



ZeroWire Reference Guide

Copyright

© 2016 UTC Fire & Security Americas Corporation, Inc.
All rights reserved.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from UTC Fire & Security Americas Corporation, Inc., except where specifically permitted under US and international copyright law.

Trademarks and patents

The ZeroWire name and logo are trademarks of UTC Fire & Security Americas Corporation, Inc.

IOS is the registered trademark of Cisco Technology, Inc.

Android, Google and Google Play are registered trademarks of Google Inc.

iPhone, Apple, iTunes are registered trademarks of Apple Inc.

App Store is a service mark of Apple Inc.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

Placed on the market by:

UTC Fire & Security Americas Corporation, Inc.
3211 Progress Drive, Lincolnton, NC, 28092, USA

Authorized EU manufacturing representative:

UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

EU compliance



EU directives

UTC Fire & Security hereby declares that this device is in compliance with the applicable requirements and provisions of one or more of the Directives 1999/5/EC, 2014/30/EU and 2014/35/EU. For more information see: www.utcfireandsecurity.com or www.interlogix.com



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Customer support

Interlogix Australia www.interlogix.com.au +61392391200

Content

Important information#vii

Limitation of liability#vii

Product Warnings#vii

Warranty Disclaimers#viii

Disclaimer#ix

Intended Use#ix

Advisory messages#x

ZeroWire Building Blocks#11

ZeroWire Menu Tree#12

Glossary#13

Menu 1 - Users#16

User First Name#16

User Last Name#16

User PIN#16

Start Date#16

End Date#16

User Type#17

User Permission 1#18

Permission Schedule 1#18

User Permission 2#18

Permission Schedule 2#18

User Permission 3#18

Permission Schedule 3#19

User Permission 4#19

Permission Schedule 4#19

Menu 2 - System Options#21

System Clock#21

General Options#21

System Timers#22

Siren Options#24

Service and Test Options#25

Status#25

Menu 3 - Zones#27

Zone Number#27

Zone Name#27

First Zone Profile#27

Second Zone Profile#29

Example#30

Menu 4 - Areas#31

Area Number#31

Area Name#31

Area Entry And Exit Times#31

Area Options#32

Area Timers#34

Area Type Settings#34

Area Event Reporting#37

Notes on Force Arming, Bypass, and Auto-Bypass#38

Menu 5 - Channels#40

Channel Number#40

Account Number#40

Format#40

Destination Email#41

Next Channel#41

Event List#41

Attempts#41

Menu 6 - Communicator#42

General Options#42

Auto Test#42

IP Configuration#43

Radio Configuration#45

Remote Access#45

System Event Reporting#46

Menu 7 - Schedules#48

Schedule Number#48

Schedule Name#48

Follow Action Number#48

Times and Days#48

Menu 8 - Actions#50

Action Number#51

Action Name#51

Function#51

Duration Minutes#51

Duration Seconds#51

Event 1#52

Event 2#52

Event 3#53

Event 4#53

Result#53

Menu 9 - Arm-Disarm#59

Arm-Disarm Number#60

Arm-Disarm Name#60

User Number#60

Schedule Number#60

Menu 10 - Devices#61

System Devices - Control#61

Interlogix Transmitters#61

Zwave Devices#62

Tablet Keypads#62

Menu 11 - Permissions#63

Permission Number#63

Permission Name#63

Control Groups#63

Permission Options#64

Area User Timers Options#65

Menu 12 - Area Groups#66

Area Group Number#66

Area Group Name#66

Area Group#66

Menu 13 - Menus#67

Menu Number#67

Menu Name#67

Menu Selections#67

Menu 14 - Holidays#68

Holiday Number#68

Holiday Name#68

Date Range#68

Menu 15 - Zone Types#70

Zone Type Number#70

Zone Type Name#70

Area Armed#70

Area Disarmed#70

Menu 16 - Zone Options#74

Zone Option Number#74

Zone Options Name#74

Zone Options#74

Zone Reporting#76

Zone Contact Options#77

Zone Report Event#77

Menu 17 - Event Lists#78

Event List Number#78

Event List Name#78

Event List#78

Menu 18 - Channel Groups#79

Channel Group Number#80

Channel Group Name#80

Channel Group#80

Menu 19 - Scenes#81

Scene Number#81

Scene Name#81

Activate Schedule#81

Activate Event Type#81

Activate Zone#81

Scene Actions#81

Menu 20 - Speech Tokens#84

Zones Tokens#84

Menu 21 - Cameras#84

Camera Number#84

Menu 22 - UltraSync#84

Appendix 1: Reporting Zone Codes in Contact I.D.#86

Appendix 2: Reporting Fixed Codes in Contact I.D.#87

Appendix 3: History Events#88

Appendix 4: Zone Options#89

Appendix 5: Zone Types#90

Appendix 6: Voice Library#91

Appendix 7: App and Web Error Messages#93

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will UTCFS be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of UTCFS shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether UTCFS has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, UTCFS assumes no responsibility for errors or omissions.

Product Warnings

YOU UNDERSTAND THAT A PROPERLY INSTALLED AND MAINTAINED ALARM/SECURITY SYSTEM MAY ONLY REDUCE THE RISK OF EVENTS SUCH AS BURGLARY, ROBBERY, FIRE, OR SIMILAR EVENTS WITHOUT WARNING, BUT IT IS NOT INSURANCE OR A GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR OR THAT THERE WILL BE NO DEATH, PERSONAL INJURY, AND/OR PROPERTY DAMAGE AS A RESULT.

THE ABILITY OF INTERLOGIX'S PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH INTERLOGIX HAS NO CONTROL AND FOR WHICH INTERLOGIX SHALL NOT BE RESPONSIBLE INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND OPERATING SYSTEM COMPATIBILITY; MONITORING SERVICES; ELECTROMAGNETIC OR OTHER INTERFERENCE, AND PROPER INSTALLATION AND MAINTENANCE OF AUTHORIZED PRODUCTS (INCLUDING ALARM OR OTHER CONTROL PANEL AND SENSORS).

ANY PRODUCT, SOFTWARE, SERVICE OR OTHER OFFERING MANUFACTURED, SOLD OR LICENSED BY INTERLOGIX, MAY BE HACKED, COMPROMISED AND/OR CIRCUMVENTED AND INTERLOGIX MAKES NO REPRESENTATION, WARRANTY, COVENANT OR PROMISE THAT ITS PRODUCTS (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICES

OR OTHER OFFERINGS WILL NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

INTERLOGIX DOES NOT ENCRYPT COMMUNICATIONS BETWEEN ITS ALARM OR OTHER CONTROL PANELS AND THEIR WIRELESS OUTPUTS/INPUTS INCLUDING BUT NOT LIMITED TO, SENSORS OR DETECTORS UNLESS REQUIRED BY APPLICABLE LAW. AS A RESULT THESE COMMUNICATIONS MAY BE INTERCEPTED AND COULD BE USED TO CIRCUMVENT YOUR ALARM/SECURITY SYSTEM.

THE EQUIPMENT SHOULD ONLY BE OPERATED WITH AN APPROVED POWER ADAPTER WITH INSULATED LIVE PINS.

DO NOT CONNECT TO A RECEPTACLE CONTROLLED BY A SWITCH.

THIS UNIT INCLUDES AN ALARM VERIFICATION FEATURE THAT WILL RESULT IN A DELAY OF THE SYSTEM ALARM SIGNAL FROM THE INDICATED CIRCUITS. THE TOTAL DELAY (CONTROL UNIT PLUS SMOKE DETECTORS) SHALL NOT EXCEED 60 SECONDS. NO OTHER SMOKE DETECTOR SHALL BE CONNECTED TO THESE CIRCUITS UNLESS APPROVED BY THE LOCAL AUTHORITY HAVING JURISDICTION.

WARNING: The equipment should only be operated with an approved power adapter with insulated live pins.

Caution: Risk of explosion if battery is replaced by an incorrect type. Dispose of batteries according to the instructions. Contact your supplier for replacement batteries.

Warranty Disclaimers

INTERLOGIX HEREBY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

(USA only) SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.

INTERLOGIX DOES NOT MAKE ANY CLAIMS OR WARRANTIES TO YOU OF ANY KIND REGARDING ANY PRODUCT, SOFTWARE OR SERVICE'S POTENTIAL, ABILITY, OR EFFECTIVENESS TO DETECT, MINIMIZE, OR IN ANYWAY PREVENT DEATH, PERSONAL INJURY, PROPERTY DAMAGE, OR LOSS OF ANY KIND WHATSOEVER.

INTERLOGIX DOES NOT REPRESENT TO YOU THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICE OR OTHER OFFERING MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

INTERLOGIX DOES NOT WARRANT THAT ANY PRODUCT (INCLUDING SECURITY PRODUCTS), SOFTWARE OR SERVICE MANUFACTURED, SOLD OR LICENSED BY INTERLOGIX WILL PREVENT, OR IN ALL CASES PROVIDE ADEQUATE WARNING OF OR PROTECTION FROM, BREAK-INS, BURGLARY, ROBBERY, FIRE, OR OTHERWISE.

INTERLOGIX DOES NOT WARRANT TO YOU THAT ITS SOFTWARE OR PRODUCTS WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS AND DOES NOT WARRANT ANY PRODUCTS AGAINST HARMFUL ELECTROMAGNETIC INTERFERENCE INDUCTION OR RADIATION (EMI, RFI, ETC.) EMITTED FROM EXTERNAL SOURCES

INTERLOGIX DOES NOT PROVIDE MONITORING SERVICES FOR YOUR ALARM/SECURITY SYSTEM (“MONITORING SERVICES”). IF YOU ELECT TO HAVE MONITORING SERVICES YOU MUST OBTAIN SUCH SERVICE FROM A THIRD PARTY AND INTERLOGIX MAKES NO REPRESENTATION OR WARRANTY WITH RESPECT TO SUCH SERVICES INCLUDING WHETHER OR NOT THEY WILL BE COMPATIBLE WITH THE PRODUCTS, SOFTWARE OR SERVICES MANUFACTURED, SOLD OR LICENSED BY INTERLOGIX.

Disclaimer

THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. UTC ASSUMES NO RESPONSIBILITY FOR INACCURACIES OR OMISSIONS AND SPECIFICALLY DISCLAIMS ANY LIABILITIES, LOSSES, OR RISKS, PERSONAL OR OTHERWISE, INCURRED AS A CONSEQUENCE, DIRECTLY OR INDIRECTLY, OF THE USE OR APPLICATION OF ANY OF THE CONTENTS OF THIS DOCUMENT. FOR THE LATEST DOCUMENTATION, CONTACT YOUR LOCAL SUPPLIER OR VISIT US ONLINE AT WWW.UTCFIREANDSECURITY.COM.

This publication may contain examples of screen captures and reports used in daily operations. Examples may include fictitious names of individuals and companies. Any similarity to names and addresses of actual businesses or persons is entirely coincidental.

The illustrations in this manual are intended as a guide and may differ from your actual unit as ZeroWire is continually being improved.

Intended Use

Use this product only for the purpose it was designed for; refer to the data sheet and user documentation. For the latest product information, contact your local supplier or visit us online at www.utcfireandsecurity.com.

The system should be checked by a qualified technician at least every 3 years and the backup battery replaced as required.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

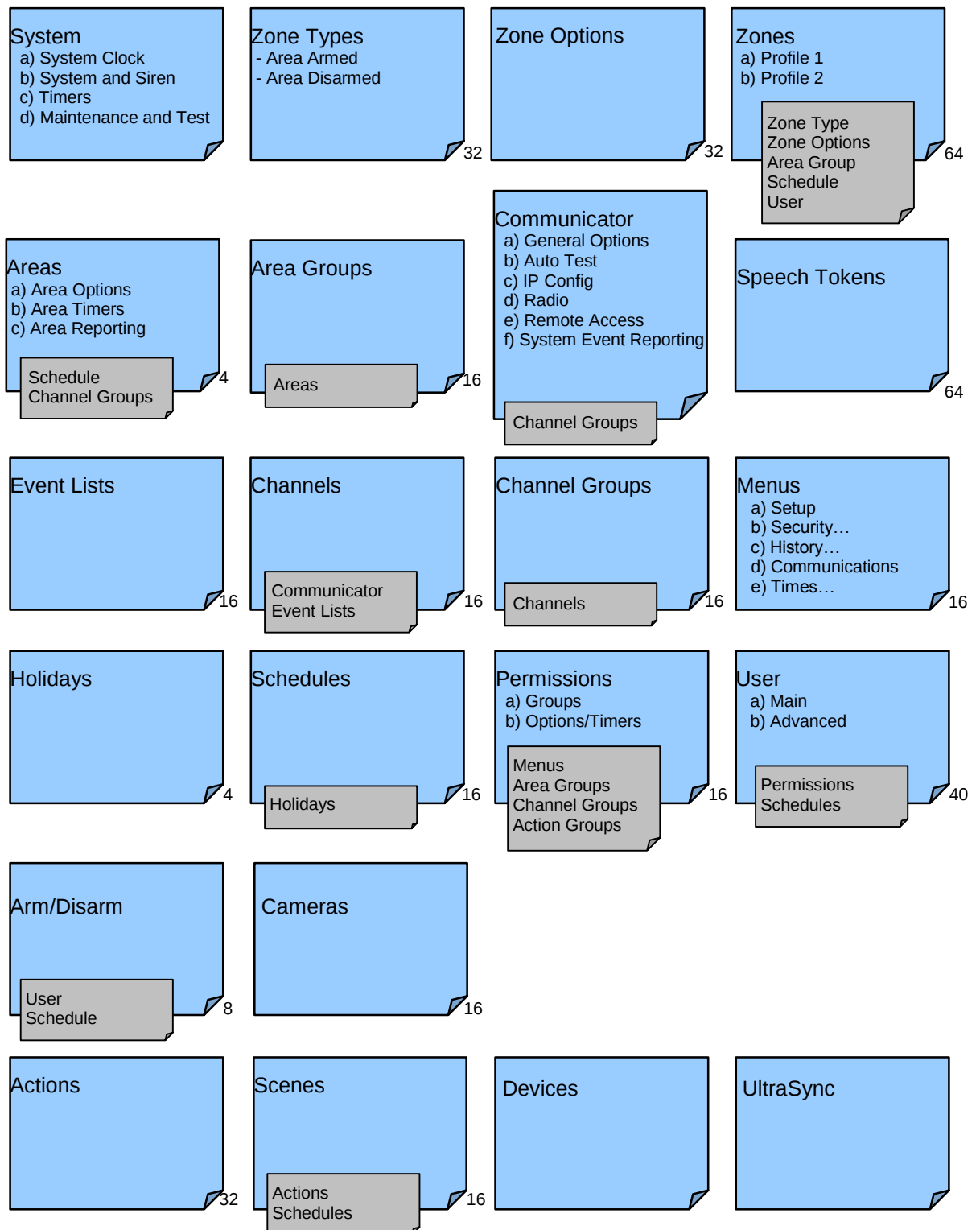
WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

ZeroWire Building Blocks

Below is the system diagram showing all the key features used to program a system. The smaller blocks indicate features used by the larger block and should be programmed first. The number on the bottom right of each block indicates system capacity (subject to the model).



ZeroWire Menu Tree

The menu structure as seen from the Advanced menu in ZeroWire Web Server:

- 1. Users**
- 2. System**
 1. System Clock
 2. General Options
 3. System Timers
 4. Siren Options
 5. Service and Test Options
 6. Status
- 3. Zones**
 1. Zone Number
 2. Zone Name
 3. First Zone Profile
 4. Second Zone Profile
- 4. Areas**
 1. Area Number
 2. Area Name
 3. Area Entry-Exit Times
 4. Area Options
 5. Area Timers
 6. Area Type Settings
 7. Area Event Reporting
- 5. Channels**
 1. Channel Number
 2. Channel Name
 3. Account Number
 4. Format
 5. Device Number
 6. Dest Phone or Email
 7. Next Channel
 8. Event List
 9. Attempts
- 6. Communicator**
 1. General Options
 2. Auto Test
 3. IP Configuration
 1. IP Host Name
 2. IP Address
 3. Gateway
 4. Subnet
 5. Primary DNS
 6. Secondary DNS
 7. Ports
 8. Time Server
 9. IP Options
 4. Radio Configuration
 5. Remote Access
 1. Panel Device Number
 2. Download Access Code
 3. Call Back Server
 4. Download Options
 6. System Event Reporting
 1. System Channel
 2. Attempts
- 7. Schedules**
 1. Schedule Number
 2. Schedule Name
 3. Follow Action Number
 4. Times and Days
- 8. Actions**
 1. Action Number
 2. Action Name
 3. Function
 4. Duration Minutes
 5. Duration Seconds
 6. Event 1
 7. Event 2
 8. Event 3
 9. Event 4
 10. Result
- 9. Arm-Disarm**
 1. Arm-Disarm Number
 2. Name
 3. User Number
 4. Schedule Number
- 10. Devices**
 1. System Devices
 1. Control
 2. Interlogix Transmitters
 1. Transmitter Number
 2. Serial Number
 3. User
 4. Options
 5. Scene
 3. Z-Wave Devices
 1. Name
 2. Basic Type
 3. Generic Type
 4. Specific Type
- 11. Permissions**
 1. Permission Number
 2. Permission Name
 3. Control Groups
 4. Permission Options
 5. User Timer Options
- 12. Area Groups**
 1. Area Group Number
 2. Area Group Name
 3. Area List
- 13. Menus**
 1. Menu Number
 2. Menu Name
 3. Menu Selections
- 14. Holidays**
 1. Holiday Number
 2. Holiday Name
 3. Date Range
- 15. Zone Types**
 1. Zone Type Number
 2. Zone Type Name
 3. Zone Type Armed
 4. Zone Type Disarmed
- 16. Zone Options**
 1. Zone Options Number
 2. Zone Options Name
 3. Zone Options
 4. Zone Reporting
 5. Zone Contact Options
 6. Zone Report Event
- 17. Event Lists**
 1. Event List Number
 2. Event List Name
 3. Event List
- 18. Channel Groups**
 1. Channel Group Number
 2. Channel Group Name
 3. Channel List
- 19. Scenes**
 1. Scene Number
 2. Scene Name
 3. Activate Schedule
 4. Activate Event Type
 5. Activate Zone
 6. Scene Actions
- 20. Speech Tokens**
 1. Zone Tokens
- 21. Cameras**
 1. Camera Number
 2. Camera Name
 3. LAN IP Address
 4. MAC Address
- 22. UltraSync**
 1. Web Access Passcode
 2. Ethernet Server 1
 3. Ethernet Server 2
 4. Ethernet Server 3
 5. Ethernet Server 4
 6. Wireless Server 1
 7. Wireless Server 2
 8. Wireless Server 3
 9. Wireless Server 4

Glossary

Action	An action allows the ZeroWire to perform automation functions. These can monitor the status up to 4 input conditions called Action Events, change state (Action State), and perform a function (Action Result) such as arming a range of areas.
Action Group	An action group is one or more actions that can be accessed by a device or user. They are assigned to a user or device via permissions.
Area	Zones are grouped into areas which can be secured independently from each other. This allows you to split your security system in to smaller components that can be separately managed. For example your system can be divided into an upstairs area and downstairs area.
Area Group	An area group is one or more areas that can be accessed by a device or user. They are assigned to a user or device via permissions.
Arm	To turn your security system On.
Arm-Disarm	Automatically arm and disarm areas by a specific user according to a specified schedule. The areas armed and disarmed will be the ones that the user has access to via their permissions.
Away Mode	To turn your security system on when you are leaving the premises.
Bypass	Zones can be temporarily disabled so they will not be monitored by the security system. For example, an interior door is left open, bypass it to temporarily ignore it and allow arming of the security system. Bypassed zones are not capable of activating an alarm. Zones will return to normal operation when the system is armed then disarmed. This prevents unintentional permanent disabling of a zone.
Central Station	A company to which alarm signals are sent during an alarm report. Also known as Central Monitoring Station (CMS).
Channel	A channel is a communication path for events to be sent from the ZeroWire panel to a selected destination. Channels can be set to UltraSync or Email. A channel has an associated event list which contains the events it is allowed to forward on.
Channel Group	A channel group is one or more destinations for event messages to be sent to. When a message is sent to a channel group, it is sent to all the channels that it contains. It forms the basis of multi-path reporting in ZeroWire.
Chime Group	All the zones that will activate chime, when in chime mode.
Chime Mode	An operational mode that will emit a ding-dong sound at the keypad when specific zones are activated.
Communicator	The communicator is responsible for notifying a control room or third party that an alarm event has occurred so an appropriate response can be made. It sends event messages to the specified destination including details such as where the event originated from and the type of event. The receiver will then log the time and date when it receives the event. For example, Alarm from Zone 2 in Area 1 at 3:00am on 5/5/2014 from Account 1234. ZeroWire has multiple communicator options including Ethernet IP interface, email, and 3G (with optional cellular radio module).
Disarm	To turn your security system Off.
Duress Code	A predetermined user PIN code that will arm / disarm the security system whilst sending a special code to the central monitoring station indicating the user is entering / leaving the premises under duress. Only applicable on monitored systems.
Entry Delay	The time allowed to disarm your security system after the first detection device has been activated.

