interlogix
United Technologies

UltraSync™
Self-Contained Hub

Security
&
Home Automation

REFERENCE GUIDE

P/N 466- 5227 • REVC • ISS 14JUN16

About navigating this electronic document:

Throughout this document there are navigational links.

Wherever you see this symbol **C** you can click on it to *return* to the table of contents.

Wherever you see this symbol **I** you can click on it to *return* to the index.

Wherever you see underlined blue text you can click on it to *navigate* to that reference.

Whenever you navigate to a new page, you can *go back* using Alt +← (left arrow)

Contents

Welcome!.......... **7**
Features & Benefits.......... 7
Included In Box.......... **8**
Optional Accessories.......... 8
Front of Panel.......... 9
Back of Panel.......... 10
1 Hardware Installation.......... **11**
What You Need.......... 11
Choose a Location.......... 11
1.1 Install the Battery.......... 12
1.2 Connect Power Lead to the panel.......... 12
1.3 Install the Hub.......... 12
1.4 Connect Power.......... 13
2 Set Up Connections.......... **15**
2.1 Select a Permanent Connection Mode.......... 15
2.2 Option 1 - Ethernet Setup.......... 16
2.3 Check Ethernet Connection to UltraSync™.......... 17
2.4 Option 2 - Wi Fi Setup.......... 18
2.5 Set Up a Web Access Passcode for UltraSync.......... 19
2.6 Scan for Wireless Networks.......... 19
2.7 Troubleshooting Wi Fi Setup.......... 21
2.8 Check Wi Fi Connection to UltraSync.......... 22
3 The UltraSync™ App.......... **23**
3.1 Install UltraSync App.......... 23
3.2 Using the App.......... 24
3.3 Recommended Items to Change.......... 27
3.4 Troubleshooting UltraSync Setup.......... 28
3.5 UltraSync Color Codes.......... 29
4 System Settings.......... **31**
4.1 Learn Sensors into the Hub.......... 31
4.2 Learn in a Keyfob.......... 36
4.3 Programming Areas.......... 39
4.4 Programming the System.......... 42
4.5 Programming Reporting and Notifications.......... 45
4.6 Programming the Network.......... 47
4.7 Programming Scenes.......... 50
4.8 Programming Schedules.......... 53
4.9 Programming Holidays.......... 55
4.10 Programming Zwave Devices.......... 57
Zwave Room Names.......... 57

Add a Zwave Device 57
Zwave Device Association 58
Zwave Maintenance 58
4.11 Wi Fi Setup 60
4.12 Set Up a Web Access Passcode for UltraSync 61
Scan for Wireless Networks 61
Troubleshooting Wi Fi Setup 63
4.13 Check Wi Fi Connection to UltraSync 64
4.14 Programming Cameras 65
Add a Camera Method 1 – Automatic Discovery 65
Viewing Cameras in UltraSync 65
4.15 Check Event History 66
4.16 Check Connection Status 67
4.17 Check Details 67
5 Advanced Installation Using Web Server 68
5.1 Advanced Programming, System 69
5.2 Advanced Programming, Sensors 78
5.3 Advanced Programming, Areas 82
Notes on Force Arming, Bypass, and Auto-Bypass 86
5.4 Advanced Programming, Reporting and Notifications 93
Configure Email Reporting 95
5.5 Advanced Programming, Communicator 96
5.6 Advanced Programming, Schedules 104
5.7 Advanced Programming, Actions 106
5.8 Advanced Programming, Auto Arm-Disarm 111
5.9 Advanced Programming, Devices 113
5.10 Advanced Programming, Permissions 117
5.11 Advanced Programming, Area Groups 121
5.12 Advanced Programming, Menus 122
5.13 Advanced Programming, Holidays 123
5.14 Advanced Programming, Sensor Types 124
Sensor Types Table 127
5.15 Advanced Programming, Sensor Options 128
Sensor Options Table 131
5.16 Advanced Programming, Event Lists 132
5.17 Advanced Programming, Channel Groups 133
Customize Reporting Codes 135
Reporting Fixed Codes in Contact I.D. 137
5.18 Advanced Programming, Scenes 138
5.19 Advanced Programming, Speech Tokens 140
5.20 Advanced Programming, Cameras 142
Add a Camera Method 2 – Manual Entry 142
Removing a Camera 143
5.21 Advanced Programming, Network Servers 144
6 Users and Permissions 146
6.1 Add Users 146
6.2 Users Submenus 148
6.3 Permissions 149
7 Cellular Radio Setup 152
7.1 Install Optional Cellular Radio 153
7.2 Connect Power 154
7.3 Check Signal Strength 154

7.4 Install External Antenna – Optional 155
7.5 Check Cellular Connection to UltraSync 157
8 Camera Setup Instructions 160
8.1 Quick Setup 160
8.2 Setting up Ethernet/Wi Fi transmission 160
8.3 Wi Fi Signal Strength 161
8.4 Add Camera via Wi Fi for iOS Device 162
8.5 Add Camera via Wi Fi for Windows PC....162
8.6 Add Camera via Ethernet for iOS Device (non DHCP) 163
8.7 Add Camera via Ethernet for Windows PC (non DHCP)....164
8.8 Add Camera via Ethernet (DHCP) 164
8.9 Add Camera to UltraSync 165
8.10 View Live Stream and Latest Clip 166
8.11 Program event triggered camera clips 166
8.12 View event triggered clips in History 168
Remove Camera from UltraSync (if needed) 168
8.13 Change Default Camera Settings (Via TruVision Navigator)....168
8.14 Camera Troubleshooting....169
9 Installation Using Keypad 170
9.1 Basic Installation 170
9.2 Learning Sensors into the System 170
Sensor Types Presets....170
9.3 Configure Sensor Names (optional)....171
9.4 Record Sensor Names (optional)....173
9.5 Test Sensor Signal Strength 173
9.6 Remove a Sensor 174
9.7 Change the User Type (optional) 174
9.8 Add a User / Keyfob 174
9.9 Record User Names (optional)....175
9.10 Remove a User 175
9.11 Add a Keyfob 176
9.12 Remove a Keyfob....176
Personalize Your System 176
9.13 Volume Level 176
9.14 Voice Annunciation 177
9.15 Full Menu Annunciation....177
9.16 Backlight Level....177
9.17 Change Time and Date 178
9.18 Adjust Area Entry or Exit Times 178
9.19 Reset Installer Account 179
9.20 Reset to Factory Default (optional)....179
9.21 Table Mount (Optional) 179
9.22 Wall Tamper Option 180
9.23 Connecting Inputs 180
9.24 Connecting Outputs 182
10 Testing the System....184
10.1 Perform a Walk Test 184
10.2 Perform a Siren Test....185
10.3 Perform a Battery Test....185
10.4 Perform a Communicator Test....185
10.5 Event History....186
11 Glossary 188

Appendices 192
A.1 DLX900 Software 192
A.2 Troubleshooting DLX900 194
A.3 Firmware Upgrade using DLX900 195
A.4 Firmware upgrade using USBUP 196
A.5 System Status Messages 197
A.6 App and Web Error Messages 198
A.7 Zwave Messages 199
A.8 History Events 200
Event ID Table 200
A.9 Event Reporting Class Table 202
A.10 Action Events: Category and Types 203
A.11 Action Results Category and Action Results Event Types 204
A.12 Building Blocks 205
A.13 Menu Tree 206
Specifications 207
UL SPECIFICATION 208
Electrical: 208
Software Version: 208
Installation Notes: 208
Compatible Receivers: 208
Listings and Approvals: 209
Minimum System Configuration: 209
Abort: 209
Quick exit: 209
Exit delay extension: 209
Exit Progress Annunciation: 210
Entry Progress Annunciation: 210
Keyfob operation / System Acknowledgement: 210
Canceling and preventing accidental alarms: 210
Recent Closing: 211
Sensor Tripping Instructions: 211
SIA CP-01-2010 Programmable Features 212
Smoke and heat detector locations: 213
PRODUCT WARNINGS 214
WARRANTY DISCLAIMERS 214
Disclaimer 214
Intended Use 215
Copyright 215
Trademarks and Patents 215
Regulatory Notices for USA 216
Regulatory Notices for Canada 217
Index 218

UltraSync
Self-Contained Hub

REFERENCE GUIDE

W

Welcome!

Thank you for purchasing your UltraSync Self-Contained Hub!

Note: The words panel and hub are used interchangeably to describe the self-contained hub.

Please read through this document before starting the installation.

