



W & WIP ALARM PANEL

DOC. - REF. 230-W-WIP-AUS LAST MODIFICATION DATE : NOVEMBER 2016 FIRMWARE VERSION : XLP.07.07.15.XXX AND LATER











INTRODUCTION

Description

Since 2002, RSI VIDEO TECHNOLOGIES provides the only wireless video verification on the market, thanks to the Motion ViewerTM detectors and to the Videofied[®] product range.

After 2 years of development, RSI VIDEO TECHNOLOGIES is proud to present the new W alarm panel.

The W alarm panel is wireless and mains powered with a backup rechargeable battery (provided). The W panel is the first Videofied[®] alarm panel that can be used as a connected device.

This panel is intended for residential and commercial markets.

Like all the Videofied $^{\otimes}$ alarm panels, the W panel is compatible with every radio device manufactured by RSI VIDEO TECHNOLOGIES.

Technology

The W alarm panel uses the S2View® patented technology. That interactive and wireless technology ensures signal integrity. The bidirectional radio link maximizes the signal reliability.

AES encryption protects the communication between the panel and the devices. Transmission security is optimal.

The jamming detection feature identifies any intentional jamming from a third party.

The supervision feature consists of transmitting signals between every device of the system and the W alarm panel. Through the supervision, the detectors transmit every 8 minutes a presence signal.

The entire RSI VIDEO TECHNOLOGIES team wishes you a successful installation.





SUMMARY

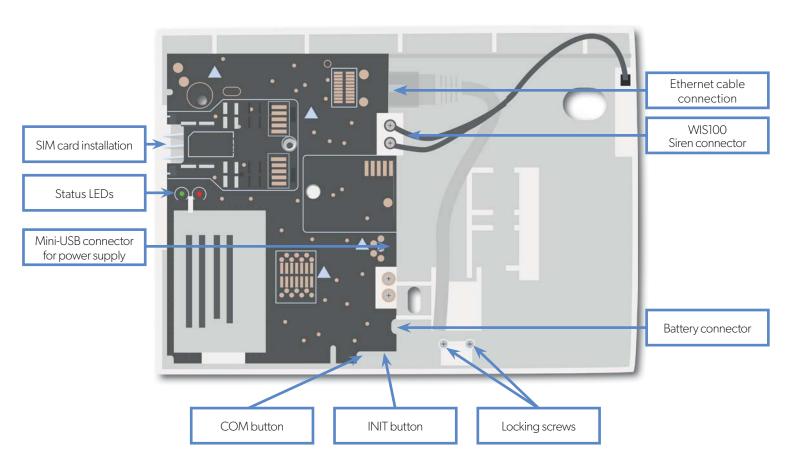
Introduction	2
Summary	3
1. W installation and setup	4
1.1 Panel overview	4
1.2 Panel mounting	4
1.3 Ethernet cable connexion	5
1.4 SIM card installation	5
1.5 Powering and initialization	5
1.6 Indicator lights	6
1.7 Pairing the keypad	6
2. W panel programming	7
3. W panel features guide	17
3.1 Get to access level 4	17
3.2 How to arm/disarm the system	17
3.3 Arming and siren mode configuration	18
3.4 Manage badges and access codes	19
3.5 Delete a device from the system	21
3.6 Read the event log	
3.7 Automatic arming/disarming	
3.8 Golden rules	
3.9 Additional features	23
4. Ethernet parameters	24
5. Transmitter events list	25
6. 2G3G error codes	26
7. Security and certifications notes	27
8. Technical specifications	29





1. W INSTALLATION AND SETUP

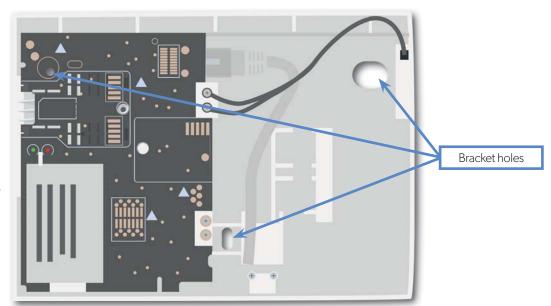
1.1 Panel overview



1.2 Panel mounting

Fix the back casing on the wall using the three mounting holes (4 mm diameter) as shown.

Mounting the panel is not required for programming.







1. W INSTALLATION AND SETUP

1.3 Ethernet cable connection

Only for WIP 720/730 models

Once the panel is fixed on the wall connect a RJ45 cable between the site internet network and the panel Ethernet port.

When the panel attempts a transmission via Ethernet, a red LED on the connector will flash. This will allow the installer to check whether the panel is connected to a valid network.

Do not touch the RJ45 cable when the panel is powered.

IMPORTANT:

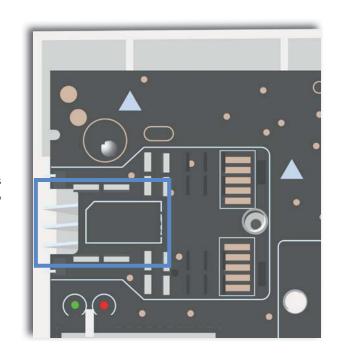
Only connect the panel on 10Base-T SELV networks.

1.4 SIM Card Installation

Insert a Mini-SIM 2FF SIM card in the location shown in the image. Please refer to the markings for the insertion direction.

Use a M2M (machine-to-machine) 2G3G SIM card. If the panel is used with a smartphone application, the SIM card shall be able to receive SMS.