Event	Events are messages that are sent by the ZeroWire due to system or area conditions. These include areas in alarm, opening and closing, zone bypass, low battery, tamper, communication trouble, and power issues.
Event List	Event lists contain events that a channel is allowed to send to the specified destination. If a channel receives an event that is not in the associated event list, then the channel will ignore the event.
Exit Delay	The time allowed to exit the premises after the security system is armed.
Forced Arming	An option that permits arming even when there are unsealed pre-selected zones. Generally assigned to zones that cover the ZeroWire (e.g.; motion zones, front door reed switches), allowing the user to arm the security system without the need to wait for those zones to be sealed. A security system that is ready to be “force armed” will flash the ready light.
Master Code	A PIN code that is used by a user to arm or disarm the security system. Its main feature is the ability to create, alter and delete user PIN codes. Can also be used as a function code for all features.
Menus	ZeroWire has a large range of features sorted into various menus such as Users, System, and Zones. Each menu item can be seen when using the ZeroWire Web Server or the UltraSync + app. Menus are used to restrict what is displayed by a device and what features a user has access to.
Monitored	A security system that is configured to send all alarm signals to a central monitoring station.
Output	Outputs on the ZeroWire panel can be connected to a siren and strobe when an alarm condition occurs on the system.
Perimeter	Typically this refers to zones located around the boundary of the protected area such as zones on doors and windows, and excludes interior motion zones.
Permission	A permission includes a list of features a user or device is allowed to access. This includes programming menus, areas, reporting channels, actions, reporting options, access control options, special options, and special timers.
Profile	Each user can have up to four (4) permission profiles. Each profile contains a set of permissions and a corresponding schedule. This allows advanced user programming and provides specific access to different features of the security system during specific dates/time. With advanced programming, profiles can be enabled/disabled in response to system conditions.
Quick Arm	An option that allows you to turn on (arm) the security system by touching the [AWAY] key.
Scene	Each scene can trigger up to 16 actions to create an automation event. This can save users time by automatically running multiple actions. A scene can be triggered manually, through a schedule, or via a system event.
Schedule	A schedule is a list of up to 16 sets of days and times. Typically these are used to provide access to users only within the specified sets of days and times. Outside of the schedule a user will not have access to the system. Schedules are used to automatically arm and disarm specified areas using the Arm-Disarm feature. Scenes can perform a set of actions according to a specified schedule. Schedules themselves can be enabled and disabled through actions. This powerful feature allows you to provide conditional access to various users and devices based on system conditions.

Sealed	A zone in a normal state is “sealed”. The security system monitors each zone for changes in state from sealed to unsealed and can respond with certain actions such as sounding the siren. For example, a reed switch on a front door may change from a sealed state to an unsealed state when the door opens.
Service Provider	The installation / maintenance company servicing your security system.
Stay Mode	To turn your security system on when you are staying in the premises, this will automatically bypass pre-programmed zones and arm others. Often used to arm only the perimeter while allowing movement inside the premises.
Tamper	A physical switch on a device that detects unauthorised access to the unit. For example opening the case of a zone or taking a keypad off the wall can trigger a tamper alarm. This can provide early warning of someone attempting to undermine the security of your system. Some devices use an optical zone to detect removal from a surface.
Token	Each token is a pre-recorded word or phrase that can be used to name zones, areas, outputs, and rooms. Each token is identified by a token number and a full list of tokens is in the "Error! Reference source not found." Error! Bookmark not defined.
UltraSync	Mobile app for smartphones to access the ZeroWire Web Server which provides access to view the status of a ZeroWire system, control zones and outputs, program users and other ZeroWire features. Available to download for Apple™ iPhone™ and Google™ Android™ from the respective app store. The UltraSync + app connects to the UltraSync server which will then connect to your ZeroWire system.
Unsealed	A zone in an abnormal state is “unsealed”. The security system monitors each zone for changes in state from sealed to unsealed and can respond with certain actions such as sounding the siren. For example, when a PIR zone detects movement it will change from a sealed state to an unsealed state.
User	An authorised person who can interact with the ZeroWire security system and perform various tasks according to the permissions assigned to them. Each ZeroWire user has a set of profile levels. These control what the user has access to, a list of functions, and when the user is allowed to perform these functions. A user is typically a person who is assigned a PIN code and arms/disarms the system with this code or keyfob device. Users can also be automatic functions of the system. For example, ZeroWire can automatically arm specific areas a user has access to at a specified time. No human interaction is required, all the permissions of the programmed user will still be applied and enforced.
User Code	A PIN code that is used by a user to arm or disarm the security system. Also can be used as a function code for certain features.
ZeroWire Panel	The main controller for the security system. It stores all programming, provides network and other connectivity options for reporting, provides physical terminals for connecting power, backup battery, zones, and outputs.
ZeroWire Web Server	ZeroWire has a built-in web server which provides access to ZeroWire features via a web browser interface or a native smartphone app. This allows you to performing programming and control of the system without needing to be physically in front of the ZeroWire keypad.
Zone	A detection device such as a Passive InfraRed motion zone (PIR), reed switch, smoke detector, panic button, etc. Zones may be physically wired to the ZeroWire system. Also known as an input or sensor on other security panels.

Menu 1 - Users

A user is a ZeroWire operator that is granted the authority to control and or configure the ZeroWire system. The Users menu is where you add, delete or modify one of the 40 ZeroWire users.

Users will typically interact with the ZeroWire system via a keypad, reader or wireless keyfob(s) for tasks such as arming and disarming an area, bypassing a zone or setting system outputs. ZeroWire system configuration authority can be granted to a user to perform tasks such as adding zones, modifying schedules or deleting users.

Users can only edit users with the same or less authority than them. If a user attempts to access a user with a higher level of access (e.g. to more menus or more areas) then the ZeroWire will deny access.

The following submenus describe the features associated with Menu 1 – Users.

User First Name

Each user can be configured with a custom 16 character first name. The user name descriptor may be displayed in the event log, keypad and when remotely connected to the ZeroWire via the management software.

User Last Name

Each user can be configured with a custom 16 character last name. The user name descriptor may be displayed in the event log, keypad and when remotely connected to the ZeroWire via the management software.

User PIN

ZeroWire users can be configured with 4 to 8 digit PIN. The user PIN is required by the ZeroWire system to determine the user number and the users associated permissions system control and configuration. Any number of users can have any digit length from 4 to 8 digits.

Start Date

The first date when this ZeroWire user can interact with the system. Future start dates can also be set here. The user will only be able to interact with the system between the start date and end date.

End Date

The last date when this ZeroWire user can interact with the system. Future end dates can also be set here. The user will only be able to interact with the system between the start date and end date.

User Type

User Type provides quick configuration of user permissions. The available user types are:

- **Standard:** Standard users can only change their own PIN codes and cannot change the settings of the system. They can arm and disarm areas they have access to.
- **Master:** Master users can change Standard user PIN codes and Master user PIN codes, and can access all menus except installation programming.
- **Engineer:** Engineer can only access installation programming menus, but no user programming menus. This user can always arm a system but only disarm areas they armed.
- **Master Engineer:** Master users can create or manage Engineer type users, and can access all menus.
- **Arm Only:** Users can only arm selected areas.
- **Duress:** Duress code will send a duress report to the specified Channel Groups under System Event Reporting. The duress code does not trigger an audible alarm.
- **Custom:** ZeroWire will apply user permissions and user permission schedules. This requires advanced programming. First create a permission using an engineer account (default “installer”), then assign it to a user with a master account (default “User 1”). A Custom user is able to modify the configuration of themselves or another user if:
 - Permission Option ‘Remote Access’ is enabled (for web page access)
 - Permission Menu ‘Users’ is enabled to allow them to assign user permissions. Otherwise they will only be able to change their own PIN code.
 - They have area access to at least one area of the user being modified. This does not check permission options.

Table 1: User Types

	Arm Only	Standard	Master	Engineer	Master Engineer	Custom User
Change their own PIN code	X	X	X	X	X	Custom
Arm areas based on permissions	X	X	X	X	X	Custom
Disarm areas based on permissions		X	X	Limited	X	Custom
Can create and modify Standard users			X		X	Custom
Program ZeroWire installation settings				X	X	Custom
Can create and modify Engineer users					X	
Can create custom permissions and schedules						X

User Permission 1

There are a total 16 unique permissions that can be configured in Menu 11 – Permissions.

User permissions determine what level of access and functionality a user has when interacting with the ZeroWire system. This includes what menus they can see, what areas they can see, areas they can arm / disarm / reset, perform special area functions of timed disarm / man down / guard tour, what actions they can use, and what channel to report on.

User type must be set to Custom to apply the permissions programmed. Otherwise the user type will be applied.

Permission Schedule 1

At default the user permission will always be active for the custom user. Assigning a permission schedule will limit **when** that user has that level of access and functionality.

ZeroWire allows each user to be allocated with up to 4 user permissions and permission schedules. This provides a high level of flexibility and user permissions can change based on time and date, or even certain system conditions when combined with actions.

User permissions are numbered from 1 to 4 where permission 1 is the highest priority and permission 4 is the lowest priority. If user permission 1 schedule is not valid then user permission 2, 3 and 4 are checked in sequence until a valid schedule can be applied.

Higher priority permissions replace lower priority level permissions when they become active. Only one permission can be active at any time. Permissions have a logic OR function.

IMPORTANT: If permission 1 is active due to a valid schedule, permission 2 will never become active. Make sure to assign/program permissions in the right order.

User Permission 2

See User Permission 1

Permission Schedule 2

See Permission Schedules 1

User Permission 3

See User Permission 1

Permission Schedule 3

See Permission Schedules 1

User Permission 4

See User Permission 1

Permission Schedule 4

See Permission Schedules 1

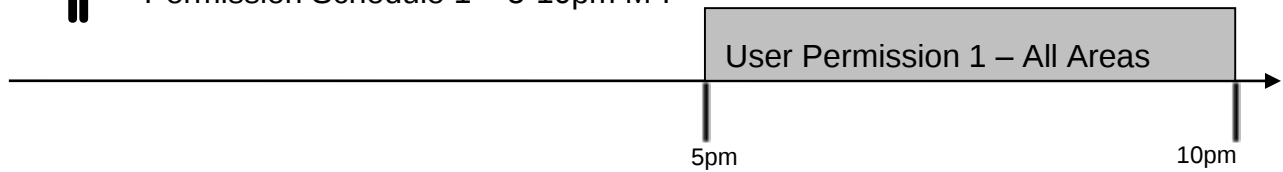
Example — Custom Permissions



Cleaner

User Permission 1 – All Areas

Permission Schedule 1 – 5-10pm M-F



A cleaner is given access to all areas after hours. They can disarm/arm the security system from 5pm to 10pm on weekdays. They have no access outside of these times and days.

A bank manager has access to the common areas of the bank 24 hours a day.

During office hours they have access to the bank vault as well. The permissions to access bank vault become active at 9am, overriding the common areas permission. When the time becomes 5pm the bank vault permissions become inactive and their lower level permissions to access the common areas becomes active again.



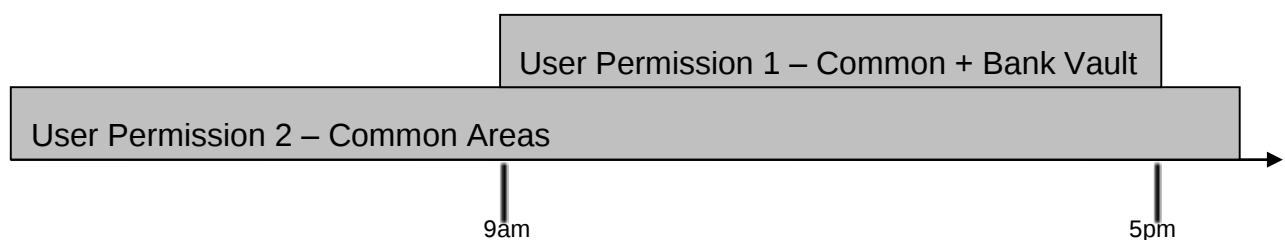
Bank Manager

User Permission 1 – Bank Vault + Common

Permission Schedule 1 – 9-5 M-F

User Permission 2 – Common Areas

Permission Schedule 1 – 24/7



IMPORTANT: Only one permission can be active at any one time. User Permission 1 overrides User Permission 2, so ensure User Permission 1 includes all the areas (and other features) you want to give access to. If User Permission 1 only included the Bank Vault, the user would NOT have access to the Common Areas.

Menu 2 - System Options

System options are used to configure system wide options, such as time and dates, system timers and maintenance.

The following submenus describe the features associated with Menu 2 – System Options.

System Clock

Date and Time

Time Zone: Hours Offset & Minutes Offset

Start Of DLST: Month 1 to 12 of year; Week of month 1 to 4 and last

End Of DLST: Month 1 to 12 of year; Week of month 1 to 4 and last

The ZeroWire system clock can manage day, time, time zone, and day light saving time settings to ensure ongoing accurate time.

When connected to an IP network the ZeroWire system clock can synchronise its time and date automatically with an Internet Time Server if configured in Menu 6 – Communicator.

General Options

Panel Zone Doubling

If enabled, the two (2) hardwired zone inputs will be doubled to support four (4) zones. The terminals for Zone 1 will represent zones 1 and 3, and the terminals for zone 2 will represent zone 2 and 4. This option cannot be selected for zones other than the two zones on the main panel. This option cannot be used in conjunction with the DEOL option.

Panel Box Tamper

The ZeroWire has a built-in normally closed tamper switch that will sound the siren if the ZeroWire is removed from the wall. This option will enable or disable this tamper switch.

System Zone Tamper

If enabled, the ZeroWire will monitor all zones except fire zones for Dual End of Line. A short or open circuit on a DEOL will activate zone tamper alarms. This feature cannot be used if Panel Zone Doubling is enabled.

Enable Celsius Scale

Disable Hardwired Zones

If enabled, the ZeroWire will disable all hardwired zone inputs. Wireless zones with zone numbers 1 to 16 may still be used.

Strobe on Away

If enabled, the system strobe will flash when an area is set in away mode. The strobe outputs must be configured to follow the area alarm event condition. The strobe is not activated on Disarm or Stay.

System Alarm Latch

If enabled, system alarms such as tampers, low battery, A/C fail and trouble requires a user with “Reset System Alarms” enabled in their current Permission Options to reset the alarm condition.

If disabled, system alarms do not latch and can be reset when a user arms or disarms an area.

Zone Inactivity

If enabled, the system ZeroWire will monitor each zone for activations. If no activations occur within the zone activity time then a failed zone activity report may be reported via the selected communication channel and a failed zone activity message set in the ZeroWire event log. For a zone to be eligible for activity monitoring, it must have “Zone Activity” set in zone options. The zone inactivity time is set in “Menu 2 – System Options - 3. System Timers”

System Timers

Siren Time

The siren time sets the time in minutes that the siren output is active.

Strobe Time

The strobe time is the duration in hours that output programmed to follow the strobe time will activate. The valid time selection in this segment is 0 to 99 hours, where ‘0’ disables the Strobe Output.

Battery Test Time

The battery test time sets the duration in minutes that the ZeroWire will perform a battery test. The ZeroWire will perform a battery test at the disarming of the first area or at midnight once each 24-hour cycle. Battery Test Time is disabled when the test duration is set to 0. Battery Test Time can also be run manually from a keypad.

AC Failure Report Delay

The AC failure report delay sets the duration in seconds that the AC power is lost or restored before a communication is initiated.

AC restore will report when power is maintained for this same duration.

Twin Trip Time

The Twin Trip time sets the duration in seconds whereby two or more zones must trip before an alarm condition will be registered or the one zone must trigger

twice within this time period, or a continuous trip longer than 10 seconds. This feature only applies to zones with the Twin Trip feature set in zone options.

Report Delay

The report delay is the duration in seconds that non-24 hour and non-fire type zones will delay before reporting. This provides a valid user the opportunity to reset an unintended alarm condition before that event is reported.

Holdup Delay

The holdup delay is the duration in second that a holdup delay zone type will wait before it activates. If additional holdup activations occur during the holdup delay period then the holdup delay will immediately expire and set the holdup alarm. If a holdup delay zone type is de-activated during the holdup delay period then the holdup alarm will reset and not activate.

Fire Verify Delay

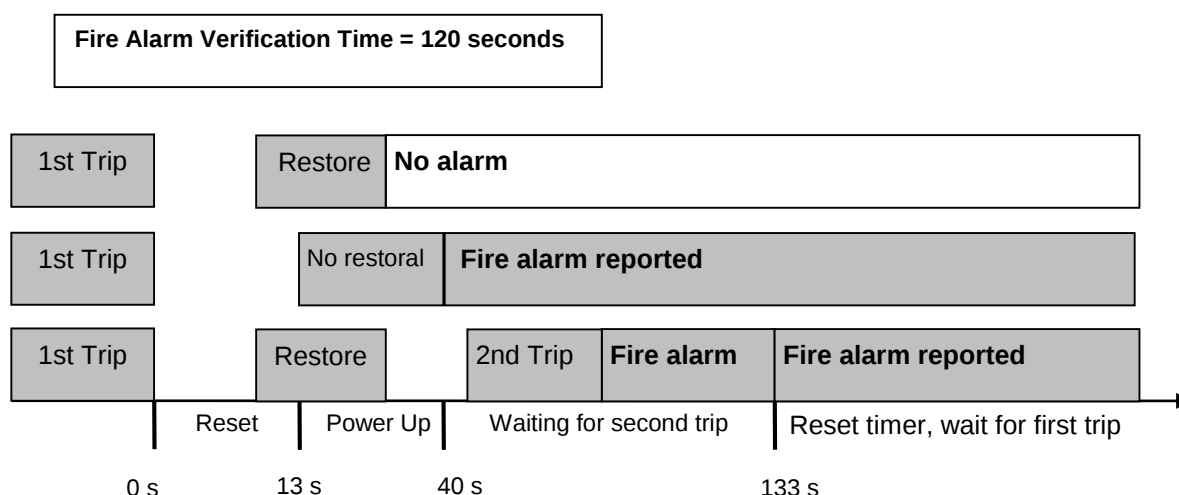
The fire alarm verification feature is designed to reduce false alarms reported by smoke detectors.