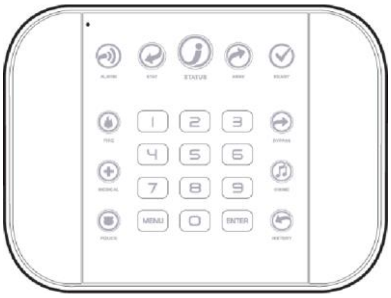
Features & Benefits

- 256 Users – enough for even moderate sized businesses
- 64 wireless sensors + 20 Keyfobs
- 4 Areas/Partitions – split your system into smaller parts you can protect individually
- Personal Voice Guided setup and menu prompts
- 2 Hardwired inputs (can be doubled to total 4)
- 2 Programmable Outputs
- 85db piezo siren
- 24 hour battery backup
- Wi Fi 802.11 b/g
- Wi Fi direct for setup
- IEEE 802.3 Compliant Ethernet

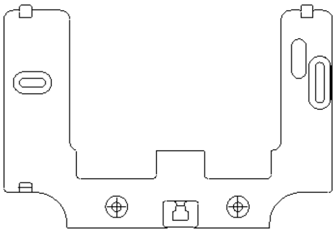
- 3G Cellular Radio Module, optional

Included In Box

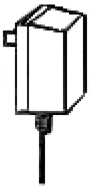
Check contents before beginning your installation.



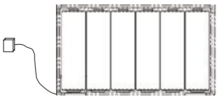
Panel



Wall Bracket

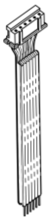


Transformer



Backup Battery Pack

Full
Reference Guide
Available Online

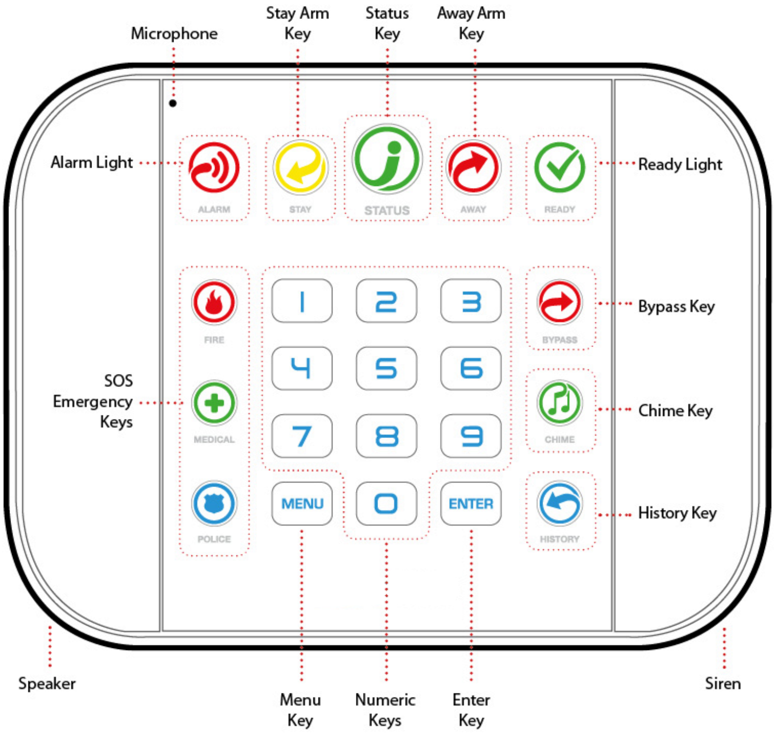


Input/Output Lead

Optional Accessories

Cellular Radio Modem	ZW-HSPA
Desk Stand	ZW-DS01
Extension Antenna	ZW-ANT3M
Battery	ZW-BAT23A
Power Supply	ZW-PS9V
Ultra Secure IP Camera	TVW-3120

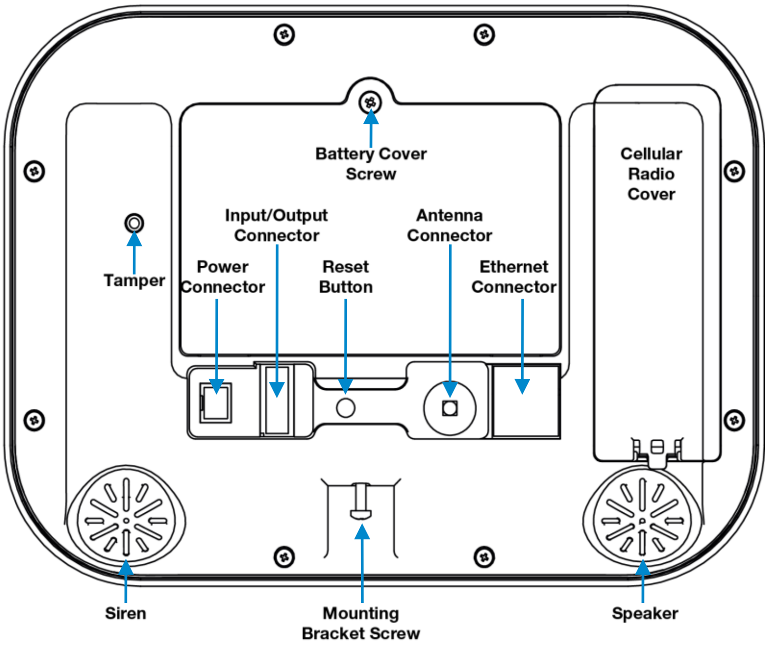
Front of Panel



Key	Color	Description
ALARM	Red	System is in alarm. Enter your PIN code then ENTER to turn off the alarm. Press the STATUS key for more info.
STAY	Yellow	System is armed in Stay mode.
	Not lit	System is disarmed if Away is also not lit. Press STAY once for Arming with Entry Delay Press STAY a second time for Arm Stay – Instant Press STAY a third time for Arm Stay – Night
STATUS	Green	System is normal.
	Yellow	Non-urgent system conditions present. Press the STATUS key to hear system conditions.
	Red	Urgent system conditions present. Press the STATUS key to hear system conditions. If you are unable to fix the issue, contact your service provider for help.
AWAY	Red	System is armed in Away mode.
	Not lit	System is disarmed if Stay is also not lit. Press the AWAY key to arm in Away mode.

Key	Color	Description
READY	Green (steady)	All sensors are ready and the system can be armed in Away or Stay mode.
	Green (flashing)	Some sensors are open but system is force-armable. If these sensors are not closed by the end of the exit time the system may go into alarm.
	Not lit	System cannot be armed, press the STATUS key for more info.
BYPASS		Press the BYPASS key if you wish to isolate (ignore) a sensor. Bypassed sensors will not be active when the system is armed in Stay or Away modes.
CHIME		Press the CHIME key to select which sensors will make a doorbell sound on the hub when they are tripped.
HISTORY		Press the HISTORY key to listen for alarm and event history.
FIRE MEDICAL POLICE		Hold down the key to send a message to a central monitoring center. Enter your PIN code then ENTER to turn off a SOS alarm. **Features may be enabled by professional security provider.**

Back of Panel



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

1 Hardware Installation

What You Need

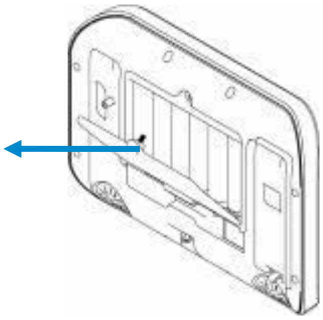
- UltraSync Self-Contained Hub
- Accessories (Intrusion Detection Devices, Lifestyle Devices, lights locks etc.)
- A mobile or smart device, or computer for programming
- List of users and PIN codes you wish to add
- Small Phillips screwdriver
- Small Flathead screwdriver
- Router supporting 802.11 b or 802.11g if using local Wi Fi features
- IP access for cell module, Wi Fi/Ethernet access

Choose a Location

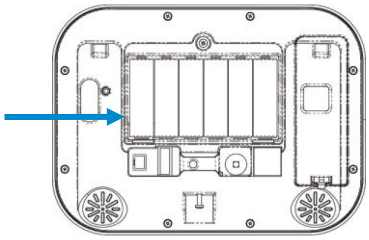
When choosing a location for your panel there are a number of appliances and areas to avoid which could interfere with the security system.

- Choose a central location that optimizes signal strength (Wi Fi, 319.5, Zwave)
- Avoid TV and other electronic appliances
- Avoid microwave ovens
- Avoid wet and moist areas such as bathrooms and toilets
- Avoid cordless telephones
- Avoid computers and wireless equipment

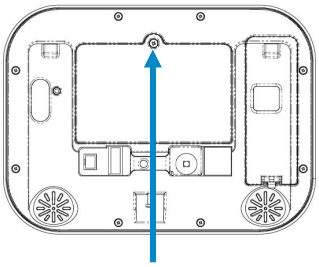
1.1 Install the Battery



Remove the battery cover with a small screwdriver.