DO NOT insert or remove the SIM card while the panel is powered.



1.5 Powering and initialization

AC Power

- Connect the backup battery.
- Install the power supply inside or outside the panel box depending on the needed cable length.
- Connect the power supply to the panel mini-USB connector.
- Plug the power supply in an electrical outlet.
- Do not connect the 12V input (sealed by a label), specifically when the panel is powered.

Initialization

- Leave the panel open. The green status LED is on. Press and hold the INIT button for 6-7 seconds until the status LED turns red for 1 second.
- The red LED blinks several times then turns off. That procedure resets the panel memory.
- The panel is now reset, a Videofied[®] keypad has to be enrolled to configure the panel.







1. W INSTALLATION AND SETUP

1.6 Indicator lights

	Red LED on	Red LED blinking (1 sec)	Red LED blinking (3 sec)	Red LED off
Green LED on (AC power detected)	N/A	Battery out of order or not detected.	Low voltage on the battery.	Normal operation
Green LED off (AC power not detected)	Low voltage on the battery	N/A	Panel working on battery. Battery OK.	Panel not powered or out of order.

1.7 Pairing the remote keypad

- Press briefly the panel INIT button and release for the enrollment of a programming keypad.
- Insert 3 or 4 LS14500 Lithium batteries into the keypad.
- Do not mount the keypad. It will display on of the following screens:



- **Press on both CLR** and **ESC NO** keys **at the same time** and release. The indicator LED on the keypad will blink rapidly. Wait for the keypad to pair.
- If the keypad does not pair up with the panel and shows "XX", it certainly means that it is stilled paired to another system. The keypad needs to be reset. Remove the batteries and press repeatedly on the keypad tamper switch for 30 seconds to 1 minute. Then proceed to the above steps.





Use the keypad to program the panel

Keypad Display

Actions and comments

KEYPAD 1 RECORDED

OK or YES

<-LANGUAGE: -> ENGLISH (UK)

for language selection

OK or YES

RADIO RANGE TEST?

OK or YES

RF TEST x/9

Attendre

RF TEST 9/9

OK or YES

RADIO RANGE TEST?

ESC NO

INSTALLER CODE

4 TO 6 DIGITS THEN OK/YES

INSTALLER CODE:

OK or YES

CONFIRM CODE

OK or YES

The system can also be programmed in: french, italian, german, dutch, spanish, swedish, portuguese, danish, czech, turkish and polish.

The language can be changed at any time once the panel is programmed in the MAINTENANCE menu.

The radio range test must be run during the device learning process in order to ensure proper pairing with the control panel.

This test is important, it measures the strength of communication between the device and the control panel. The keypad will display a real time radio range value on a

To receive the most accurate results you must run the radio range test for at least 30 seconds.

Result must be 8 out of 9 or better for reliable transmission.

Using the alphanumeric keypad, enter the installer code of your choice.

The installer code will be used for all future maintenance and configuration.

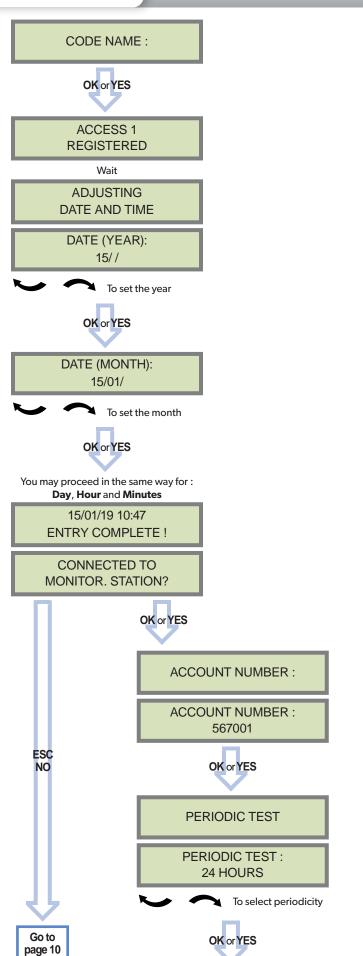
This code is important to keep track of.

There is no back door or Default codes to the system.

Please refer to the restriction rules for codes (Chapter 3.4). Some codes are already used by default and therefore cannot be used.







You may name the installer code using the alphanumeric keypad.

If using automatic setting (called installer default list), enter the name of the list.

Warning: If the wrong installer list name is used, it cannot be set later, the system must be defaulted.

Leaving the name blank by pressing **ESC NO**, it will be named 'ACCESS 1' by default.

