique and not in use by any of the control panels***

In Repeater IN there is no Restore event after sending a life signal, when the Test time expires without receiving any event

- *When the repeater is in OUT mode, the channels backup one another by their order: if Channel 1 becomes faulty, the event buffer is routed to Channel 2, and so on, in a loop. When Channel 1 is restored, the events are routed back to it.*
- *When the repeater is in IN mode, events are accepted from all the channels without any priority.*

3.11.1. Formats

3.11.1.1. Repeater IN

In the repeater's properties window, the Format is followed by the PAF/PID system ('S'), that receives the events. Other parameters like the Routing table, Decoder ID, and Account Prefix are displayed the same as in the Line format (see section 3.7.1.2, on page 22)

3.11.1.2. Repeater OUT

The same as in the repeater IN, the Format is followed by the System, only here it is the System that relays the events.

- *Repeater IN "Test Time" should be at least 1.5 times longer than the Repeater OUT.*
- *"4x2" format stands for a group of formats, like MILCOLD, PLS, DTMF and more. If you need to distinguish between specific formats, add another format system to the repeater.*
- *Non "DOS Compatible" repeaters convert CID's qualifier from '6' (Status) to '1' (Alarm).*
- *When using Sentinel Line for Repeater OUT, chances for delays are very high. Therefore, we recommend to use Line, only as the last backup channel.*
- *If no account and timeout are defined in the Repeater channel, a fault event is sent under the main fault account (see the Fault Codes appendix, on page 41). There is no restore report for this event*
- *In you use several radio channels, set a different "Transmit Delay" for each.*

3.12. Diagnostic Tools

3.12.1. Monitor

Sentry's monitor displays the incoming and outgoing events, the same as a debugging tool - all the available data is displayed, with some indications that can only be viewed in the monitor.

The Monitor has 2 operating modes: General and Debug. To switch between the two, double-click on Mode, on the right pane.

In both modes the last 1024 events are displayed chronologically, and are updated online, with new events at the top.

3.12.1.1. Debug mode

In this mode, in addition to the general data, the events are displayed as raw hex byte frames - this enables the user to view the data before and after Sentry resolves it. The purpose of this feature is to record and figure any errors in any module of PimaGuard or the control panels.

The debug log file size has the same logic as all other log files. See Logs, on page 32.

3.12.1.2. Filters

Selecting a filter in the monitor is implemented immediately. In addition, the filters in the *Debug* mode behave differently than any other filter in Sentry:

a) In any filter other than "Channel", the Debug frames are displayed during the whole Sentry activity, displaying only valid resolved frames that are applied by the filter - this is because filters can only be applied after data is resolved

b) In the "Channel" filter the monitor displays the filtered frames. The channel (physical or logical) is known, so raw frames can be filtered before resolving them

3.12.2. Configuration Analyzer

The *Configuration Analyzer* is a tool for detecting configuration errors - it checks for programming errors continuously. Double-clicking an error or warning shifts the window to the incorrect configuration location.

Note that the analyzer serves only as a diagnostic tool, and does prevent saving incorrect configurations.

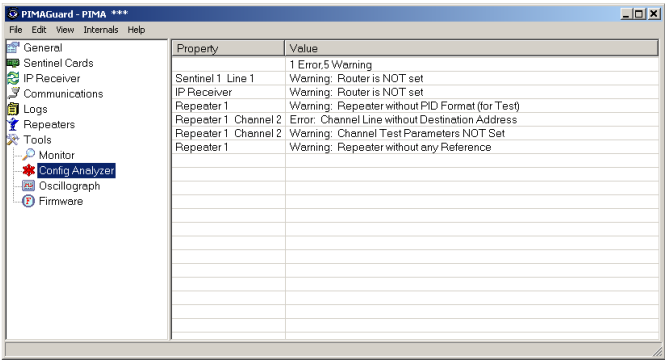


Figure 14. The Configuration Analyzer window

The icon of the analyzer has 3 colors:

Color	Description
White	No errors or warnings are detected
Green	Warning: a configuration error that may lead to loss of data
Red	Critical error: a configuration error that must be resolved, or PimaGuard will malfunction.