When a smoke detector is first tripped, the ZeroWire will raise an Action Event 'Smoke Power Reset'. For hard wired 4-wire smoke detectors, you may program the output to follow the action event and power-cycle the detector(s). Hard wired detectors will be given 13 seconds to power-cycle.

The ZeroWire will wait 40 seconds to allow the smoke detector to power up and settle. If a second trip occurs after this but before the end of the Fire Verify Delay time, a fire alarm will be generated. If no restoral is received after the first trip, a fire alarm will also be generated.

The valid time selection in this segment is 120 to 255 seconds. The communicator will delay for a specified time before reporting the fire alarm.

Here are some scenarios:



Zone Inactivity Time

Zones programmed with Zone Inactivity enabled in the Zone Options must be sealed and unsealed within the time programmed here (in minutes). If they do not, a Zone Inactivity will report.

This system feature can be enabled in “Menu 2 – System Options”. Then, enabled per zone under Zone Options.

Zone Inactivity option is disabled for all default Zone Options, and this timer is set to 0 minutes.

Fire Supervise Time

This applies only to wireless zones programmed as fire type. Detectors send a reduced packet count supervisory signal every 60 minutes (check your detector manual for most up to date details). If no supervisory signal is received by the panel within the time specified here then the detector will be reported as missing.

When set to 0 the default of 14,400 seconds (4 hours) will be used. Check your local regulations for the correct value to use.

Burglary Supervision Time

This applies only to wireless zones programmed as non-fire type. Detectors send a reduced packet count supervisory signal every 15 minutes (check your detector manual for most up to date details). If no supervisory signal is received by the panel within the time specified here then the detector will be reported as missing.

When set to 0 the default of 43,200 seconds (12 hours) will be used. Check your local regulations for the correct value to use.

Short Supervision Time

This applies only to wireless zones programmed as non-fire type. Detectors send a reduced packet count supervisory signal every 15 minutes (check your detector manual for most up to date details). If no supervisory signal is received by the panel within the time specified here, then a local zone supervision fault will be displayed, this is NOT reported to a control room until the Burglary Supervision Time above elapses. The default is 20 minutes.

Siren Options

Siren Once Per Zone

If enabled, the ZeroWire will only set the siren once per zone in a given arm cycle and will not set the siren again even if that siren time expires and that zone reactivates. Every zone will have one siren activation attempt before that zone cannot reactivate the siren. If this option is not enabled, at the expiry of the siren time any zone can reactivate the siren an unlimited number of times.

Siren At System Away or Disarm

If enabled, the ZeroWire will activate the built-in siren briefly, every time the last area in the system is set in away mode or when the first area is disarmed. To individually enable this function by area, leave this function disabled in this section, and enable the “Siren at Away/Disarm” in Menu 4 – Areas.

Siren At End Of Exit

If enabled, the ZeroWire will activate the built-in siren briefly every time the system is set in away mode and the exit delay expires.

Siren At Arm Report

If enabled, the ZeroWire will activate the siren output every time the system is set in away mode with a key-switch or wireless keyfob, the exit delay expires and a successful system arm report is completed. The sirens will chirp three times.

Service and Test Options

Status Email Intervals

If enabled, the ZeroWire will report a system status email via one or more email channels. The number entered for Status Email Interval is the number of days between status reports. For example entering a 7 will cause a report to be sent every 7 days.

The interval starts from either the first time you program an interval in here or when it is powered up.

This is sent via the System Event Reporting – Reporting Channels.

Status Email Time

The status email time sets the time of day that the status email will report. This is set as 24-hour time in hours and minutes.

Service Phone Number

When a system fault is present, the Status key will be red. Pushing the Status key will announce this number to the end-user. Typically this is the contact number of the installation company.

Status

This menu provides diagnostic information on the connection status of the ZeroWire.

LAN Status

Status of the connection to the Local Area Network.

LAN Media

When connected to the Local Area Network whether this is via Ethernet or WiFi.

Cell State

Status of the connection to the cellular radio network.

UltraSync Status

Status of the connection to the cloud servers.

UltraSync Media

When connected to the cloud servers whether this is via LAN (Ethernet/WiFi) or cellular radio.

Cell Service

When connected to the cellular radio network this will display what level of service is provided.

If the optional radio module is installed with a valid SIM card, and this shows restricted service, please contact your service provider as your SIM card may not be provisioned correctly.

Signal strength

If the optional radio module is installed with a valid SIM card, this will show the numeric signal level.



- If the reported value is -121 to -86 then the signal level is too low. Install an external antenna to improve the signal level.
- If the reported value is -87 to -51 then the signal level is OK.

Operator ID

If the optional radio module is connected to the network this will display the ID of the network operator.

Radio Technology

If the optional radio module is connected to the network this will display the connection technology such as GSM or UMTS.

Automation Menu

This menu allows integration of 3rd party apps and devices.

- Automation Username
- Automation PIN

Menu 3 - Zones

A zone (sometime referred to as an input) on the ZeroWire is a single physical hardwired connection or a non-physical wireless connection. Additionally zones on the ZeroWire can be used as logic inputs within actions (see Menu 8 – Actions) and / or be configured as one of many zone types that greatly increase the functionality of the ZeroWire system.

Zone Number

The ZeroWire can support a total of 64 zones. Each zone is identified by a unique zone number, which cannot be altered, and remains as the key reference for each zone.

Zone Name

Each zone can be configured with a custom 32 character name. The zone name is displayed wherever a zone is referenced on the ZeroWire system.

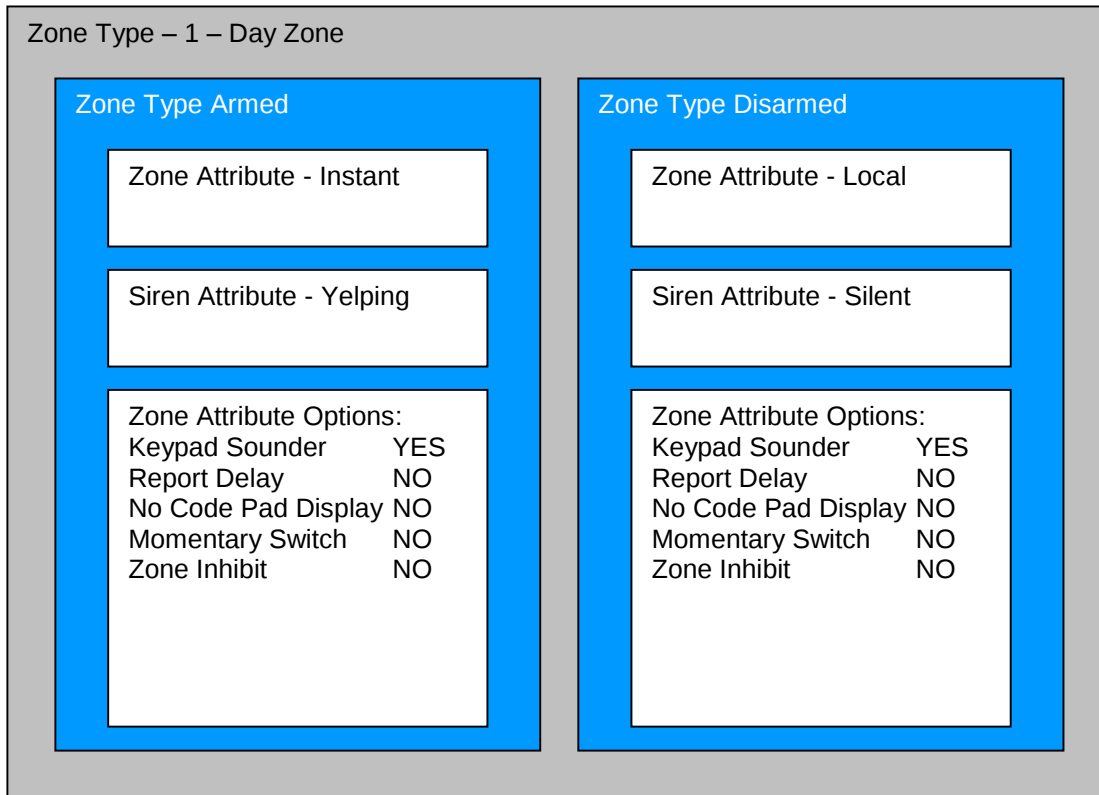
First Zone Profile

Zone profiles determine the zone type (Entry, 24 hour, fire, key switch, etc.) and the zone options (bypass, force arm, Twin Trip, stay mode, etc.). Zone profiles also determine the area in which the zone resides in. Additionally, each profile has a schedule that ZeroWire uses to determine which of the two zone profiles to use and when to use them.

Zone Type

Zone types are configured in Menu 15 – Zone Types. One of 32 configurable zone types may be allocated to any zone's zone type. Each zone type can behave independently between an arm and disarmed state. Zone types determine the zone attributes, siren attributes and zone attribute options.

Here is an example of a default zone type:



Zone Options

Zone options are configured in Menu 16 – Zone Option. One of 32 configurable zone options may be allocated to any zone's zone options. Zone options determine the zone attributes such as a zone's ability to be bypassed, force arm, Twin Trip, stay mode, etc. Additionally zone options determine the zone's reporting attributes.

Area Group

Area groups are configured in Menu 12 – Area Groups. One of 128 configurable area groups can be allocated to any zone's area group. Area groups are simply a list of ZeroWire areas. When an area group is allocated to a zone, that zone will then belong to all the areas in the area group.

If an area Group with no areas is used, then the zone will never report.

Schedule Number

Schedules are configured in Menu 7 – Schedules. One of 96 configurable schedules can be allocated to any zone's schedule number. Zone profile schedules determine when to allocate a zone profile to a zone. The first zone profile has the highest priority and the second zone profile has the lowest priority.

ZeroWire will check if the current time and day fall within the schedule of the first zone profile or if the schedule is disabled (thus always active). If the schedule is active then that profile is applied to that zone.

If the first zone profile's schedule is not active then it will check the second zone profile. If the schedule is active then that profile is applied to that zone.

User Number

The zone user number feature is used whenever the zone type is set to "keyswitch". Users are configured in Menu 1 – Users. One of 40 configurable users can be allocated to any zone's user number. ZeroWire zone profile user number is a powerful feature that is used to apply the selected users attributes to a keyswitch operation. When the keyswitch is activated, ZeroWire will check the user permissions and permission schedules to determine which areas are accessible. Additionally, area open and close reports will also report the user number selected in this option. If the user number is programmed to 0, the ZeroWire will use a default User number of 999 and will operate on all areas in the zones area group.

Second Zone Profile

Refer to the first zone profile.

Zone Type

Refer to first zone profile.

Zone Options

Refer to first zone profile.

Area Group

Refer to first zone profile.

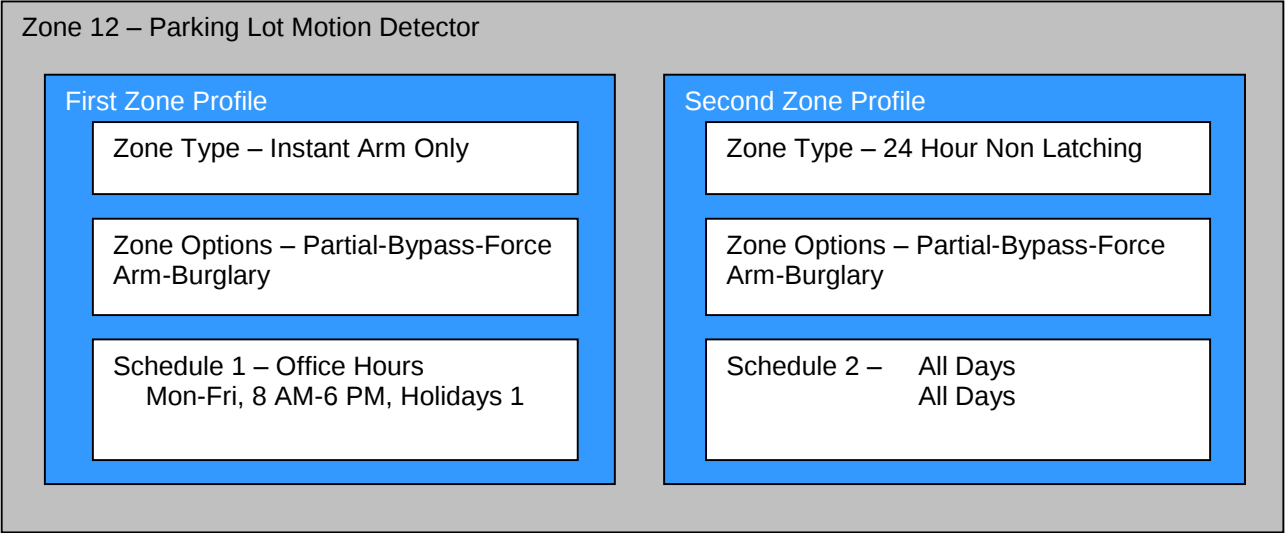
Schedule Number

Refer to first zone profile.

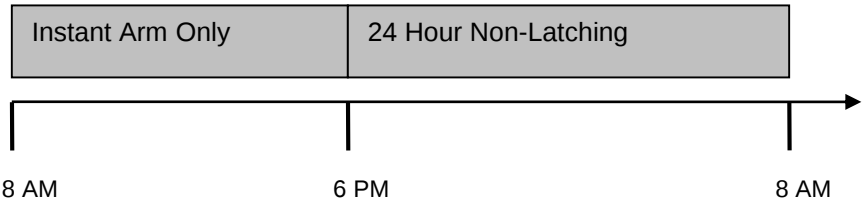
User Number

Refer to first zone profile.

Example



Zone Programming



Menu 4 - Areas

The ZeroWire can support a total of 8 areas; each area is configured with its entry and exit times, area options, area timers, area type and reporting characteristics.

Area Number

The ZeroWire can support a total of 8 areas. Each area is identified by a unique area number, which cannot be altered, and remains as the key reference for each area.

Area Name

Each area can be configured with a custom 32 character name. The area name is displayed wherever an area is referenced on the ZeroWire system.

Area Entry And Exit Times

ZeroWire uses the area entry and exit timers to delay the activation of an alarm event when entry/exit zone types are activated.

When an area is turned on, it will start an Exit 1 timer. When the Exit 1 timer expires it will start the Exit 2 timer.

While an Exit 1 timer is running – Entry 1, Entry 2, and Handover zone types will not create an alarm. While an Exit 1 or Exit 2 timer is running – Entry 2 zones will not create an alarm.

Once all exit delays are expired, an activation on an Entry 2 zone type will start an Entry delay with the Entry 2 time and an activation of an Entry 1 zone type will start an Entry delay with the Entry 1 time.

If an entry delay is running and a zone is activated with an entry time that is less than the time remaining, the timer will be reduced to the time of that new zone.

Activation of a Handover zone while an entry timer is not running will create an instant alarm.

If a zone is in more than 1 area, the zone will use the have the longest entry and exit delay time of the programmed area. If an area greater than 1 has the time set to 0, that area will use the time programmed in Area 1.

If area settings are set to 0, then the area will automatically inherit Area 1 settings.

Entry Time 1

Entry time 1 is used to time the entry delay when an entry delay is started by an entry 1 zone type.

Exit Time 1

Whenever an area is turned on, it will start an Exit 1 timer. Entry 1, Entry 2, and Handover zone types will not create an alarm while an Exit 1 timer is running.

Entry Time 2

Entry time 2 is used to time the entry delay when an entry delay is started by an entry 2 zone type

Exit Time 2

When the Exit 1 timer expires it will start the Exit 2 timer. Entry 2 zones will not create an alarm while an Exit 2 timer or an Exit 1 timer is running.

Stay Entry Time

The stay entry time is the entry warning time that applies to all zones armed in the stay mode. This stay entry time does not apply to fire zone types.

Area Options

Arm/Disarm Report

If enabled, this area will send open and close reports via one or more appropriately configured channels.

Quick Away

If enabled, this area can be armed in away mode via a single away mode key press. When area is armed via quick away mode, the closing user number is the default user of 999.

Arm In Stay If No Exit

If enabled, arms the area in stay mode automatically after the exit timer expires and no Entry/Exit zones are tripped.

Quick Stay Mode Disarm

If enabled, this will allow the stay mode to be disarmed by pressing the stay key on the keypad. This is only possible if there is no alarm active **and** the stay entry delay is not running.

This is a convenience feature avoiding the need to enter the PIN to disarm from stay mode.

Siren Chirp Away

If enabled, the ZeroWire will activate the built-in siren every time the system is set in away mode or disarmed with a key-switch or wireless keyfob.

Siren Chirp Stay

If enabled, the ZeroWire will activate the built-in siren output briefly every time the system is set in stay mode with a key-switch or wireless keyfob.

Force Arm With Bypass

If enabled, the area can be armed even if zones are not ready. Any zones that are not ready will automatically be bypassed, log the bypass, and optionally report the bypass.

The automatic bypass will be applied when the zone is capable of causing an alarm condition due to a state change such as an area arming, schedule or action. This avoids false alarms.

If an auto-bypassed zone becomes ready after it is armed, that zone will automatically remove the bypass, log the bypass restore, and optionally report the bypass restore.

Individual zones can be made “force armable with auto-bypass” by leaving this area option off, then enabling Forced Arm Enable in Zone options, and enabling Zone Inhibit in the Zone Type Profile.

Force Arm Without Bypass

If enabled, the area can be armed even if zones are not ready. Any zones that are not ready will NOT be automatically be bypassed and may cause an alarm condition because they could still be in a not ready state once the area becomes armed.

This option is overridden if the Force Arm With Bypass is enabled.

Individual zones can be made “force armable without auto-bypass” by leaving this area option off, then enabling Forced Arm Enable in Zone options, and disabling Zone Inhibit in the Zone Type Profile.

Silent Exit

If enabled, ZeroWire not sound the exit warning beeper.

Manual Fire

If enabled, the manual fire button will be enabled on keypads. Press and hold for 2 seconds to send a fire event. Default is off.

If disabled, on selected models will enable the Fire button on the ZeroWire keypad to send a Key A event which can be used for automation programming in Scenes.

Manual Auxiliary

If enabled, the manual auxiliary button will be enabled on keypads. Press and hold for 2 seconds to send an auxiliary event. Default is off.

If disabled, on selected models will enable the Medical/Auxiliary button on the ZeroWire keypad to send a Key B event which can be used for automation programming in Scenes.

Manual Panic

If enabled, the manual panic button will be enabled on keypads. Press and hold for 2 seconds to send a panic event. Default is off.

If disabled, on selected models will enable the Police button on the ZeroWire keypad to send a Key C event which can be used for automation programming in Scenes.

Use Area 1 Options

If enabled, the area will use Area 1 options. Default is on.

Bypass Requires PIN

If enabled, a valid PIN code with access to this area is required to bypass zones in this area.

Manual Panic is Silent

If enabled, manual panic alarms will not trigger an audible alarm.

