

ZeroWire



Wireless security & home automation



Installation manual

ZeroWire - v 1.0

P/N 466-2520 • REV 01 • DRAFT 00.05

Copyright	© 2014 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	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.  2002/96/EC (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.
Contact information	For contact information, see www.utcfireandsecurity.com
Customer support	For customer support in EU, see www.utcfssecurityproducts.eu .

Content

Important information iii

Limitation of liability iii

Advisory messages iii

Welcome 1

Features and benefits 1

Your new security system 2

Optional parts: 2

Front of ZeroWire 3

Back of ZeroWire 4

Install Your ZeroWire 5

What You Need 5

Choose a Location 5

Install the Battery 5

Install Cellular Radio 6

Install ZeroWire on Wall 6

Connect Power 8

Add Your Sensors 9

Unpack Sensors 9

Learning Sensors into ZeroWire 9

Install Sensor in Home 9

Remove a Sensor 10

Add Users and Keyfobs 11

Introduction 11

Add a User 11

Add a Key Fob 11

Remove a User 12

Change User Type 12

Customize Your ZeroWire 13

Volume Level 13

Voice Annunciation 13

Full Menu Annunciation 13

Backlight Level 14

Change Time and Date 14

Adjust Partition Entry or Exit Times 15

Configure Sensor Names 15

Record Sensor Names 16

Maintenance 17

System Tests 17

Perform a Walk Test	17
Perform a Siren Test	17
Perform a Battery Test	18
Perform a Communicator Test	18
Advanced Installation	19
Reset to Factory Default	19
Reset Installer Account	19
Switch Connection Modes	19
ZeroWire Web Server	20
Connecting Inputs	31
Connecting Outputs	32
Changing Keyfob Options	34
Add IP Cameras	34
Viewing Cameras	35
Programming Cameras	36
View Camera Clips	38
Add Z-Wave Devices	39
Access via UltraConnect App	40
Using the App	42
DLX900 Software	45
System Status Messages	47
UltraConnect App Status and Error Messages	48
Voice Library	50
ZeroWire Menu Tree	51
Upgrading Firmware using USBUP	52
Upgrading Firmware using DLX900	53
Specifications	54
Index	55

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.

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.

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.

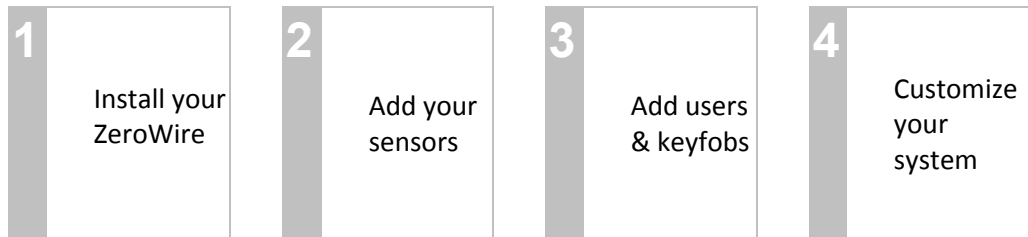
Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

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.

Welcome

Thank you for purchasing ZeroWire!

ZeroWire can be set up in 4 steps and the voice guide will walk you through each of the menus and settings.



Instead of using the keys on the front of ZeroWire, you can also set up the system with the built-in web server interface using a browser (see "ZeroWire Web Server" on page 20).

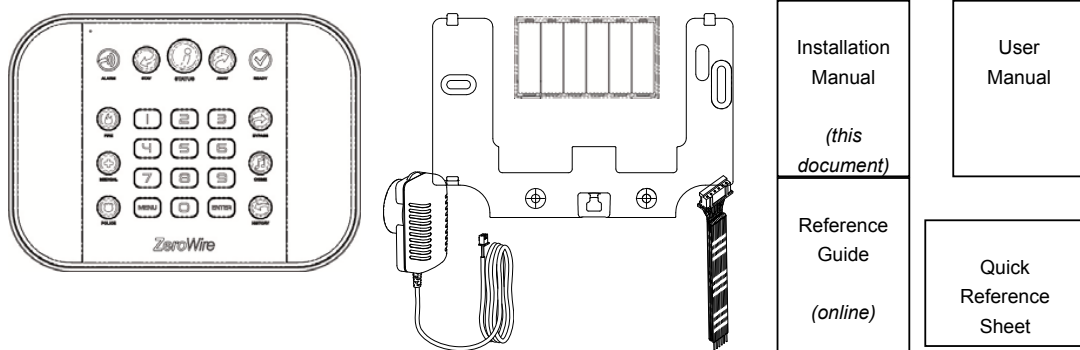
Please read through this guide before starting the installation.

Features and benefits

- 255 Users – enough for even moderate sized businesses
- 64 Sensors + 25 Keyfobs – provides a large coverage area
- 8 Partitions – split your system into smaller parts you can protect individually
- Dynamic Key Lighting – lights up the available options to make it easier to program
- Personal Voice Guide – steps you through customizing your system
- 2 Inputs – integrate non-wireless devices to your security system
- 2 Programmable Outputs – connect other devices such as siren and strobe
- Loud internal piezo siren – warns intruders they have been detected and encourages them to leave quickly
- Modern self contained unit – all in one box
- Battery backup – your property is still protected if there is a loss of power
- 802.11 b/g WiFi – enables remote access via a web browser or smart phone
- IEEE 802.3 Compliant Ethernet – use hardwired cable instead of wireless, the choice is yours
- 3G Cellular radio support – allows reporting alarm messages without a fixed line telephone service

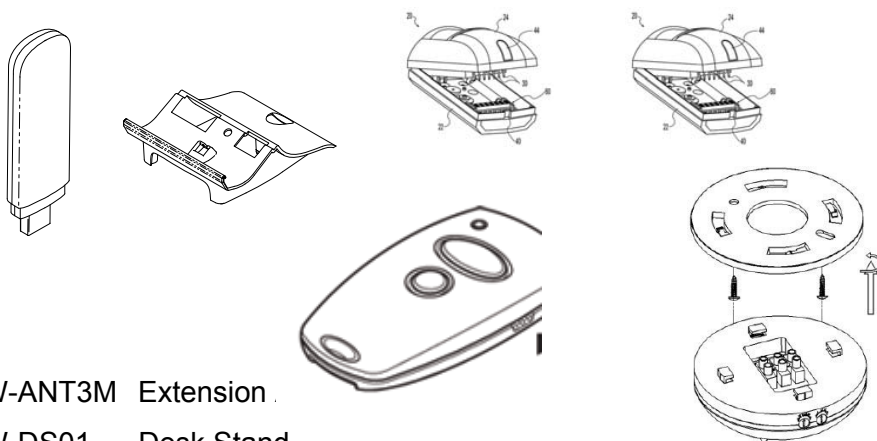
Your new security system

Check that everything is complete before beginning your installation. If anything is missing please contact the customer service.



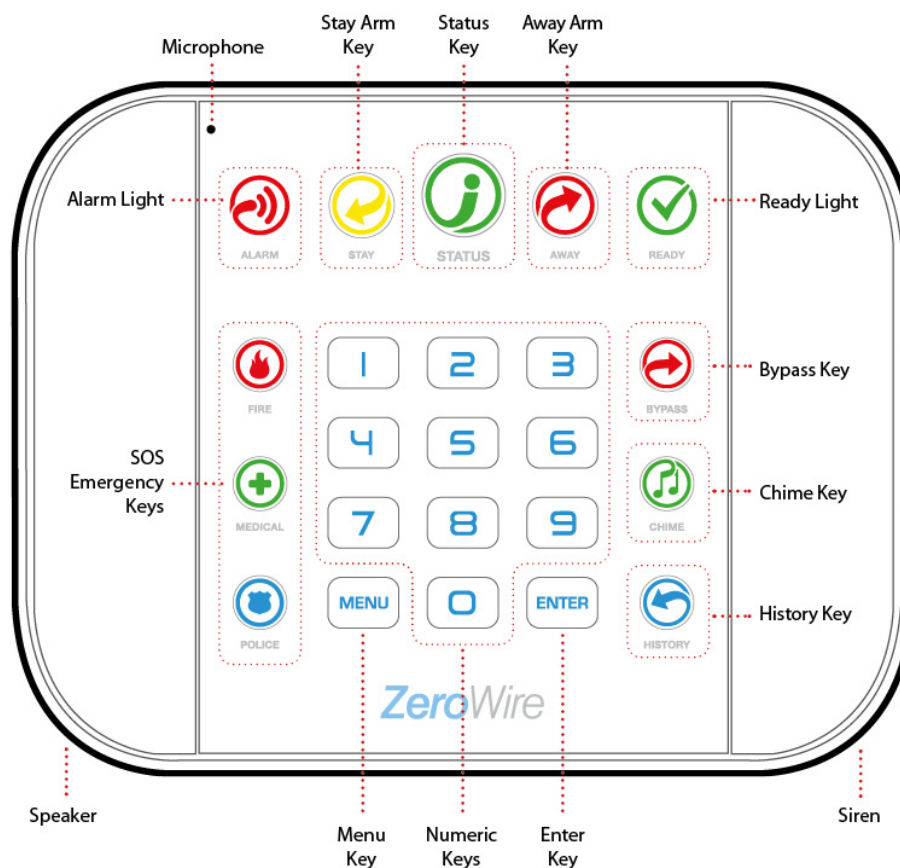
- ZeroWire with Wall Bracket
- 9 VDC Power Pack
- Backup Battery Pack
- Input/Output Lead
- Installation Manual (this document)
- User Manual
- Quick Reference Guide

Optional parts:



- ZW-ANT3M Extension
- ZW-DS01 Desk Stand
- ZW-HSPA Cellular Modem
- Wireless Sensors
- Wireless Keyfobs

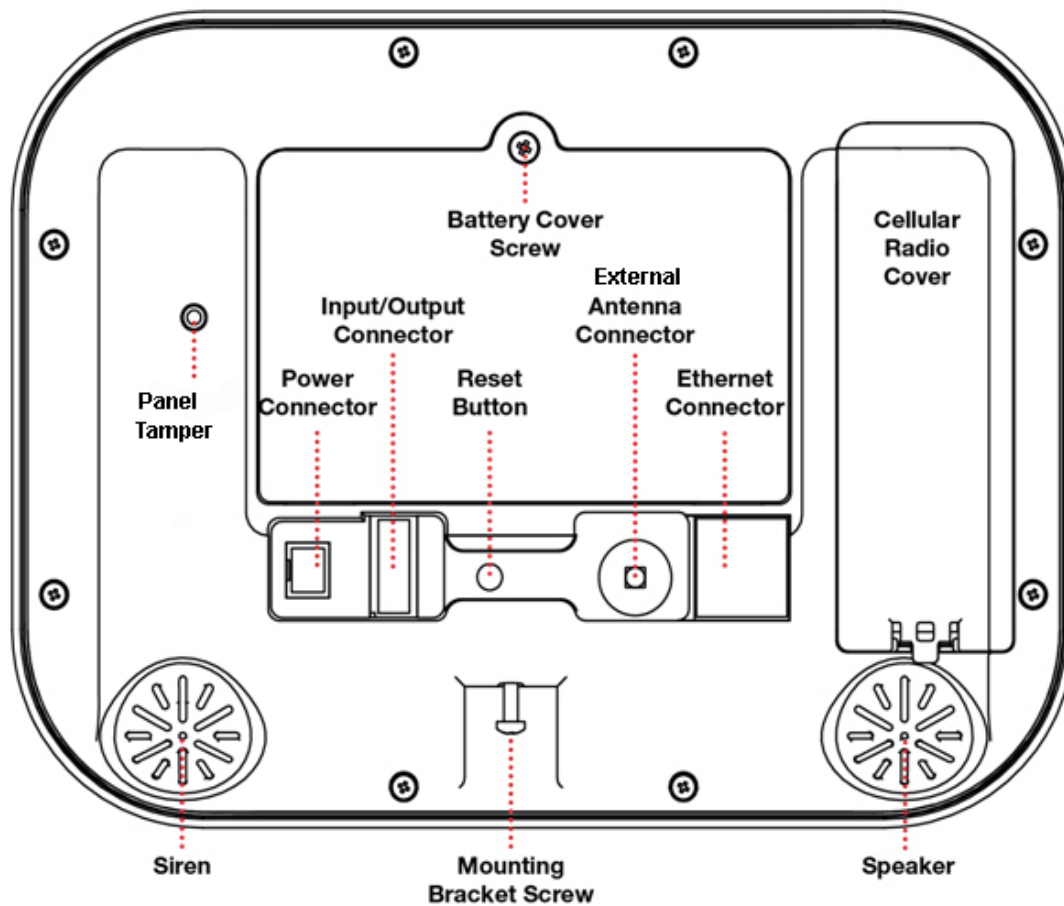
Front of ZeroWire



Key	Colour	Description
 ALARM	Red	System is in alarm. Enter your PIN code then ENTER to turn off the alarm. Press STATUS key for more info.
 STAY	Not lit Yellow	System is disarmed if Away is also not lit. Press the STAY key to arm in Stay mode. System is armed in the "STAY" mode.
 STATUS	Green Yellow Red (steady)	System is normal. Non-urgent system conditions present. Press the STATUS key to hear system conditions. Urgent system conditions present. Touch the STATUS key to hear system messages. If you are unable to fix the issue, contact your service provider for help.
 AWAY	Not lit Red	System is disarmed if Stay is also not lit. Press the AWAY key to arm in Away mode. System is armed in the "AWAY" mode.
 READY	Not lit	System cannot be armed, press STATUS key for more info.