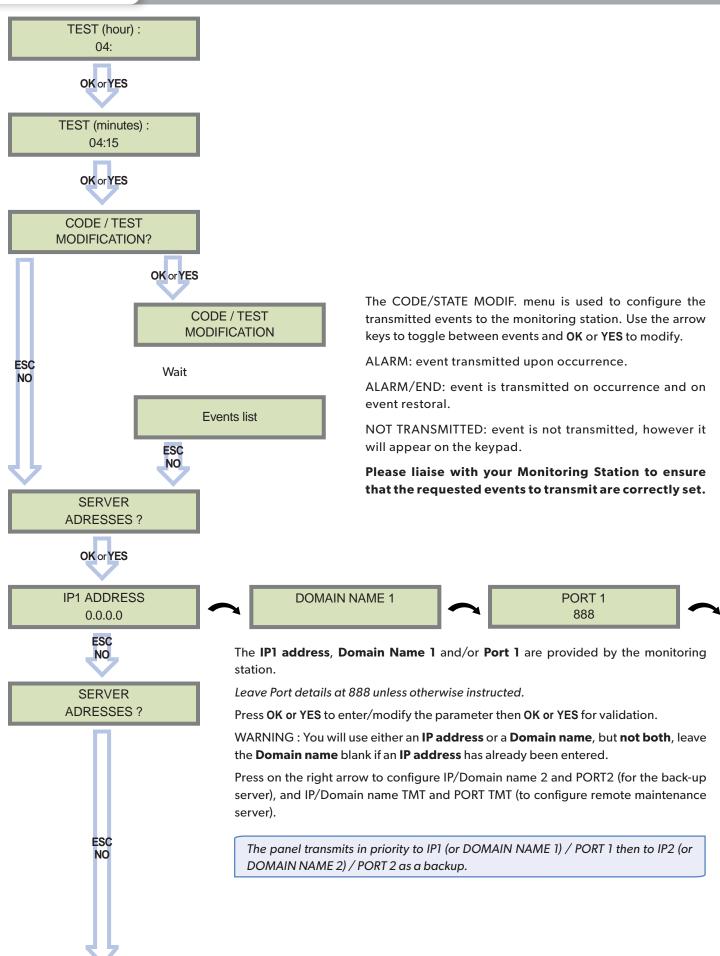
Use the alphanumeric keypad to enter in a 4-8 digit account number provided by the Central Station

Test Periodicity: 1 hour, 12 hours, 24 hours, 48 hours, 7 days or no tests.

We suggest a 24 hours periodic test call.



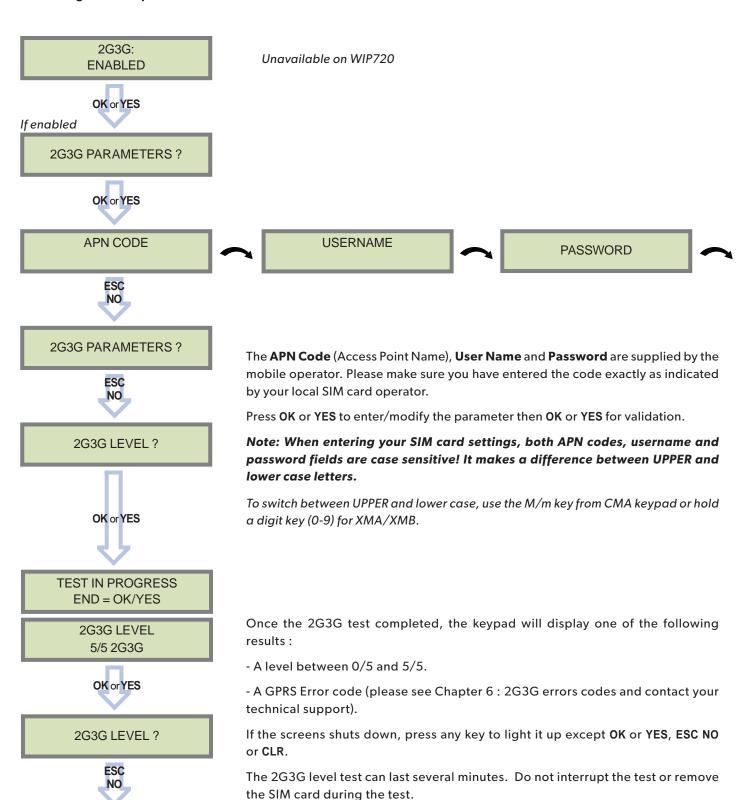








Transmission channels selection According to the W panel reference and WWB100 module

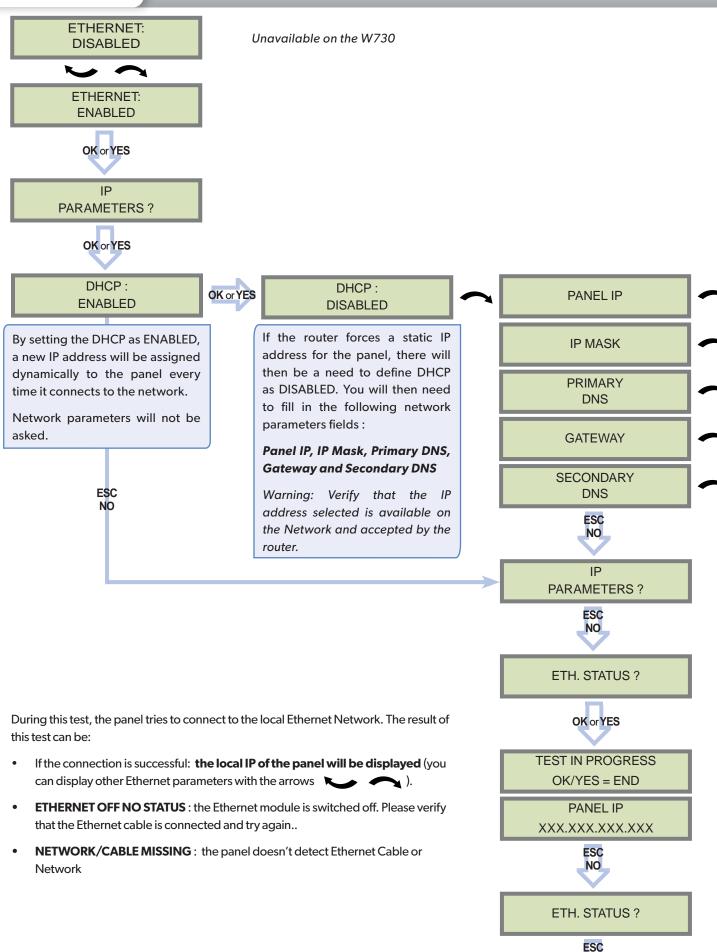


transmission of Video alarms.