Arm In Instant If No Exit

If enabled, will arm panel in instant mode (no entry delay) after the exit timer expires and no Entry/Exit zones are tripped. This assumes the person arming the system did not leave, and is still within the protected area. This provides greater security because any attempt to enter the area even through a designated Entry/Exit zone will trigger an instant alarm.

Area Timers

Auto Arm Warning

If the area type is Standard and Arm / Disarm is configured, this timer delays arming by the minutes entered.

If the area type is Timed Disarm, Man Down, or Guard Tour, this setting is a warning time given to a user once the user's Disarm Time, Man Down Time, or Guard Tour Time has expired. During this warning time a user can cancel the automatic re-arming and event report by entering their code, this will also restart the appropriate user timer. At the end of the warning time the ZeroWire will re-arm the area and send the appropriate event (closing, man down, guard tour fail).

If the area type is Early Open & Late Close, this timer sets the period after the start (opening) and after the end (closing) of the area type schedule that the area can be disarmed or armed. Otherwise an early to open or late to close report will be sent if enabled in user permissions. Fail to open and fail to close report will be sent if Arm-Disarm Reports is enabled in area options.

Valid values are from 0 to 99 minutes.

Local Alarm Reminder

If set, the local alarm reminder is the period in hours between 0 and 12 that may elapse between starting a local alarm and the local alarm reactivating if that zone has remained open.

For example, the tamper will trip if a smoke detector is removed to change the battery; if a user resets the alarm on the xGen but does not replace the smoke

detector within the local alarm reminder time, then the fire alarm tamper will retrigger.

Area Type Settings

Area Type

Standard: The area functions as normal.

Timed Disarm: Timed disarm is used when an authorized user can disarm an area for a predetermined period of time. At the end of this disarm time the area will start the auto-arm process ensuring that the area is not accidentally left disarmed. The following conditions must be true before a timed area disarm function will occur:

- The area type must be set to Timed Disarm.
- The area type schedule must be active.
- The user's active profile's permission must have:
 - This area set in the permission's timed disarm area group.
 - The permission must be in schedule.
 - The permission's Area Type Override must NOT be set.

At the end of the user's disarm time, the Auto Arm Warning will activate for the set period. At the end of the Auto Arm Warning period the area will arm and start the Exit Delay and if configured, report a closing using via the last user number to have time disarmed the area.

Anytime during the timed disarm period, authorized users with Area Type Override set in their active profile can cancel the disarm time period by arming or disarming the area.

The user's permission determines how long the area will be disarmed for.

Man Down: Man down is used when an authorized user(s) is working in a hazardous area (or the like), and there is a requirement that the user(s) regularly "check-in" to notify others that the user(s) is safe. If the authorized user(s) fails to perform this action the system can set an audible warning and send a report.

The following conditions must be true before man down function will occur:

- The area type must be selected to man down.
- The area type schedule must be active (after the start time and before the end time).
- The user's active profile's permission must have:
 - This area set in the permission's man down group.
 - The permission must be in schedule.
 - The permission's Area Type Override must NOT be set.

The man down timer is set in the user's permission.

At the end of the user's man down time, the Auto Arm Warning will activate for the set period. At the end of the Auto Arm Warning period the area will arm and if configured, report a man down alarm. Anytime during the man down period, authorized users with the Area Type Override set in their active profile will cancel the man down time period by disarming or disarming the area.

Guard Tour: Guard tour is used when an authorized user(s) (such as a guard) is required to regularly "check-in" to notify others that they have physically attended to a location(s) on the site. If the authorized user(s) fails to perform this action the system can set an audible warning and report a "Guard Tour Fail" event.

The following conditions must be true before guard tour function will occur:

- The area type must be selected to guard tour.
- The area type schedule must be active (after the start time and before the end time).
- The user's active profile's permission must have:
 - This area set in the permission's guard tour group.
 - The permission must be in schedule.
 - The permission's Area Type Override must NOT be set.

The guard tour time is set in the user's permission.

At the end of the user's guard tour time, the Auto Arm Warning will activate for the set period and keypad sounder will be active. At the end of the Auto Arm Warning period the area will arm and if configured, report a Guard Tour Fail alarm. Anytime during the guard tour period, authorized users with the Area Type Override set in their active profile will cancel the guard tour time period by disarming or disarming the area.

Early Open/Late Close: If the area type is Early Open & Late Close, the Auto Arm Warning sets the period after the start (opening) and the end (closing) of the area type schedule that the area must be either disarmed or armed.

For example, if the area type schedule is set between 8:00 AM (opening time) and 5:00 PM (closing time) and the Auto Arm Warning is set to 15 minutes; then the area must be disarmed between 8:00 AM and 8:15 AM otherwise if it is disarmed before 8:00 AM it is an early open, if it is disarmed after 8:15 AM it is late to open. Likewise the area must be armed between 5:00 PM and 5:15 PM otherwise if it is armed before 5:00 PM it is an early close, if it is armed after 5:15 PM it is late to close.

Area Type Schedule

Schedules are configured in Menu 7 – Schedules. One of 96 configurable schedules can be allocated to the area type schedule. The area type schedule determines the schedule that the selected area type is active. Area types are not active when the schedule is not active. If an area type schedule is disabled (always active) that area will always have the type characteristics programmed in Area Type.

Example:

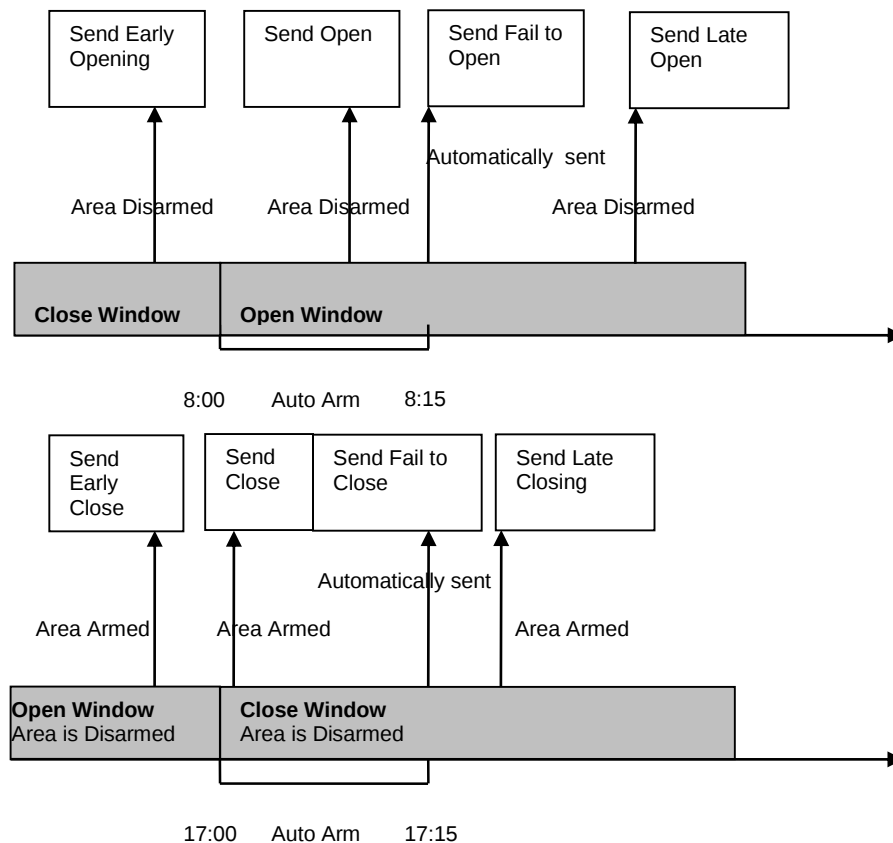
Area Type – Early Open & Late Close

Area Type Schedule – 8:00 to 17:00

Auto Arm Warning – 15 min

User Permissions–Options–Open/close, Early open report, Late close report

Area Options – Arm-Disarm Reports



Area Event Reporting

Area Account

If set, the area Account Number is a system unique 4 to 10 digit code (format dependent) used to associate area related alarm reporting events to this area. If the area Account Number is equal to the default of 0, the channel Account Number will be used for this area's alarm reporting events. If the channel Account Number is equal to the default of 0, the channel 1 Account Number is used. If the channel 1 Account Number is 0 then the account will be sent as 0.

Channel Group

The channel group determines which communicator channel(s) area events will be reported to. Channel groups are programmed in Menu 18 (Channel Groups). If the bit corresponding to one of the 16 reporting channels is set to on, area events will always be reported to this channel. It is referred to as a primary reporting channel. If a report is unsuccessful to a particular primary channel it will attempt that channel's backup channels if there are any.

Notes on Force Arming, Bypass, and Auto-Bypass

AREA 1 - Office	
☐ Force Arm With Bypass	
☐ Force Arm Without Bypass	
ZONE 1 – Door Reed Switch	
ZONE TYPE ☐ Zone Auto-Bypass	ZONE OPTIONS ☐ Force Armed Enabled ☐ Bypass
ZONE 2 – Reception PIR	
ZONE TYPE ☐ Zone Auto-Bypass	ZONE OPTIONS ☐ Force Armed Enabled ☐ Bypass

Normally to arm an area it must first be “Ready to Arm”. This means all zones in that area must be sealed.

For example, if the front door is open, then a user would need to close it first and ensure there is no movement in the reception area. This provides the Ready to Arm status in Area 1 that is needed before attempting to arm. However, this is not always user friendly or practical.

The term force arm refers to the ability to arm an area even though zones are not ready. It is usually only used with motion zones as these are self-restoring and will be restored by the time the exit delay ends (e.g. the person arming the system leaves the building causing the Reception PIR to restore.)

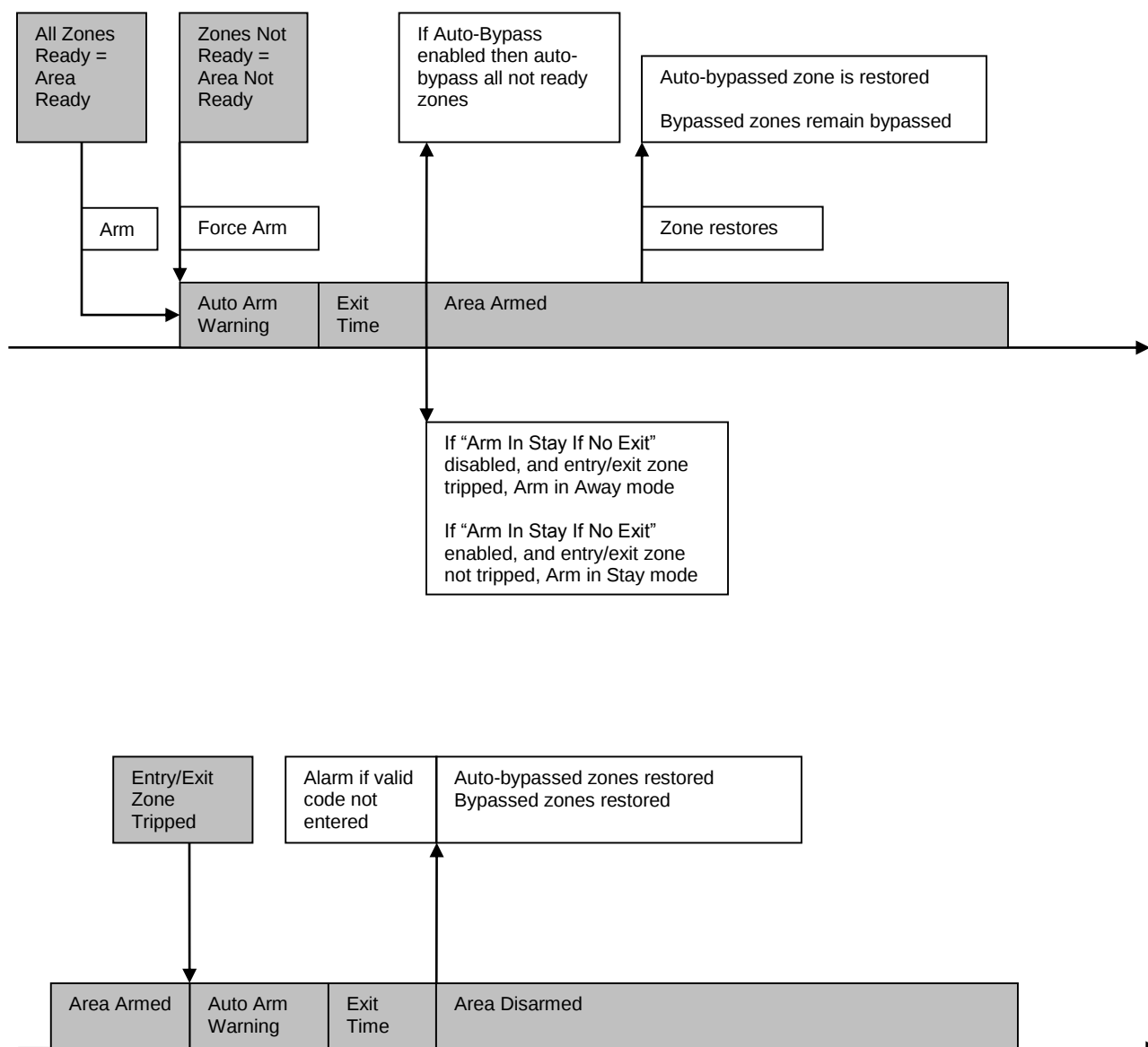
If the front door is not closed properly then Area 1 would go into alarm at the end of the Exit time. To avoid this false alarm we enable “Force Arm With Bypass” so all zones that are not sealed (i.e. not ready) by end of the exit time will be “Auto-Bypassed”.

If after the Area is armed, that zone restores (e.g. the person double checks and secures the front door) then the Auto-Bypass will be removed from the zone and it will be active. If subsequently the zone is triggered then Area will go into alarm.

Auto-bypass will be applied (if enabled, and if necessary) to a zone whenever a change in state occurs that would result in an alarm condition. These include arming an area with a not-ready zone, a zone changing profile, Arm-Disarm function, or due to an action or schedule.

Enabling Auto-Bypass for the area will apply the feature to all zones in that area as well.

In general disabling “Zone Auto-Bypass” is not recommended because of the potential to create a false alarm but there are applications where it is desired. Use “Force Arm Without Bypass” at the area level to prevent zones from being auto-bypassed when Force Armed.



Menu 5 - Channels

The ZeroWire can support a total of 16 channels; each channel is a communication path for events to be sent from the ZeroWire panel to a selected destination.

Default configuration reserves Channels 1 – 3 for UltraSync format, Channels 4 – 16 are Email or Push Notification format.

Email is a “best-effort” system and there is no guarantee messages will be delivered by the network. When the network is busy, messages can be dropped. This is why central control room monitoring is highly recommended as each event is acknowledged on receipt to ensure an appropriate response can be made.

Email addresses can only be configured by Master, Engineer, Master Engineer, and Custom Users with Channel menu permission.

Master users can only see channels configured as e-mail, Standard users cannot change the e-mail address.

Smartphone push notifications are configured from the specific smartphone. When push notifications are enabled on that device from the UltraSync + app, it will use the next available channel on the ZeroWire panel. When push notifications are disabled on that device, it will delete the channel it was using. The maximum number of devices that can use push notifications is 13.

Push notifications are sent from UltraSync servers to Apple and Google servers for delivery to the selected device. Delivery is “best-effort” and no guarantee is made for the successful delivery of messages.

Channel Number

The ZeroWire can support a total of 16 channels. Each channel is identified by a unique channel number, which cannot be altered, and remains as the key reference for each channel.

Account Number

This is the Account Number that will be reported with the event in email reports. When UltraSync format is selected, this field will not be used.

Format

This is the communication format for the selected channel. Select from:

- Use as Backup
- Email
- UltraSync

Destination Email

The e-mail address of the selected destination.

Next Channel

If the channel selected is unable to deliver the event to the selected destination, ZeroWire will try to use this backup channel instead. The Next Channel specified here must be greater than the Channel Number.

A number lower than the current Channel Number will end the chain. This is to prevent accidental programming of endless loops.

Event List

Select the pre-programmed list of events that will be sent via this channel. The specific events in each event list is programmed in Menu 17 (Event Lists).

Attempts

Enter the number of times ZeroWire should try to send the events to the UltraSync server. After the number of attempts has been exhausted the ZeroWire will try the Next Channel if specified.

Menu 6 - Communicator

The ZeroWire Communicator is a core component of the ZeroWire System used in conjunction with the Channels feature to report events to a monitoring company or third party. In this menu you can configure the settings for various methods of reporting.

General Options

First Disarm Last Arm

If enabled, the ZeroWire will only send a closing report when the last area is armed. Note: the last area to arm must have open/close reports enabled. The ZeroWire will only send an opening report when the first area is disarmed.

This feature is used in place of Individual area Open and close. If you enable open and close in the area you will get both individual open and close and System open close

Report Once Per Zone

If enabled, this will limit reporting to only once per zone each time you arm or disarm an area. This stops the control room or reporting destination to be flooded by multiple reports that the same zone is being activated (for example the intruder may be moving around and is being picked up by the zone on that zone.)

Suppress Force Arm Bypass

If enabled, the ZeroWire does not send bypass reports when a zone is forced armed.

If not enabled, when a zone is forced armed and it remains in a state of creating an alarm, bypass reports are sent at the end of exit time. For example this would occur if it remains unsealed at the end of the exit time, or due to change of zone type caused by a schedule.

If forced armed zones re-seal during the armed period, bypass restores are sent.

Immediate Restore

If enabled, the ZeroWire will immediately send all restores as the zone reports the event.

If not enabled, the ZeroWire will send restoral events all at the same time when the area is disarmed.

Auto Test

Auto Test Intervals

Set day of the week to send an automatic test report to the system channel group (Communicator\System Event Reporting\System Channels). You may also set auto-test to Daily.

Auto Test Time

Enter the time at which the automatic test report should be sent. This should be in 24-hour format. For example 18:00

IP Configuration

IP Host Name

A text label assigned to the ZeroWire communicator so you do not have to remember the IP Address. Enter //[IP Host Name] in a Microsoft Windows web browser to access the ZeroWire Web Server.

Note this only works on local LAN and with Microsoft Windows PC, or an Apple device with the .local extension. Does not work remotely over the internet.

IP Address

The IP address assigned to the ZeroWire communicator to enable it to connect on to the local LAN. This will allow you to access the embedded web server from a web-enabled device to program and view the status of the system. It is also used for alarm reporting.

Gateway

If required, the IP address of the router which is needed when remote IP communications are used

Subnet

The subnet mask for the network.

For example, 255.255.255.0 is the network mask for 192.168.1.0/24

Primary DNS

The IP address of the Primary Domain Name Server. The DNS is used to translate host names for time servers and UltraSync servers.

Secondary DNS

The IP address of the Secondary Domain Name Server, used if the Primary DNS is not available.

WiFi SSID

The Service Set Identifier, uniquely identifies the WiFi network and allows devices to connect to it.

WiFi Security Type

Select the security protocol for the network. Options available include: None, WPA2, WPA, WEP, WEP 128, none.

WiFi Password

Password required to access the WiFi network. Ask the administrator if you are not sure.

Ports

Here are the ports that the computer needs to communicate with the ZeroWire system.