Key	Colour	Description
 READY	Green (steady) Green (flashing)	All sensors are ready and the system can be armed in Away or Stay mode. Sensors are currently unsealed but system is force-armable. If these sensors are not sealed by the end of the exit time the system will go into alarm.
 BYPASS		Press the BYPASS key if you wish to isolate (ignore) a sensor. Bypassed sensors will not be active when you arm the system in Stay or Away modes.
 CHIME		Press the CHIME key to select which sensors will make a doorbell sound on the ZeroWire when they are tripped.
 HISTORY		Press the HISTORY key to listen for alarm and event history.
FIRE MEDICAL POLICE		Feature must be enabled by your security provider. Check what response will be provided. Hold down the key to send a message to a central monitoring centre. Enter your PIN code then ENTER to turn off a SOS alarm.

Back of ZeroWire



Connections for the cellular radio module are located under the cover on the right.

Install Your ZeroWire

What You Need

- ZeroWire and everything inside the box
- Sensors and key fobs you will add
- List of users and PIN codes you wish to add
- Wall socket for powering ZeroWire
- Small Phillips head screwdriver
- Small Flathead screwdriver
- Router supporting 802.11 b or 802.11g if using local WiFi features
- Optional – desk stand
- Optional – internal or external siren and strobe

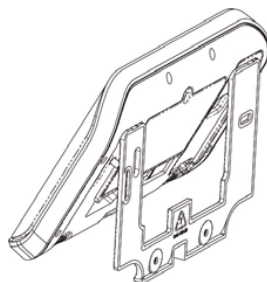
Choose a Location

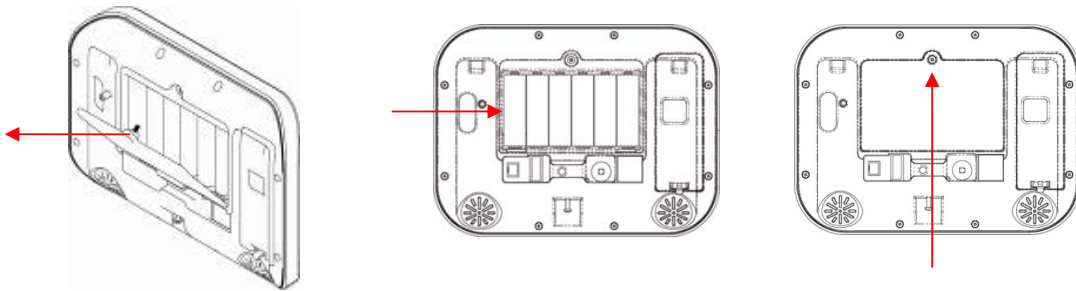
When choosing a location for your ZeroWire there are a number of appliances and areas to avoid which could interfere with the security system.

- Choose a central location for the best reception to all wireless sensors and Z-Wave devices
- If the ZeroWire Cellular Radio is installed select a location with sufficient signal
- Avoid TV and other electronic appliances
- Avoid microwave ovens
- Avoid wet and moist partitions such as bathrooms and toilets
- Avoid cordless telephones
- Avoid computers and wireless equipment

Install the Battery

1. Loosen the screw from a bottom of ZeroWire, this will allow the wall bracket to be removed from the unit.





2. Remove battery cover with a small screwdriver.
3. Connect battery pack lead to connector on left.
4. Replace battery cover and screw.

Note: The battery wire cannot be under the battery or the cover will not fit properly.

Note: The battery is not designed as a long-term power source. Plugging in the battery should be followed quickly with the plugging in of the DC power supply.

Install Cellular Radio

If the ZeroWire Cellular Radio installation is planned it should be done before plugging in the main DC power cord. Refer to the ZeroWire Cellular Radio installation Manual for details.

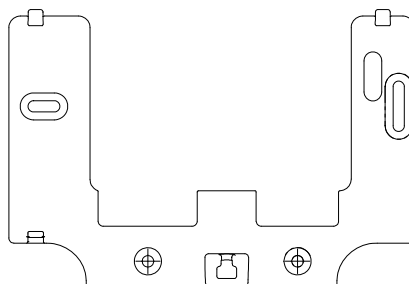
1. Check the radio signal strength (see "3G Cellular Radio Setup" on page 26).
2. Ensure the Signal Strength is -87 to -51 dbm.



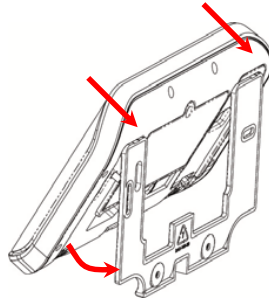
3. If it is too low, move the unit to the location with better signal or install an external antenna.

Install ZeroWire on Wall

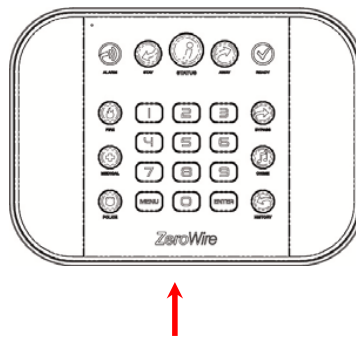
1. Install the bracket on a wall by using the supplied screws. Make sure the power lead can reach the ZeroWire when plugged in to a power source.



2. Align the ZeroWire to the top clips on the wall bracket, then slide the ZeroWire in to place so it sits flat against the wall.

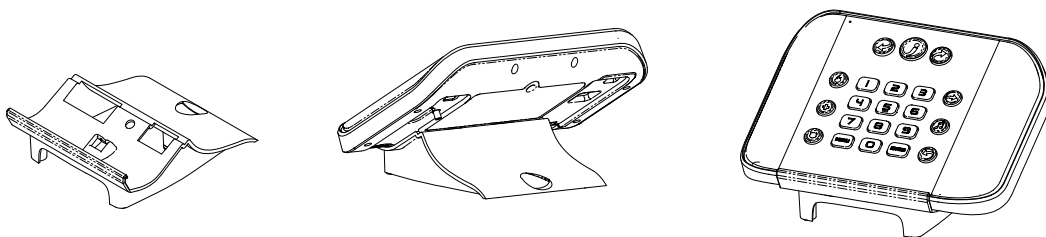


3. Use a screwdriver to tighten the screw you loosened previously.



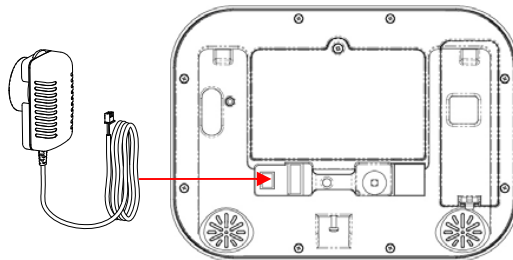
You may enable the box tamper feature from the System Menu – General Options via the ZeroWire Web Server. This will cause an alarm to occur if the ZeroWire is removed from the wall.

If you do not wish to install the product on a wall, you may use the optional table bracket to place the ZeroWire on a secure flat surface.



Connect Power

1. Connect a DC power lead from power pack to the back of the ZeroWire, it only fits when inserted in the correct direction. Make sure a correct polarity is observed.



2. Connect the power pack to its own power outlet and turn it on.
 - **CAUTION:** Wall tamper is an optional security feature that is disabled by default. When enabled it will sound the siren when power is connected. Press 9 7 1 3 Enter to turn the siren off. If this does not work, proceed to "Reset Installer Account" on page 19 to enable this code.
 - Lights should be lit on the ZeroWire when the power is turned on. If not check that the power lead is connected securely to the rear of the ZeroWire.
 - Avoid using multiple power adapters and power boards.

Note: ZeroWire should be connected to a power source at all times. The battery is a backup power source, and the ZeroWire is designed to run on the battery pack during a power failure only, and NOT for prolonged periods of time.

Add Your Sensors

Unpack Sensors

These instructions are for general information only. Please refer to the manual included with each sensor for further details.

1. Remove the sensor from packaging.
2. Remove a battery cover of the sensor.
3. Install batteries taking care to insert them correctly. Batteries inserted with reverse polarity may damage the sensor.

Learning Sensors into ZeroWire

Example: Add a PIR motion detector to ZeroWire and assign it as sensor 1.

1.   Select Sensor Configuration.
2.  Enter your Installer code.

3.  Select 1 to add sensor.
4.  Activate the sensor learn-in sequence (see specific wireless sensor manual for instructions).
ZeroWire will announce that the sensor or keyfob is detected.
5.   Assign the sensor as sensor number 1, or just press Enter to automatically assign a number. Press 1-6 for the sensor group.
6.    Exit from the menu.

Install Sensor in Home

1. Replace battery cover.
2. Install sensor in a suitable location. Here are some tips:
 - Wireless sensors feature low power transmission to maximize battery life. This means you should place the ZeroWire in a central location and install sensors as close to the ZeroWire as possible.
 - Signals from each sensor will reduce in strength as they pass through different building materials with brick and concrete absorbing more of the signal.
 - Keep sensors away from household appliances and metal surfaces (e.g. refrigerator, TV, washing machine, garage door). Metal surfaces will reflect the signal away.

- If you have a double-storey property, it is suggested the ZeroWire unit be installed on the highest level for the best signal strength.
 - ZeroWire installed below ground level (e.g. basement) may have reduced range.
 - Movement / Passive Infra-Red (PIR) sensors should be installed to look over the partition you want to protect. The path of an intruder should walk across the front of the PIR. A PIR is less sensitive to an intruder walking directly towards it. Avoid pointing the PIR at windows or heat sources as these may cause the PIR to operate incorrectly.
 - Reed switches should be installed across doors/windows where two surfaces open and close. Place the sensor on the frame and the magnet on the door/window. Take care to close the door / window and note any gap between the magnet and the sensor. If the gap is large the sensor will always be in an open state and prevent you from arming / disarming the system. A plastic spacer can be used to ensure the reed switch seals correctly.
4. Use Menu 4 – 4 to test sensor signal level.

If signal is low, then move sensor to another location. Alternatively move your ZeroWire to a more central location.

Remove a Sensor

Example: Remove sensor 8

- | | | |
|----|---|--|
| 1. |   | Select Sensor Configuration. |
| 2. |  | Enter your Installer code. |
| |  | |
| 3. |  | Select 2 to remove sensor or keyfob. |
| 4. |  | Select 2 to remove sensor. |
| 5. |   | Select the sensor number that needs to be removed. |
| 6. |    | Exit from Advanced system configuration. |

Add Users and Keyfobs

Introduction

ZeroWire allows you to add up to 255 users. Each user is assigned a PIN code and a user number. This allows them to interact with the system.