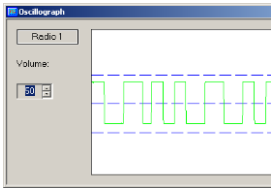
3.12.3. Oscillograph

The *Oscillograph* enables setting the volume of the Sentinel's radio amplifier. The volume is displayed as a virtual Oscillograph.

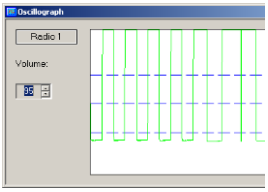
While setting the volume, PimaGuard cannot receive events. A warning message is displayed before taking this action. When you close the Oscillograph window, reception is returned

To use the Oscillograph, do the following:

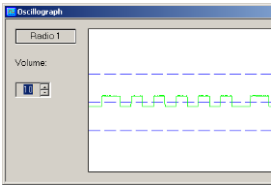
1. Click *Oscillograph* on the left pane.
2. Double-click Sentinel 1-4.
3. Click Radio X button.
4. Use the Vol. buttons to increase/decrease the volume while transmitting. The volume should not pass either the upper or lower limits and not be to low (close to the mid line). See the next examples.



Normal level volume



Abnormal high volume



Abnormal low volume

3.12.4. Firmware

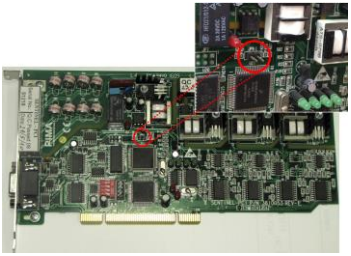
Do not upgrade the Sentinel's Firmware version before consulting PIMA support team!

To install a new Sentinel Firmware version, do the following:

1. Click *Tools* on the menu tree
2. Click *Firmware*.
3. Double-click *Sentinel 1-4*. The Firmware window properties are:

Property	Details
Firmware File	The Firmware file path
Firmware File Version	The selected file version
Firmware Version	The current SENTINEL firmware version
Program	See below
Test RAM	See below

4. Click *Browse* and locate the Firmware file (*.S19)
5. Click *Program* to install the file, and follow the installation steps.
6. Place the Sentinel's *VFP jumper* in place. Sentry will now erase the current installed Firmware and install the new one.



7. The message "Programming PASS" is displayed when installation ends successfully. If not, an error message is displayed.
8. Remove the jumper. PimaGuard will now verify the installation.
9. Click *Test RAM*, and then click *Start*. Wait for the message "Test RAM PASS" to be displayed.

While installing a Sentinel Firmware, Sentry cannot receive events - a warning message is displayed before taking this action. When installation is complete, reception is regenerated.

3.13. Filters

A filter in Sentry enables you to decide which events will be acknowledged by Sentry, and which will be ignored. All the filters work the same in every module level of the software.

The available filters are: Account, Event, Date, Days, Time, Format, and Channel. In addition to that, you can create a text file with specific name and extension and a list of accounts (records), and Sentry will filter only these accounts (or part of them. See next sub-sections). This filter is applied only after all the other filters are.

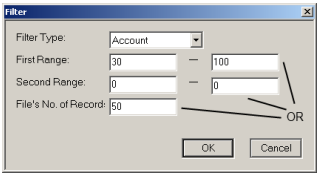
3.13.1. Filter operators

A filter in Sentry has the following optional operators:

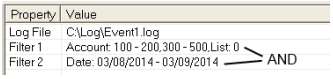
- OR: acknowledges events that are either within the selected filter's ranges, or within the no. of records (see below)
- AND: acknowledges events within several different filters

3.13.1.1. Examples

1. In this example, Sentry will accept events from account no.'s 30-100, OR if the account no. is within the first 50 accounts in the accounts file.



2. In this example, Sentry will accept events according to Filter #1 (account no's 100-200, OR 300-500), AND Filter #2 (between the dates 03/08/2014 to 03/09/2014).