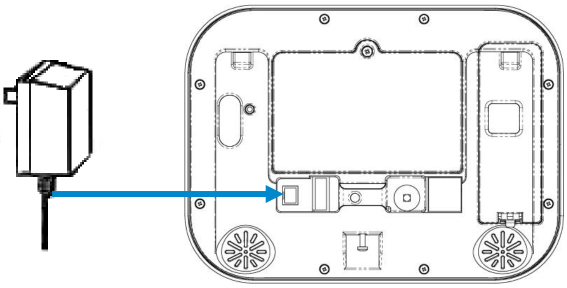
Connect battery pack lead to connector on the left inside battery compartment.
Connectors are keyed.



Replace battery cover and screw.

1.2 Connect Power Lead to the panel

Connect power lead from power supply to the back of the panel. The connector is keyed and fits only one way. For installations requiring a longer power lead, use 22AWG wire with a maximum of 164 ft. (50m).



1.3 Install the Hub

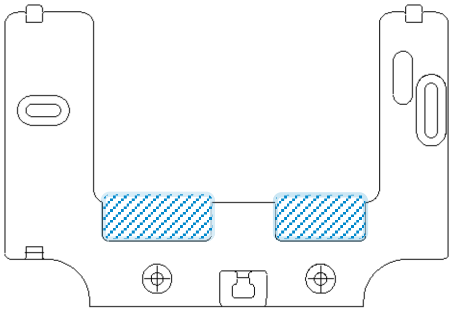
The panel may be mounted on a wall (recommended) or on a table.

For table mount information please reference Section 9.21

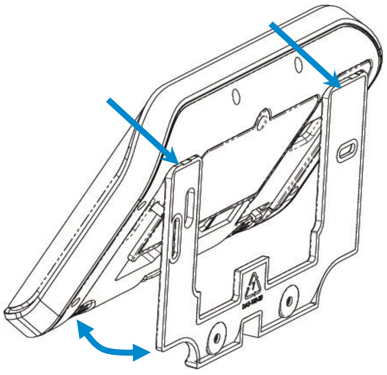
Install the bracket on a wall by using the supplied screws. Make sure the power lead can reach the panel when plugged in to a power source.

Note: Holes in the wall supplying Ethernet, power, antenna or I/O connector *must* be in the shaded area to ensure the unit mounts flat on the wall; See the drawing on the next page.

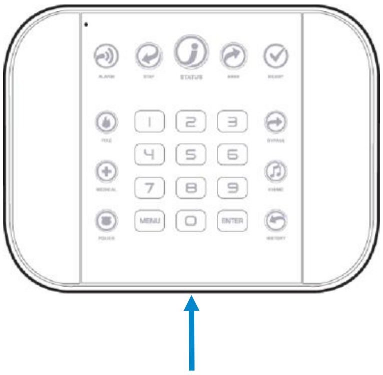
Hole location, shading:



Align the panel with the top clips on the wall bracket, and then push the hub so it sits flat against the wall.



Note: Ensure the screw on the underside of the panel is loosened enough so that the wall bracket clears the screw head; if not it may not fit flush against the wall. Then re-tighten the screw to ensure a secure fit.



1.4 Connect Power

Connect the power supply to receptacle.

Warning: Do not connect to a receptacle controlled by a switch.

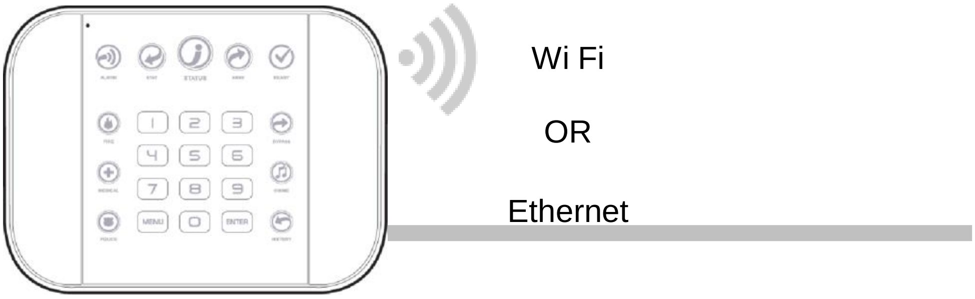
2 Set Up Connections

2.1 Select a Permanent Connection Mode

Select a method to connect your panel to a network so it can report events via UltraSync™, and allow you to configure settings using the built-in Web Server or UltraSync app. The recommended installation is to use IP as primary reporting with cellular backup. However IP only or cellular only installations may be used. For cellular radio setup reference Section 7

Option 1 – Ethernet Setup – This is the easiest to set up. The panel is set to use Ethernet by default. It requires a hardwired Ethernet connection to the panel. You will need to provide an Ethernet router and an internet connection for reporting and remote access.

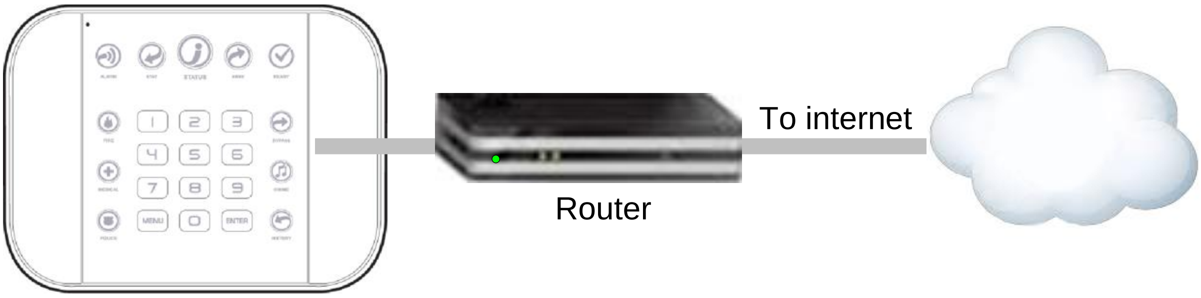
Option 2 – Wi Fi Setup – This connects the panel to a local Wi Fi network. You will need to provide a wireless router and a secure internet connection for reporting and remote access.



To switch between Wi Fi or Ethernet modes:

1.	MENU 9	Select main menu - Option 9, Advanced system configuration
2.	INSTALLER CODE ENTER	Enter Installer code
3.	7	Toggles between WiFi or Ethernet connections
4.	MENU MENU	Exits from Advanced system configuration menu

2.2 Option 1 - Ethernet Setup



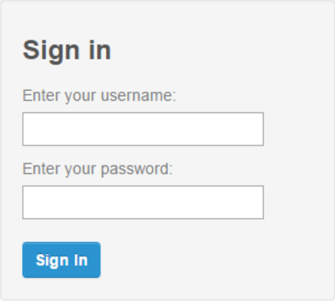
Connect power to your panel.

If this panel was previously connected via Wi Fi, switch connection to Ethernet:

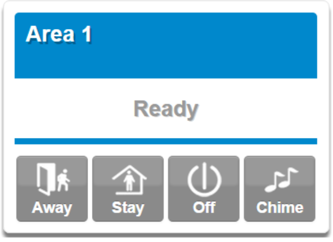
1.	MENU 9	Select main menu - Option 9, Advanced system configuration
2.	INSTALLER CODE ENTER	Enter Installer code
3.	7	Toggles between WiFi or Ethernet connections
4.	MENU MENU	Exits from Advanced system configuration menu

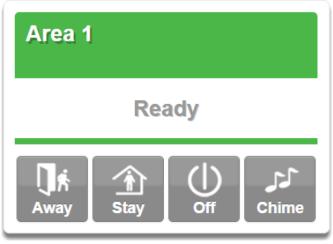
Connect an Ethernet cable to the rear of the panel and wait 10 sec for the local router to assign the panel an IP address.

On the panel press **Menu – 8 – [PIN] – 6** and note the IP address announced. This is the IP address of your panel. If you hear “IP address is not configured” then wait a further 30s and repeat this step. Open your web browser. Enter **IP address**. The login screen should appear:



Enter your username and password. By default this is: **installer** and **9-7-1-3**.
You should now see a screen similar to one of the below:





Your panel is now successfully connected to your Ethernet network.
Press **Settings** or Advanced to program your panel.