IMPORTANT: Videofied will require a 3/5 grade or better for reliable



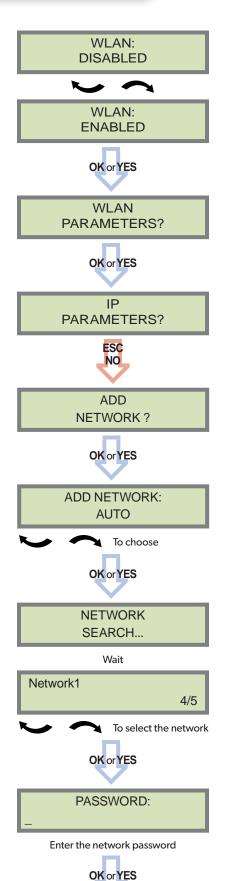




NO







Enable the WLAN.

Please choose between:

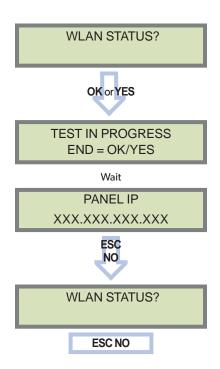
AUTO: The WWB100 scans automatically every WLAN network available and displays them for selection.

WPS: The WWB100 only scans the available WPS networks and displays them for selection.

MANUAL: The WWB100 does not scan for networks and the user must enter the network ID (SSID) to connect.

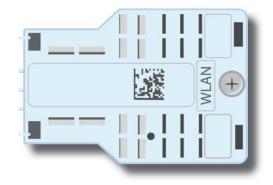






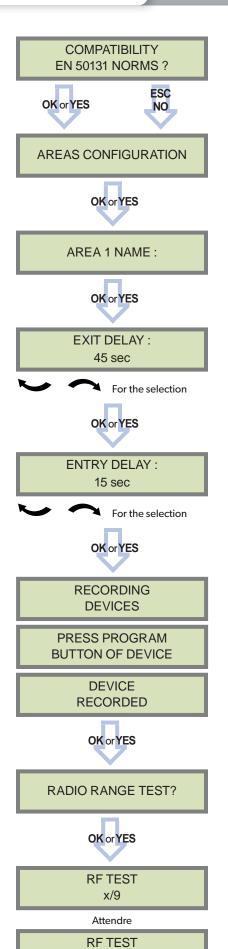
WLAN errors

NET NOT FOUND: 389	T FOUND: 389 Wrong network password.	
NET NOT FOUND: 396 No password entered or password too short.		
NET NOT FOUND: 395	Network off or non existent.	









For full compatibility with EN50131 norms, press **OK** or **YES**. Otherwise, press **ESC NO**.

Press ESC NO to default the area names.

Enter the name of Area 1 and confirm with **OK** or **YES**.

Repeat the procedure for areas 2,3 and 4.

For further details, please refer to chapter 3.3.

Available delays are: 2 min, 1 min, 45 sec.

Available delays are: 15 seconds, 30 seconds, 45 seconds, 1 minute et 2 minutes.

Each device has a unique programming button or a specific manipulation. Please refer to the Installation Sheet for the device you would like to program.

Please check the radio level of each device on its final location.

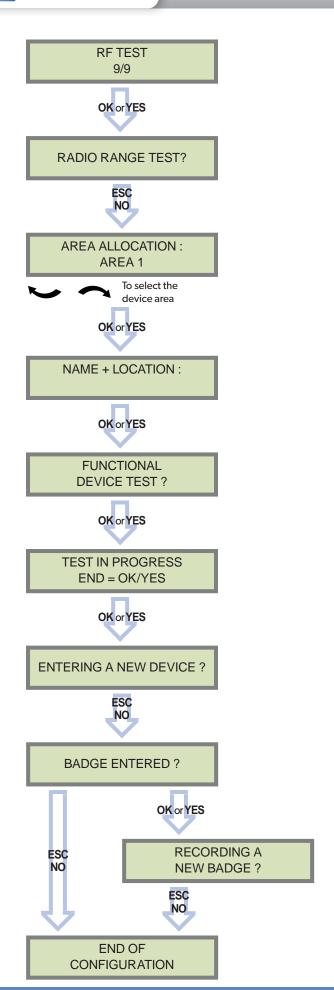
The result must be 8 out of 9 as a minimum.

Please refer to the RF test section on page 6 for further details.

9/9







Each device is recorded in an area.

Each area can be configured as delayed or immediate. Areas are used to set up special arming modes as well.

Please refer to the chapter 3.3 for further details about special arming modes.

By default (area set as Automatic), area 1 is delayed whereas areas 2, 3 and 4 are immediate. Recording a keypad or a badge reader in an area will automatically delay that area.

The name of the device shall contain every needed information to be properly processed in case of alarm.

During the functional device test, the device LED turns on when it detects an intrusion.