3.13.2. Filter types

Filter	Description
Account	The account filter allows setting up to 2 account ranges and a limit of records on the filter file
File's no. of records	The no. of the first records in the filter file that will be accepted. For example, if the file contains 1,000 accounts, and the no. set here is 400, then only the first 400 records will be accepted
Event	The event no. has decimal values, where: • CID/PID: 3 decimal digits. Range: 0-999

Filter	Description
	• PAF/NPAF:
	PAF: Range: 0-400 How to convert PK in PAF to the filter's value? In ASCII P=0x50, K=0x4B => ((0x50-0x41)*26) + (0x4B-0x41) => 400
	How to convert the filter's value of 400 to a PAF event? 0x41 (ASCII)+ (400/26) = > 0x50 (ASCII) => P, 0x41+ (400%26) = > 0x4B => K => PK PK is the filter's highest event range in PAF and NPAF
	EPAF: Ranges: up to ZZ, 0-680 To convert a 2 letter event in EPAF to the filter's value, see the PAF formula above. How to convert event no. 680 to the filter's value? 680-(((0x5A-0x41)*26) + (0x5A-0x41)) => 5-1 (start from 0) => 04, the event 04 is the filter top range in EPAF table
	How to the filter's value of 27 to an EPAF event? ((0x5A-0x41)*26) + (0x5A-0x41) + 27 => 702+1 (start from 0) => 703
	SIA: The same formula as in PAF above
Date	From/to days range ***Verify the PC time before using the Date and Days filters.***
Days	Number of days
Time	From/to hour range
Format	Select up to 2 formats per Line/Radio/Channel
Channel	Physical or logical channel filter. For example, in the Monitor, you can filter events and see only those who are received through SENTINEL 1 Line 2

Note

- *When multiple filters are in use, the filter's operator is "AND"*
- *A range includes both margins*
- *Filters are applied after resolving the event (except the Channel filter)*
- *Fault events and* Sentry *internal events are not filtered by any of the filters*

3.13.3. Filter file

The name of the accounts file tells PimaGuard where to apply the filter. The structure of a generic filter filename is TSCFN.FLL, where:

- T: Type. The type options are listed in the next table
- S: event Source (Sentinel, Repeater or COM's index number)
- C: Channel index number
- F: Format index number
- N: filter index Number

3.13.3.1. Type options

Letter	Type	Source	Channel	Format	Filter No.
S	Sentinel Card	0-3	Line: 0-3, Radio: 4-5	0-9, A-V	0-1
N	IP Receiver	0			
C	COM	0-9, A-F			
L	Log	0-7			
R	Repeater	0-9, A-F	0-3	0-9, A-V	
M	Monitor	0			

3.13.3.2. Examples

- S14B0.FLL

Sentinel #2, Radio #1, format # 12

- C10.FLL

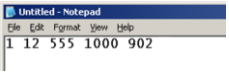
COM #2

- R201.FLL

Repeater #3, channel #1, filter #2

3.13.3.3. How to create a filter file

1. Open Windows Notepad or any text editor.
2. Type in the Account or Event numbers, leaving a space between the values.



3. Click Save As and save the file under the folder "C:\Program Files\Common Files\SIS" (Sentry's default installation folder), with a file name according to the type and level of the filter (see the table in section 3.13.3.1) and the extension 'fll', for example, **S11V0.fll**. Note that the file name is not case sensitive.

Appx A. Transceiver's settings and recommended specifications

Transceiver	Settings and recommended specifications
Squelch	1. The squelch switch can be manually adjusted. 2. The squelch should not change when the transceiver is turned off. 3. The internal squelch can be turned off.
Output signal	1. A speaker switch is optional 2. The maximum output signal (of the external speaker) should not exceed 1Vp-p. 3. The output signal should not changed at all time - it should not be volume or speaker switch dependent. 4. The output signal should not include any data, for example, start-up ID, pre-transmission message, etc.
Transmission	Transmission should not be conditioned with any other parameter, for example, transmission should start even if it the frequency is busy.
PTT	Response time should not exceed 150msec.
I/O Interface	• Wires length should be up to 1 meter long. • PTT should be controlled • The transceiver should be connected to ground • The transceiver should have Audio In connection (a microphone input can also be used). • The transceiver should have Audio Out connection.