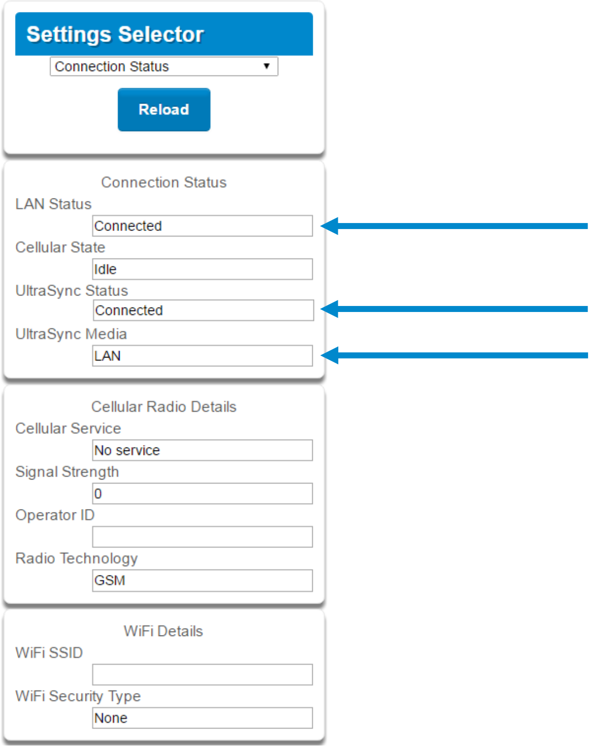
2.3 Check Ethernet Connection to UltraSync™

Login to the hub’s Web Server from your mobile device or computer using the IP address announced. Press or click **Settings**.

Select **Connection Status** in the drop down menu.

Check that

a. LAN Status should display **Connected**.
b. LAN Media should display **Ethernet**.
c. UltraSync Status should display **Connected**.
d. UltraSync Media should display **LAN**.



Connection Status

LAN Status
Connected

Cellular State
Idle

UltraSync Status
Connected

UltraSync Media
LAN

Cellular Radio Details

Cellular Service
No service

Signal Strength
0

Operator ID

Radio Technology
GSM

WiFi Details

WiFi SSID

WiFi Security Type
None

If it does not:

e. Check cable connection.
f. Check router settings.

2.4 Option 2 - Wi Fi Setup

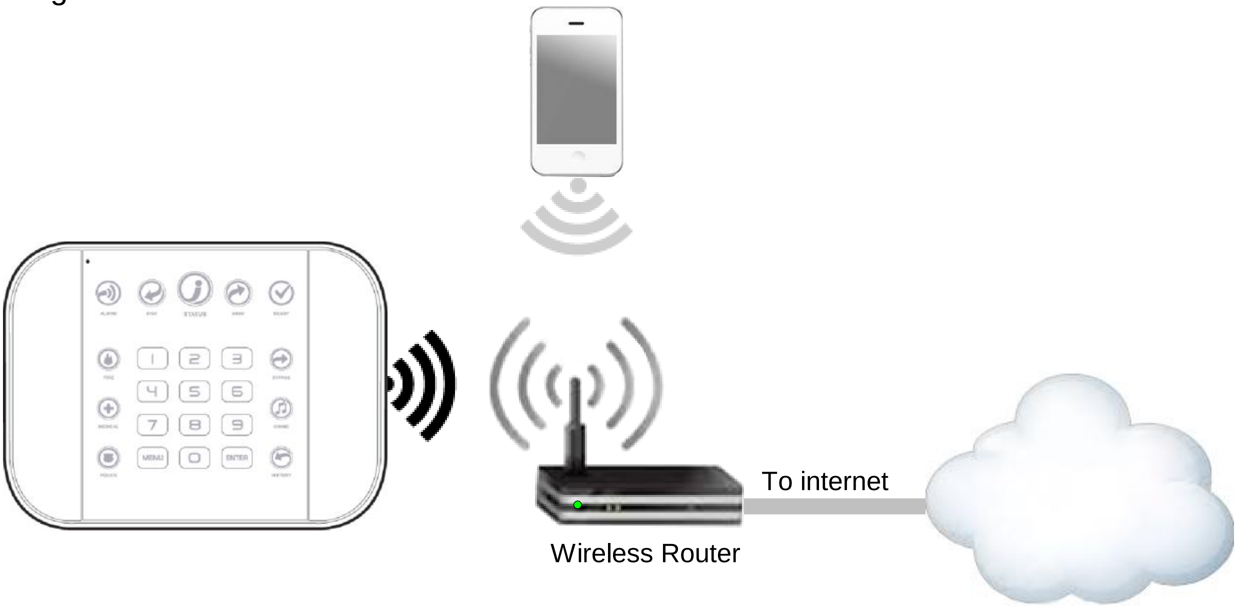
Turn on **Wi Fi Discovery Mode** – this provides direct access to the panel from a mobile device such as a smart phone, tablet, or laptop:

1.	MENU 9	Select main menu - Option 9, Advanced system configuration
2.	INSTALLER CODE ENTER	Enter Installer code
3.	8	Turn on WiFi Discovery Mode for 10 min
4.	MENU MENU	Exits from Advanced system configuration menu

Enable Wi Fi on your mobile device

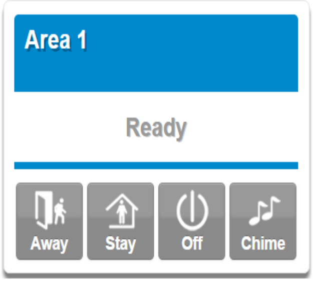
On your mobile device, browse for available Wi Fi networks and select the **ZeroWire_xxxx** network to connect to it. Only a single user can connect at any time and there is no Wi Fi password. Once connected the panel will be assigned a fixed IP address of 192.168.1.3.

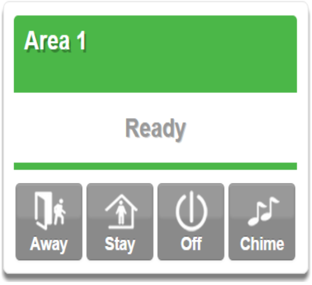
Use your device to connect to your panel . The wireless router must support 802.11 b or 802.11g.



Open your web browser and enter **192.168.1.3**. The login screen should appear.

Enter your username and password, by default this is: **installer** and **9-7-1-3**.
Press **Sign In**. You should now see a screen similar to one of the below:





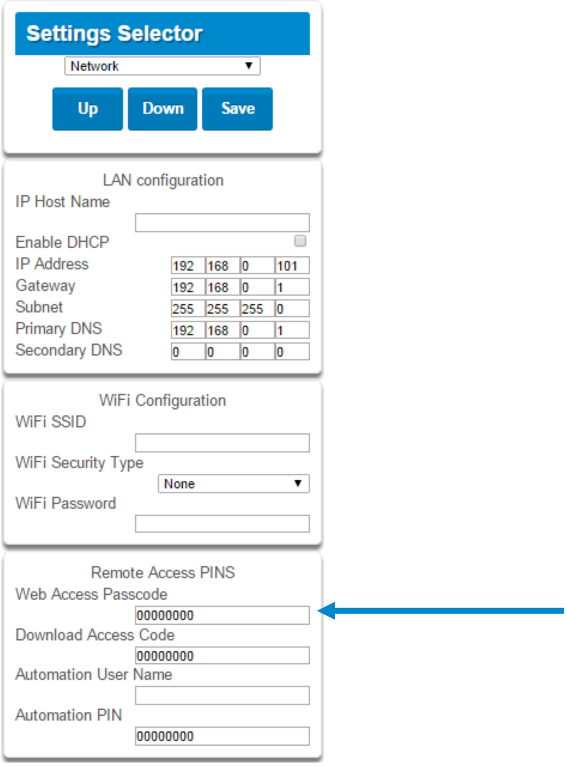
2.5 Set Up a Web Access Passcode for UltraSync

For security, remote access via the UltraSync app is disabled by default. Follow these steps to enable it:

Press ••• More then ⚙ Settings for the Settings Selector page.

Select **Network** from the drop down menu. Enable remote access for the UltraSync app by changing the Web Access Passcode (WAP). This is an eight digit code that permits access from the UltraSync application. The default Web Access Passcode of 00000000 prevents remote access.

Note: If you are connecting to the system via the LAN the WAP is not required.



LAN configuration

IP Host Name				
Enable DHCP	□			
IP Address	192	168	0	101
Gateway	192	168	0	1
Subnet	255	255	255	0
Primary DNS	192	168	0	1
Secondary DNS	0	0	0	0

WiFi Configuration

WiFi SSID:

WiFi Security Type: None

WiFi Password:

Remote Access PINS

Web Access Passcode: 00000000

Download Access Code: 00000000

Automation User Name:

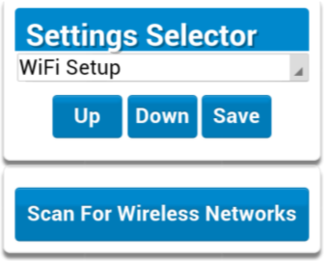
Automation PIN: 00000000

Press **Save**.