Defaults:

- HTTP Port = 80
- HTTPS Port = 443
- Download Port = 41796

Time Server

Enter the URL or IP address of a time server to allow the ZeroWire to automatically update and synchronise its clock without user intervention. The default is pool.ntp.org

IP Options

- **Enable DHCP:** Allow the ZeroWire panel to be automatically assigned an IP address by the network.
- **Enable Ping:** Allow the ZeroWire panel to respond to the PING command.
- **Enable Clock Updates:** Allow the ZeroWire internal clock to synchronise with the internet time server specified.
- **Enable Web Program:** Enabling this option will cause ZeroWire Web Server and UltraSync + app to always display the Advanced menus when an installer logs in.
Disabling this option will hide the Settings and Advanced menu on ZeroWire Web Server and UltraSync + app regardless of the login. To reveal the Settings and Advance menus, have a Master User press Menu 8 and enter their PIN code on the ZeroWire keypad. This provides greater security by disabling web programming until a user with adequate permissions enters their PIN on the physical ZeroWire panel on-site.
- **Always Allow DLX900:** Enabling this option will allow DLX900 to connect at any time if the correct Download Access Code is provided. Disabling this option provides greater security by only allowing DLX900 to connect when program mode is active. This allows the system to have DL900 access disabled until a user on site with physical access to the keypad enters program mode with a valid PIN code.
ZeroWire will be in program mode if a user gains authorized access to menu 5, 8, or 9.
- **Monitor LAN:** When the Monitor LAN option is enabled the panel will monitor the Ethernet port for a valid Ethernet cable. If the Ethernet cable is disconnected while this option is enabled, and the panel is unable to communicate, it will log a Fail To Communicate event.

- **Enable UltraSync:** This is an automatic feature of ZeroWire. It is recommended you leave this setting on. Enable this option to allow ZeroWire to send email reports via the UltraSync servers. This is independent of the Web Access Passcode which when set to 00000000 will prevent the UltraSync + app from connecting. If any channel is set to Email format reporting, then ZeroWire will override ignore this setting and allow email reporting via UltraSync cloud servers. If you wish to prevent connections to the ZeroWire cloud servers, then uncheck this option and do not use the UltraSync reporting format.

Features	Email Reports	UltraSync + app
Enable UltraSync = OFF Web Access Code = 00000000	No	No
Enable UltraSync = OFF Web Access Code = not 00000000	Yes	Yes
Enable UltraSync = ON Web Access Code = 00000000	Yes	No
Enable UltraSync = ON Web Access Code = not 00000000	Yes	Yes

- **Enable WiFi, Disable Ethernet:** Enabling this option will cause the ZeroWire to use WiFi as the primary medium to connect to the Internet. Disabling this option will switch the connection mode to Ethernet. If switching between WiFi and Ethernet modes, logout of webpage, keypad programming, and app to end current session. This allows the panel to reconnect on the new mode. WiFi and Ethernet cannot be enabled simultaneously.

Radio Configuration

These are the credentials used by the cellular radio module, if installed, to connect to the mobile network. Check with your service provider for the correct settings.

- GPRS User Name
- GPRS Password
- APN

Remote Access

Panel Device Number

A number from 0 to 4,294,967,295 that must be entered in to the desktop software for remote access to take place.

Download Access Code

A variable length code for the computer user. This code gives the software complete authority over all menus including those that are locked. For convenience DLX900 will also try installer/9713 to allow a connection for first time set up if the Download Access Code does not work, this is why changing the default code is important.

Changing this code may lock out your control room monitoring service and prevent you from maintaining your system. It is advised you contact your control room before changing this code.

Users must have access to the Communicator menu in order to change this setting. This can be programmed in menus, and assigning the Advanced menu.

Call Back Server

If an IP address or hostname is programmed into this feature, and “Call Back Before Download Session” is enabled, the ZeroWire will disconnect for approximately 10 seconds and then connect to this IP address.

This should be the IP address of the computer where DLX900 is installed, not the IP address of the ZeroWire panel.

IMPORTANT: the call back IP address should always be reviewed for accuracy before disconnecting!

Download Options

- **Call Back Before Download:** If a download is requested the ZeroWire will hang up and make a call to the Call Back Number. This is to increase the security of remote access.
- **Lock Local Programming:** Prevent changes to the ZeroWire system via a keypad, all changes **MUST** be made using the remote access software.
- **Lock Communicator Programming:** Local programming locks all programming unless accessed with the Download Access code. Lock communicator locks local programming of communicator features unless accessed by the Download Access Code.
- **Lock Download Programming:** Prevents the programming of the Remote Access Menu without using the Download Access Code.
- **Call Back at Auto Test:** When an auto test is initiated, perform a call back to the IP address specified.

System Event Reporting

System Channels

Enter the Channel Group that the ZeroWire will send system events to.

Sequence Attempts

This is the number of times the ZeroWire will sequence back to the primary channel if the backup channels all fail. This applies to ALL communication attempts including zone and area events.

Menu 7 - Schedules

Schedule Number

The ZeroWire can support a total of 16 schedules. Each schedule is identified by a unique schedule number, which cannot be altered, and remains as the key reference for each schedule.

Schedule Name

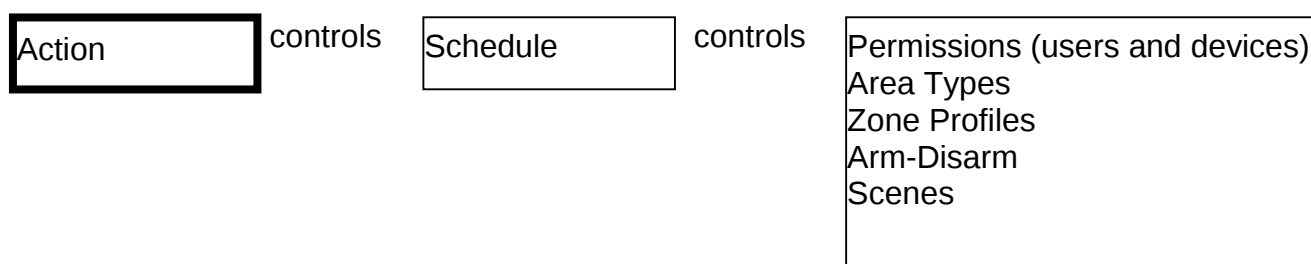
Each schedule can be configured with a custom 32-character name. The area name is displayed wherever a schedule is referenced on the ZeroWire system.

Follow Action Number

If an action number is specified, then the schedule becomes enabled when the action is true. When the action becomes false, then the schedule becomes disabled.

Schedules can be used to control various parts of the system such as when a user's permissions are applied. The "Follow Action Number" option allows you to use actions to control schedules.

The result is actions can control when permissions are applied, when area types are applied, zone behaviours, when arm-disarm can occur, and when scenes play.



This allows you to create conditional schedules that only become active when certain conditions are met. For example you could create a user that only becomes active (because of the linked schedule) under certain conditions like a fire alarm.

Times and Days

Up to 16 sets of time and days can be specified here.

ZeroWire handles schedules that span midnight automatically.

For example, if a schedule is to cover Fri 8:00pm to Sat 6:00am, then only tick Fri and ZeroWire will automatically manage the time after midnight.

Thurs	Fri ✓	Sat	Sun
			

Tick only Fri

If you tick Fri and Sat, the schedule will cover Fri 8:00pm – Sat 6:00am and Sat 8:00pm – Sun 6:00am.

Thurs	Fri ✓	Sat ✓	Sun
			

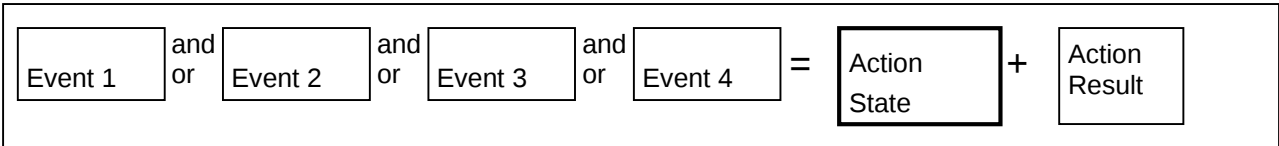
Tick Fri and Sat

- **Start Time**
- **End Time**
- **All Days**
- **All Week Days**
- **All Weekend**
- **Monday**
- **Tuesday**
- **Wednesday**
- **Thursday**
- **Friday**
- **Saturday**
- **Sunday**
- **Holidays 1:** If enabled, it means the item assigned this schedule will NOT have access during the specified holiday dates. See feature Holiday to program these dates.
- **Holidays 2:** If enabled, it means the item assigned this schedule will NOT have access during the specified holiday dates. See feature Holiday to program these dates.
- **Holidays 3:** If enabled, it means the item assigned this schedule will NOT have access during the specified holiday dates. See feature Holiday to program these dates.
- **Holidays 4:** If enabled, it means the item assigned this schedule will NOT have access during the specified holiday dates. See feature Holiday to program these dates.

Menu 8 - Actions

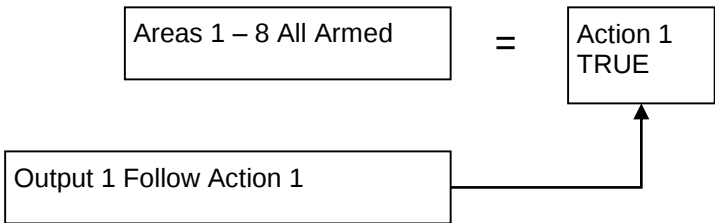
The ZeroWire features powerful automation control which can interact with different parts of the system. It can perform functions based on the status of one or more system conditions.

Each action has an on and off state. The state is controlled by up to 4 conditions called Action Events, each of which can have a range of items.



Action

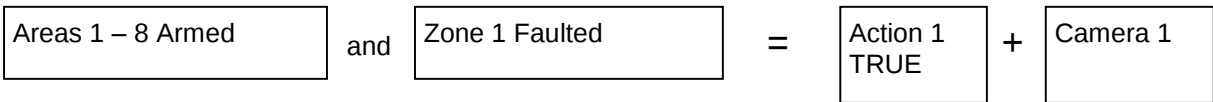
When all 4 Action Events are met, then the Action State will be set. The Action State can be monitored by the main ZeroWire Panel, Schedules, Devices with outputs, and Scenes to activate/deactivate.



For example, a strobe connected to Output 1 can be programmed to follow Areas 1-8 being armed.

Each Action can also directly control selected parts of your ZeroWire when all 4 Action Events are met. This is called the Action Result. Its behaviour also follows the Action State.

For example, when all areas are armed and there is activity on zone 1, activate a



camera recording:

The main panel supports 32 actions. They have been pre-programmed in the defaults to allow quicker programming. You may re-program any of these for other use.

Action Number

The ZeroWire can support a total of 32 Actions. Each Action is identified by a unique number, which cannot be altered, and remains as the key reference for each Action.

Action Name

Each Action can be configured with a custom 32-character name. The name is displayed wherever an Action is referenced on the ZeroWire system.

Function

Timed

The action state turns on for the time specified.

Follow

The action state turns on once the Event conditions have been satisfied, then off once the Event conditions are not true.

On Delay

The action state becomes on after the programmed time period unless logic result is no longer active.

Off Delay

Follows the result of the logic equation, but remains active for the time programmed after the logic result is no longer active.

Pulsed

Action state turns on for the programmed time or the active period of the logic result, whichever is the SHORTEST.

Latch

The action state stays on once the Event conditions have been satisfied

Duration Minutes

Where the Function requires duration, this determines how long the action should stay on for in minutes.

Duration Seconds

Where the Function requires duration, this determines how long the action should stay on for in seconds.

Event 1

Event Category

Select the category of the first event. This will determine what events you can select in Event Type.

Reference the Table 2 on page 54.

Event Type

Select the event that you want the Action to monitor.

Reference the Table 2 on page 54.

Event Start Range

Select the starting number of the event that you want the Action to monitor. This is related to a number range. For example this might be the first area or zone number.

Event End Range

Select the ending number of the event that you want the Action to monitor. This is related to a number range. For example this might be the last area or zone number.

If you just want to monitor one item then leave it at the default of zero, or enter the same number as Event Start Range.

Event Combination Logic

The logic condition to apply to Event 1.

- **OR:** e.g., Area 1 Armed Away OR Area 2 Armed Away
- **Inverted OR:** e.g., NOT Zone 1 Bypass OR Zone 2 Bypass
- **AND:** e.g., Area 1 Armed Away AND Area 2 Armed Away
- **Inverted AND:** e.g., NOT Zone 1 Bypass AND Zone 2 Bypass
- **RESET:** Reset any latched event.

The Combination Logic selected for each event places the logic prior to the event in an equation. Selecting the AND logic closes a parenthesis for the previous event. The DLX900 software displays an Event Equation field to make it easier to construct Actions.

For example, Event 1 Inverted OR, Event 2 OR, Event 3 AND, Event 4 OR produces a logic equation of:

(NOT Event 1 OR Event 2) AND (Event 3 OR Event 4)

Event 2

- Event Category
- Event Type

- Event Start Range
- Event End Range
- Event Combination Logic

Event 3

- Event Category
- Event Type
- Event Start Range
- Event End Range
- Combination Logic

Event 4

- Event Category
- Event Type
- Event Start Range
- Event End Range
- Event Combination Logic

Result

The ZeroWire can also perform an additional function once the Action Event conditions are satisfied, this is called an Action Result.

For example, when a fire alarm is active, you could disable Users 1-40 to prevent them from being able to control the alarm system.

Result Category

The category of the Action Result to perform. Reference the Table 3 on page 56.

Result Type

The event of the Action Result to perform. Reference the Table 3 on page 56.

Result Start Range

Select the starting number of the event that you want the Action Result to affect.

Result End Range

Select the ending number of the event that you want the Action Result to affect.

Result User Number

Select the User that you want the Action Result to behave as. This will apply this user's full permissions to the Action Result you select.

Table 2: Action Events Category and Action Event Types

Action Events Category	Action Event Type
Zone Events	Disabled
	Faulted
	Not Faulted
	Alarm
	Bypass
	Tamper
	Low Battery
	Trouble
	Supervision
	Chime Enabled
	Inhibited
	Alarm Memory
Area Events	Disabled
	Armed Away
	Armed Away + Bypass
	Armed Partial
	Auto Arm Warning
	Holdup Delay
	Timed Disarm
	Guard Tour Time
	Guard Tour Fail
	Man Down Timer
	Man Down Fail
	Entry
	Exit 1 or Exit 2
	Exit 1
	Exit 2
	Silent Exit Active
	Exit Error
	Abort Window
	Cancel Window
	Zone Twin Trip Timing
	Zone Bypass
	Zone Tamper
	Zone Not Ready
	Zone Low Battery
	Zone Supervision Fault
	Chime On (from zone)
	Walk Test (from zone)
	Trouble (from zone)
	Any Alarm
	Burg Alarm
	Fire Alarm

	Panic Alarm Auxiliary Alarm Any Siren Fire Siren Nonfire Siren Keypad Sounder DLX900 Turn off command DLX900 Turn on partial DLX900 Turn on away Manual Fire Manual Panic Manual Auxiliary User Arm Trigger User Disarm Trigger Area Not Armed Away Key A Key B Key C
User Events	Disabled PIN entered PIN Entered out of schedule Void PIN Entered Lost PIN Entered Expired PIN Entered Turn On By User Turn Off By User Geosphere 1 Entered Geosphere 1 Exited Geosphere 2 Entered Geosphere 2 Exited
Logic State	Disabled Action State True Manual Output On Manual Output Off Scene Activated Action State False
Schedule States	Disabled Schedule State
Device Status	Disabled Fire Alarm Verification Box Tamper Local Programming Remote Programming Battery Test Off line Power Up delay Shut Down

	Phone Communicator trouble
	Phone Line fault
	Ethernet Communicator Trouble
	Ethernet No Link
	Ethernet Server Fault
	Radio Communicator Trouble
	Radio No Link
	Communicator Active
	Smoke Power Fail
	Mains Fail
	Low System Battery
	Strobe On
	Siren On
	Siren Tamper
System Events	Disabled
	Reserved
	Watchdog Reset

Table 3: Action Results Category and Action Results Event Types

Action Results Category	Action Results Event Type
Zone Results	Zone Trip Toggle
	Zone Trip
	Zone Restore
	Zone Bypass Toggle
	Zone Bypass
	Zone Unbypass
	Zone Chime Toggle
	Zone Chime On
	Zone Chime Off
	Send Zone Notification
Area Results	Arm Away
	Turn Off
	Silence
	Arm Stay Toggle
	Arm Stay
	Arm Away No Auto Stay
	Chime Toggle
	Chime On
	Chime Off
	Automatic Zone Test Toggle
	Automatic Zone Test On
	Automatic Zone Test Off
	Auto Arm Timer Restart
	Disarm Timer Restart
	Man Down Timer Restart
	Guard Tour Timer Restart

	Hold Up Timer Restart Activity Timer Restart Arm or Disarm Test Timer Restart Send Area Notification
User Results	User Expire or Activate User Activate User Deactivate
System Results	Disabled Detector Reset Communicator Test Send Notification or Email
Device Results	Disabled Battery Test Start Siren Device Bypass Device Unbypass
Scene Results	Scene 1 Scene 2 Scene 3 Scene 4 Scene 5 Scene 6 Scene 7 Scene 8 Scene 9 Scene 10 Scene 11 Scene 12 Scene 13 Scene 14 Scene 15 Scene 16
Camera Results	Camera 1 Camera 2 Camera 3 Camera 4 Camera 5 Camera 6 Camera 7 Camera 8 Camera 9 Camera 10 Camera 11 Camera 12 Camera 13 Camera 14 Camera 15

Menu 9 - Arm-Disarm

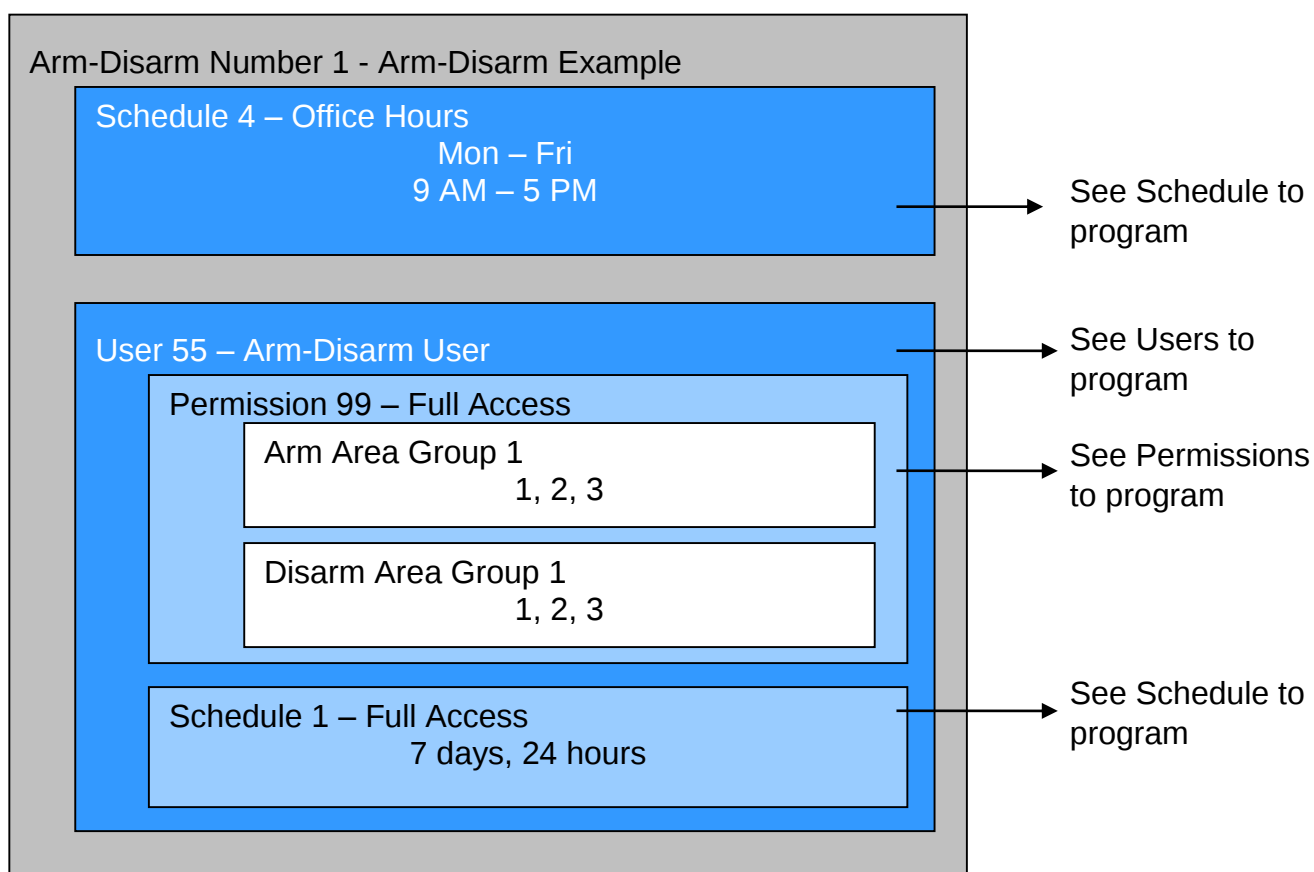
The ZeroWire Communicator has a powerful automation feature which simulates a user performing arming and disarming of the system according to a specified schedule.