Press **OK** or **YES** to enter another device or **ESC NO** to move on to the next step.

Each system can embrace a maximum of 25 devices, **programming keypad included**.

Press **OK** or **YES** if you use one or more badges. **ESC NO** if you are not using any badges.

These badges will be used as a first user access (Level 3) and will be mandatory to access the engineer level (Level 4).

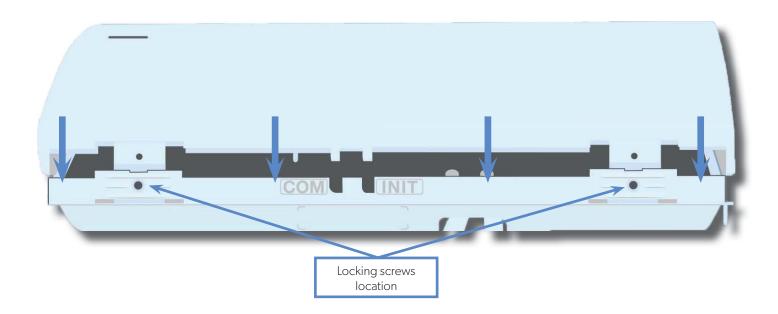
If you wish to use an user code, please skip this step and when initial programming is completed go to the BADGES/ACCESS CODES menu (please refer to chapter 3.4 for further details).

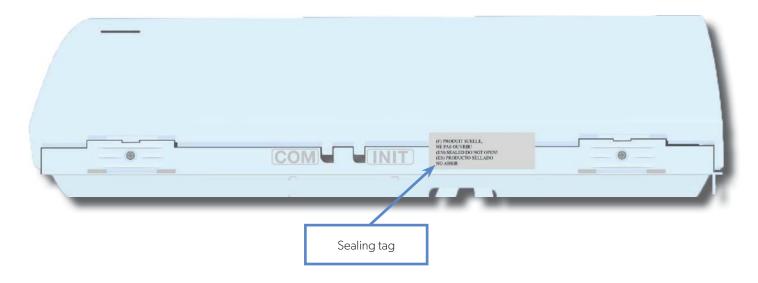
Badges and codes are limited to 49 user accesses and 1 engineer code.





When the configuration is over, close the panel box as shown below and lock the panel. You can find screws to lock the panel inside the box (see chapter 1.1 on page 4). Then stick the provided tag to seal the panel.





The keypad displays:



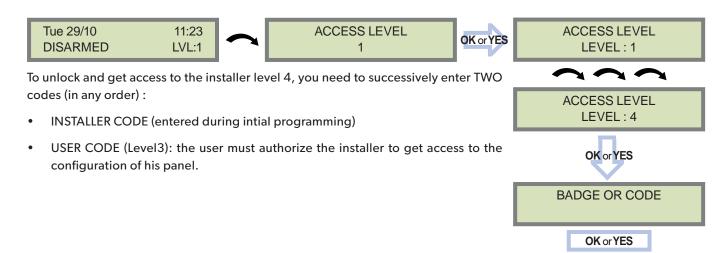
Before completing programming make sure that no device is tampered. Each device must be closed and its LED indicator shall be turned off.

After initial programming has been completed, make use of the menu overview document (available on our technical support portal), to see full programming options.





3.1 Get to Access level 4



3.2 How to Arm/Disarm the System

When in standby mode, the system can be armed with the remote keypad, the remote keyfob and/or the remote badge reader.

	Full arming with personal code	Full arming with badge	Special Arming 1	Special Arming 2
With remote keypad	Enter your user code and press OK or YES	Present your badge on the keypad (XMB model only)	Press ① enter your user code and press OK or YES	Press press OK or YES and enter your user code
With remote badge reader BR250	N/A	Present your badge on the badge reader	N/A	N/A
With remote keyfob	N/A	N/A	Press 🐧	Press 🙋





3.3 Arming and Siren Mode Configuration

• Use to go to menu:

CONFIGURATION (LEVEL 4) > SPECIAL ARMING MODES > FULL ARM, SP1 or SP2

• There are 3 different arming modes:

FULL ARM: Arming of all areas and all devices. Use a badge or a user code and press **OK** /

SP1 : Partial Arming (1) is enabled by entering the user code and pressing 🗓 on the keypad or 🐧 on the keyfob.

SP2: Partial Arming (2) is enabled by pressing and entering the user code. On the keyfob, SP2 is enabled by pressing 2.

For each arming mode, it is possible to specify how each of the 4 areas will be armed and how the system will behave during an alarm.

Areas: 1 2 3 4 Each time you press the corresponding number, the system will toggle the arming

state for the respective area.

State: A A A A Press **OK/YES** after this configuration step. The system will then display what siren

mode will be in effect for this special profile. Select the siren mode using the direction

arrows then press OK/YES.