Add a User

Example: Add a new user to ZeroWire and assign them a PIN code 2580. We will add this as user 4.

1.  Select User Configuration menu.
2.  Enter your Installer code.

3.  Select 1 to configure user PIN.
4.  Select user 4.
5.  Set user 4 PIN code as 2580.
6.  Exit from Advanced system configuration.

Add a Key Fob

Example: Add a new key fob and assign it as sensor 65

1.  Select Sensor Configuration.
2.  Enter your Installer code.

3.  Select 1 to add a keyfob.

4. Activate the keyfob learn-in sequence (see specific wireless keyfob manual for instructions).
ZeroWire will announce that the keyfob is detected.
5.  Select the number that will be assigned to this keyfob, followed by Enter. Press Enter for the next keyfob.
6.  Exit from the menu.

Remove a User

Example: Remove user 4 from your system

1.   Select User Configuration menu.
2.  Enter your Installer code.
3.  Select 1 to configure user PIN.
4.  Select user 4.
5.   Press Bypass to disable the selected user's PIN code.
6.  Exit from the menu.
7.    Exit from the menu.

Change User Type

Example: Change user 6 to a master user (installer) and allow to add/remove other users.

1.   Select User Configuration menu.
2.  Enter your Installer code.
3.  Select 2 to configure user type.
4.  Select the user number.
5.   Select 2 for the installer user type (available options: 1-Standard, 2-Installer, 3-Arm Only.).
6.  Exit from the menu.
7.    Exit from the menu.

Customize Your ZeroWire

Volume Level

Example: Set volume level to 6

1.   Select main menu - Option 1, Volume level.
2.  Set volume level to 6.
3.   Exit from the menu.

Voice Annunciation

Example: Turn on/off the voice when arming and disarming

1.   Select main menu - Option 8, Basic system configuration.
2.  Enter your Installer code.

3.  Pressing [4] toggles voice annunciation on / off.
Pressing [5] toggles full menu annunciation on / off.
4.   Exit from the menu.

Full Menu Annunciation

Turning this feature On, gives full descriptions to all the options within the main menu.
Turning this feature Off shortens the descriptions.

1.   Select main menu - Option 8, Basic system configuration.
2.  Enter your Installer code.

3.  Pressing [4] toggles voice annunciation on / off.
Pressing [5] toggles full menu annunciation on / off.
4.   Exit from the menu.

Backlight Level

Example: Set run mode brightness level to 8

1.   Select main menu – Option 2, Backlight level.
2.  [1] Run mode backlight level
[2] Idle mode backlight level
3.  Set brightness level to 8.
4.   Exit from the menu.

Idle mode is when your ZeroWire is not being used. The lights on the screen dim for your comfort at night. All security functions work normally. Pressing any button will bring the LEDs back up for normal operation.

Example: Set idle mode brightness level to 1. (A default setting is zero so normally no lights are on after the keypad light timer expires.)

1.   Select main menu – Option 2, Backlight level.
2.  [1] Run mode backlight level.
[2] Idle mode backlight level
3.  Set brightness level to 1.
4.   Exit from the menu.

Change Time and Date

Time and date are normally automatically updated with an internet time server.

Example: Setting the time as 9.30AM, and the date as 19.6.2014

1.   Select main menu - Option 8, Basic system configuration.
2.  Enter your Installer code.

3.  Select time and date configuration.
4.  [1] To configure the time and date.
[2] To configure the date.
5.   Enter the hours value.
6.   Enter the minutes value.
7.  Press 1 for AM.
Press 2 for PM.
8.   Enter the day.

9.   Enter the month.
 10.      Enter the year, it must be 4 digits.
 11.    Exit from the menu.

Adjust Partition Entry or Exit Times

Example: Setting the entry time as 90 seconds

1.   Select main menu - Option 8, Basic system configuration.
 2. 

 Enter your Installer code.
 3. [2] Select partition entry time.
[3] Select partition exit time.
 4.    Enter the new entry/exit time.
 5.    Exit from the menu.

Configure Sensor Names

All sensors can be named using library words on page 50. This makes it easier to identify the correct sensor in the event of a condition. You may enter up to eight words to achieve your desired description.

Example: Configure sensor 1 name as “Dining Room Sensor”

- | | | |
|----|--|--|
| 1. | MENU 8 | Select main menu - Option 8, Basic system configuration. |
| 2. | YOUR 4 OR 6 DIGIT INSTALLER CODE
ENTER
4 | Enter your Installer code.
Select sensor name recording. |
| 3. | 1 ENTER | Select sensor 1. |
| 4. | 5 3 ENTER | Select word "Dining" from the word library. |
| 5. | 1 1 7 ENTER
1 2 1 ENTER | Select word "Room" from the word library.
Select word "Sensor" from the word library. |
| 6. | MENU MENU MENU | Exit from the menu. |

If you do not require all eight words, just press MENU as in step 6 after you have entered the last word number.

Record Sensor Names

You can also record the names of the first 64 sensors using your voice.

Example: Record user name for sensor 1

- | | | |
|----|--|--|
| 1. | <div>MENU</div> <div>8</div> | Select main menu - Option 8, Basic system configuration. |
| 2. | <div>YOUR 4 OR 6 DIGIT INSTALLER CODE</div> <div>ENTER</div> | Enter your Installer code. |
| 3. | <div>4</div> | Select sensor name recording. |
| 4. | <div>1</div> <div>ENTER</div> | Select sensor 1. |
| 5. | <div>HOLD DOWN HISTORY</div> | Activate recording mode. |
| 6. | ((SPEAK NAME)) | Record voice, maximum 2 seconds. |
| 7. | <div>RELEASE HISTORY</div> | Stop recording mode. |
| 8. | <div>MENU</div> <div>MENU</div> <div>MENU</div> | Exit from the menu. |

Maintenance

System Tests

Your security system is only as effective as each of the components. This includes your sirens, communicator, back up battery, and detection devices.

Each of these should be regularly tested and maintained to provide the highest level of security. Failure to conduct regular testing can result in system failure when most required.

The four system tests to perform are:

Perform a Walk Test

This is an important test to use regularly to verify that each sensor is working correctly.

Example: How to perform a sensor walk test

1.   Select main menu - Option 4, System Test
2.  Enter your Installer code.
3.  Select sensor walk test
4.  Walk past each motion sensor, open and close windows and doors with sensors
The ZeroWire will chirp the siren and announce the sensor name and the signal level of each sensor that is triggered.
5.  Hear the status of each sensor that has been tested.
6.    Exits from System Test

Perform a Siren Test

The Sirens are used as audible deterrents in the event of your security system activating. As this test sounds all the audible devices connected to your security system, it is advisable to notify neighbors and other persons within the premises prior to activating this test. Using hearing protection is also recommended.

Example: How to perform a siren test

1.   Select main menu - Option 4, System Test.
2.  Enter your Installer code.
3.  Select siren test.
4.  Press Mute to stop sirens (within 30 seconds).
5.  Exit from the menu.
6.   

Perform a Battery Test

The backup battery is located on the rear of the ZeroWire behind a cover. It provides temporary power to the ZeroWire when mains power is not available. This may occur during a power outage or an intruder cutting power to a property.

The ZeroWire will automatically test the battery each day. If the battery fails then your system can no longer protect your property in a power outage. This is why replacing it when needed is very important.

The battery is a consumable part of the system and should be replaced ~~every 3 years~~ (to be completed) or when the battery test fails (whichever is sooner). Contact your service provider for replacement parts.

Example: How to perform a battery test

1.   Select main menu - Option 4, System Test.
2.  
3.  Select battery test.
4.    Exit from the menu.

Perform a Communicator Test

The communicator is a part of the ZeroWire responsible for sending alarm messages. The communicator test is only available if your security system has been set up to report to a central monitoring station. Proper operation of this is very important for alarm reporting.

When testing your communicator, no sirens will sound and a test message will be sent to the central monitoring station.

Example: Perform a communicator test

1. Call your central monitoring station and tell them you are performing a communicator test.
2.   Select main menu - Option 4, System Test.
3.  
4.  Select communicator test.
5. The central monitoring station will confirm the test message was received.
6.    Exit from the menu.
7. If the communicator test fails, notify your service provider.

Advanced Installation

Reset to Factory Default

Follow these steps to reset your ZeroWire back to factory default settings:

1.

MENU

9

 Select main menu - Option 9.
2.

YOUR 4 OR 6 DIGIT INSTALLER CODE

 Enter your Installer code.
3.

ENTER

 Select resetting to the factory defaults.
4.

0

 Confirm by pressing the BYPASS key, and then wait for 10 seconds.
5.

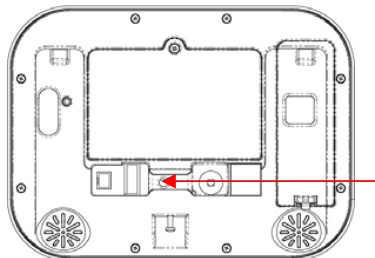
BYPASS

 Exit from the menu.

Reset Installer Account

Lost your installer PIN code? Follow these steps to reset it:

1. Use a small screwdriver to hold down the reset button **before** you turn on power.



2. Wait 3 seconds after turning on the power, then release the reset button. This will reset user 40 to PIN 9713 and username "installer".

Switch Connection Modes

A few connection methods are supported:

1. WiFi Discovery Mode – this provides direct access to the ZeroWire from a mobile device such as a smart phone or tablet for programming settings and initial set up only.
2. Wireless LAN Setup – this connects the ZeroWire to a local WiFi network. You will need to provide an internet connection and wireless router for the permanent connection. A mobile device such as a smart phone or tablet is needed to set up this connection.
3. Wired LAN Setup – this is the easiest to set up but requires a physical Ethernet connection to the ZeroWire. You will need to also provide the internet connection and Ethernet router.

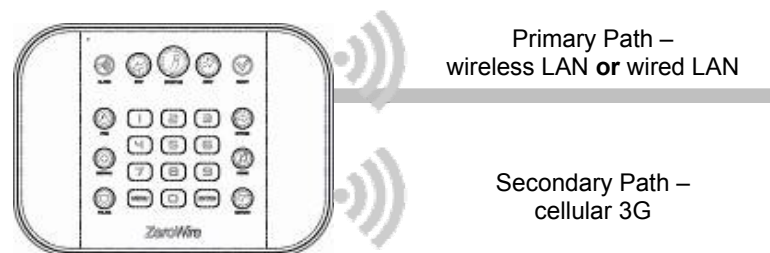
4. 3G Cellular Radio Setup – this provides a direct connection for secure reporting with no configuration needed in most cases, just plug and play. The only requirement is good mobile phone reception.

To activate WiFi Discovery mode for direct access:

1.   Select main menu - Option 9, Advanced system configuration.
2.  Enter your Installer code.

3.  Turn on WiFi Discovery Mode for 10 min.
4.   Exit from the Advanced system configuration menu.

For redundancy, 3G cellular radio will provide the backup path for reporting in case the wireless/wired LAN connection stops working.



To select between Wireless LAN or Wired LAN modes:

1.   Select main menu - Option 9, Advanced system configuration.
2.  Enter your Installer code.

3.  Toggle between Wireless LAN and Wired LAN connection modes.
4.   Exits from Advanced system configuration menu.

ZeroWire Web Server

ZeroWire has a built in web server which makes it easy and simple to set up your system from a web browser instead of the keypad.