A. Installation checklist

The transceiver should follow these guidelines:

1. Narrowband receiver (12.5 KHz)
2. No data transmission (like ID, pre-transmission message) is allowed within the transmission
3. The squelch should be turned OFF permanently (signal and noise are fully transferred to the SENTINEL). It can be set manually or be internally:
   c) Manually: turning the receiver on and off does not affect the squelch
   d) Internal squelch: the squelch is turned Off by the manufacturer
4. The receiver signal output should not exceed 1Vp-p and be steady. It should not be effected by the volume control knob or the received signal strength (Automatic Gain Control (AGC) must be turned off)
5. The radio should always transmit unconditionally (some transmitters interrogate the network when the PTT is pressed and will not transmit if it is busy)
6. The transmitter wakeup time should be less than 150 ms.

B. Antenna and cable

1. The antenna should have at least 4.7 dB attenuation
2. Use RG-213 cable when the distance between the antenna base and the radio is less than 20 meters. Use Helix antenna cable when the distance is longer than 20 meters
3. The antenna should be lightning protected
4. All antenna connections should be sealed against wetness
5. The antenna cable should not run in parallel to any electric wires, to avoid RF interferences. If you must, leave minimum 1 meter between the cable and the electric wires
6. Voltage Standing Wave Ratio (VSWR) should be 1.5V max

Appx B. Fault Codes

A. Sentry

All Sentry fault codes are sent in 4x2 format with the fault account number, or the repeater's supervision account number (if set).

Code	Description	Code	Description
00	Test	--	--
01	Phone Line 1 Fail	81	Phone Line 1 Restore
02	Phone Line 2 Fail	82	Phone Line 2 Restore
03	Phone Line 3 Fail	83	Phone Line 3 Restore
04	Phone Line 4 Fail	84	Phone Line 4 Restore
05	Phone Line 5 Fail	85	Phone Line 5 Restore
06	Phone Line 6 Fail	86	Phone Line 6 Restore
07	Phone Line 7 Fail	87	Phone Line 7 Restore
08	Phone Line 8 Fail	88	Phone Line 8 Restore
09	Phone Line 9 Fail	89	Phone Line 9 Restore
0A	Phone Line 10 Fail	8A	Phone Line 10 Restore
0B	Phone Line 11 Fail	8B	Phone Line 11 Restore
0C	Phone Line 12 Fail	8C	Phone Line 12 Restore
0D	Phone Line 13 Fail	8D	Phone Line 13 Restore
0E	Phone Line 14 Fail	8E	Phone Line 14 Restore
0F	Phone Line 15 Fail	8F	Phone Line 15 Restore
10	Phone Line 16 Fail	90	Phone Line 16 Restore
11	Radio 1 Fail	91	Radio 1 Restore
12	Radio 2 Fail	92	Radio 2 Restore
13	Radio 3 Fail	93	Radio 3 Restore
14	Radio 4 Fail	94	Radio 4 Restore
15	Radio 5 Fail	95	Radio 5 Restore
16	Radio 6 Fail	96	Radio 6 Restore
17	Radio 7 Fail	97	Radio 7 Restore
18	Radio 8 Fail	98	Radio 8 Restore
19	COM 1 Fail	99	COM 1 Restore
1A	COM 2 Fail	9A	COM 2 Restore
1B	COM 3 Fail	9B	COM 3 Restore
1C	COM 4 Fail	9C	COM 4 Restore
1D	COM 5 Fail	9D	COM 5 Restore
1E	COM 6 Fail	9E	COM 6 Restore