A	Armed	
D	Disarmed	
P	Perimeter (by default: all opening contacts*)	
Е	External (by default : all opening contacts with external access*)	

Siren	Immediate triggering of all sirens	
Delay Beeps	Entry/Exit delay beeps, then triggering of all sirens	
Silent	No Sirens, No Beeps	
Without Siren	Beeps on the keypad only	

^{*} You can set your devices as : External, Perimeter, ou External +Perimeter. Please go to the menu:

 ${\tt CONFIGURATION\,(LVL\,4)>AREAS\,AND\,DEVICES>DEVICES>DEVICES\,CONFIGURATION>DEVICE\,TYPE}$





3.4 Manage badges and access codes

Access Level

Access Level	Definition & Rights	
LVL 1	Standby Level	
LVL 2	Restricted USER level, where it is only possible to arm/disarm the system.	
LVL 3	USER level, where it is possible to arm/disarm the system, check the event log, test the devices. Modifications of the settings are not possible at this level. User Level 3 can create Level 2 or Level 3 access codes or badges.	
LVL 4	INSTALLER level, where it is possible to modify the setup of the panel To access Level 4, the approval of a Level 3 oe Level 2 user is required. Installer Level 4 can create the first Level 3 access code only.	

Codes and badges get rights access to one of the 4 available levels of access.

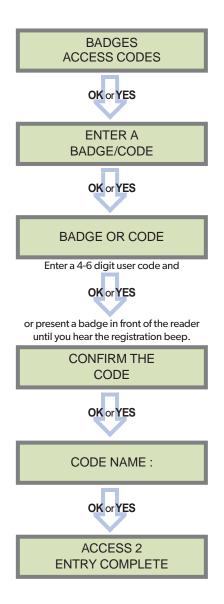
How to return to the LVL1?

- After 1 min of no use of the keypad and no tests running, the display returns to the standby display and LVL1.
- When standby display, if the **ESC NO** key is held during 5s, the level is changed to LVL1.

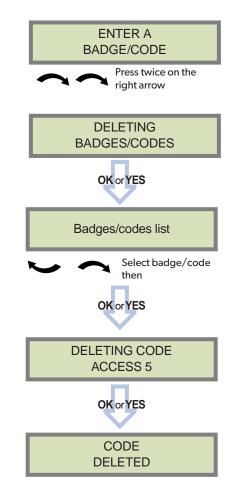




Enter a new end user Badge/Code



Delete an end user Badge/Code



Reserved Codes

Up to 49 codes (or badges) can be registered into the panel with the engineer code

A code has 4 to 6 digits (0 to 9).

The table presents the **reserved** code possibilities that cannot be used.

Those codes are used for maintenance or as panic/duress codes.

A total of 186 codes are forbidden.

	Reserved Codes	
	000000	
	From 9998 to 9999	
	From 99998 to 99999	
	From 999898 to 999999	
	From 314157 to 314159	
	All user codes +1	
	All user codes +2	
	All user codes -1	
	All user codes -2	
Ī	·	

When a code is created (1000 for example), the 2 next codes and previous codes (0998, 0999, 1001 and 1002) will be automatically reserved.

The +1 code (1001) is used for disarming under duress.

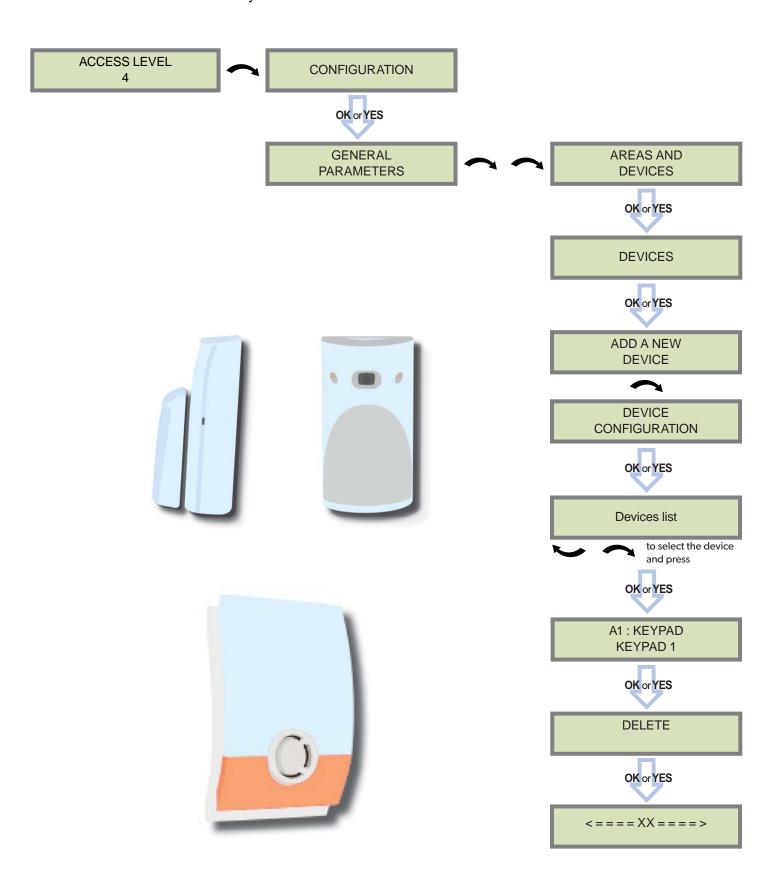
The +2 code (1002) is used for panic.

The -1 and -2 codes (0998 et 0999) are reserved to prevent conflicts when creating a new user code.





3.5 Delete a device from the system



You can now remove the batteries from the device





3.6 Read the event log

When the user disarms the system, the keypad indicates the last event.

In case of the user needs to read the full log file, use the keypad to go in EVENT LOG, press **OK** or **YES** on SELECT LAST EVENTS and use arrow to list the events.