When a Schedule becomes valid (inside valid time zone) the ZeroWire will disarm all Areas that are in the User's - Active Profile - Disarm Area Group.

When the Schedule becomes invalid (out of time zone) then ZeroWire will arm all areas that are in the User's - Active Profile - Arm Area Group.

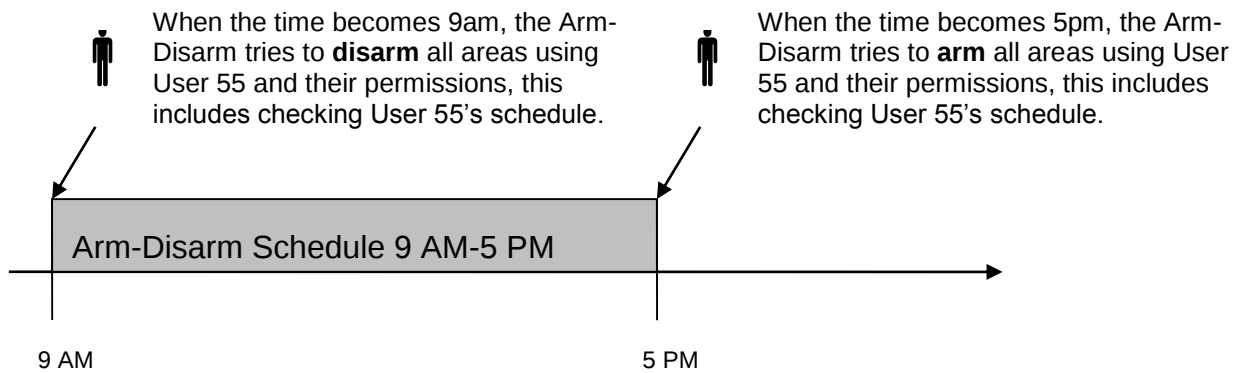
For example if we had Schedule 4 Mon-Fri 9am-5pm, and User 55 with permission to arm and disarm area 1, 2, and 3, plus their schedule was 24 hours 7 days a week.

Then each weekday at 9am the system would disarm areas 1, 2, and 3 as if it were user 55. At 5pm each weekday the system would arm areas 1, 2, and 3 as if it were user 55.



For an Arm-Disarm to occur, both the Arm-Disarm schedule here and the User Schedule need to be valid at the time the Arm-Disarm is triggered.

The Arm-Disarm Schedule determines what the operation is. The leading edge causes a disarming function and trailing edge causes an arming function. The Users Permissions then determines which areas if any are armed or disarmed. If the function is to disarm, the Users Disarm Area Groups will be disarmed. If the function is to arm, the Users Arm Area Group will be armed.



More complex interactions with the system are possible by modifying the schedule selected here, the schedule assigned to the user, and even combining actions to control schedules. Also, user permissions can have up to 4 permission and schedule pairs.

Arm-Disarm Number

The ZeroWire can support a total of 16 Arm-Disarm. Each Arm-Disarm is identified by a unique number, which cannot be altered, and remains as the key reference for each function.

Arm-Disarm Name

Each group can be configured with a custom 32 character name. The name is displayed wherever an Arm-Disarm is referenced on the ZeroWire system.

User Number

The user number that will perform the Arm-Disarm. The user's schedule and permissions will be checked and applied to all areas in the user's arm or disarm area group at the time of the Arm-Disarm.

Schedule Number

The schedule number specified here determines when the arm and disarm is performed by the user number. The starting date/time of the schedule will perform a disarm, the ending date/time of the schedule will arm.

Menu 10 - Devices

This menu allows you to program devices connected to the ZeroWire system. The specific menus that appear are dependent on the device(s) you connect and may not match this section exactly.

System Devices - Control

Control UID

Serial number of the ZeroWire.

Control Name

The name of the ZeroWire system.

Control Info

Version information about the ZeroWire including firmware, voice, web, and MAC address.

Control Outputs

The ZeroWire has 2 on-board outputs which can be programmed to follow actions.

- **Output Name:** Each output can be configured with a custom 32 character name.
- **Action Assignment:** The output will activate while the selected action state is true. If the action state becomes false then the output will deactivate.
- **Schedule Number:** If a schedule is entered here then the output will only be active when the schedule is valid. If no schedule is entered then the output will always function.
- **Invert:** Invert the output.

Interlogix Transmitters

Transmitter Number

Serial Number

User: By default all keyfobs are reported as user 999. To enable individual keyfob reporting, assign a user number here.

Options: Allows the installer to configure options for wireless transmitters including:

- **Tamper** – enable the tamper, for keyfobs this is the dual press of the first two buttons.
- **Police** – enable the manual police button on four button keyfobs.
- **Auxiliary** – enable the manual auxiliary, for four button keyfobs this is the dual press of the last two buttons.

- **Disable Supervision** – disables supervision monitoring of zone, no report or local alarm will occur if ZeroWire does not receive a supervisory message from the wireless zone within the supervisory times.
- **Disable Internal Reed** –this applies to transmitters with an internal reed switch.
- **Norm Open External Contact** – this applies to transmitters with an external input.
- **No Siren on Police** – disables the siren if the manual police is triggered on a keyfob.

Scene: On a four-button keyfob, this allows the user to activate a scene when the fourth button is pressed.

Signal Strength: Signal level received from wireless zone.

Zwave Devices

Device Number

Device Name

Basic Type

Generic Type

Specific Type

Tablet Keypads

Keypad Number

Keypad Name

Serial Number

Area Group: What areas can this keypad view and control

Keypad Options:

- **Silent Keypad** – If enabled, keypad will not sound beeps for entry/exit delay and alarms.
- **Require PIN for Scene** – if enabled, requires a PIN code to run a scene.

Menu 11 - Permissions

Permissions control what a user or device has access to on the ZeroWire system and what they can do.

Permission Number

The ZeroWire can support a total of 16 Permissions. Each set of Permissions is identified by a unique number, which cannot be altered, and remains as the key reference for each Permission.

Permission Name

Each group can be configured with a custom 32-character name. The name is displayed wherever Permissions are referenced on the ZeroWire system.

Control Groups

Menu Group

This controls what menus the user or device can access

Arm Area Group

This controls which areas can be armed.

Disarm Area Group

This controls which areas can be disarmed.

Reset Only Area Group

This controls which areas can be reset only.

For example, if a guard is present on the site you may not want them to be able to disarm any areas. By assigning them a Reset Only Area Group, they can turn off alarms, but they cannot accidentally disarm an area.

Timed Disarm Area Group

This controls which areas can be timed disarm.

Man Down Area Group

This controls which areas will have man down monitoring.

Guard Tour Area Group

This controls which areas are a part of the guard tour.

Report Channel Group

This controls what channels the user can modify.

Stay Arm Area Group

This controls what areas can be stay armed.

Permission Options

Remote Access

Enables and disable remote web access to the permission. If this is not enabled, a user will not be able to access the web interface directly or via a smartphone app.

Duress Code

Designates this user as a duress code, whenever this code is entered on the ZeroWire keypad a duress message is sent.

Reset System Alarms

When System Option - System Alarm Latch is enabled, system alarms include panel box tamper can only be reset by a user with this permission. Users without this permission will be able to arm and disarm areas as normal, but system alarms will stay latched.

Auto Un-Bypass

When enabled, a bypassed zone will be reset when disarming. When disabled, the zone will remain bypassed even after the system has been disarmed.

Disarm Area In Alarm

When disabled, this user will not be able to disarm and reset an area in alarm. Even if the user has permission in their Disarm Area Group, this option will override disarm authority.

Area Type Override

Applies to non-standard area types 'Time Disarm' 'Man Down' 'Guard Tour'. When set, disables the feature for the user.

Disarm Action Trigger

When enabled, this user will trigger the Action trigger event "User Disarm Trigger" when disarming an area, used for programming actions.

Arm Action Test

When enabled, this user will trigger the Action trigger event "User Arm Trigger" when arming an area, used for programming actions.

Report Arm/Disarm

Where a system is already configured to send Arm-Disarm reports this option allows a user to NOT send a report. When enabled, the reports will be sent. When disabled, reports will not be sent.

Report Arm-Disarm Exceptions

When enabled all four reports are sent as appropriate.

- Early Opening
- 'Fail To Open' and the reset report 'Late Open'
- Early Close
- 'Fail To Close' and the reset report 'Late Closing'

When this setting is disabled, only reports 'Fail To Open' and 'Fail To Close' are sent with their respective resets – 'Late Open' and 'Late Close'. Both the 'Early Open' and 'Early Close' reports are suppressed.

- 'Fail To Open' and the reset report 'Late Open'
- 'Fail To Close' and the reset report 'Late Closing'

See Area Type for more details.

Log PIN Use

Log will show "Valid Code Entered" when enabled. Must be enabled to allow actions and scene events to monitor user interaction.

Area User Timers Options

- **Disarm Time**
- **Man Down Time**
- **Guard Tour Time**

These timers apply to a user when allocated this permission and:

- the Area Type is set to Timed Disarm, Man Down, or Guard Tour,
- is inside Area Type schedule,
- and Area Type Override is NOT enabled under Permission Options.

If the value of the associated timer is zero, then the system will apply a timer of 45min.

See Menu 4 – Areas, Area Type Settings for a more detailed description on these features.

Menu 12 - Area Groups

When assigned to a user, an area Group controls what areas the user can see and control. When assigned to a device, an area Group controls what it can display and control. When assigned to a Zone, an area Group determines what Areas that Zone will report and display in.

Area Group Number

The ZeroWire can support a total of 16 Area Groups. Each Area Group is identified by a unique number, which cannot be altered, and remains as the key reference for each area.

Area Group Name

Each group can be configured with a custom 32 character name. The name is displayed wherever an area Group is referenced on the ZeroWire system.

Area Group

Select the areas that should be part of this Area Group.

Menu 13 - Menus

Menu Groups are assigned to users and devices to control what menus can be accessed. A total of 16 Menus can be configured.

Menu Number

Each Menu is identified by a unique number, which cannot be altered, and remains as the key reference for each Menu.

Menu Name

Each Menu can be configured with a custom 32 character name. The name is displayed wherever a Menu is referenced on the ZeroWire system.

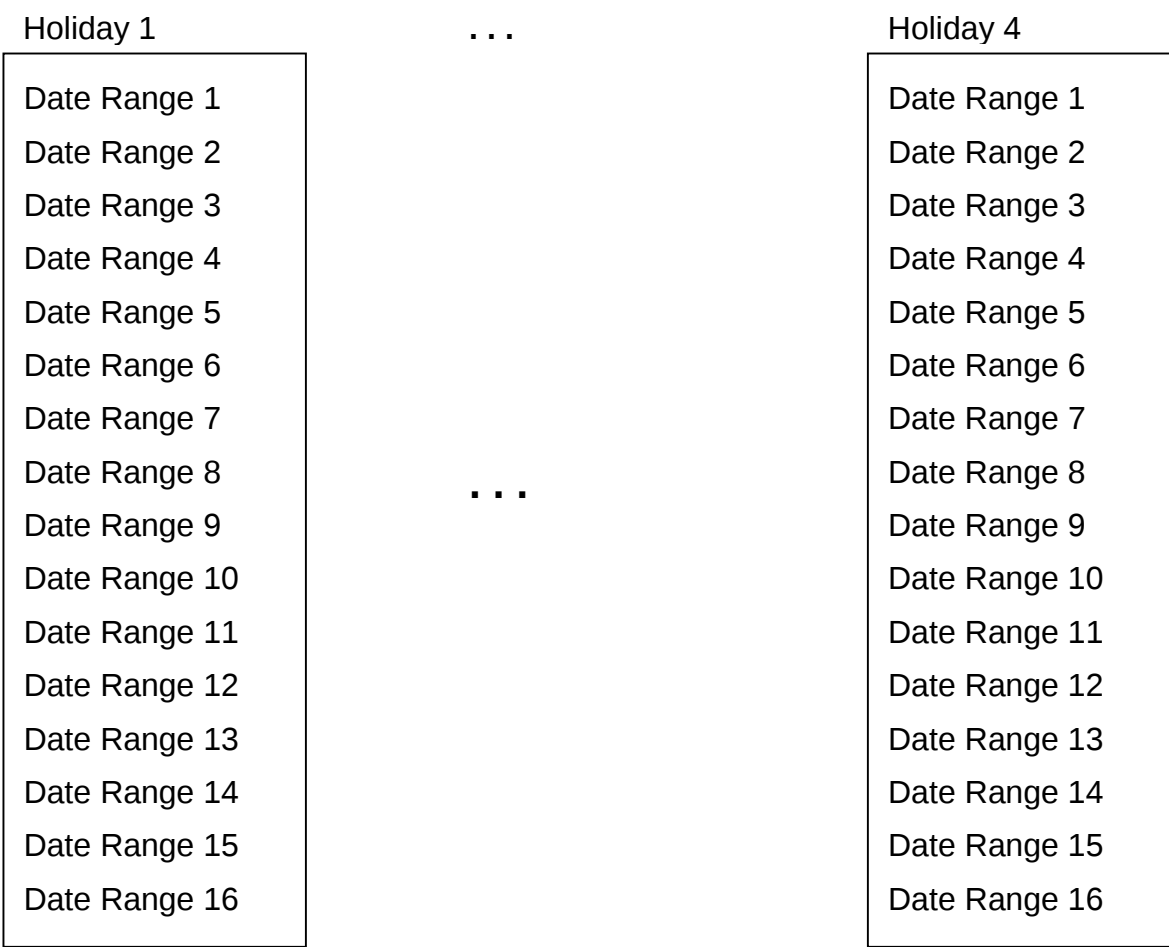
Menu Selections

Tick each item to give a user access to that menu. For example, ticking Labels permits a user with this Menu in their permission to change the text labels (names) of zones, areas, outputs, etc.:

- History
- Cameras
- Rooms
- Lights
- HVAC
- Intercom
- Smoke Reset
- Users
- Testing
- Reporting
- Scenes
- Clock
- Holidays
- Schedules
- Entry & Exit
- Z-Wave
- Labels
- Keypad Setting
- Devices
- Status
- Advanced

Menu 14 - Holidays

ZeroWire supports up to 4 sets of holiday dates, each set can have up to 16 date ranges. Holidays are used as part of Schedules to control access to the system on specified dates.



Holiday Number

The ZeroWire can support a total of 4 Holidays. Each Holiday is identified by a unique number, which cannot be altered, and remains as the key reference for each area.

Holiday Name

Each holiday can be configured with a custom 32 character name. The name is displayed wherever a Holiday is referenced on the ZeroWire system.

Date Range

Select the date range for the Holiday by specifying the start and stop date. A total of 16 ranges can be entered for each Holiday.

Start Date

End Date

Example

Holiday 1 – Australian NSW 2014 Holidays

Date Range 1 – 01/01/2014 – 01/01/2014

Date Range 2 – 26/01/2014 – 27/01/2014

Date Range 3 – 18/04/2014 – 18/04/2014

Date Range 4 – 21/04/2014 – 21/04/2014

Date Range 5 – 25/04/2014 – 25/04/2014

Date Range 6 – 09/06/2014 – 09/06/2014

Date Range 7 – 25/12/2014 – 26/12/2014

Date Range 8 – 06/10/2014 – 06/10/2014

Date Range 9

Date Range 10

Date Range 11

Date Range 12

Date Range 13

Date Range 14

Date Range 15

Date Range 16



Office Worker

User Permission 1 – All Areas

Permission Schedule 1 – 8am-8pm M-F

Holidays 1 (selected)

An office is not staffed during a public holiday and you want to **prevent** access to the building to staff on this date. First we program the holiday dates in this section under “Holiday 1”, then go to Schedules and select “Holidays 1”, then assign that schedule to the User.

Menu 15 - Zone Types

Zones can be programmed to be one of 32 different zone configurations. Zones are fully configurable in the ZeroWire panel. These features are considered advanced programming and should only be changed with a thorough understanding of the operation of each bit.

Zone type profiles can also change depending on whether the areas they are in are armed or disarmed. This provides the ultimate flexibility in panel programming.

Zone Type Number

The ZeroWire can support a total of 32 Zone Types. Each Zone Type is identified by a unique number, which cannot be altered, and remains as the key reference for each Zone Type.

Zone Type Name

Each Zone Type can be configured with a custom 32 character name. The name is displayed wherever a Zone Type is referenced on the ZeroWire system.

Area Armed

Zone Attribute

See descriptions below; this is how the zone will behave when the partition it is in is armed.

- **Disabled:** Zone is disabled.
- **Entry 1:** Zone will follow entry/exit timer 1.
- **Entry 2:** Zone will follow entry/exit timer 2.
- **Handover:** Instant alarm type unless an entry zone is tripped first.
- **Instant:** Zone goes into alarm as soon as it is tripped.
- **Trouble Zone:** Zone reports zone trouble alarm and keypad sounds trouble beeps when tripped.
- **Fire:** Smoke detectors must be wired Normally Open. A short on a fire zone will create an alarm condition when the system is armed or disarmed. An open will create a Trouble condition that is always reported for this zone type, regardless of the Zone Trouble reporting option. After a fire activation, use the keypad to clear & reset fire detector by pressing Menu – 7 – Zone Reset.
- **Holdup delay:** When tripped, starts the holdup timer, if the timer is reached then a hold up alarm is sent.
- **Holdup reset:** When this zone is tripped, the holdup timer is stopped.

- **Keyswitch:** A momentary key switch can be used to arm/disarm the panel when it is momentarily shorted from a sealed condition. Use a 3.3K resistor for this zone type. Or, if DEOL monitoring is enabled in System Options, use two 3.3K resistors to allow full line monitoring.
- **Event Only:** This zone only creates an event when tripped and is stored in the event log.