Code	Description	Code	Description
1F	COM 7 Fail	9F	COM 7 Restore
20	COM 8 Fail	A0	COM 8 Restore
21	COM 9 Fail	A1	COM 9 Restore
22	COM 10 Fail	A2	COM 10 Restore
23	COM 11 Fail	A3	COM 11 Restore
24	COM 12 Fail	A4	COM 12 Restore
25	COM 13 Fail	A5	COM 13 Restore
26	COM 14 Fail	A6	COM 14 Restore
27	COM 15 Fail	A7	COM 15 Restore
28	COM 16 Fail	A8	COM 16 Restore
29	Log 1 Fail	A9	Log 1 Restore
2A	Log 2 Fail	AA	Log 2 Restore
2B	Log 3 Fail	AB	Log 3 Restore
2C	Log 4 Fail	AC	Log 4 Restore
2D	Log 5 Fail	AD	Log 5 Restore
2E	Log 6 Fail	AE	Log 6 Restore
2F	Log 7 Fail	AF	Log 7 Restore
30	Log 8 Fail	B0	Log 8 Restore
31	Repeater 1 Channel 1 Fail[1]	B1	Repeater 1 Channel 1 Restore[1]
32	Repeater 1 Channel 2 Fail[1]	B2	Repeater 1 Channel 2 Restore[1]
33	Repeater 1 Channel 3 Fail[1]	B3	Repeater 1 Channel 3 Restore[1]
34	Repeater 1 Channel 4 Fail[1]	B4	Repeater 1 Channel 4 Restore[1]
35	Repeater 2 Channel 1 Fail[1]	B5	Repeater 2 Channel 1 Restore[1]
36	Repeater 2 Channel 2 Fail[1]	B6	Repeater 2 Channel 2 Restore[1]
37	Repeater 2 Channel 3 Fail[1]	B7	Repeater 2 Channel 3 Restore[1]
38	Repeater 2 Channel 4 Fail[1]	B8	Repeater 2 Channel 4 Restore[1]
39	Repeater 3 Channel 1 Fail[1]	B9	Repeater 3 Channel 1 Restore[1]
3A	Repeater 3 Channel 2 Fail[1]	BA	Repeater 3 Channel 2 Restore[1]
3B	Repeater 3 Channel 3 Fail[1]	BB	Repeater 3 Channel 3 Restore[1]
3C	Repeater 3 Channel 4 Fail[1]	BC	Repeater 3 Channel 4 Restore[1]
3D	Repeater 4 Channel 1 Fail[1]	BD	Repeater 4 Channel 1 Restore[1]
3E	Repeater 4 Channel 2 Fail[1]	BE	Repeater 4 Channel 2 Restore[1]
3F	Repeater 4 Channel 3 Fail[1]	BF	Repeater 4 Channel 3 Restore[1]
40	Repeater 4 Channel 4 Fail[1]	C0	Repeater 4 Channel 4 Restore[1]
41	Repeater 5 Channel 1 Fail[1]	C1	Repeater 5 Channel 1 Restore[1]
42	Repeater 5 Channel 2 Fail[1]	C2	Repeater 5 Channel 2 Restore[1]
43	Repeater 5 Channel 3 Fail[1]	C3	Repeater 5 Channel 3 Restore[1]
44	Repeater 5 Channel 4 Fail[1]	C4	Repeater 5 Channel 4 Restore[1]
45	Repeater 6 Channel 1 Fail[1]	C5	Repeater 6 Channel 1 Restore[1]
46	Repeater 6 Channel 2 Fail[1]	C6	Repeater 6 Channel 2 Restore[1]
47	Repeater 6 Channel 3 Fail[1]	C7	Repeater 6 Channel 3 Restore[1]
48	Repeater 6 Channel 4 Fail[1]	C8	Repeater 6 Channel 4 Restore[1]
49	Repeater 7 Channel 1 Fail[1]	C9	Repeater 7 Channel 1 Restore[1]
4A	Repeater 7 Channel 2 Fail[1]	CA	Repeater 7 Channel 2 Restore[1]
4B	Repeater 7 Channel 3 Fail[1]	CB	Repeater 7 Channel 3 Restore[1]
4C	Repeater 7 Channel 4 Fail[1]	CC	Repeater 7 Channel 4 Restore[1]
4D	Repeater 8 Channel 1 Fail[1]	CD	Repeater 8 Channel 1 Restore[1]
4E	Repeater 8 Channel 2 Fail[1]	CE	Repeater 8 Channel 2 Restore[1]
4F	Repeater 8 Channel 3 Fail[1]	CF	Repeater 8 Channel 3 Restore[1]
50	Repeater 8 Channel 4 Fail[1]	D0	Repeater 8 Channel 4 Restore[1]
51	Repeater 9 Channel 1 Fail[1]	D1	Repeater 9 Channel 1 Restore[1]
52	Repeater 9 Channel 2 Fail[1]	D2	Repeater 9 Channel 2 Restore[1]
53	Repeater 9 Channel 3 Fail[1]	D3	Repeater 9 Channel 3 Restore[1]
54	Repeater 9 Channel 4 Fail[1]	D4	Repeater 9 Channel 4 Restore[1]