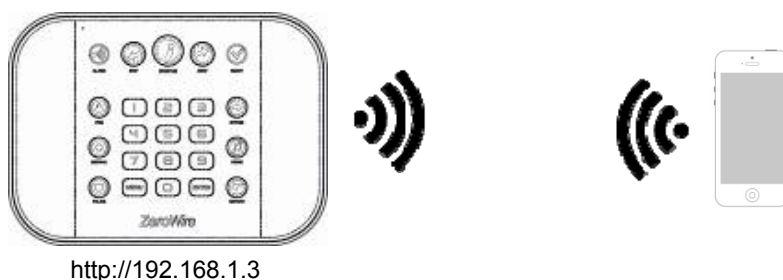
Features

- Simple forms to set up most commonly used features
- View status of partitions
- View system conditions
- Remotely arm and disarm partitions

- Turn chime mode on and off
- Bypass/Un-bypass sensors
- Add, remove and edit users
- Add, remove and edit Z-Wave devices
- View Z-Wave device status
- Control Z-Wave devices
- Enter Installation menu and perform advanced programming for ZeroWire

WiFi Discovery Mode

ZeroWire provides a temporary WiFi Discovery Mode to allow initial configuration from a mobile device such as a smart phone or tablet. This wireless connection is between the ZeroWire and the mobile device only.



1. Power on - Connect power to your ZeroWire
2. Enable WiFi on ZeroWire - On the ZeroWire press Menu – 9 – [PIN] – 8. This will enable WiFi Discovery Mode for 10 min.
3. Enable WiFi on your device - Turn on WiFi on your smart phone, tablet, or laptop.
4. Connect to ZeroWire - Browse for available WiFi networks and select the 'ZeroWire_xxxx' network to connect to it. Only a single user can connect at any time and there is no WiFi password. Once connected the ZeroWire will be assigned a fixed IP address of 192.168.1.3.
5. Open Web Browser - Open your web browser and enter http://192.168.1.3. The ZeroWire login screen should appear:

ZeroWire

Sign in

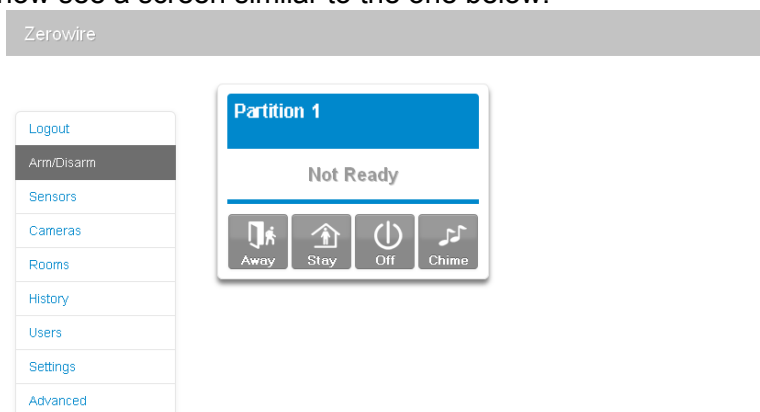
Enter your username:

Enter your password:

Sign In

6. Login - Enter your username and password, by default this is "installer" and "9713"

7. You should now see a screen similar to the one below:

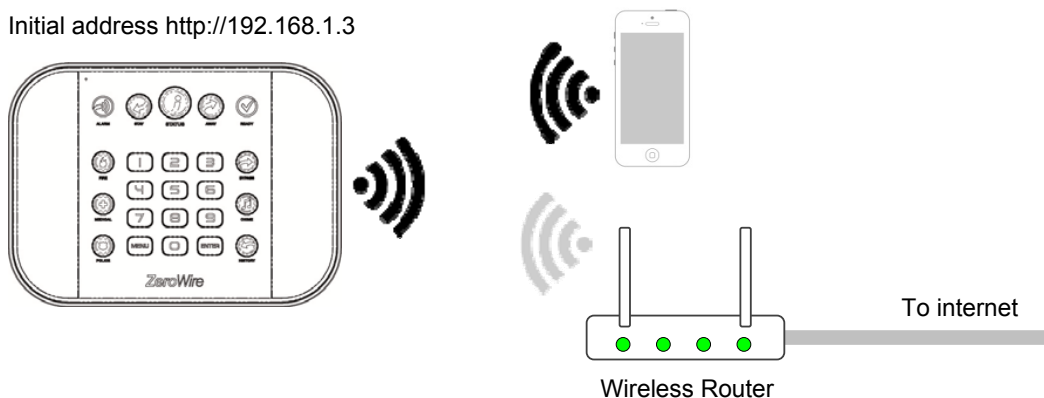


8. Click Menu – **Settings** to program your ZeroWire.
9. See the next section “Wireless LAN Setup”, “Wired LAN Setup”, or “3G Cellular Radio Setup” to connect your ZeroWire permanently to a network so it can report events.

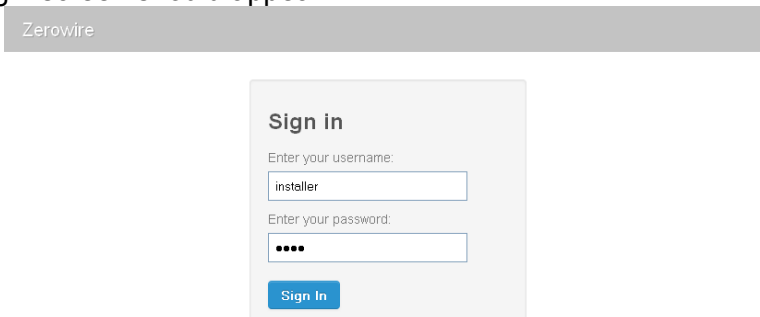
Wireless LAN Setup

We will use your mobile phone or computer to connect ZeroWire to your existing WiFi network. Your wireless router must support 802.11 b or 802.11g.

1. See above for instructions on accessing the ZeroWire Web Server from a mobile device.

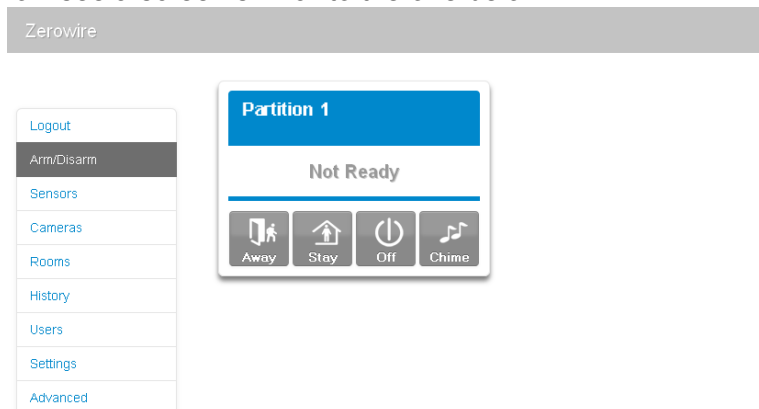


2. Open Web Browser - Open your web browser and enter <http://192.168.1.3>. The ZeroWire login screen should appear:

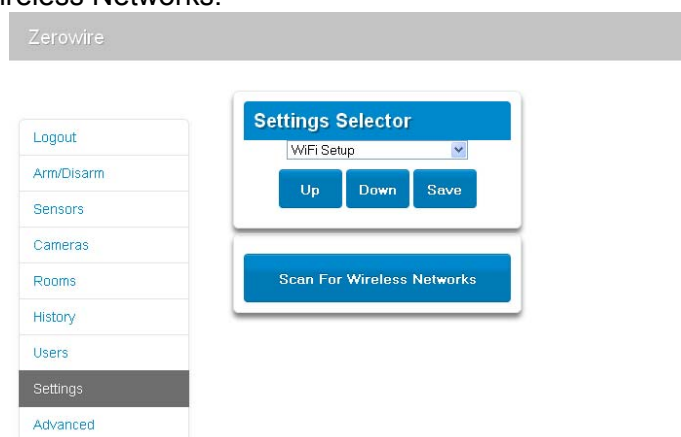


3. Login - Enter your username and password, by default this is "installer" and 9713.

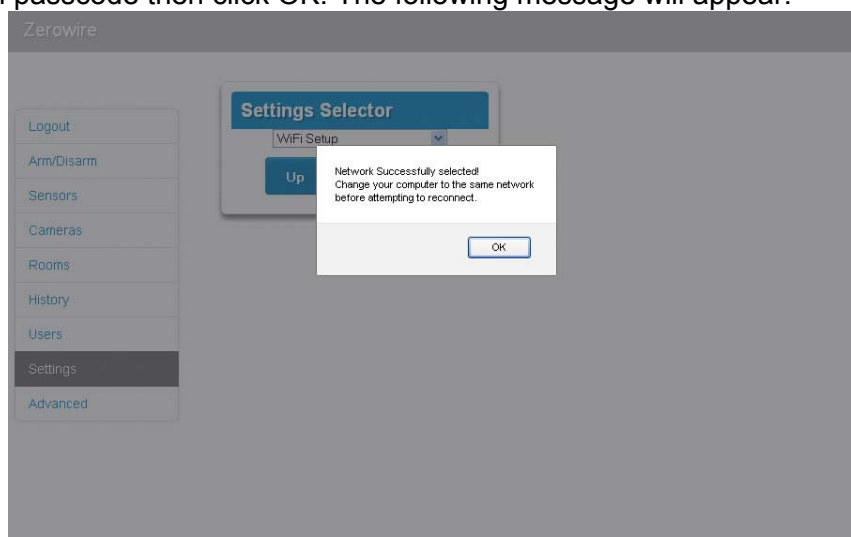
4. You should now see a screen similar to the one below:



5. Click Settings – WiFi Setup.
6. Click Scan for Wireless Networks:



7. Click the WiFi network name you wish ZeroWire to connect to.
8. Enter WiFi passcode then click OK. The following message will appear:



9. On your device, connect to the same WiFi network you selected in step 7.

10. On the ZeroWire press Menu – 8 – [PIN] – 6 and note the IP address announced. If you hear “IP address is not configured” then wait a further 30 s and repeat this step.
11. Open your web browser and enter `http://[IP address]`. The ZeroWire login screen should appear:

ZeroWire

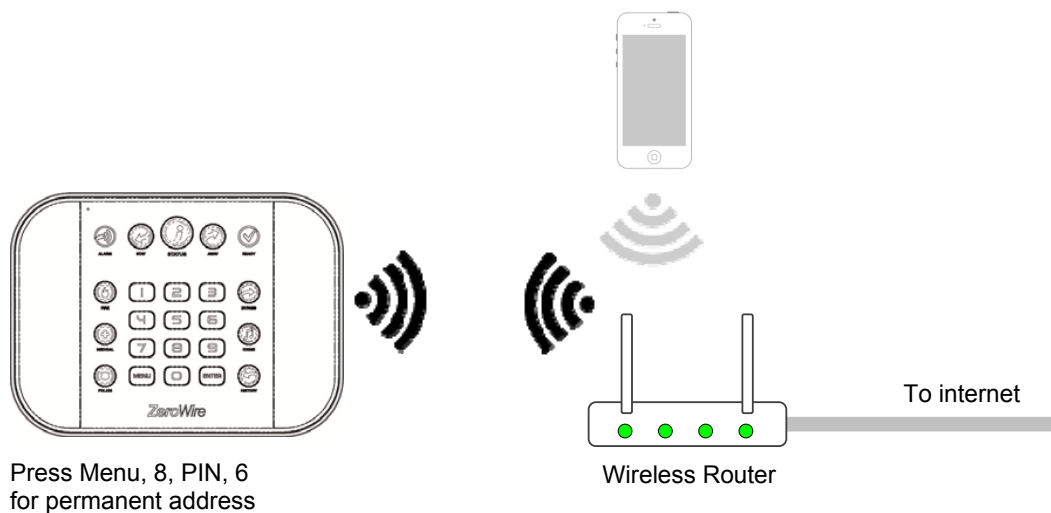
Sign in

Enter your username:

Enter your password:

Sign In

12. Your ZeroWire is now successfully connected to your WiFi network:



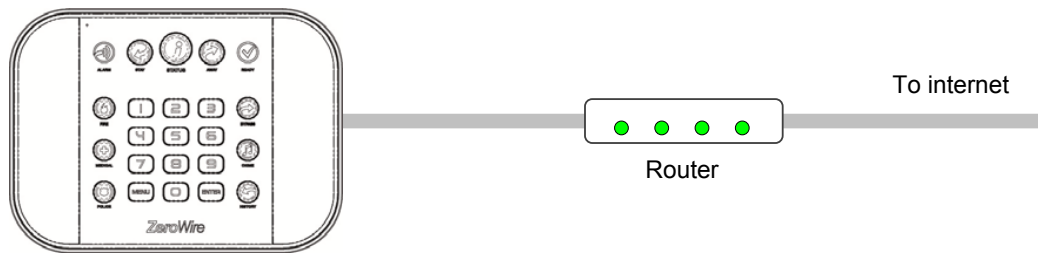
Troubleshooting

If the connection does not work or you cannot get an IP address, close the web browser on your phone, and restart your wireless router, and start again from step 1.