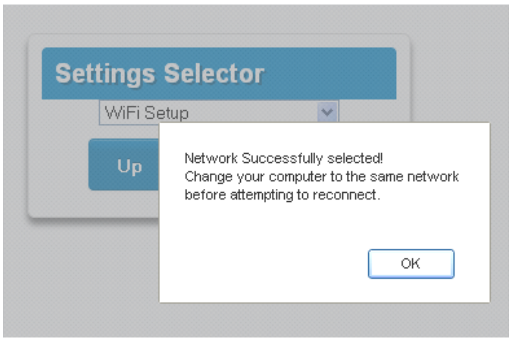
For a detailed explanation of the function of the Web Access Passcode please see section 4.6 Programming the Network

2.6 Scan for Wireless Networks

Press **Settings**.
Select **Wi Fi Setup** from the drop down menu.
Press **Scan for Wireless Networks**:



Press the Wi Fi network name you wish to connect to.
Enter Wi Fi passcode then press **OK**. “Network Successfully selected” will appear as shown below. Your mobile device will be disconnected from the panel.

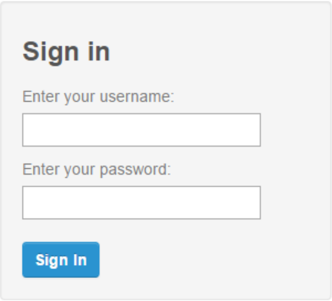


Network Successfully selected!
Change your computer to the same network before attempting to reconnect.

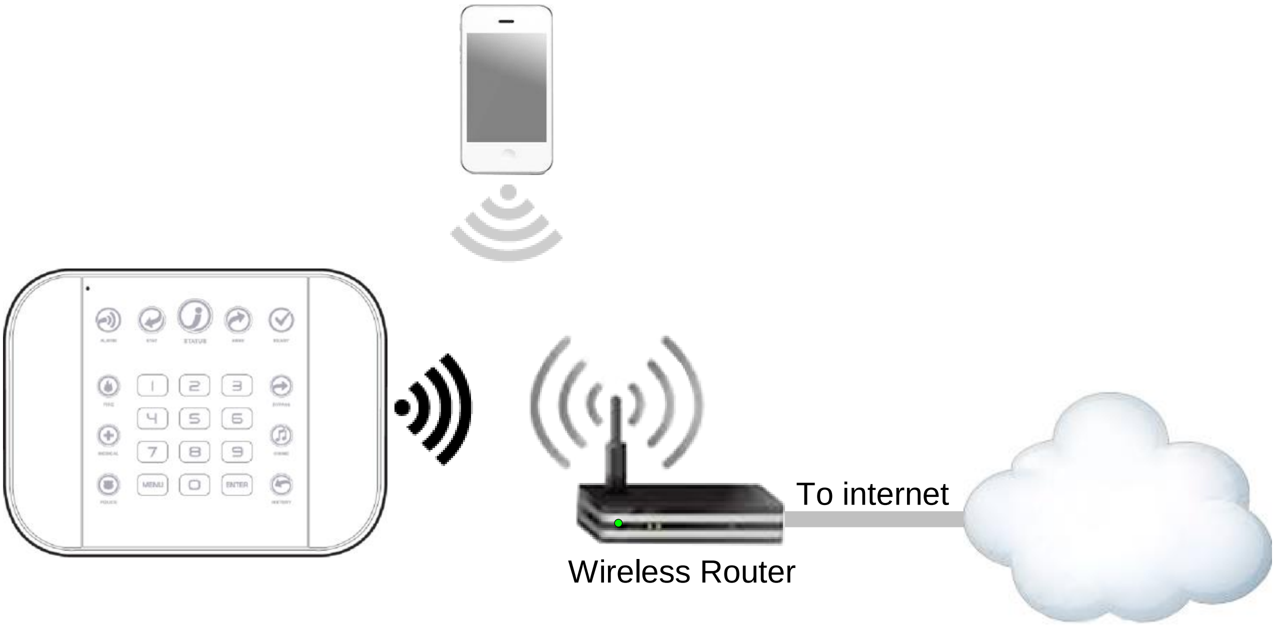
On your mobile device, connect to the same Wi Fi network found by the scan.
On the panel press **Menu – 8 – [PIN] – 6** and write down the IP address announced. This is the IP address of your panel. If you hear “IP address is not configured” then wait a further 30 seconds and repeat this step.

Open your web browser.

Enter the announced **IP address**. The login screen should appear:



Your panel is now successfully connected to your Wi Fi network.



2.7 Troubleshooting Wi Fi Setup

1. Cannot get an IP address	
Cause	Solution
Connection does not work	*Close the web browser on your device, and restart your wireless router, and start again from step 1.*
The wireless/router may not be configured for automatic DHCP or certain security settings may be enabled.	*Check your router settings and try again.*

2. Network connections fail	
Cause	Solution
Some newer routers will have these off at factory default. Some 802.11n access points may not accept 802.11g connections.	*Check if Wi Fi router allows b and g connections.*
	Check if router is within range and has good signal, otherwise a Wi Fi range extender may help.
	Ensure auto-correct is turned off (when typing the pass phrase).
	Ensure wireless router has DHCP enabled.
	Ensure wireless router does not have firewall or security rules that prevent additional connections.
	Ensure IP addresses are available; for example connect a new device to it and verify it has an internet connection.

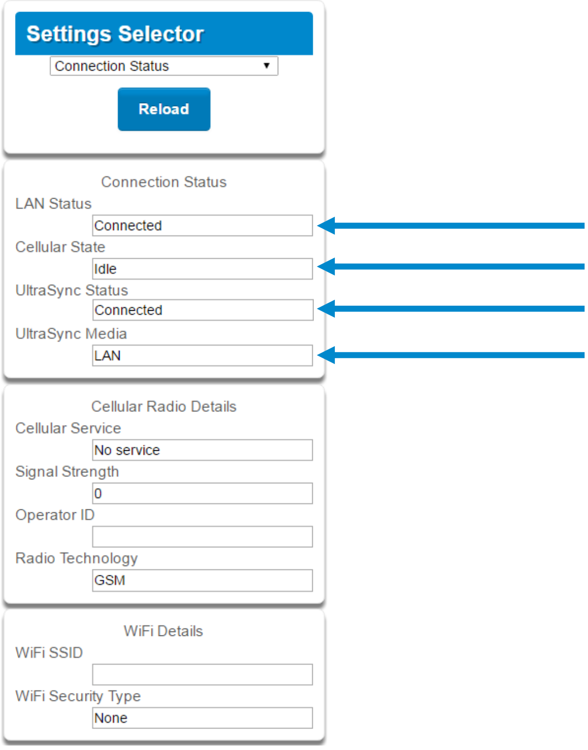
2.8 Check Wi Fi Connection to UltraSync

Login to the hub’s Web Server from your mobile device or computer using the IP address announced. Press **Settings**.

Select or press **Connection Status** in the drop down menu.

Check that

a. LAN Status should display **Connected**.
b. LAN Media should display **Wi Fi**.
c. UltraSync Status should display **Connected**.
d. UltraSync Media should display **LAN**.



Connection Status

LAN Status: Connected
Cellular State: Idle
UltraSync Status: Connected
UltraSync Media: LAN

Cellular Radio Details

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

WiFi Details

WiFi SSID:
WiFi Security Type: None

If it does not:

e. Check cable connection.
f. Check router settings.

3 The UltraSync™ App

3.1 Install UltraSync App

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

On Apple® devices go to the App Store™. On Android devices go to the Google Play™ store.

Available on the App Store   GET IT ON Google play

Search for **UltraSync**.

Install the app.

Press the icon on your device to launch it.

Press **+** on the top right to add a new site, or the blue arrow to edit an existing site.

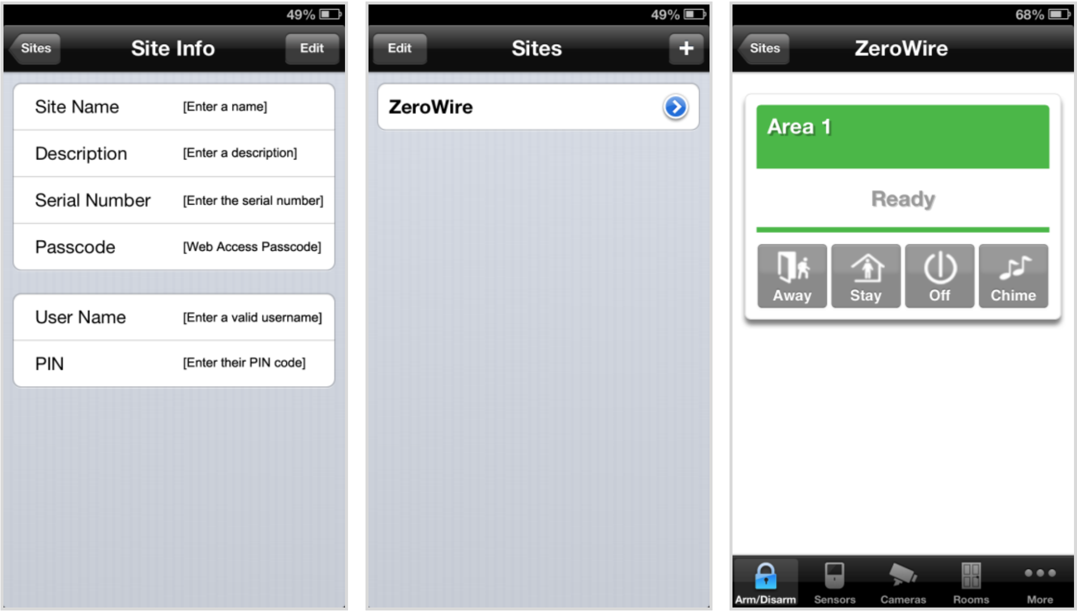
Enter the details of your security system and choose the language you want to use.