OK or YES

SELECT LAST
EVENTS

OK or YES

15/10/13 11:29
MODIFIED PARAMET

SYSTEM DISARMED

V

Press **OK** or **YES** for more information about an event

3.7 Automatic arming/disarming

Scheduling: This feature arms or disarms the system automatically at a defined hour and weekday.

15/10/13

The scheduling feature description is available in the EN- PANEL - SCHEDULING - NOTE application note (available on videofied.helpserve.com).

Autoarming Delay: Defines an automatic rearming after every system disarming. Once the delay has expired, the panels arms automatically. Enter 0 to disable the feature.

3.8 Golden rules

- 1. Area 1 device are **delayed** by default (Area mode parameter set as Auto). When you register a keypad or a badge reader into an area set as Auto, that area will automatically be delayed.
- 2. **Never position** a panel next to a **high voltage** electrical cabinet. The interference will affect radio and 2G3G performance.
- 3. Press CLR to erase a typing mistake.
- Never register the same device twice (delete from the system first).
- 5. The panel can register of **up to 25 devices** of all types, including the keypad and the keyfobs.
- 6. Follow the Motionviewer installation instructions. Consider the infrared field of detection when installing the Motionviewer cameras, in order to protect goods or an entry point instead of a zone.

- 7. Do not fix the keypad at the beginning of the installation as it will need to be portable during programming.
- 8. Always clean the lens of the cameras after the installation. Use a clean, dry cloth, taking care not to exert pressure on the lens.
- Internal components are fragile, be careful opening or closing the panel.
- LCD screen goes dark after 30 seconds of inactivity, press an arrow or numeric key to light it up.
- 11. Infrared detectors should never be installed in stairs or close to stairs (false alarm risks).
- 12. A colon display [:] means that the parameter can be changed. Press **OK / YES** to display the colon



3.9 Additional features

	Description	Application note
Partitioning	Partitioning allow to arm two adjoining sites independently with a single alarm panel. Each of these sites can be individually armed thanks to badges, codes or keyfobs assigned to each site.	EN - PANEL - PARTITIONING - NOTE*
РСМ & Арр	Videofied [®] alarm panels can be controlled by a smartphone application. To use the App, specific parameters shall be configured. The PCM connection allow the panel to be constantly connected to a Smartphone App server.	EN - AFF - MON - NOTE*
Chime	The Chime feature allow Videofied [®] systems to generate a welcome tone when a door contact opens or closes.	EN - PANEL - CHIME - NOTE*
Swinger Shutdown	In case of frequent false alarms, the Swinger Shutdown feature can inhibit a Videofied [®] intrusion detector for a defined period.	

^{*}Application notes available on videofied.helpserve.com





4. ETHERNET PARAMETERS

To configure Ethernet parameters, using the direction arrows, go to the menu:

CONFIGURATION OK OF YES GENERAL PARAMETERS OK OF YES ETHERNET

To configure or modify Ethernet Parameters, go to:

IP Parameters:

If you wish to use the Ethernet transmission mode, two options are available:

- 1. **DHCP Enable**: IP address is assigned by the DHCP service on the network. (Dynamic IP address). This is the default option.
- 2. DHCP Disable: IP address must be defined in Ethernet parameters. IP address will NOT be automatically obtained from DHCP service on the network. Each connection from the panel to the network (alarms transmission), the XT-iP will have the same connection parameters. You must first connect to the router in order to get the network parameters and all available IP addresses. The following parameters must be filled in the IP PARAMETERS sub-menu: PANEL IP, IP MASK, GATEWAY, PRIMARY DNS, SECONDARY DNS.

• Constant Ethernet:

Three options are available:

1. "Auto" Mode - We recommend this mode. If main powered, the panel will be connected constantly to the local Network. In case of an alarm, the alarm will be sent in few seconds to the monitoring station. When the main power is cut, the Ethernet module will switch off after a delay (DELAY BEFORE OFF – 30 by default) in order to save battery life. In case of an alarm, the panel will at first connect to the local Network. It adds few seconds to the total process of sending an alarm.

You can set the delay in this menu:

CONFIGURATION (LVL 4) > GENERAL PARAMETERS > ETHERNET > CONSTANT ETH. > DELAY BEFORE OFF.

- 2. "ON" Mode The panel will be connected constantly to the local Network. This option will impact back-up battery life.
- 3. "OFF" Mode For each transmission of alarm and video, the panel will connect to the local Network.

• PING reply, Time Out Server, Max Seg. Size:

- PING REPLY: Enables ping response.
- Time Out Server: In case of disconnection to the local Network, the panel will try after that time to re-connect.
- Max Seg. Size: Maximum size of packet sent.





5. TRANSMITTED EVENTS LIST

The W panel can be configured to enable or disable the transmission of specific events like alarms or malfunctions.

The installer can modify the default sending settings for those events, although it will end the EN50131 standard compliance.

These are the default transmitted events:

DEVICE (intrusions)

ALERT (Panic Buttons)

PANEL LOW BATT.

TAMPER

DEVICE LOW BATT.

PERIODIC TEST

DURESS CODE

FIRE

MEDICAL ASSIST.

ETHERNET CABLE

AC POWER LOSS (AC Power supply)

The following events are not sent by default:

PANEL RESET

PHONELINE FAULT

RADIO JAMMING

SUPERVISION

5 WRONG CODES

ALARM CANCEL

ARM/DISARM (On/Off)

ZONE BYPASS (bypass function enabling/dsiabling)

SWINGER SHUTDOWN

There is 3 different transmission states:

ALARM: event transmitted upon occurrence

ALARM/END: event is transmitted on occurrence and on event restoral

NOT TRANSMITTED: event is not transmitted, however it will appear on the keypad.