Sometimes settings on your wireless router may prevent a connection. Check:

- it is within range and has good signal, otherwise a WiFi range extender may help
- the wireless router has DHCP enabled
- does not have firewall or security rules that prevent additional connections
- IP addresses are available, for example connect a new device to it and verify it has an internet connection

Wired LAN Setup



1. Connect power to your ZeroWire.
2. If this ZeroWire was previously connected via WiFi, see page 19 to Switch Connection Modes.
3. Connect an Ethernet cable to the rear of the ZeroWire and wait 10 sec for the local router to assign the ZeroWire an IP address.
4. On the ZeroWire press Menu, 8, [PIN], 6 and note the IP address announced. If you hear "IP address is not configured" then wait a further 30s and repeat this step.
5. Open your web browser.
6. Enter the IP address from step 3 and the ZeroWire login screen should appear. Some browsers may require you to enter http:// before the IP address.

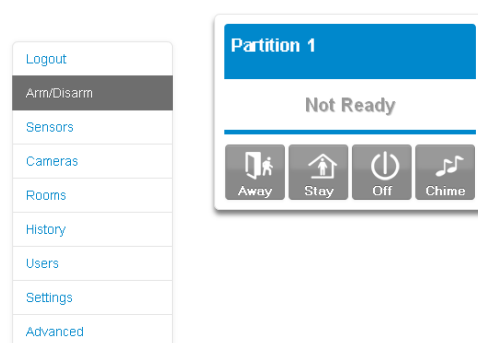
ZeroWire

Sign in
Enter your username:

Enter your password:

7. Enter your username and password, by default this is installer and 9713.
8. You should now see a screen similar to the one below:

ZeroWire

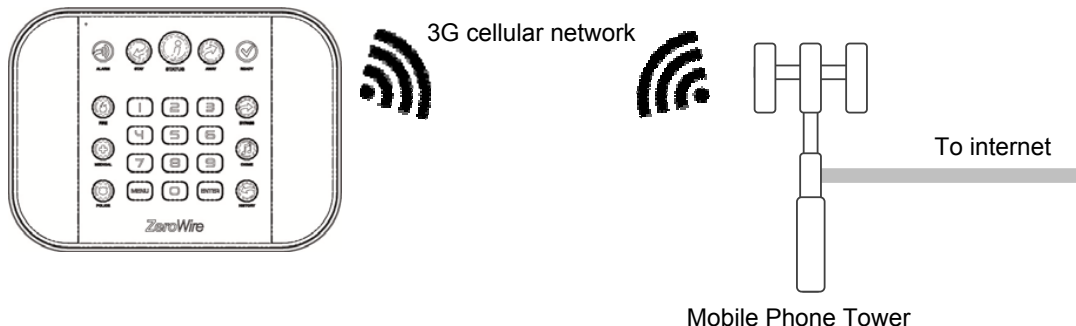


9. Click Advanced to program your ZeroWire.

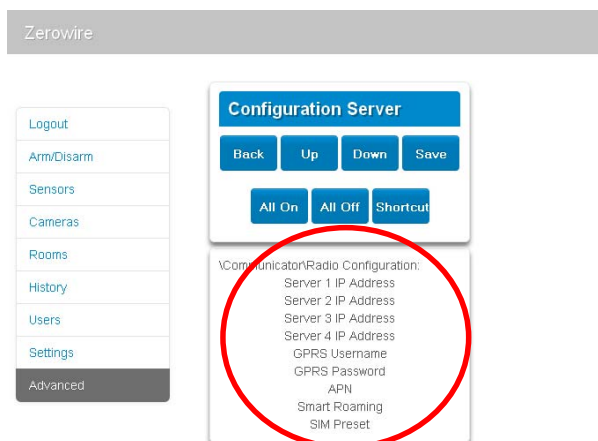
3G Cellular Radio Setup

An optional 3G cellular radio modem provides a back up reporting path to the central monitoring station over a cellular network if the Ethernet/WiFi connection is not working.

Your cellular radio module should be pre-configured and function once plugged in to the ZeroWire. If not, please refer the manual that comes with the cellular radio for instructions on how to install it.



If you need to make changes, open the ZeroWire Web Server and go to Advanced – Communicator – Radio Configuration:



Only change these settings as instructed by your supplier or telecommunications provider.

In order to check the 3G radio signal strength:

1. Login to the ZeroWire Web Server (see "ZeroWire Web Server" on page 20).
2. Click Settings – Connection Status and look at Signal Strength.

[Logout](#)
[Arm/Disarm](#)
[Sensors](#)
[Cameras](#)
[Rooms](#)
[History](#)
[Users](#)
[Settings](#)
[Advanced](#)

Settings Selector

Connection Status

Up Down Reload

Connection Status

LAN Status: Connected
LAN Media: Ethernet
Cell State: Idle
UltraAgent Wired: Idle
UltraAgent Wireless: Idle
xConnect Status: Idle
xConnect Media: LAN

Radio Details

Cell Service: No service
Signal Strength: 0
Operator ID:
Radio Technology: GSM

- Ensure the Signal Strength is -87 to -51 dbm.



- If it is too low, move the unit to an area with a better signal or install an external antenna.

Enable UltraConnect App (optional)

1. To enable the UltraConnect app click Settings – Network.
2. Enter a Web Access Passcode:

ZeroWire

Settings Selector

Network

Up Down Save

LAN configuration

IP Host Name: Qiang_ZW2

Enable DHCP: ☒

IP Address: 192.168.1.182

Gateway: 192.168.1.1

Subnet: 255.255.255.0

Primary DNS: 192.168.1.1

Secondary DNS: 0.0.0.0

WiFi Configuration

WiFi SSID:

WiFi Security Type: None

WiFi Password:

Remote Access PINs

Web Access Passcode: 23456789

Download Access Code: 12345678

3. Enter a first name:

ZeroWire

Configure Users

Add Edit Delete Save

Select User: ☐ Sort By Name

User1 (1)

User Number: 1

First Name: Sarah

Last Name:

PIN: 1234

Recommended Items To Change

- Installer Code. This is the master key to most features. Always change this to prevent accidental modifications by end-users and an unauthorized access to the security system.
- User 1 PIN code is 1234 at default. Always change this to prevent unauthorized access to the security system.

- User 1 username is “User1” at default. This is required to provide access to the ZeroWire Web Server and UltraConnect app. Leave it blank to prevent end-user access.

ZeroWire

[Logout](#)
[Arm/Disarm](#)
[Sensors](#)
[Cameras](#)
[Rooms](#)
[History](#)
[Users](#)
[Settings](#)
[Advanced](#)

Configure Users

Add Edit Delete Save

Select User ☐ Sort By Name
User1 (1)

User Number
First Name
Last Name
PIN

Sarah
1234

- Enable remote access for UltraConnect app by changing Web Access Code. The default Web Access Passcode of 00000000 prevents remote access. To change it, login to ZeroWire Web Server and go to Settings - Network.

ZeroWire

[Logout](#)
[Arm/Disarm](#)
[Sensors](#)
[Cameras](#)
[Rooms](#)
[History](#)
[Users](#)
[Settings](#)
[Advanced](#)

Settings Selector

Network

Up Down Save

LAN configuration
IP Host Name
Enable DHCP
IP Address
Gateway
Subnet
Primary DNS
Secondary DNS

Qiang_ZW2
☒
192 168 1 182
192 168 1 1
255 255 255 0
192 168 1 1
0 0 0 0

WiFi Configuration
WiFi SSID
WiFi Security Type
WiFi Password

None

Remote Access PWS
Web Access Passcode
Download Access Code

23456789
12345678

- Enable remote access for DLX900 by changing Download Access Code. The default Download Access Passcode of 00000000 prevents remote access. To change it, login to ZeroWire Web Server and go to Settings - Network.

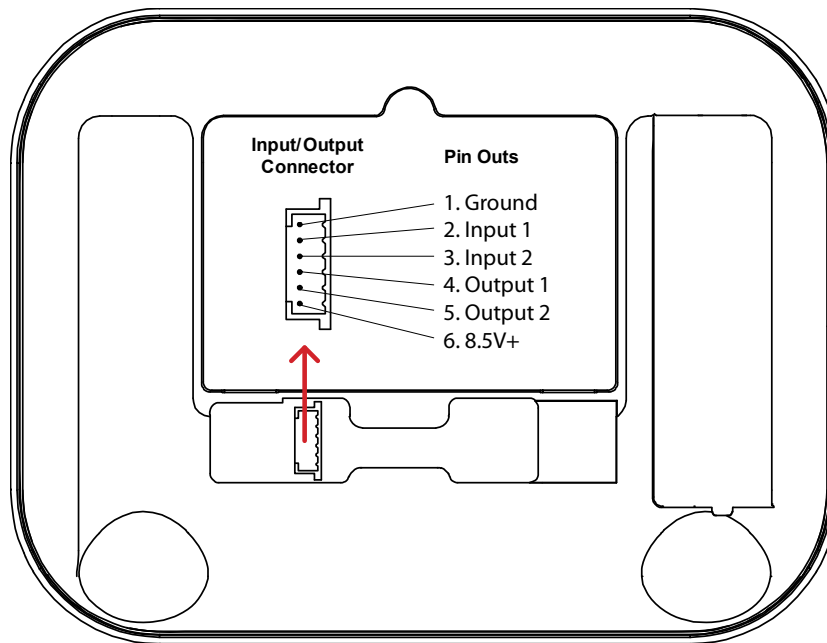
- **Installer Phone Number.** This is announced to the user when certain status conditions occur. For example when there is a low battery. Add your phone number under Advanced\ \System\Service and Test Options.
- **Web Access Passcode and Download Access Code.** These provide access to the ZeroWire Web Server, UltraConnect app, and upload/download from the DLX900 management software.

Troubleshooting

Problem	Solution
Cannot get IP address	If you are unable to get an IP address then your wireless/router may not be configured for automatic DHCP or certain security settings may be enabled. Check your router settings and try again.
Cannot see local WiFi access point from smartphone	Ensure your WiFi access point is able to accept 802.11b or 802.11g. Some 802.11n access points may not accept 802.11g connections.

Connecting Inputs

ZeroWire has two general purpose inputs located on the rear of the unit. These can be connected to up to 4 devices when Zone Doubling is enabled. Use the supplied header cable.