The serial number is printed on the back of the panel. Alternatively login to UltraSync 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 the hub's Web Server and go to Settings - Network.

The default username and PIN code is: **installer** and **9**-**7**-**1**-**3**, and **User 1** and **1**-**2**-**3**-**4**. You may also use any other valid user account. Users will only see and have access to menus at their permission level.

Press **Done** button to save the details, then Sites to go back.
Press the name of the Site; the app will now connect you to your hub.



Site Info

Site Name [Enter a name]

Description [Enter a description]

Serial Number [Enter the serial number]

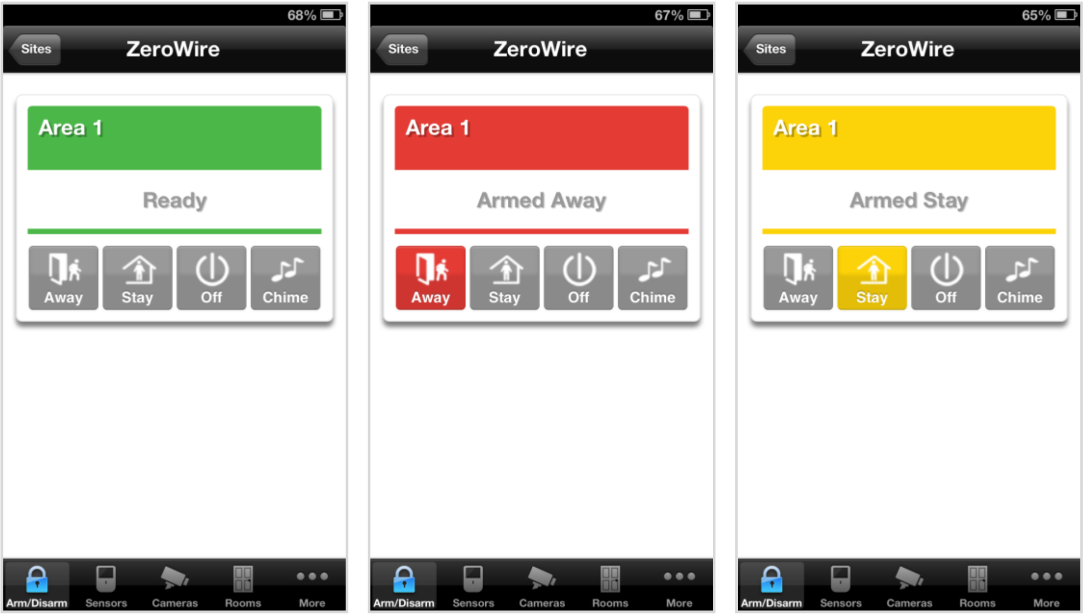
Passcode [Web Access Passcode]

User Name [Enter a valid username]

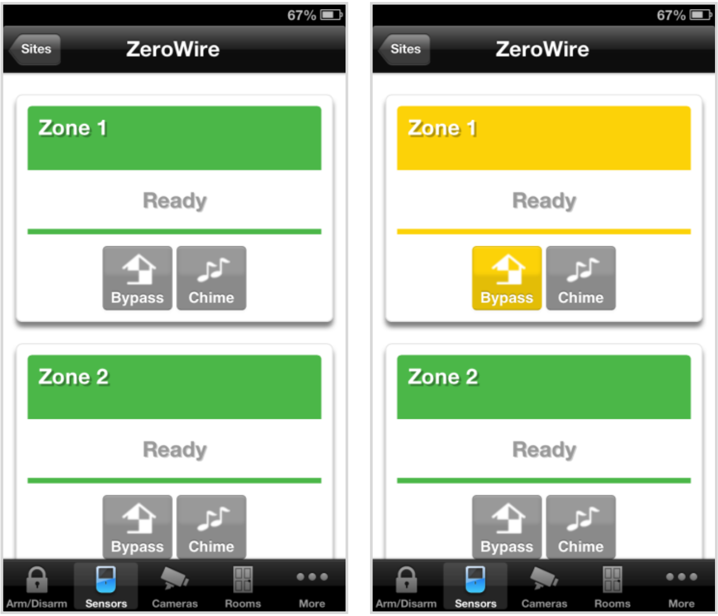
PIN [Enter their PIN code]

3.2 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 areas by pressing **Away**, **Stay**, or **Off**. From this screen you can also enable or disable Chime mode.



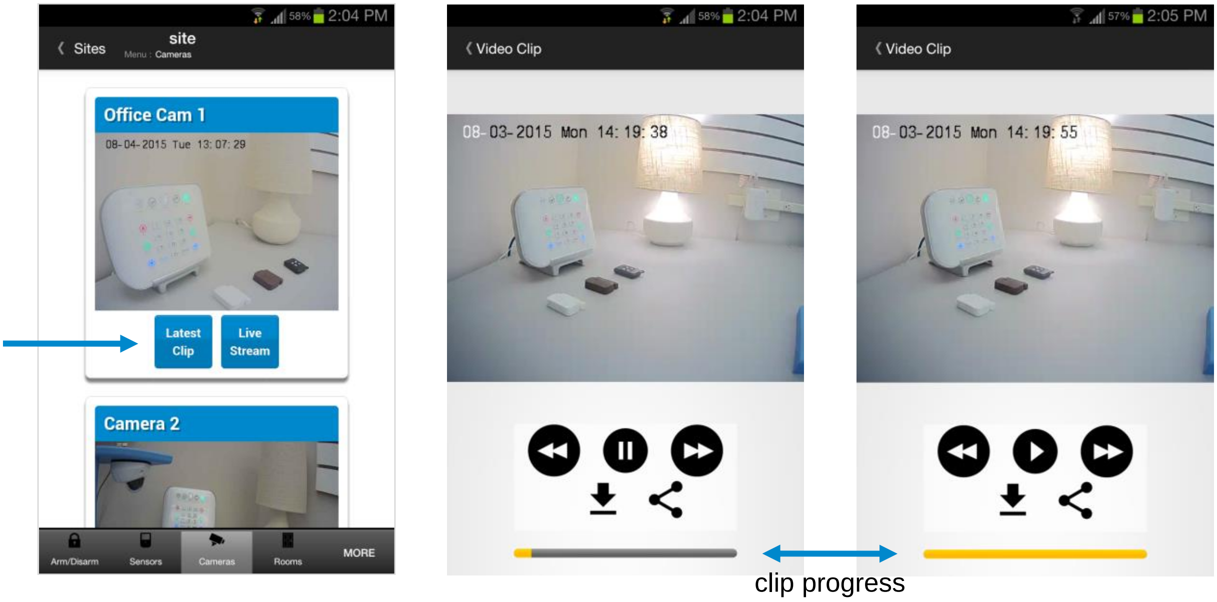
The menu bar is located along the bottom of the screen. Press **Sensors** to view sensor status. From the Sensors screen you can press **Bypass** to ignore a sensor or press it again to restore it to normal operation. You may also add or remove a sensor from the Chime feature.



Press **Cameras** to view any cameras connected to the system.

This is a live view of the camera.

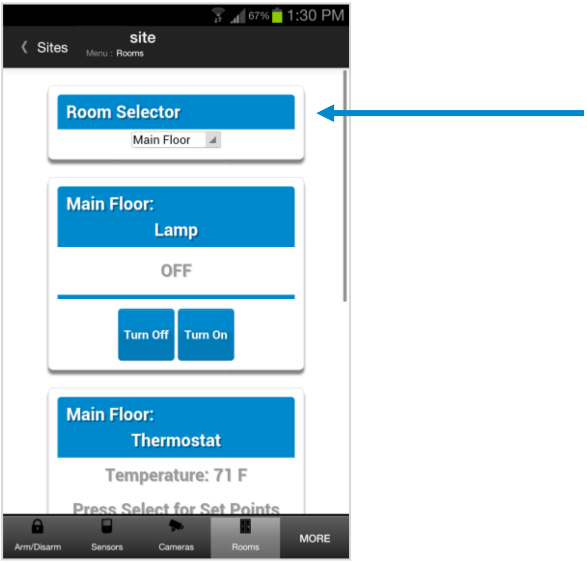
Press **Latest Clip** to view the last recorded clip by that camera.