Code	Description	Code	Description
55	Repeater 10 Channel 1 Fail[1]	D5	Repeater 10 Channel 1 Restore[1]
56	Repeater 10 Channel 2 Fail[1]	D6	Repeater 10 Channel 2 Restore[1]
57	Repeater 10 Channel 3 Fail[1]	D7	Repeater 10 Channel 3 Restore[1]
58	Repeater 10 Channel 4 Fail[1]	D8	Repeater 10 Channel 4 Restore[1]
59	Repeater 11 Channel 1 Fail[1]	D9	Repeater 11 Channel 1 Restore[1]
5A	Repeater 11 Channel 2 Fail[1]	DA	Repeater 11 Channel 2 Restore[1]
5B	Repeater 11 Channel 3 Fail[1]	DB	Repeater 11 Channel 3 Restore[1]
5C	Repeater 11 Channel 4 Fail[1]	DC	Repeater 11 Channel 4 Restore[1]
5D	IP Receiver Fail	DD	IP Receiver Restore
5E	IP Receiver Cellular Multiple Offline	DE	IP Receiver Cellular Multiple Offline Restore
5F	IP Receiver Ethernet Multiple Offline	DF	IP Receiver Ethernet Multiple Offline Restore
60	Tamper Open[2]	E0	Tamper Restore[2]
61	Zone 1 Open[2]	E1	Zone 1 Restore[2]
62	Zone 2 Open[2]	E2	Zone 2 Restore[2]
63	AC Fault[2]	E3	AC Restore[2]
64	Low Battery Fault[2]	E4	Low Battery Restore[2]
65	Repeater 12 Channel 1 Fail[1]	E5	Repeater 12 Channel 1 Restore[1]
66	Repeater 12 Channel 2 Fail[1]	E6	Repeater 12 Channel 2 Restore[1]
67	Repeater 12 Channel 3 Fail[1]	E7	Repeater 12 Channel 3 Restore[1]
68	Repeater 12 Channel 4 Fail[1]	E8	Repeater 12 Channel 4 Restore[1]
69	Repeater 13 Channel 1 Fail[1]	E9	Repeater 13 Channel 1 Restore[1]
6A	Repeater 13 Channel 2 Fail[1]	EA	Repeater 13 Channel 2 Restore[1]
6B	Repeater 13 Channel 3 Fail[1]	EB	Repeater 13 Channel 3 Restore[1]
6C	Repeater 13 Channel 4 Fail[1]	EC	Repeater 13 Channel 4 Restore[1]
6D	Repeater 14 Channel 1 Fail[1]	ED	Repeater 14 Channel 1 Restore[1]
6E	Repeater 14 Channel 2 Fail[1]	EE	Repeater 14 Channel 2 Restore[1]
6F	Repeater 14 Channel 3 Fail[1]	EF	Repeater 14 Channel 3 Restore[1]
70	Repeater 14 Channel 4 Fail[1]	F0	Repeater 14 Channel 4 Restore[1]
71	Repeater 15 Channel 1 Fail[1]	F1	Repeater 15 Channel 1 Restore[1]
72	Repeater 15 Channel 2 Fail[1]	F2	Repeater 15 Channel 2 Restore[1]
73	Repeater 15 Channel 3 Fail[1]	F3	Repeater 15 Channel 3 Restore[1]
74	Repeater 15 Channel 4 Fail[1]	F4	Repeater 15 Channel 4 Restore[1]
75	Repeater 16 Channel 1 Fail[1]	F5	Repeater 16 Channel 1 Restore[1]
76	Repeater 16 Channel 2 Fail[1]	F6	Repeater 16 Channel 2 Restore[1]
77	Repeater 16 Channel 3 Fail[1]	F7	Repeater 16 Channel 3 Restore[1]
78	Repeater 16 Channel 4 Fail[1]	F8	Repeater 16 Channel 4 Restore[1]
79	Not in use	--	--
7A	Invalid Account Addition	--	--
7B	Invalid Repeater Event	--	--
7C	Pattern Error	--	--
7D	Call ID\IP Error	--	--
7E	Critical Temperature[3]	FE	Critical Temperature Restore[3]
7F	General Fault[4]	FF	General Fault Restore[4]