To disable the inputs:

- Set System Menu -> General Options -> Disable Hardwired Sensors = ON

To enable 2 inputs:

- Set System Menu -> General Options -> Disable Hardwire zones = OFF
- Set System Menu -> General Options -> Panel Zone Doubling = OFF
- Set System Menu -> General Options -> Double EOL = ON for tamper monitoring, or OFF for no tamper

To enable 4 inputs without tamper monitoring:

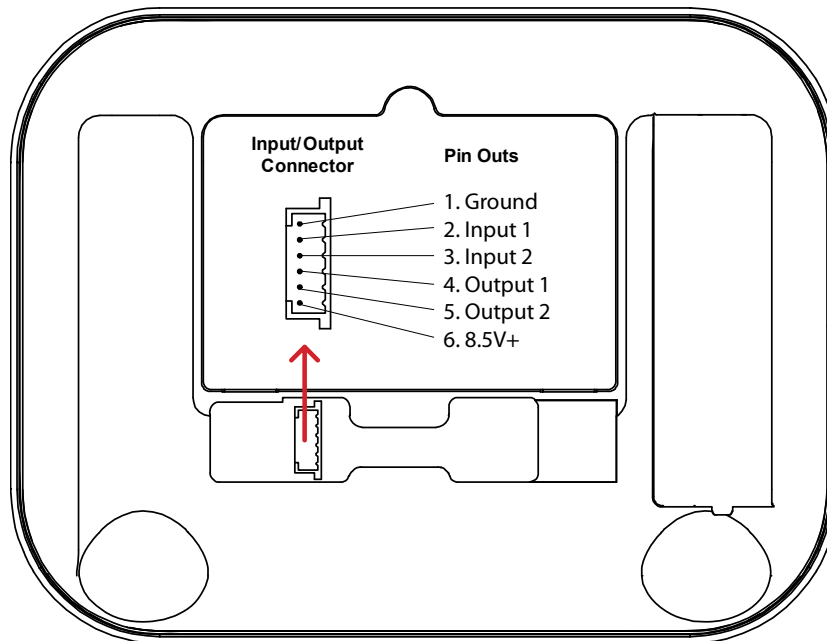
- Set System Menu -> General Options -> Disable Hardwire Sensors = OFF
- Set System Menu -> General Options -> Panel Zone Doubling = ON
- Set System Menu -> General Options -> Double EOL = OFF

IMPORTANT NOTES:

- If hard wired inputs are programmed as sensor 1, 2, 3, and/or 4, then these will take priority over the wireless sensors.
- System Double EOL will take priority over Sensor EOL setting. If Sensor EOL is OFF and Double EOL is on, Double EOL tamper monitoring will be active.
- Normally Open or Normally Closed state can be set in Zone Options -> Options.

Connecting Outputs

ZeroWire has two general purpose outputs located on the rear of the unit. These can be connected to up to 2 devices. Use the supplied header cable.



Outputs are controlled by Actions in the ZeroWire.

When an output is configured with an action, the output will monitor the status of the action:

- When the action logic is true, the output will be on
- When the action is false, the output will be off

If no action is assigned to an output the default behavior is:

- Output 1 = Siren
- Output 2 = Strobe

To program outputs from ZeroWire Web Server:

1. Click Advanced – Actions
2. Create an Action – refer to ZeroWire Reference Guide for more help
3. Click Advanced – Devices – System Devices – Control
4. Click “Control Output 1” or “Control Output 2”

5. Click Access Function

ZeroWire

[Logout](#)
[Arm/Disarm](#)
[Sensors](#)
[Cameras](#)
[Rooms](#)
[History](#)
[Users](#)
[Settings](#)
[Advanced](#)

Configuration Server

[Back](#) [Up](#) [Down](#) [Save](#)

[All On](#) [All Off](#) [Shortcut](#)

\Devices\System Devices\Control\Device
Number\Control Output 1:

1 Control

Output Name

Access Function

Schedule Number

Invert

6. Click the drop down action menu and select the action you want to control the output.

ZeroWire

[Logout](#)
[Arm/Disarm](#)
[Sensors](#)
[Cameras](#)
[Rooms](#)
[History](#)
[Users](#)
[Settings](#)
[Advanced](#)

Configuration Server

[Back](#) [Up](#) [Down](#) [Save](#)

[All On](#) [All Off](#) [Shortcut](#)

\Devices\System Devices\Control\Device
Number\Control Output 1\Access Function:

1 Control

Action

disabled

Door

0

Floor

0

7. The output will now be controlled by the state of the selected action.

Changing Keyfob Options

1. Login to ZeroWire Web Server or UltraConnect.
2. Click Settings – Keyfobs

Zerowire

Logout

Arm/Disarm

Sensors

Cameras

Rooms

History

Users

Settings

Advanced

Settings Selector

Keyfobs

Up

Down

Save

Sensor Add/Remove Functions

Learn

Remove

Cancel

Select Keyfob to Configure:

65 KeyFob

User

Use FOB Number as Standard User

Police

Medical

Fire

Scene

disabled

Serial Number

2EF67

Add IP Cameras

ZeroWire supports the following cameras:

- (to be completed)

Cameras should be configured as a static IP address and connected to the same network as ZeroWire. Default settings for the camera should be used that allows access without a password.

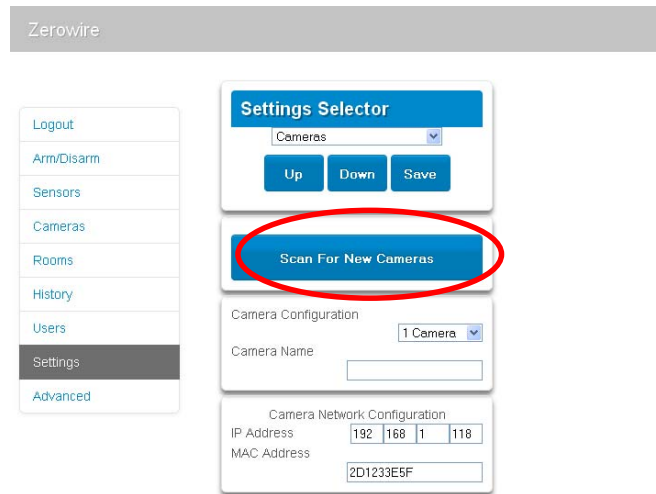
Method 1 – Automatic Discovery

On power up the ZeroWire will automatically find and add all cameras on the same network.

To add cameras at a later time:

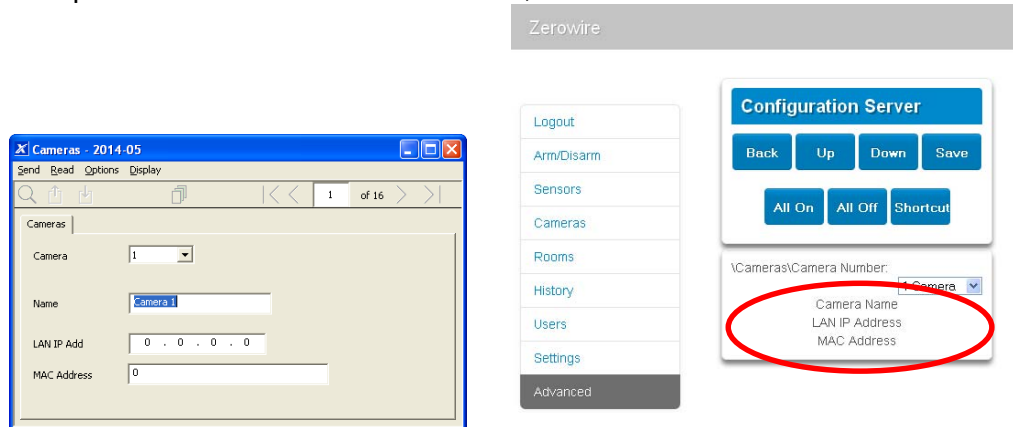
1. Install camera according to the manual supplied with the camera.
2. Login to ZeroWire Web Server.

3. Click Settings - Cameras.
4. Click Scan For New Cameras.



Method 2 – Manual Entry

1. Install camera according to the manual supplied with the camera.
2. Assign each camera a static IP address.
3. Open the Cameras menu in DLX900, or Advanced-Cameras in ZeroWire Web Server.



4. Enter a name for the camera.
5. Enter the IP address and MAC address.
6. Your camera will now be viewable from the ZeroWire Web Server and UltraConnect app.

Viewing Cameras

1. Log in to ZeroWire Web Server or UltraConnect app.
2. Click Cameras.
3. You will now be able to view the live camera feed.



Programming Cameras

ZeroWire can automatically capture a short video clip when selected events occur on the system.

These clips can later be viewed from the History screen of the ZeroWire Web Server and UltraConnect app. This is achieved using the Scenes feature.

1. Log in to ZeroWire Web Server or UltraConnect app.
2. . . . Click Settings – Scenes.



Settings Selector

Scenes

Select Scene to Configure:

Scene Name

Scene Trigger

Activate Schedule

Activate Event Type

Activate Sensor

Scene Action 1

Action Device

3. Enter a scene name.
4. Select the Activate Schedule drop down box to restrict when the scene will be enabled.
5. Select the event that will trigger recording a video clip using the Activate Event Type drop down box.
6. Select the Activate Sensor/Partition/User/Action if applicable.
7. Select Action Device (1) Alarm System, Action Type “Trigger Camera Video Clip”, then the cameras you wish to record a video clip when the event is triggered.

ZeroWire

[Logout](#)
[Arm/Disarm](#)
[Sensors](#)
[Cameras](#)
[Rooms](#)
[History](#)
[Users](#)
[Settings](#)
[Advanced](#)

Settings Selector

Scenes
▼

Up
Down
Save

Select Scene to Configure: 1 Scene 1 ▼

Scene Name

Scene Trigger

Activate Schedule Always On ▼

Activate Event Type Exit Delay 1 ▼

Activate Area 1 Area 1 ▼

Scene Action 1

Action Device (1) Alarm System ▼

Action Type Trigger Camera Video Clip ▼

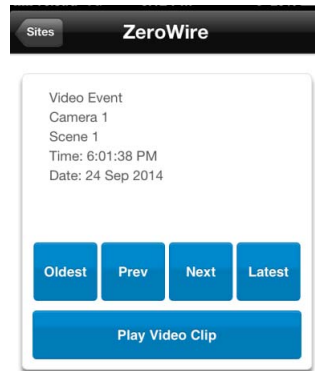
1 Camera 1 ☒

2 Camera 2 ☐

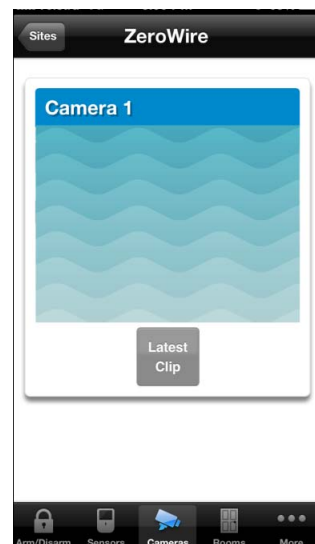
8. Click Save

View Camera Clips

1. Open UltraConnect app.
2. Click History.
3. Find the event of interest. If a video clip has been recorded then “Play Video Clip” will be enabled.



4. Touch “Play Video Clip” and wait for the video to load.
You can also go to the Cameras screen to view the latest clip.



Add Z-Wave Devices

1. Log in to ZeroWire Web Server or UltraConnect app.
2. Click Settings, Rooms and edit Room Names.
3. Click Settings, Z-Wave Add/Remove.

Zerowire

Logout

Arm/Disarm

Sensors

Cameras

Rooms

History

Users

Settings

Advanced

Settings Selector

Zwave Add/Remove

UpDownSave

Zwave Device Selector

(1) Room 1 - (1) Alarm System

Device Room Location

Room 1

Device Name:

(1) Alarm System

Device Add/Remove Functions

AddRemoveCancel

☒ Tick For High Power Add Option

4. Click Add.

The screenshot shows the ZeroWire web interface. On the left is a sidebar menu with the following items: Logout, Arm/Disarm, Sensors, Cameras, Rooms, History, Users, Settings (highlighted), and Advanced. The main content area displays three stacked panels. The top panel, titled 'Settings Selector', has a dropdown menu set to 'Zwave Add/Remove' and three buttons: 'Up', 'Down', and 'Save'. The middle panel, titled 'Zwave Device Selector', has a dropdown menu set to '(1) Room 1 - (1) Alarm System' and a text box containing the message: 'Adding - Learn Ready. Activate Device Learn Sequence or Press Cancel'. The bottom panel, titled 'Device Room Location', has a dropdown menu set to 'Room 1', a text box for 'Device Name:' containing '(1) Alarm System', and a section titled 'Device Add/Remove Functions' with three buttons: 'Add', 'Remove', and 'Cancel'. At the bottom of this panel is a checkbox labeled 'Tick For High Power Add Option' which is checked.