Siren Attribute

Select from these 4 options to control what sound the siren makes when this zone goes into alarm.

- **Silent:** siren makes no sound
- **Steady:** constant siren sound
- **Yelping:** siren makes a yelping sound
- **Pulsing:** siren pulses on and off

Zone Attribute Options

- **Keypad Sounder:** If enabled, the panel will announce alarm, tamper, or trouble conditions. Default is on.
- **Report Delay:** If enabled, the panel will delay reporting zone activations until the next scheduled report. This setting is ignored if the zone is a Fire type and zone activations are reported immediately. When disabled zone activations (trip, bypass and restores) are reported immediately. Default is off.
- **No Keypad Display:** If enabled, any zone conditions, such as alarm and tamper, will not illuminate the Alarm Light. Conditions will still report and function as normal. Default is off.
- **Momentary Switch:** If enabled, the zone will not latch. If it is triggered again then it will send another report immediately. Default is off.
- **Zone Inhibit:** This feature is designed to reduce false alarms at arming/disarming. If enabled, a zone that is currently faulted that could cause an alarm condition will be temporarily bypassed when changing armed states.
This typically occurs when forced arming and the zone is unsealed, or when a schedule change occurs that changes the zone type. The bypass will be applied to the zone if it remains unsealed at the end of the exit timer.
“Inhibit” is removed when the zone restores at any time. This is different to a bypass, which is only removed at disarm.
Default is off.
- **Swinger Shutdown:** Default is off.

Area Disarmed

Zone Attribute

See descriptions above, this is how the zone will behave when the area it is in is disarmed.

Siren Attribute

See descriptions above, this is how the siren will behave when the area it is in is disarmed.

Zone Attribute Options

See descriptions above, this is how the zone will behave when the area it is in is disarmed.

Table 4: Default Zone Types

Default Number	Default Name	Zone Attribute	Siren Attribute	Keypad Sounder	Report delay	No Keypad Display	Momentary	Zone Inhibit
Armed								
1	Day Zone	Instant	Yelping	Y	N	N	N	N
2	24 Hour Audible	Instant	Yelping	Y	N	N	N	N
3	Entry Exit Delay 1	Entry 1	Yelping	Y	N	N	N	N
4	Entry Exit Delay 2	Entry 2	Yelping	Y	N	N	N	N
5	Follower	Handover	Yelping	Y	N	N	N	N
6	Instant	Instant	Yelping	Y	N	N	N	N
7	24 Hour Silent	Instant	Silent	N	N	N	N	N
8	Fire Alarm	Fire	Steady	Y	N	N	N	N
9	Entry Exit Delay 1 Auto-Bypass	Entry 1	Yelping	Y	N	N	N	Y
10	Entry Exit Delay 2 Auto-Bypass	Entry 2	Yelping	Y	N	N	N	Y
11	Instant Auto-Bypass	Instant	Instant	Y	N	N	N	Y
12	Event Only	Event Only	Silent	N	N	Y	N	N
13	Momentary Key Switch	Keyswitch	Silent	N	N	N	Y	N
14	Latching Key Switch	Keyswitch	Silent	N	N	N	N	N
15	CO Detector	Instant	Pulsing	Y	N	N	N	N

Disarmed								
1	Day Zone	Instant	Yelping	Y	N	N	N	N
2	24 Hour Audible	Instant	Yelping	Y	N	N	N	N
3	Entry Exit Delay 1	Entry 1	Yelping	Y	N	N	N	N
4	Entry Exit Delay 2	Entry 2	Yelping	Y	N	N	N	N
5	Follower	Handover	Yelping	Y	N	N	N	N
6	Instant	Instant	Yelping	Y	N	N	N	N
7	24 Hour Silent	Instant	Silent	N	N	N	N	N
8	Fire Alarm	Fire	Steady	Y	N	N	N	N
9	Entry Exit Delay 1 Auto-Bypass	Entry 1	Yelping	Y	N	N	N	Y
10	Entry Exit Delay 2 Auto-Bypass	Entry 2	Yelping	Y	N	N	N	Y
11	Instant Auto-Bypass	Instant	Instant	Y	N	N	N	Y
12	Event Only	Event Only	Silent	N	N	Y	N	N
13	Momentary Key Switch	Keyswitch	Silent	N	N	N	Y	N
14	Latching Key Switch	Keyswitch	Silent	N	N	N	N	N
15	CO Detector	Instant	Pulsing	Y	N	N	N	N

Menu 16 - Zone Options

Zones are fully configurable in the ZeroWire panel. These features are considered advanced programming and should only be changed with a thorough understanding of the operation of each bit.

Zone Option Number

The ZeroWire can support a total of 32 Zone Options. Each Zone Option is identified by a unique number, which cannot be altered, and remains as the key reference for each Zone Option.

Zone Options Name

Each Zone Option can be configured with a custom 32 character name. The name is displayed wherever a Zone Option is referenced on the ZeroWire system.

Zone Options

Bypassed Stay Mode

If enabled, this zone is automatically bypassed when the area is armed in stay mode. For example, it is an interior zone.

Force Arm Enabled

If enabled, this zone type may be unsealed while arming if forced arming is enabled in the area options. Normally all zones in an area must be sealed before a user can attempt to arm that area.

Bypass

If enabled, this zone may be bypassed.

Twin Trip

This zone type will require two triggers or another zone would have to have been triggered before it will activate an alarm.

EOL

Enable End Of Line resistor tamper monitoring.

Automatic Zone Test

If enabled, this test is controlled by action results automatic test on and off.

Night Mode

If enabled, sensor is bypassed in Stay Mode or Instant Stay Mode, and active in Stay Night Mode.

Zone Inactivity Test

If enabled, this zone will check for Zone Inactivity. The Zone Inactivity setting must be enabled under System Options > General Options. And the time is programmed in System Options > System Timers > Zone Inactivity Time.

Follow Any Armed Area

If enabled, and a zone is in more than 1 area it will create an alarm if triggered when any area is armed. If this feature is off then all the areas must be armed before the zone will become active.

If zone is type 10 zone (Interlogix Door/Window detector) then these two options apply:

- **Disable Internal Reed Switch** – tick this box when using external contacts.
- **Normally Open External Contact** – tick this box when external contact is normally open.

These two options appear in the Web Server – Settings – Zones page.

Table 5: Default Zone Options

Default Number	Default Name	Bypassed Stay Mode	Forced Arm Enabled	Bypass	Twin Trip Time	EOL	Automatic Zone Test	Zone Inactivity Test	Follow Any Armed Area	Alarms reporting	Alarm restore reporting	Bypass-Unbypass reporting	Zone Lost-Low Battery reporting	Zone trouble and restore reporting	Normally Open	Fast Loop	Zone Report Event
1	Bypass			x		x				x	x	x	x	x			134:BA
2	Bypass Stay	x	x		x					x	x	x	x	x			130:BA
3	Bypass – Forced Arm		x	x		x				x	x	x	x	x			134:BA
4	Bypass – Twin Trip			x	x	x				x	x	x	x	x			134:BA
5	Fire		x			x				x	x	x	x	x			110:FA
6	Panic		x			x				x	x	x	x	x			120:PA
7	Silent Panic					x				x	x	x	x	x			122:HA
8	Normally Open no EOL			x						x	x	x	x	x	x		130:BA
9	Normally Closed no EOL			x						x	x	x	x	x			130:BA
10	Gas Detected					x				x	x	x	x	x			151:GA
11	High Temp					x				x	x	x	x	x			158:KA

12	Water Leakage			x		x	x	x	x	x	154:WA
13	Low Temp			x		x	x	x	x	x	159:ZA
14	High Temp			x		x	x	x	x	x	158:KH
15	Fire Alarm Pull Station			x		x	x	x	x	x	110:FA
16	Blank	x	x	x		x	x	x	x	x	130:BA
17	Blank	x	x	x		x	x	x	x	x	130:BA
18	Blank	x	x	x		x	x	x	x	x	130:BA
19	Blank	x	x	x		x	x	x	x	x	130:BA
20	Blank	x	x	x		x	x	x	x	x	130:BA
21	Blank	x	x	x		x	x	x	x	x	130:BA
22	Blank	x	x	x		x	x	x	x	x	130:BA
23	Blank	x	x	x		x	x	x	x	x	130:BA
24	Blank	x	x	x		x	x	x	x	x	130:BA
25	Blank	x	x	x		x	x	x	x	x	130:BA
26	Blank	x	x	x		x	x	x	x	x	130:BA
27	Blank	x	x	x		x	x	x	x	x	130:BA
28	Blank	x	x	x		x	x	x	x	x	130:BA
29	Blank	x	x	x		x	x	x	x	x	130:BA
30	Blank	x	x	x		x	x	x	x	x	130:BA
31	Blank	x	x	x		x	x	x	x	x	130:BA
32	Blank	x	x	x		x	x	x	x	x	130:BA

Zone Reporting

Alarms Reporting

If enabled, this zone will report alarms.

Alarm Restores Reporting

If enabled, this zone will report alarms.

Bypass-Unbypass Reporting

If enabled, this zone will report bypasses and unbypass restores.

Zone Lost-Low Battery Reporting

If enabled, this zone will report loss of wireless supervision and low battery faults.

Zone Trouble and Restore

If enabled, this zone will report zone trouble and restores. Fire type zones will always report regardless of this option.

Zone Contact Options

These options apply to the hardwire inputs, not wireless zones.

Normally Open no EOL

If enabled, the zone circuit is normally open. Default is off.

Fast Loop

If enabled, the ZeroWire will be more sensitive and respond quicker to a change in state to hardwired zones. For example, we could enable this on a door contact to trigger the turning on of lights quicker when someone opens the door by using an Action. Depending on the application this may increase the chance of a false alarm if the zone is used for intrusion detection.

Zone Report Event

Select the CID and SIA event code to report when this zone is tripped. Refer to Appendix 1: Reporting Zone Codes in Contact I.D. on page 86.

Menu 17 - Event Lists

Event Lists are monitored by Channels to determine if they should be reported. Only events on a Channel's associated Event List will be reported.

Event List Number

The ZeroWire can support a total of 16 Event Lists. Each Event List is identified by a unique number, which cannot be altered, and remains as the key reference for each Event List.

Event List Name

Each Event List can be configured with a custom 32 character name. The name is displayed wherever an Event List is referenced on the ZeroWire system.

Event List

Select the events that you want to be part of this Event List.

- | | |
|---------------------------|-----------------------------------|
| 1. Alarms | 12. Reporting Trouble |
| 2. Alarm Restores | 13. AC Failure |
| 3. Arm/Disarm | 14. Low Battery |
| 4. Bypass/Restore | 19. Log Full |
| 5. Zone Trouble/Restore | 20. Auto Test |
| 6. Zone Tamper/Restore | 21. Start/End Programming |
| 7. Zone Lost | 22. Start and End Remote Download |
| 8. Zone Low Battery | 23. System Troubles |
| 9. Cancel Code | 24. Access Events |
| 10. Recent Arm/Exit Error | 25. Video Events |
| 11. Tamper | |

Menu 18 - Channel Groups

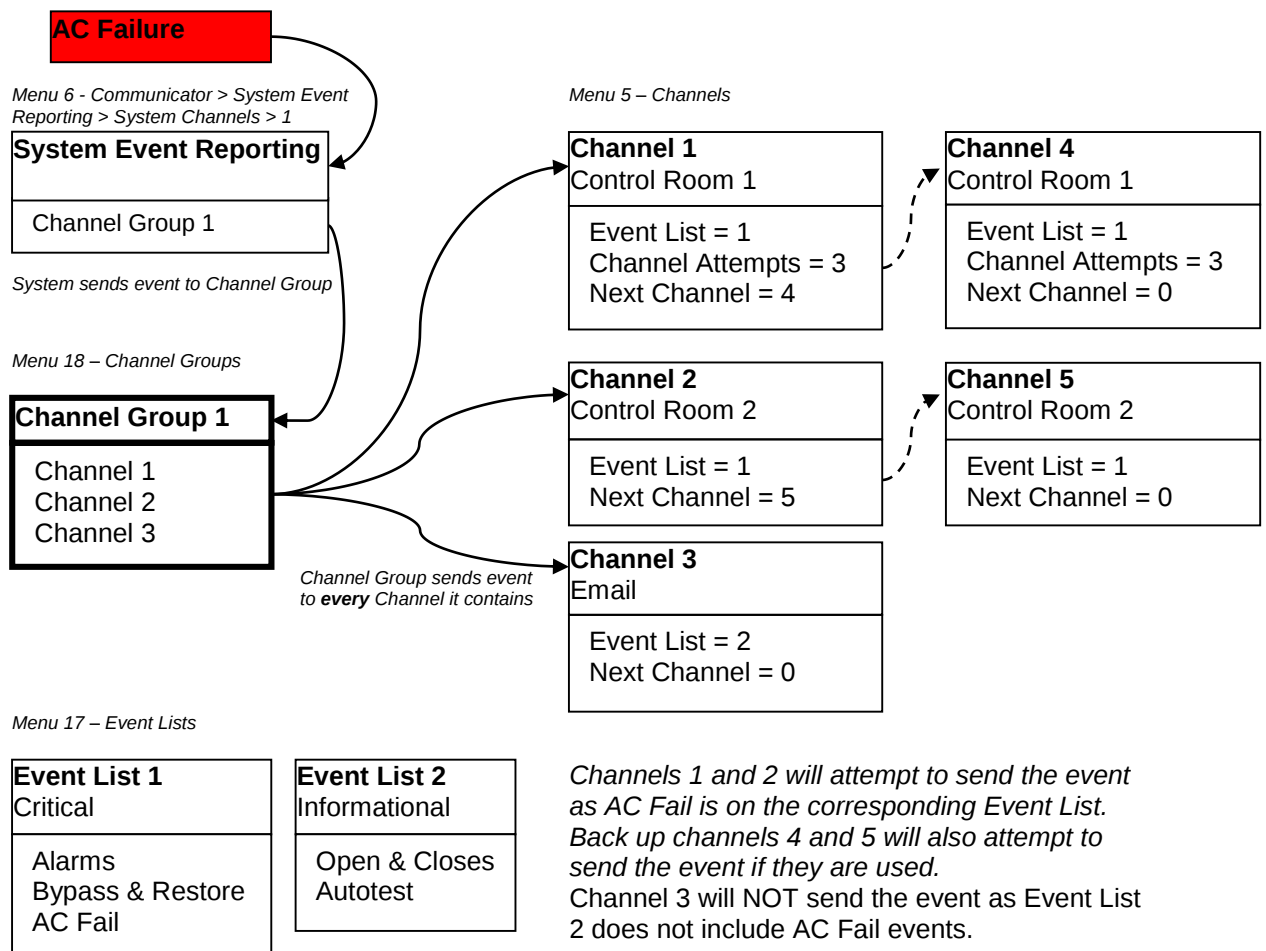
The ZeroWire provides you powerful and flexible reporting capability through its Channel feature. They are fully configurable to suit your needs by allowing you to specify what events to report to single and multiple destinations, with multiple levels of back up paths.

The relevant menus are:

- Channels
- Channel Groups
- Event List

When a system event occurs, it is routed to the System Event Channel Group (Communicator\System Event Reporting\System Channels). The Channel Group will forward the event to each of the Channels it contains. If the event is on the Channel's Event List, the Channel will attempt to send the event to the Channel's destination.

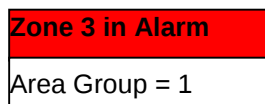
Example



If a zone or area event is generated, then the event is sent to the Channel Group specified (Area > Area Event Reporting > Channel Group) in the lowest area the zone belongs to. The Channel Group forwards the event to each of the Channels it contains. Each Channel checks its Event List to determine if the event should be sent.

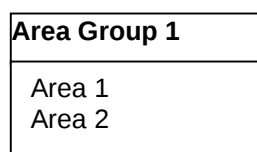
Example

Menu 3 – Zones



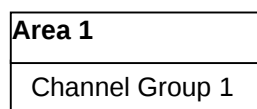
Zone sends alarm to area group

Menu 12 – Area Groups



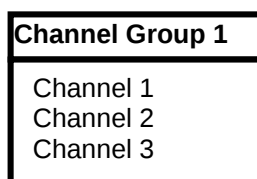
Event sent to **lowest** area

Menu 4 – Areas



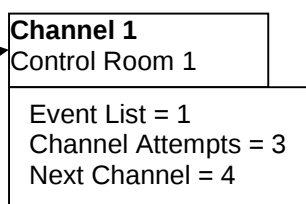
Area sends event to Channel Group

Menu 18 – Channel Groups

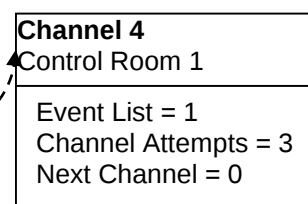


Channel Group sends Event to **every** Channel It contains

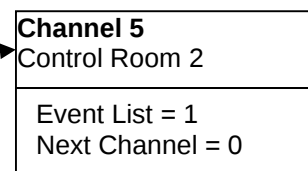
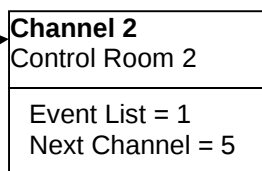
Menu 5 – Channels



Channel checks to see if the event is on its Event List, if yes it will attempt to send, if not then it stops



If it does not succeed after Channel Attempts, it will try sending on the next Channel



Channel Group Number

The ZeroWire can support a total of 16 Channel Groups. Each Channel Groups is identified by a unique number, which cannot be altered, and remains as the key reference for each Channel Group.

Channel Group Name

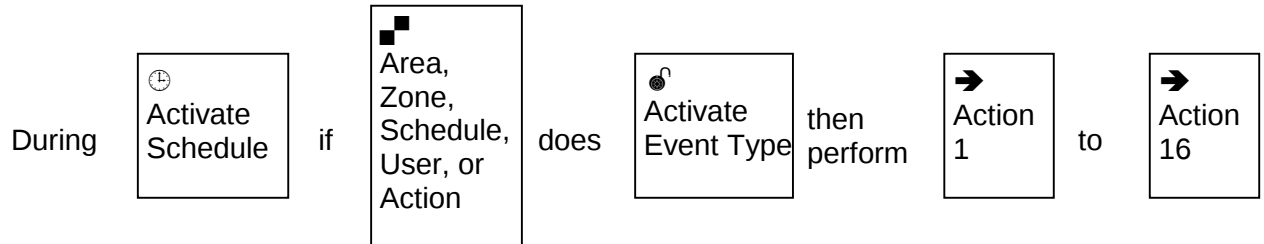
Each group can be configured with a custom 32 character name. The name is displayed wherever an Action Group is referenced on the ZeroWire system.

Channel Group

For each Channel Group, select the Channels where the event should be sent.

Menu 19 - Scenes

Each scene can trigger up to 16 scene actions when a certain condition is met. This can save users time by automatically running multiple actions. A scene can be triggered manually, through a schedule, or via a system event.



Scene Number

The ZeroWire can support a total of 16 Scenes. Each Scene is identified by a unique number, which cannot be altered, and remains as the key reference for each Scene.

Scene Name

Each Scene can be configured with a custom 32 character name. The name is displayed wherever a Scene is referenced on the ZeroWire system.

Activate Schedule

Select the Schedule that controls when this Scene is active. If the current date and time is outside of the selected schedule, then the Scene will not run.