[1] If a repeater test/fail account is set, the repeater faults are sent with TN in "DOS Compatible" mode or 334 if not. Else, they are sent with the above fault codes

[2] SAR-100 codes

[3] "SpeedFan©" or any other temperature monitor code

[4] Includes "Invalid Repeater Event", "SENTINEL Fault", "Not Enough Memory is Available" and any undefined error. Not all general faults have a restore event

B. Repeater

Repeater fault codes (not 4x2 faults) are reported only if the account and test times are set (see repeater IN, section 3.11.1.1, on page 34)

Code	Description
SN	DOS compatible test (PAF)
TN	DOS compatible fault (PAF)
602	Not DOS compatible test (PID)
334	Not DOS compatible test (PID)

C. Sentinel status

The Status of the SENTINEL is reported in 2 bytes, as 7F events. It is bitwise and can indicate more than one problem, for example 0003 means both Overflow and Not Responding.

The Status indications are as follows:

Status	Fault	Resolve
0001	Chip overflow	External hardware connected to SENTINEL is causing chip overflow: • Check transmitter voltage and currents • Check phone lines voltage • Reset card slots. See section 3.5.4, on page 18
0002	Unresponsive SENTINEL	• Verify that the SENTINEL is inserted in the PCI slot properly • Verify the SENTINEL physical address
0010	Configuration file error	Check configuration and re-install if required
00FF	General error	Contact PIMA tech support

Appx C. Communication Formats

A. How to create custom COM formats

1. Click "General"
2. Click "COM Format".
3. Double-click "Modify COM Format" on the right. The properties of this window are:

Property	Details
Format Name	Must be a unique name
ACK Pattern[1,2]	Patterns to send events or expect them in Software and External modes
Idle Pattern[1,2]	
Structure X	Select up to 4 structures (multiple selection allowed), each with "Format Types", "Built-in Conditions", "Event Conversion" and "Pattern". A selected format type cannot be selected in a different structure.
Built-in Conditions	Relevant if [SSS…] is set in one of the above patterns (field size is equal to number of "S" characters) The conditions apply to the following formats: • Atia 1389, 13489, 123459 • Andromeda • Comfuture • Format • Galaxy • Ademco 685
Event Conversion	Use it to convert any format type to the following: ○ Hex 2 Digits ○ CID
Pattern[2]	The actual data placement for each structure, according to "Legend of COM Pattern Symbols" Pattern: \0A## AAAA 18 [Q0U1E3R6P]EEE PP ZZZ \0D

[1] "Legend of Pattern Symbols" is not applicable in these patterns, except for Decoder ID (**) and Channel numbers (##)

[2] A Backslash "\" must be followed by two hex characters, representing a byte value, e.g. \0D => CR (Carriage return), \2B => "+" (ASCII)

B. Examples

Custom 1 format

The patterns in the following figure are based on "Surgard"

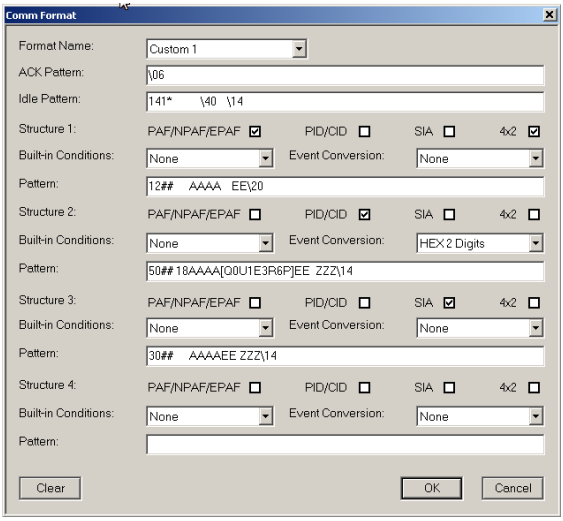


Figure 15. Custom format #1

The changes that were made in the "Surgard" format are:

- The Idle pattern was changed from "1011 \40 \14" to "141* \43 *4". The asterisk will be replaced by the main Decoder ID
- "Structure 1" pattern was changed by replacing "10" with "12" in the pattern's header, and "\14" with "\20" in pattern's end
- The "Event Conversion" on "Structure 2" was changed to "Hex 2 Digits": CID event #120 will be output as 78
- The pattern of "Structure 2" was changed from two event characters ("EE") to three ("EEE") Also the alarm bit condition was changed from [Q0U1E3R6P] to [Q1E3R6P]: all CID events other than alarms, restores and statuses will be outputted as alarm (1\E)

Custom 2 format

The patterns in the following figure are also based on "Surgard":

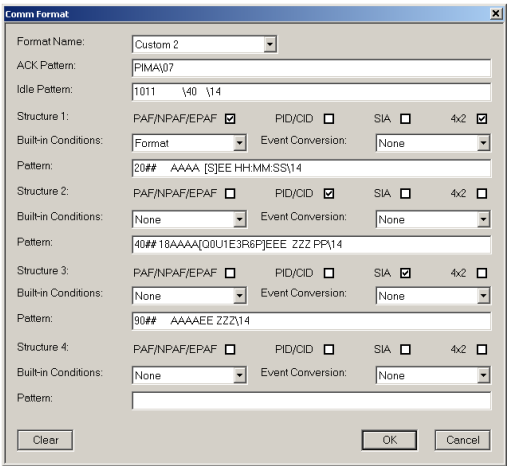
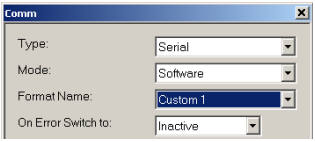


Figure 16. Custom format #2

The changes that were made in the "Surgard" format are:

- The ACK pattern was changed from "\06" to "PIMA\07"
- "Structure 1" "Built-in Conditions" were set as "Format", and the [S] operator was placed in the pattern. This change means that incoming events will be checked against the structure's formats (PAF/NPAF/EPAF/4x2 in this example) and replaced by a digit, representing the format
- "Structure 1" pattern was changed by adding hour legend to end "HH:MM:SS"
- "Structure 2" pattern was changed by adding "PP" to indicate on partitions
- The pattern's header of Structures 1, 2 and 3 was changed to a different number: "Structure 1" changed from "10" to "20", "Structure 2" from "50" to "40" and "Structure 3" from "30" to "90". After setting the custom formats, you can select them in the Communication menu



Limited warranty

PIMA Electronic Systems Ltd. shall have no liability for any death, personal and/or bodily injury and/or damage to property or other loss whether direct, indirect, incidental, consequential or otherwise, based on a claim that the Product failed to function.

Please refer to a separate warranty statement on PIMA website at:
http://www.pima-alarms.com/site/Content/t1.asp?pid=472&sid=57

Warning: The user should follow the installation and operation instructions and among other things test the Product and the whole system at least once a week. For various reasons, including, but not limited to, changes in environment conditions, electric or electronic disruptions and tampering, the Product may not perform as expected. The user is advised to take all necessary precautions for his/her safety and the protection of his/her property.

All efforts have been made to ensure that the content of this manual is accurate. Pima retains the right to modify this manual or any part thereof, from time to time, without serving any prior notice of such modification.

Please read this manual in its entirety before attempting to program or operate your system. Should you misunderstand any part of this manual, please contact the supplier or installer of this system.

Manufactured by:

PIMA Electronic Systems Ltd.

www.pima-alarms.com

5 Hatzoref Street, Holon 5885633, ISRAEL.

Tel: +972.3.6506414

Fax: +972.3.5500442

Email: support@pima-alarms.com

P/N: 4410051

Revision: XX en, H, Oct. 2019