5. Initiate LINK or ADD mode on Z-Wave device. See your Z-Wave device's manual for instructions.
6. Note: If a Z-Wave device has been added before or to another system, you must first remove it before adding it to this system. To do this, click Remove, then activate LINK or REMOVE mode on the device.
7. Click Rooms.
8. Check you can see the device you just added. Click a button such as ON or OFF to verify you can control the device.

Access via UltraConnect App

UltraConnect is an app that allows you to control your ZeroWire from an Apple® iPhone/iPad, or Google Android device. First set up the ZeroWire Web Server then download this app. Carrier charges may apply and an Apple iTunes or Google account is required.

1. On your iPhone go to the Apple® App Store™ or Google Play™ store.



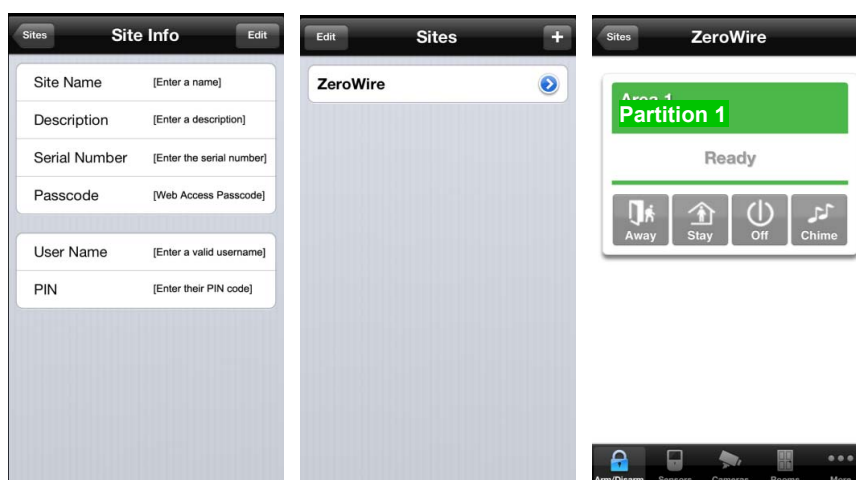
2. Search for UltraConnect.
3. Install the app.
4. Click the icon on your device to launch it.
5. Click + on the top right to add a new account, or the blue arrow to edit an existing site.
6. Enter the details of your security system.

The serial number is printed on the back of the ZeroWire unit. Alternatively login to ZeroWire Web Server and go to Settings – Details to view it.

The default Web Access Passcode of 00000000 disables remote access. To change it, login to ZeroWire Web Server and go to Settings - Network.

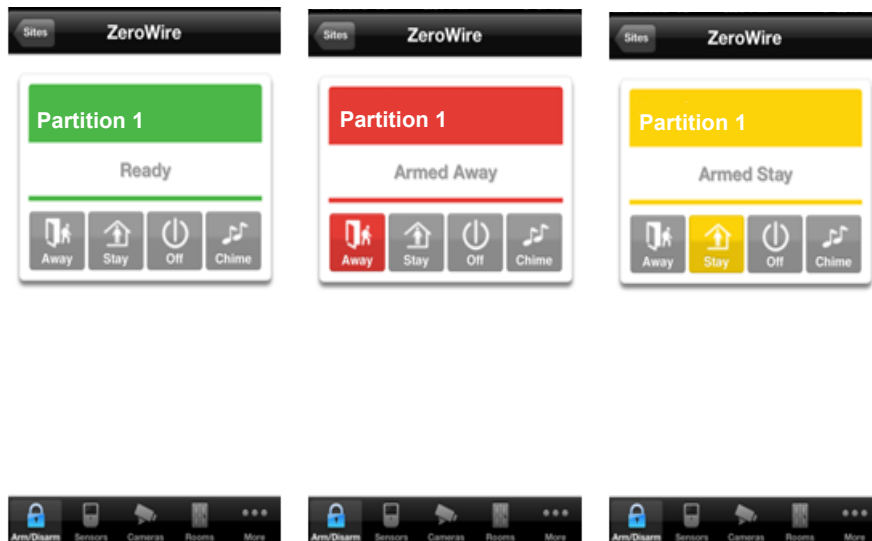
The default username and PIN code is installer 9713. You may also use any other valid user account.

7. Click Done button to save the details, then Sites to go back.
8. Click the name of the Site, the app will now connect you to ZeroWire.

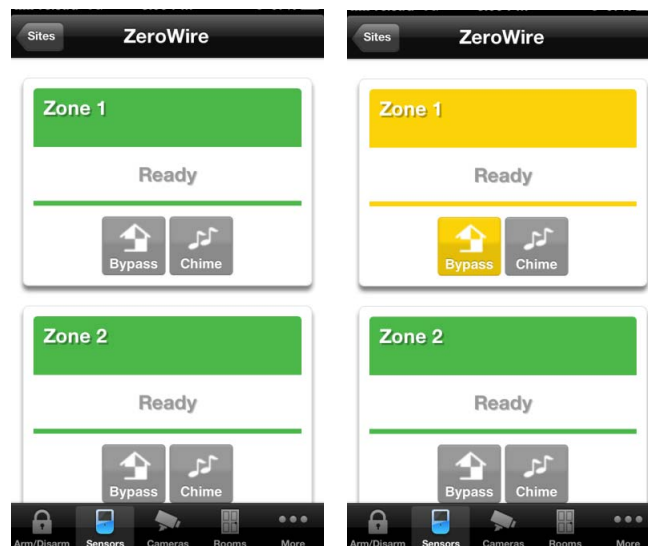


Using the App

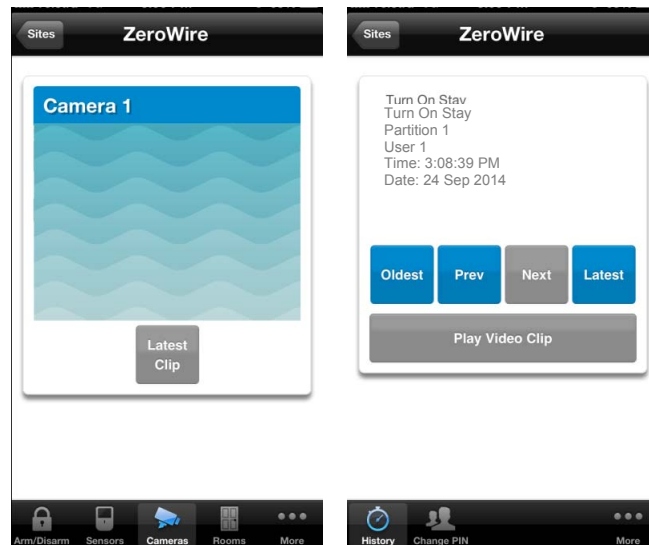
The first screen that will appear once you connect is Arm/Disarm. This will display the status of your system and allows you to arm or disarm partitions by touching Away, Stay, or Off. From this screen you can also enable or disable Chime mode.



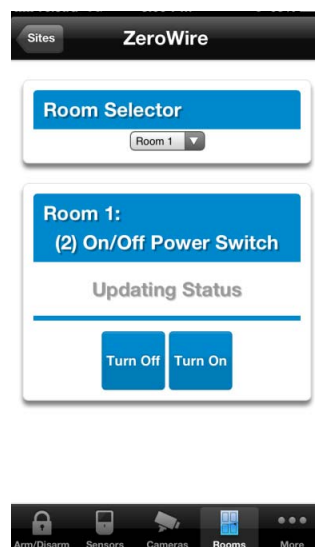
The menu bar is located along the bottom of the app. Touch Sensors to view sensor status. From the Sensors screen you can touch Bypass to ignore a sensor or touch it again to restore it to normal operation. You may also add or remove a sensor from the Chime feature.



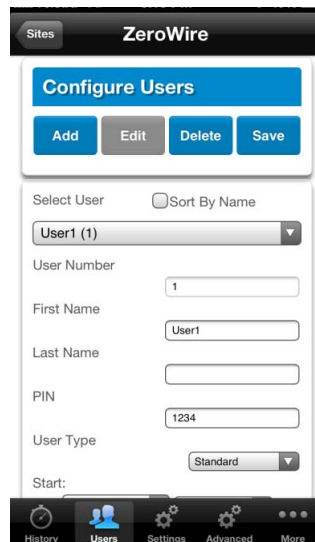
Touch Cameras to view any cameras connected to the system, this is a live view of the camera. Touch Latest Clip to view the last recorded clip by that camera. You can also access video clips linked to History events by touching Play Video Clip from the History screen.



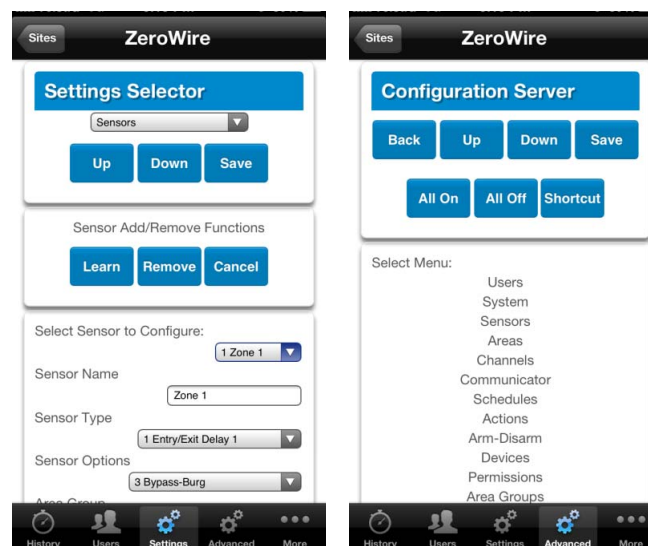
If you have Z-Wave devices installed, touch Rooms to view and control them.



Master users will have access to the full Users menu for creating and managing users.



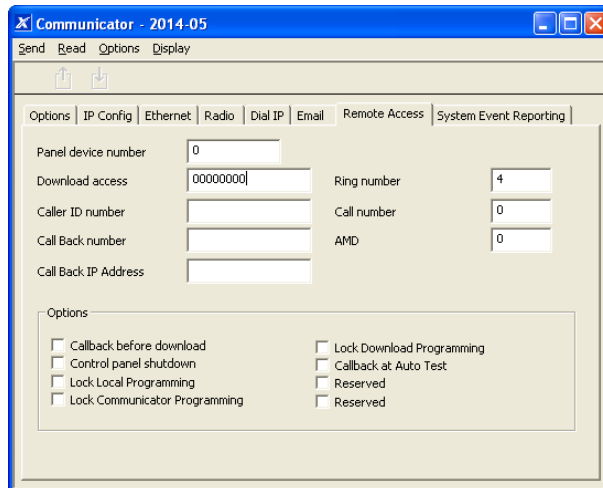
When you login with the installer account you will also have access to additional menus for setting up and programming the ZeroWire. Refer to the ZeroWire Reference Guide for additional help on the Advanced screen.



DLX900 is a fully featured management tool for control rooms and security professionals. Compatible with Microsoft Windows 7 and 8, this is available to download from our website (to be completed).

- the IP address of the ZeroWire (or use the Discover feature for LAN connections)
- to know the Download Access Code (see Troubleshooting section on page 46) and
- if Always Allow DLX900 is enabled then you will be allowed to connect, if Always Allow DLX900 is disabled then you must first put the ZeroWire into program mode, this can be changed in Settings-Network.

1. Install and launch DLX900 software.
2. Create a new customer and select ZeroWire for the Panel.
3. Enter the TCP/IP address of the ZeroWire, Click Save.
4. Go to Communicator – Remote Access.