You can also access video clips linked to History events.

Press **Play Video Clip** from the History screen.

If you have ZWave devices installed, press **Rooms** to view and control them.



Room Selector: Main Floor

Main Floor: Lamp

OFF

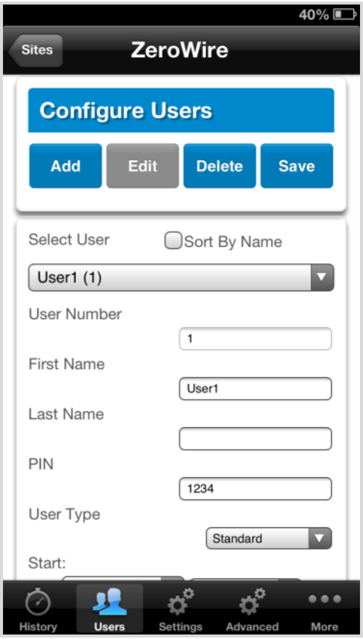
Main Floor: Thermostat

Temperature: 71 F

Press Select for Set Points

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

See Section 6, Users and Permissions for definitions of user levels and permissions.



Select User ☐ Sort By Name

User1 (1)

User Number: 1

First Name: User1

Last Name:

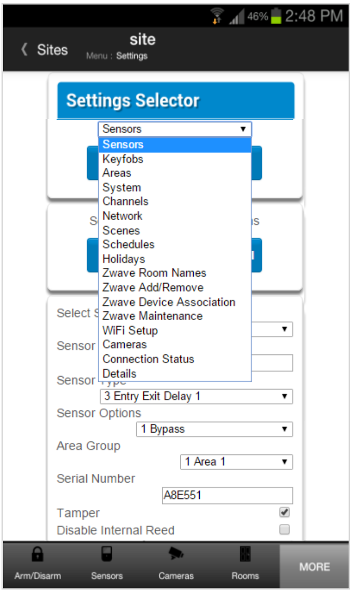
PIN: 1234

User Type: Standard

Start:

When you login with the Installer account you will also have access to additional menus for setting up and programming the hub.

Installer menu, Settings



Sensor Type: 3 Entry Exit Delay 1

Sensor Options: 1 Bypass

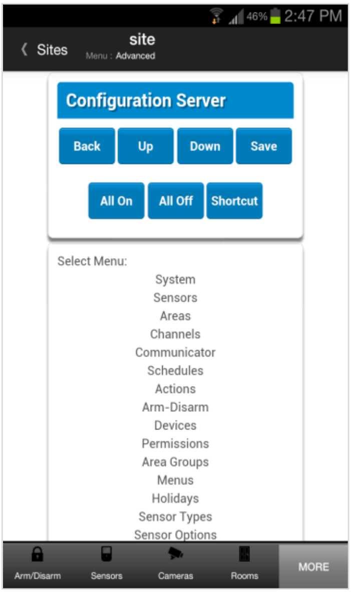
Area Group: 1 Area 1

Serial Number: A8E551

Tamper ☑

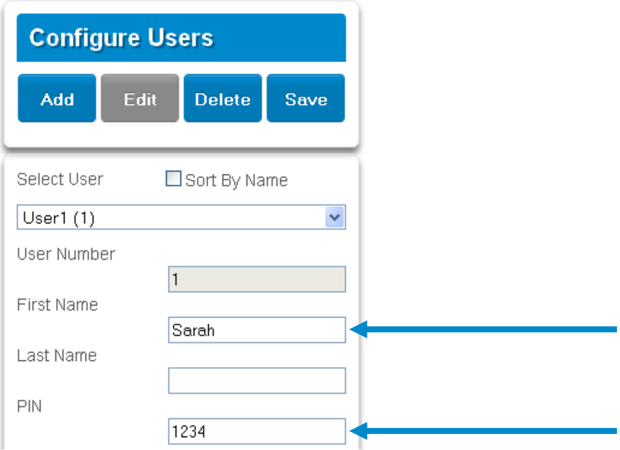
Disable Internal Reed □

Installer menu, Advanced



3.3 Recommended Items to Change

- INSTALLER CODE This is the dealer's access key to most features. Always change this to prevent accidental modifications by end-users and unauthorized access to the security system.
- 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. See system Programming (Advanced) Service and Test Options
- USER 1 NAME User 1 username is "**User 1**". At default, there is a space between "User" and "1". Usernames are required to provide access to the Web Server and UltraSync app. Make the username blank to prevent end-user access.
- USER 1 PIN User 1 PIN code is **1**-**2**-**3**-**4** at default. Always change this to prevent unauthorized access to the security system.
- WEB ACCESS PASSCODE
  DOWNLOAD ACCESS CODE These provide access to the hub's Web Server, UltraSync app, and upload/download from the DLX900 management software.



Select User □ Sort By Name

User1 (1)

User Number: 1

First Name: Sarah

Last Name:

PIN: 1234

3.4 Troubleshooting UltraSync Setup

1. UltraSync Site Creation fails

Cause	Solution
Settings are entered incorrectly	*Check the serial number, web access passcode, user name and PIN codes match those in the hub.*
	Web Access Passcode must not be 00000000.
	User Name must be entered with a space between the first and last name and with correct capitalization.

2. Cannot see local Wi Fi access point from smartphone

Cause	Solution
Some hotspot access points may not accept 802.11g connections.	*Ensure your Wi Fi access point is able to accept 802.11b or 802.11g.*

3. Network connections fail

Cause	Solution
Ethernet not working	*If connected by Ethernet, check that the cable is plugged in and the connection is working.*
Wi Fi not working	*If connected by Wi Fi, check that the connection is working.*
Network not set	*Check Settings – Network – Enable UltraSync is checked.*

4. Cannot get IP address

Cause	Solution
The wireless/router may not be configured for automatic DHCP or certain security settings may be enabled.	*Check your router settings and try again.*

5. Cannot access internet

Cause	Solution
Mobile device has no access	*Open a web browser on your mobile device to double check access.*
	Try disabling Wi Fi on your device once the hub is configured and using the 3G/4G data connection of your device with the UltraSync app.

6. Server connections fail

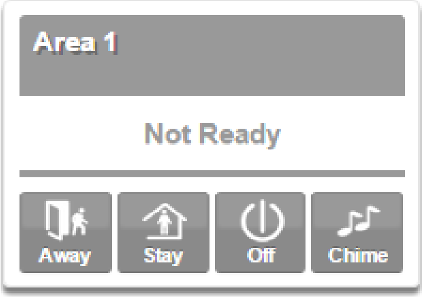
Cause	Solution
Server addresses are incorrect	*Check the UltraSync servers are correct. See Advanced Programming, Network Servers for reference.* *a. Ethernet Server 1 - zw1.UltraSync.com:443* *b. Ethernet Server 2 - zw1.zerowire.com:443* *c. Wireless Server 1 - zw1w.UltraSync.com:8081* *d. Wireless Server 2 - zw1w.zerowire.com:8081*

7. Configuration setting changes fail

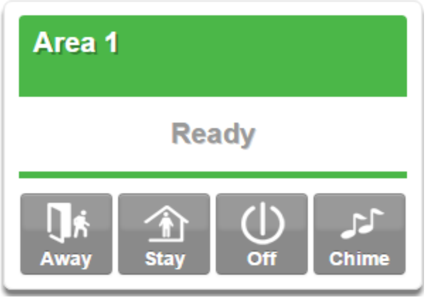
Cause	Solution
Devices are not responding to inputs	*Re-initialize equipment. Power cycle connected equipment including the panel and customer supplied router(s).*

3.5 UltraSync Color Codes

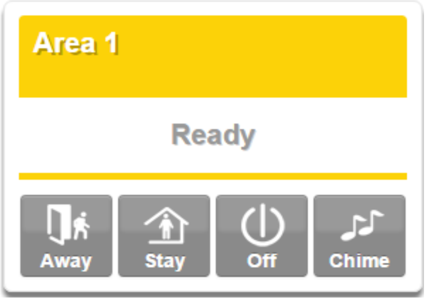
UltraSync’s display tiles are color coded for easy recognition.