Example:

If the monitoring station system is set to receive arms and disarms, the **ARM / DISARM** parameter must be changed from NOT TRANSMITTED to ALARM / END.

How to modify the transmission state

At initial programming, right after the PERIODIC TEST CALL step:

CODE/STATE MODIFICATION

Press OK or YES to access EVENT TRANS. MODIFICATION menu.

After initial programming, using a remote keypad:

Use the arrows





to access:

CONFIGURATION (level 4) > CONFIGURATION MONITOR. STATION > MONITORING PARAMETERS > EVENT TRANS. **MODIFICATION**

Then use the arrows





to determine the event to modify. Press **OK** or **YES** to edit.





6. 2G3G ERROR CODES

Security limitations on the SIM card must be disabled.

The PIN of the SIM card has to be disabled or 0000.

The following is a list of error codes that can appear after the 2G3G test.

2G3G LEVEL: **ERROR XXX**

In case of 2G3G errors during initial programming, we strongly suggest to continue with the installation and perform the 2G3G level test again once achieved.

This is not a comprehensive list, but it is representative of most cases. Some events or codes are subject to change by SIM card operators.

> However, the 2G3G level test errors results in the majority of cases have the following causes:

This error checklist is provided for information purposes only.

Codes **Errors** No network coverage or no SIM card 03 ou 04 inserted 003 SIM card not detected/not inserted

PIN code necessary 011 -> PIN code must be deactivated 012 PUK code necessary, SIM card blocked 013 Default SIM card

SIM not inserted

SIM card busy

Error on SIM

010

014

015

030, 043,

057, 102,

132, ...

No network coverage Typographical error in the APN Code,

username, password SIM card not activated

SIM Card activation Delay:

Some operators require an additional delay up to 48 hours to activate automatic data transmission. Please check with your operator prior to installation.

APN CODE, USERNAME and PASSWORD:

The 2G3G settings are supplied by the operator. Please make sure you have entered the code exactly as indicated by your local SIM card operator.

Note: When entering your SIM card settings, both APN codes, username and password fields are case sensitive! (It makes a difference between UPPER and lower case letters).

To switch between UPPER and lower case, use the M/m key from CMA keypad or hold a digit key (0-9) for XMA/XMB.

Insufficient GPRS Network:

When the panel is unable to find any signal, proceed to GPRS level test in another location on site. You can also find the network state or condition of use by directly contacting your local operator.





7. SECURITY AND CERTIFICATION NOTES

Certifications

920MHz (W730 & WIP720/730)



Australia A-Tick (AS/NZS4268, AS/CHS42 and AS/NZS 60950)



This symbol on the product or on its packaging indicates that this product should not be treated as household waste. It must be handed over to the applicable collection point for the recycling of electrical and electronic equipment. By ensuring this product is disposed of correctly, you will help prevent potential negative consequences for the environment and human health. The recycling of materials will help to conserve natural resources. For more information about recycling of this product, please contact your local municipality, your waste disposal service or the company that installed the product.





8. TECHNICAL SPECIFICATIONS

ELECTRICAL DATA

Power supply	
W730 & WIP 720/730	
	12VDC/1A - Wire connection

Backup battery	
Battery technology	Rechargeable 3.7V Lithium-ion battery
Battery voltage (Fully charged)	4.1 V
Low battery level	3.95 V
Guaranteed autonomy when the low battery level is reached 36h	
Average current consumption in standby mode	
	600 μΑ
Max consumption	1 A

RF S2View [®] technology	
Radio type	Bidirectional RF
Operating frequency 920MHz - FHSS - W730 & V	WIP720/730 (Australia, South America)
Transmission security	AES encryption algorithm
Radio jam detection	Yes
Supervision	Yes
Radio Antenna	integrated

Tamper Detection	
Tamper	Wall and cover tamper detection

BOX

Control Panel / Base

Physical and Environmental Data	
Operating temperature	-10°/+55°C
Maximum relative humidity	75%, non-condensing
International Protection Marking	IP31 / IK06
Material	ABS—ULVO

143 mm x 200 mm x 44 mm

Two screws secures control panel cover to base Three screws secure control panel base to the wall

TRANSMISSION

Communicator	
Communicator type	3G (W730)
	LAN Ethernet (WIP720) 3G & LAN Ethernet (WIP730)
C	Frontel
Security protocol	Frontei
IP stack	TCP/IP
Video transmission By Frontel protocol to central monitoring station or App servers	
2G3G Antenna	Integrated
2030 AIILEIIIIa	integrated

Optional modules	
Wi-Fi	WWB100 (WLAN 802.11 b/g/)
Wired Input/Outputs	WIO100 (out of NF&A2P compliance)
Wired Siren	WIS100
W.d.	
Video	
Video Format	WMV or MPEG
Images per second	5
Image size	320x240 or 640x480 pixels
Video length	4 to 12 seconds

Miscellaneous	
Programming	Keypad
Max number of devices	24
Max number of codes/badges	50
Arming modes	4
Areas	4
Event log	4000 events stored on flash memory

Video Alarm Technologies Pty Ltd. Enquiries: + 61 7 5491 7415 / 1300 46 44 55 Info@videoalarmtechnologies.com.au www.videoalarmtechnologies.com.au