5. Enter the Download Access Code to match the one configured on the ZeroWire panel.
6. Click the Connect TCP/IP button.

Troubleshooting

Problem	Solution
Cannot connect over TCP/IP	Check you can ping the ZeroWire. Check the Download Access Code. Check that remote access is enabled on the ZeroWire. You generally need to be on the same network to connect via TCP/IP. If you are connecting from a separate network, you will need to set up port forwarding to port 41796 on the router the ZeroWire is connected to. Consult your router manual or your IT department for assistance. Technical support is unable to assist with setting up port forwarding due to differences in customer networks and equipment.
Do not know Download Access Code	Login to ZeroWire Web Server and go to Settings – Network. Generally this will need to be done on-site with an internet browser. At factory default, DLX900 will automatically allow a connection using the default Go To Program Code / Installer Code of 9713, even if the Download Access Code is unknown or set to default of 00000000 (disable upload/download). This is a convenience feature for installers and control rooms when a system is first installed. This is why you must change the Installer Code to protect the system from further changes. Once the Installer Code has been changed, this feature no longer works and you must have the correct Download Access Code.

System Status Messages

Various messages may appear on the Status screen of ZeroWire Web Server and UltraConnect App. These are also announced by voice when the Status button is pressed.

System
• AC power fail – The security system has lost its electricity power • Low battery – The security system's back up battery requires charging • Battery test fail – The security system's back up battery requires changing • Box tamper – The security system's cabinet tamper input has activated • Siren trouble – The security system's external siren has a problem • Over current – The security system is drawing too much current • Time and date loss The security system time and date need resetting • Communication fault – The security system has detected a problem with the phone line • Fire alarm – A fire alarm has been activated from the ZeroWire unit • Panic – A panic alarm has been activated from the ZeroWire unit • Medical – A medical alarm has been activated from the ZeroWire unit

Partition Number. Partition Name
• Is On in the away mode – This partition is armed in the away mode • Is On in the stay mode – This partition is armed in the stay mode • Is ready – This partition is secure and ready to be armed • Is not ready – This partition is NOT ready to be armed, a zone is not secure • All partitions are on in the away mode – All partitions in this multi partition system are armed in the away mode • All partitions are on in the stay mode – All partitions in this multi partition system are armed in the stay mode • All partitions are ready – All partitions in this multi partition system are secure and ready to be armed

Sensor Number. Sensor Name
• In Alarm – This zone has triggered a system alarm condition • Is bypassed – This zone is isolated (disabled) and will not activate an alarm • Chime is set – This zone is part of the chime group • Is not secure – This zone is not closed • Fire alarm – This zone has triggered a fire alarm • Tamper – This zone has triggered a tamper alarm • Trouble fault – This zone has an open circuit • Loss of wireless supervision – This zone is a wireless device and has lost its communication link with the control panel • Low battery – This zone is a wireless device and needs its battery changed

UltraConnect App Status and Error Messages

Below you can find troubleshooting, status and error messages displayed on the smartphone screen in the UltraConnect application.

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"

Sensors page

- "No Sensors Configured For Your Access" - Displayed on Sensors page when there are no sensors available to view.

WiFi

- "Connection Was lost before a response was received" - Sent when no response received on a WiFi network change.

Data entry formatting 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 []"

Z-Wave messages

- "Unavailable - Failed Device Function in progress" - An attempt was made to enter an add/remove mode when the failed device mode is active.
- "Unavailable - Add mode active" - An attempt was made to enter an add/remove mode when the add mode is active.
- "Unavailable - Remove mode active" - An attempt was made to enter an add/remove mode when the remove mode is active.
- "Unavailable - Resetting Network" - An attempt was made to enter an add/remove mode when the resetting mode is active.
- "Unavailable - Backing Up Network" - An attempt was made to enter an add/remove mode when the backup mode is active.
- "Unavailable - Restoring Network" - An attempt was made to enter an add/remove mode when the restore mode is active.
- "Busy, Try Again Momentarily" - This message is received when the Z-Wave module is attempting to execute a command and a new command was submitted.
- "Not primary controller" - An attempt was made to perform device functions when not a primary controller.
- "Device Not found in failed list" - An attempt was made to remove a failed device that is now responding.
- "Remove Device failed - already in process" - An attempt was made to enter a remove mode when the remove mode is active.
- "Replace Device failed - already in process" - An attempt was made to enter a replace mode when the replace mode is active.
- "Remove Failed" - An attempt to remove a device from the network has failed.
- "Replace Failed" - An attempt to replace a device from the network has failed.
- "Function timed out or canceled" Add/Remove/Replace function timed out.
- "Unavailable, Try Again Later" - This message is received when the Z-Wave module is still initializing.
- "Command Failed" - A Z-Wave command has failed.
- "You must press Select to choose a set point" - A set point change was attempted without selecting a set point to change.
- "There are no Failed Devices" - Displayed in the failed device dialog when no failed devices detected.

Voice Library

These words can be used to customize your sensor names in Menu 6-4.

0	zero	43	cellar	86	infra red	129	small
1	one	44	childs	87	inside	130	smoke
2	two	45	alert	88	instant	131	south
3	three	46	closet	89	interior	132	stairs
4	four	47	computer	90	key switch	133	storage
5	five	48	cool	91	Keychain	134	study
6	six	49	curtain	92	kitchen	135	temperature
7	seven	50	data	93	lounge	136	spare
8	eight	51	den	94	laundry	137	toilet
9	nine	52	detector	95	lift	138	training
10	ten	53	dining	96	light	139	T V
11	eleven	54	door	97	living	140	upstairs
12	twelve	55	downstairs	98	location	141	user
13	thirteen	56	driveway	99	master	142	utility
14	fourteen	57	duress	100	medicine	143	volt
15	fifteen	58	east	101	meeting	144	veranda
16	sixteen	59	emergency	102	motion	145	wall
17	seventeen	60	entry	103	night	146	warehouse
18	eighteen	61	family	104	north	147	water
19	nineteen	62	fan	105	nursery	148	west
20	twenty	63	fence	106	office	149	window
21	thirty	64	fire	107	output	150	windows
22	forty	65	forced arm	108	outside	151	wireless
23	fifty	66	foyer	109	panic	152	yard
24	sixty	67	freezer	110	pantry		
25	seventy	68	front	111	partial		
26	eighty	69	games	112	perimeter		
27	ninety	70	garage	113	pool		
28	hundred	71	gas	114	rear		
29	thousand	72	gate	115	reception		
30	air conditioner	73	glass	116	remote		
31	area	74	glass break	117	roof		
32	attic	75	ground	118	room		
33	automatic	76	guest	119	rumpus		
34	auxiliary	77	gun	120	safe		
35	back	78	gym	121	security		
36	basement	79	hall	122	sensor		
37	bathroom	80	hallway	123	shed		
38	bedroom	81	heat	124	shock		
39	boat	82	heating	125	shop		
40	cabinet	83	hold-up	126	side		
41	car park	84	home	127	skylight		
42	ceiling	85	home theatre	128	sliding		

ZeroWire Menu Tree

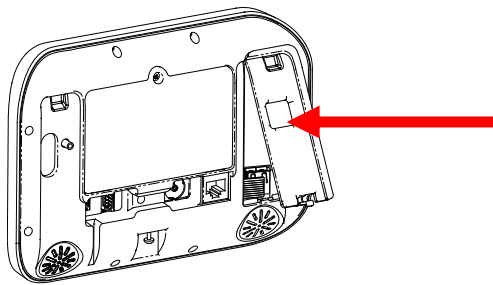
The menu structure as seen from the Advanced menu in ZeroWire Web Server:

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

Upgrading Firmware using USBUP

Upgrading firmware on your ZeroWire is easy using a USBUP.

1. Check with your supplier to download the latest firmware file for your device.
2. Create a folder on the USBUP called "ZEROWIRE".
3. Copy the firmware files into this folder.
4. Take the ZeroWire off the wall and remove the USB modem cover on the right.
5. A USB modem may be pre-installed. Take it out of the ZeroWire but leave it connected.
6. The USBUP header is inside the ZeroWire panel where the arrow indicates:

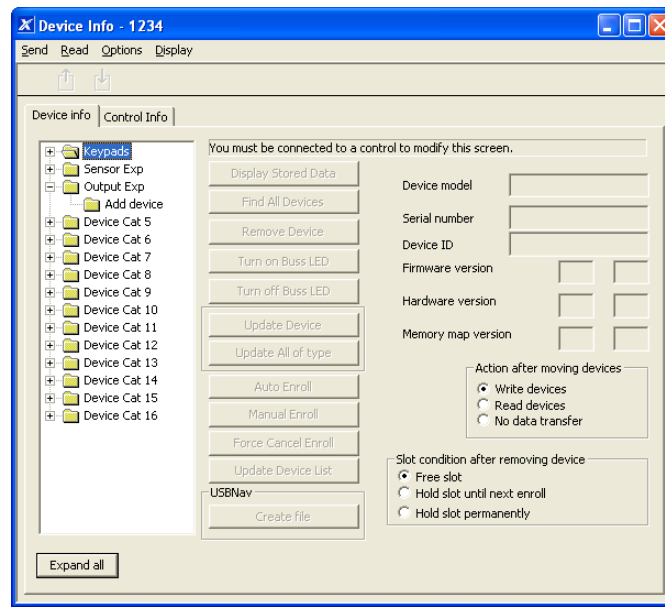


7. Connect your USBUP to this header using the 5 pin cable supplied with your USBUP.
8. Press and hold the button on the USBUP until the light begins to flash green rapidly. Release the button and USBUP will continue the firmware transfer.
9. When the light stays lit orange the firmware was successful. Disconnect the cable and replace the USB modem and cover.
10. If the light flashes red slowly then there has been an issue performing the upgrade. Check the files are correct and in the right folders on the USBUP then try again. You may also open the log file that is written to the USBUP for more diagnostic information.

Upgrading Firmware using DLX900

Upgrading firmware can be performed remotely using DLX900.

1. Check with your supplier to download the latest firmware file for your device.
2. Open DLX900 and go to Devices – Device Info:



3. Select the device you want to upgrade. If you wish to update the ZeroWire control panel, select the Control Info tab.
4. Click Update Device, Update All of Type, or Update Control.
5. Select the firmware file.
6. Click OK.
7. Wait for the firmware files to transfer to your device(s).

Specifications

Voltage	9 VDC regulated
Current	
maximum	210 mA
without voice	165 mA
Back Up Battery	Rechargeable Ni-MH battery pack
Inputs	2x sensor inputs up to 6.6 V, seal with 3.3k EOL
Outputs	2x open collector outputs at 100 mA 30 V (max)
Dimensions (W × H × D)	190 mm x 140 mm x 32 mm
Operating temperature	0 to 50°C
Shipping weight	1 kg

Index

3

3G, 26

A

access

via UltraConnect, 40

adding

IP cameras, 34

Z-Wave devices, 39

adding a keyfob, 11

adding a user, 11

adding users and keyfobs, 11

B

back of ZeroWire, 4

battery, 5

battery test, 18

C

cameras

programming, 36

viewing, 35

changing

day and time, 14

changing keyfob options, 34

changing user type, 12

communicator test, 18

connecting

inputs, 31

outputs, 32

connecting power, 8

customizing, 13

D

date and time, 14

DLX900, 53

DLX900 software, 45

F

factory default, 19

front of ZeroWire, 3

I

inputs, 31

installation, 5

installation on wall, 6

IP cameras, 34

K

keyfob

adding, 11

keyfobs

adding, 11

changing options, 34

removing, 12

L

learning sensors, 9

location, 5

M

maintenance, 17

menu tree, 51

O

outputs, 32

R

removing users, 12

resetting, 19

S

sensor names, 15

sensors

learning, 9

set description, 5

setup

3G, 26

wireless LAN, 22

signal strength, 6, 27

siren test, 17

specifications, 54

system status messages, 47

system tests, 17

U

UltraConnect app, 40

using, 42

UltraConnect app messages, 48

upgrading firmware

DLX900, 53

USBUP, 52

USBUP, 52

user

adding, 11

users

adding, 11

using

UltraConnect, 42

V

voice library, 50

W

walk test, 17
web server, 21
welcome, 1

what's inside, 2
wifi, 21
wireless LAN, 22

Z

ZeroWire menu tree, 51
Z-Wave devices, 39