Activate Event Type

Select the event that will trigger this Scene. Reference the Table 6: Activate Events Types table on page 82.

Activate Zone

Select which Area \ Zone \ Schedule \ User \ Action \ Device will provide the trigger.

Scene Actions

Each scene can perform up to 16 Scene Actions. These are simplified actions that allow you to control devices on your system. There are two types of Scene Action - Alarm System Action and Z-Wave Device Action.

Alarm System Action

- **Result Type:** The event of the Action Result to perform. Reference the Table 7 on page 83.
- **Result Number:** Select the area / scene / camera number to control.

Z-Wave Device Action

To display Z-Wave Action Types you must first learn in a Z-Wave device. The Z-Wave device name will then appear.

- **Action Device:** select the Z-Wave device you want to control
- **Z-Wave Type 8 Setting 1:** depends on Z-Wave device. May include options such as On, Off, Heat, Cool, Auto, Up, Down, Lock, Unlock.
- **Z-Wave Type 8 Setting 2:** depends on Z-Wave device
- **Z-Wave Type 8 Setting 3:** depends on Z-Wave device
- **Z-Wave Type 8 Setting 4:** depends on Z-Wave device
- **Z-Wave Type 8 Setting 5:** depends on Z-Wave device
- **Z-Wave Type 8 Setting 6:** depends on Z-Wave device
- **Z-Wave Type 8 Setting 7:** depends on Z-Wave device
- **Z-Wave Type 8 Setting 8:** depends on Z-Wave device

Table 6: Activate Events Types

Scene Event Type	Scene Event Type
Disabled	Area Siren
Zone Open	Area Fire Siren
Zone Not Open	User PIN Entered
Zone Alarm	Action Function True
Area On Away	Action Function False
Area On + Bypass	Schedule Activated
Area On Stay	Schedule Deactivated
Area Not On Away	Smoke Power Reset
Entry Delay	Turn On By User
Exit Delay 1	Turn Off By User
Exit Delay 2	Geosphere 1 Entered
Area Zone Bypass	Geosphere 1 Exited
Area Tamper	Geosphere 2 Entered
Area Not Ready	Geosphere 2 Exited
Area Zone Low Battery	Key A
Area Zone Supervision Fault	Key B
Area Alarm	Key C
Area Burg Alarm	Siren On
Area Fire Alarm	Z-Wave Devices
Area Panic Alarm	
Area Auxiliary Alarm	

Table 7: Scene Action and Scene Action Events Types

Scene Action	Action Event Type
Alarm System Action	Disabled
	Zone Bypass
	Turn On Away
	Turn Off
	Turn On Stay
	Reset Autoarm Timer
	Turn On Away, No Auto Stay
	Chime On
	Chime Off
	Activate Scene
	Trigger Camera Video Clip
	Send Area Notification
	Send Zone Notification
	Send Notification
	Start Siren
The available functions depend on the Z-Wave device(s) installed. Here are some examples:	
Z-Wave Device Action	Disabled
	On
	Off
	Heat
	Cool
	Auto
	Cool Set Point
	Heat Set Point
	Lock
	Unlock

Menu 20 - Speech Tokens

ZeroWire allows you to customize the name of zones.

There is a library of pre-recorded tokens (see "Appendix 6: Voice Library" on page 91) you can use to create the desired name.

Zones Tokens

Zone Number

- Name Token 1
- Name Token 2
- Name Token 3
- Name Token 4
- Name Token 5
- Name Token 6
- Name Token 7
- Name Token 8

Menu 21 - Cameras

ZeroWire allows you to add up to 16 IP cameras that can be triggered to record using Action Results. Only specific camera models for ZeroWire are supported.

Camera Number

Camera Name: name of the camera. Each camera can be configured with a custom 32-character name. The name is displayed wherever a Camera is referenced on the system.

LAN IP address: the local IP address of the camera. The camera must be on the same subnet as the panel.

MAC Address: The unique MAC address of the camera. This is required to register the camera with UltraSync.

Menu 22 - UltraSync

ZeroWire can establish a secure VPN connection to UltraSync Servers to allow simplified set up and configuration of email reporting and remote access features.

The server addresses are pre-programmed and SHOULD NOT be modified unless you are instructed to by technical support staff.

Web Access Passcode

This 8 digit code is required to allow remote access to your ZeroWire system via a smartphone app. Set this to 00000000 to disable this feature.

UltraSync Ethernet Server 1

The IP address or server name of the primary UltraSync Ethernet server.

UltraSync Ethernet Server 2

The IP address or server name of the backup UltraSync Ethernet server.

UltraSync Ethernet Server 3

The IP address or server name of the backup UltraSync Ethernet server.

UltraSync Ethernet Server 4

The IP address or server name of the backup UltraSync Ethernet server.

UltraSync Wireless Server 1

The IP address or server name of the primary UltraSync wireless server.

UltraSync Wireless Server 2

The IP address or server name of the backup UltraSync wireless server.

UltraSync Wireless Server 3

The IP address or server name of the backup UltraSync wireless server.

UltraSync Wireless Server 4

The IP address or server name of the backup UltraSync wireless server.

Appendix 1: Reporting Zone Codes in Contact I.D.

The ZeroWire control panel has the ability to report Ademco Contact I.D. transmissions. Each report in Contact I.D. consists of an event code and the zone I.D. generating the alarm. The event code will come from the chart below and can be programmed in Zone Options.

Programmed Event Code	Contact I.D. Code	SIA Event Code	Description
0	Use default code for Zone Type	Use default code for Zone Type	
1	110	FA	Fire Alarm
2	120	PA	Panic Alarm
3	130	BA	Burglary Alarm
4	131	BA	Perimeter Alarm
5	132	BA	Interior Alarm
6	133	UA	24 Hour (Safe)
7	134	BA	Entry/Exit Alarm
8	135	BA	Day/Night Alarm
9	150	UA	Non Burglary 24 Hour
10	121	HA	Duress Alarm
11	122	HA	Silent Panic
12	100	MA	Auxiliary Alarm
13	123	PA	Audible Panic Alarm
14	137	TA	Tamper Alarm
15	602	RP	Periodic Test
16	151	GA	Gas Detected
17	158	KA	High Temp
18	154	WA	Water Leakage
19	140	QA	General Alarm
20	140	SA	General Alarm
21	159	ZA	Low Temp
22	158	KH	High Temp
23	115	FA	Fire Alarm Pull Station

Appendix 2: Reporting Fixed Codes in Contact I.D.

The table below lists the CID event codes sent for the following reports (if enabled). The number in *brackets* following the event is the number that will be reported as the zone number if extended Contact I.D. is enabled in the system options. Otherwise zone '0' will always be reported. If there are no parentheses, the zone will be reported as '0'.

Report	Contact I.D. Event		
Manual Test	601	AC Restore	301
Auto test Open (<i>user number</i>)	602	Box Tamper	137
Close (<i>user number</i>)	401	Box Tamper Restore	137
Cancel (<i>user number</i>)	406	Keypad Tamper	137
Download Complete	412	Keypad Panic	120
Start Program	627	Duress	121
End Program	628	Keypad Fire	110
Ground Fault	310	Keypad Medical	100
Ground Fault Restore	310	RF Zone Lost (<i>zone number</i>)	381
Recent Close (<i>user number</i>)	401	RF Zone Restore (<i>zone number</i>)	381
Exit Error (<i>user number</i>)	457	Zone Low Battery (<i>zone number</i>)	384
Event Log Full	605	Zone Battery Restore (<i>zone number</i>)	384
Fail To Communicate	354	Zone Trouble (<i>zone number</i>)	380
Expander Trouble	333	Zone Trouble Restore (<i>zone number</i>)	380
Expander Restore	333	Zone Tamper (<i>zone number</i>)	137
Telephone Fault	351	Zone Tamper Restore (<i>zone number</i>)	137
Telephone Restore	351	Zone Bypass (<i>zone number</i>)	570
Siren Tamper	321	Bypass Restore (<i>zone number</i>)	570
Siren Restore	321	Zone Inactivity	391
Aux Power Over Current	312	Late To Close	454
Aux Power Restore	312	Forced Door	423
Low Battery	309		
Low Battery Restore	309		
AC Fail	301		

Appendix 3: History Events

The table below lists events that can appear in the event log.

24 Hour Alarm	Expander DC Loss	Reserved
24 Hour Alarm Restore	Expander DC Loss Restore	Reserved Zone Event Types/Restores
Abort	Expander Low Battery	Zone Low Battery
Activity Monitor fail	Expander Low Battery Restore	Zone Low Battery Restore
Alarm Aborted	Fail To Close	Serial Bus Expansion Event
Automatic Test	Fail to Open	Siren Tamper
Battery Low Event	Fire Alarm	Siren Tamper Restore
Battery Low Event Restore	Fire Alarm Restore	Start Listen In
Box Tamper	Fire Maintenance Alarm	Start Local Program
Box Tamper Restore	Fire Maintenance Alarm Restore	Start Remote Program
Burg Alarm	Fire Supervision	Start Walk Test Mode
Burg Alarm Restore	Fire Supervision Restore	Start Zone Test
Bypass	First Open	System Device Bypassed
Bypass Restore	Ground Fault	System Device Unbypassed
Cancel	Ground Fault Restore	System Shut Down
Checksum Fault	Guard Tour Fail	System Turn On
Checksum Fault Restore	Code pad Lockout	Tamper
Clock Changed	Last Close	Tamper Restore
Close	Late Closing	Technician Arrival
Communication Failure	Late Opening	Technician Left
Communication Failure Restore	Mains Fail Event	Telephone Fault
Twin Trip initial trip	Mains Fail Event Restore	Telephone Fault Restore
Twin Trip initial trip Restore	Man Down	Trouble
Device Enrolled	Manual Audible Panic	Trouble Restore
Device Failure	Manual Fire	User Activated Output
Device Failure Restore	Manual Medical	Valid Code Entered
Door Access	Manual Silent Panic	Valid Code expired
Door Access Denied	Manual Test	Valid Code lost
Door Forced	Manual Test Restore	Valid Code out of Schedule
Door Forced	Open	Valid Code Void
Door Propped	Output Activated	Walk Test Fail
Door Propped	Output Restored	Walk Test Pass
Duress	Over Current	Watchdog Reset
Early Opening	Over Current Restore	Wireless Jam
Early Opening	Partial Close	Wireless Jam Restore
End Listen In	Partial Open	Wireless Supervision
End Local Program	Power Up	Wireless Supervision Restore
End Remote Program	Power Up Restore	Zone Activity Supervision
End Walk Test Mode	Recent Close	Zone Activity Supervision Restore
End Zone Test	Remote Program Fail	
Exit Error		

Appendix 4: Zone Options

Default Number	Default Name	Bypassed Stay Mode	Forced Arm Enabled	Bypass	Twin Trip Time	EOL	Automatic Zone Test	Zone Inactivity Test	Follow Any Armed Area	Alarms reporting	Alarm restore reporting	Bypass-Unbypass reporting	Zone Lost-Low Battery reporting	Zone trouble and restore reporting	Normally Open	Fast Loop	Zone Report Event
1	Bypass		x		x				x	x	x	x	x				134:BA
2	Bypass Stay	x	x		x				x	x	x	x	x				130:BA
3	Bypass – Forced Arm		x	x		x			x	x	x	x	x				134:BA
4	Bypass – Twin Trip			x	x	x			x	x	x	x	x				134:BA
5	Fire		x			x			x	x	x	x	x				110:FA
6	Panic		x			x			x	x	x	x	x				120:PA
7	Silent Panic					x			x	x	x	x	x				122:HA
8	Normally Open no EOL			x					x	x	x	x	x	x			130:BA
9	Normally Closed no EOL			x					x	x	x	x	x				130:BA
10	Gas Detected					x			x	x	x	x	x				151:GA
11	High Temp					x			x	x	x	x	x				158:KA
12	Water Leakage					x			x	x	x	x	x				154:WA
13	Low Temp					x			x	x	x	x	x				159:ZA
14	High Temp					x			x	x	x	x	x				158:KH
15	Fire Alarm Pull Station					x			x	x	x	x	x				110:FA
16	Blank		x	x		x			x	x	x	x	x				130:BA
17	Blank		x	x		x			x	x	x	x	x				130:BA
18	Blank		x	x		x			x	x	x	x	x				130:BA
19	Blank		x	x		x			x	x	x	x	x				130:BA
20	Blank		x	x		x			x	x	x	x	x				130:BA
21	Blank		x	x		x			x	x	x	x	x				130:BA
22	Blank		x	x		x			x	x	x	x	x				130:BA
23	Blank		x	x		x			x	x	x	x	x				130:BA
24	Blank		x	x		x			x	x	x	x	x				130:BA
25	Blank		x	x		x			x	x	x	x	x				130:BA
26	Blank		x	x		x			x	x	x	x	x				130:BA

Default Number	Default Name	Bypassed Stay Mode	Forced Arm Enabled	Bypass	Twin Trip Time	EOL	Automatic Zone Test	Zone Inactivity Test	Follow Any Armed Area	Alarms reporting	Alarm restore reporting	Bypass-Unbypass reporting	Zone Lost-Low Battery reporting	Zone trouble and restore reporting	Normally Open	Fast Loop	Zone Report Event
27	Blank	x	x		x				x	x	x	x	x				130:BA
28	Blank	x	x		x				x	x	x	x	x				130:BA
29	Blank	x	x		x				x	x	x	x	x				130:BA
30	Blank	x	x		x				x	x	x	x	x				130:BA
31	Blank	x	x		x				x	x	x	x	x				130:BA
32	Blank	x	x		x				x	x	x	x	x				130:BA

Appendix 5: Zone Types

Default Number	Default Name	Zone Attribute	Siren Attribute	Keypad Sounder	Report delay	No Keypad Display	Momentary	Zone Inhibit
Armed								
1	Day Zone	Instant	Yelping	Y	N	N	N	N
2	24 Hour Audible	Instant	Yelping	Y	N	N	N	N
3	Entry Exit Delay 1	Entry 1	Yelping	Y	N	N	N	N
4	Entry Exit Delay 2	Entry 2	Yelping	Y	N	N	N	N
5	Follower	Handover	Yelping	Y	N	N	N	N
6	Instant	Instant	Yelping	Y	N	N	N	N
7	24 Hour Silent	Instant	Yelping	Y	N	N	N	N
8	Fire Alarm	Fire	Steady	Y	N	N	N	N
9	Entry Exit Delay 1 Auto-Bypass	Entry 1	Yelping	Y	N	N	N	Y
10	Entry Exit Delay 2 Auto-Bypass	Entry 2	Yelping	Y	N	N	N	Y

11	Instant Auto-Bypass	Instant	Instant	Y	N	N	N	Y
12	Event Only	Event Only	Silent	N	N	Y	N	N
13	Momentary Key Switch	Keyswitch	Silent	N	N	N	Y	N
14	Latching Key Switch	Keyswitch	Silent	N	N	N	N	N
15	CO Detector	Instant	Pulsing	Y	N	N	N	N

Disarmed								
1	Day Zone	Instant	Yelping	Y	N	N	N	N
2	24 Hour Audible	Instant	Yelping	Y	N	N	N	N
3	Entry Exit Delay 1	Entry 1	Yelping	Y	N	N	N	N
4	Entry Exit Delay 2	Entry 2	Yelping	Y	N	N	N	N
5	Follower	Handover	Yelping	Y	N	N	N	N
6	Instant	Instant	Yelping	Y	N	N	N	N
7	24 Hour Silent	Instant	Yelping	Y	N	N	N	N
8	Fire Alarm	Fire	Steady	Y	N	N	N	N
9	Entry Exit Delay 1 Auto-Bypass	Entry 1	Yelping	Y	N	N	N	Y
10	Entry Exit Delay 2 Auto-Bypass	Entry 2	Yelping	Y	N	N	N	Y
11	Instant Auto-Bypass	Instant	Instant	Y	N	N	N	Y
12	Event Only	Event Only	Silent	N	N	Y	N	N
13	Momentary Key Switch	Keyswitch	Silent	N	N	N	Y	N
14	Latching Key Switch	Keyswitch	Silent	N	N	N	N	N
15	CO Detector	Instant	Pulsing	Y	N	N	N	N

Appendix 6: Voice Library

These words can be used to customize your zone names (see "Menu 20 - Speech Tokens" on page 84).

0	zero	11	eleven	22	forty
1	one	12	twelve	23	fifty
2	two	13	thirteen	24	sixty
3	three	14	fourteen	25	seventy
4	four	15	fifteen	26	eighty
5	five	16	sixteen	27	ninety
6	six	17	seventeen	28	hundred
7	seven	18	eighteen	29	thousand
8	eight	19	nineteen	30	air conditioner
9	nine	20	twenty	31	area
10	ten	21	thirty	32	attic

33	automatic	73	glass	113	pool
34	auxiliary	74	glass break	114	rear
35	back	75	ground	115	reception
36	basement	76	guest	116	remote
37	bathroom	77	gun	117	roof
38	bedroom	78	gym	118	room
39	boat	79	hall	119	rumpus
40	cabinet	80	hallway	120	safe
41	car park	81	heat	121	security
42	ceiling	82	heating	122	zone
43	cellar	83	hold-up	123	shed
44	childs	84	home	124	shock
45	alert	85	home theatre	125	shop
46	closet	86	infrared	126	side
47	computer	87	inside	127	skylight
48	cool	88	instant	128	sliding
49	curtain	89	interior	129	small
50	data	90	key switch	130	smoke
51	den	91	keychain	131	south
52	detector	92	kitchen	132	stairs
53	dining	93	lounge	133	storage
54	door	94	laundry	134	study
55	downstairs	95	lift	135	temperature
56	driveway	96	light	136	spare
57	duress	97	living	137	toilet
58	east	98	location	138	training
59	emergency	99	master	139	TV
60	entry	100	medicine	140	upstairs
61	family	101	meeting	141	user
62	fan	102	motion	142	utility
63	fence	103	night	143	volt
64	fire	104	north	144	veranda
65	forced arm	105	nursery	145	wall
66	foyer	106	office	146	warehouse
67	freezer	107	output	147	water
68	front	108	outside	148	west
69	games	109	panic	149	window
70	garage	110	pantry	150	windows
71	gas	111	partial	151	wireless
72	gate	112	perimeter	152	yard

Appendix 7: App and Web Error Messages

Various error messages may appear on the ZeroWire Web Server and UltraSync + app.

Advanced/Settings Configuration Menus

"You must select a Menu before you can scroll" – An attempt was made to scroll up or down from the top level menu.

"Select a submenu from the list or select back to access the main menu" – An attempt was made to scroll up or down from a submenu that has no additional levels

"Defaulting requires 2 levels" – a Shortcut was entered without two levels.

Read Write errors and results

"Write Access Denied"

"Nothing displayed can be Saved"

"Program Success!"

"Name Saved"

Zones Page

"No Zones Configured For Your Access" – Displayed on Zones page when there are no zones available to view

WiFi

"Connection Was lost before a response was received" – Sent when No response received on a WiFi network change

Data Entry Errors

"Data must only contain the following characters"

"Date must be of the form YYYY–MM–DD."

"Day must be from 1 to 31"

"Data entry must only contain the numbers 0 – 9 and A–F"

"Data entry must only contain the numbers 0 – 9"

"Data must be a number from X to Y"

"Improper Time Value"

"must be 4 to 8 digits"

"You must enter a user Number between 1 and 1048575"

"PIN digits must be between 0 and 9"

"PIN Must be 4–8 digits from 0–9"

"Data must not contain the following characters []"