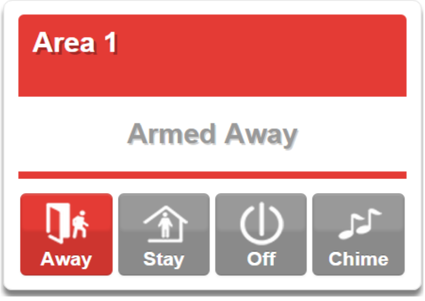
Not Ready



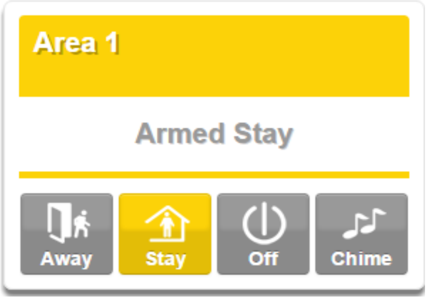
Ready



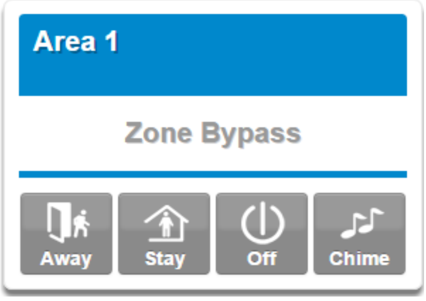
Ready with at least 1 sensor bypassed



Armed, Away



Armed, Stay



Message, Error

4 System Settings

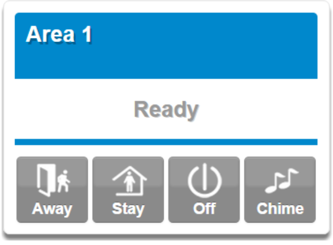
These instructions describe how to program all of the devices, schedules and areas used by the system.

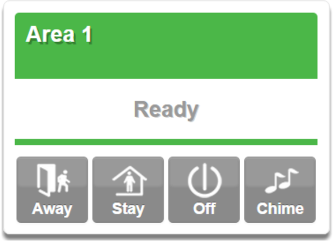
4.1 Learn Sensors into the Hub

Connect to the hub’s Web Server (either via Wi Fi Discovery Mode, Wi Fi Setup, Ethernet Setup, or the UltraSync app).

Enter your username and password. By default this is **installer** and **9-7-1-3**.
Press **Sign In**.

You should see a screen similar to one of the below:

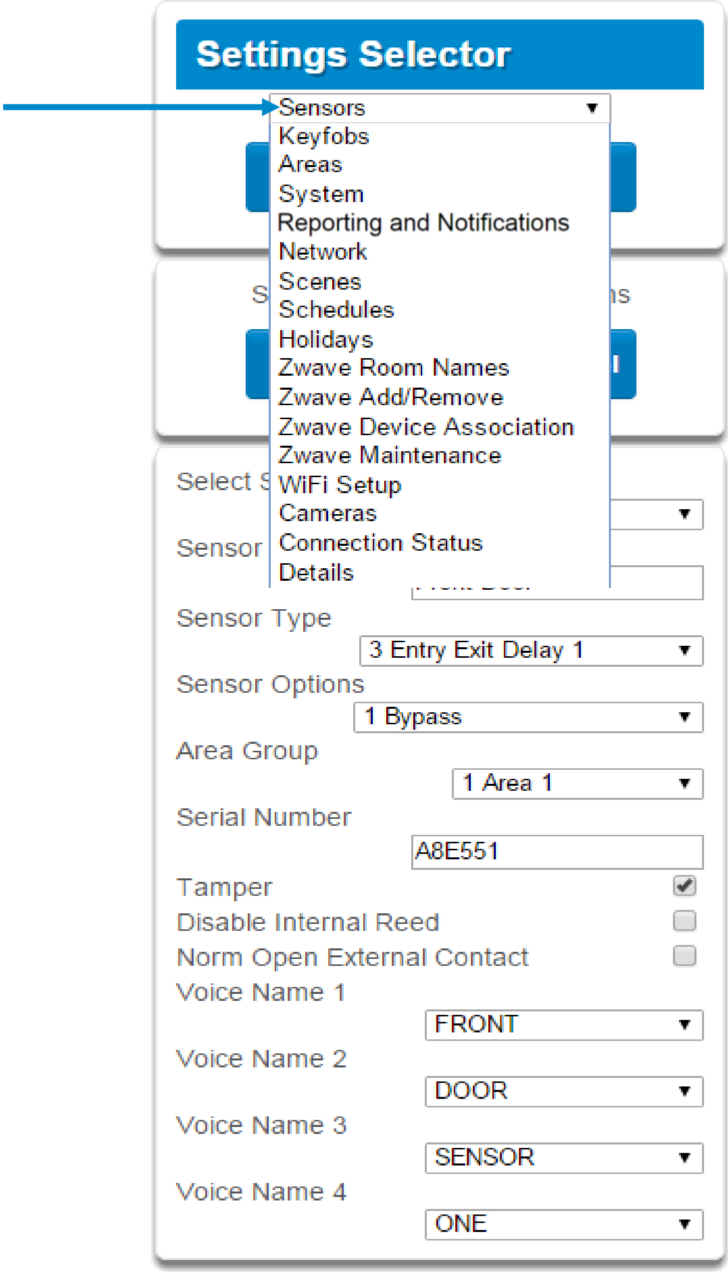




From the UltraSync app press the ••• More button then Settings

You are on the **Settings Selector** page.

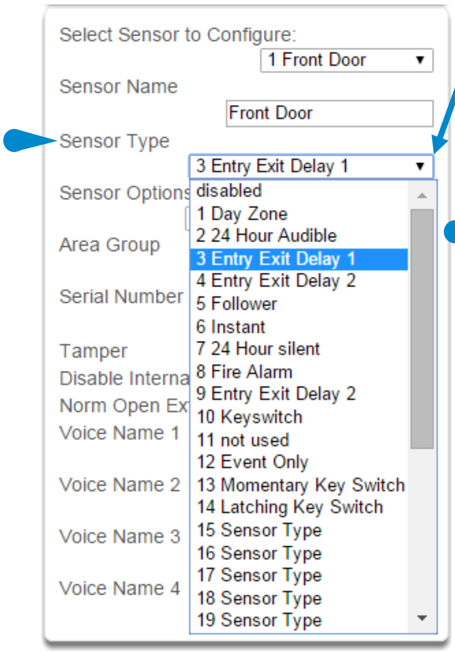
Select the drop down menu under **Sensors** to see the list of programmable items.
Select **Sensors**.



Sensor Type	3 Entry Exit Delay 1
Sensor Options	1 Bypass
Area Group	1 Area 1
Serial Number	A8E551
Tamper	☑
Disable Internal Reed	☐
Norm Open External Contact	☐
Voice Name 1	FRONT
Voice Name 2	DOOR
Voice Name 3	SENSOR
Voice Name 4	ONE

At this point you can type the name of the sensor and define its profile, by determining the sensor type (Entry, 24 hour, fire, key switch, etc.) and the sensor options (bypass, force arm, Cross Zone, stay mode, etc.). You can also assign it a specific area. Each of these has a drop down menu to make selections.

Sensor Type



Select Sensor to Configure:
1 Front Door ▾

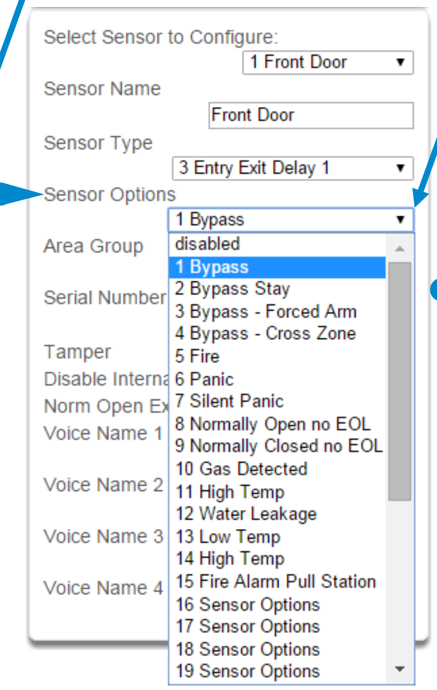
Sensor Name
Front Door

Sensor Type
3 Entry Exit Delay 1 ▾

Sensor Options
Area Group
Serial Number
Tamper
Disable Interna
Norm Open Ex
Voice Name 1
Voice Name 2
Voice Name 3
Voice Name 4

disabled
1 Day Zone
2 24 Hour Audible
3 Entry Exit Delay 1
4 Entry Exit Delay 2
5 Follower
6 Instant
7 24 Hour silent
8 Fire Alarm
9 Entry Exit Delay 2
10 Keyswitch
11 not used
12 Event Only
13 Momentary Key Switch
14 Latching Key Switch
15 Sensor Type
16 Sensor Type
17 Sensor Type
18 Sensor Type
19 Sensor Type

Sensor Options



Select Sensor to Configure:
1 Front Door ▾

Sensor Name
Front Door

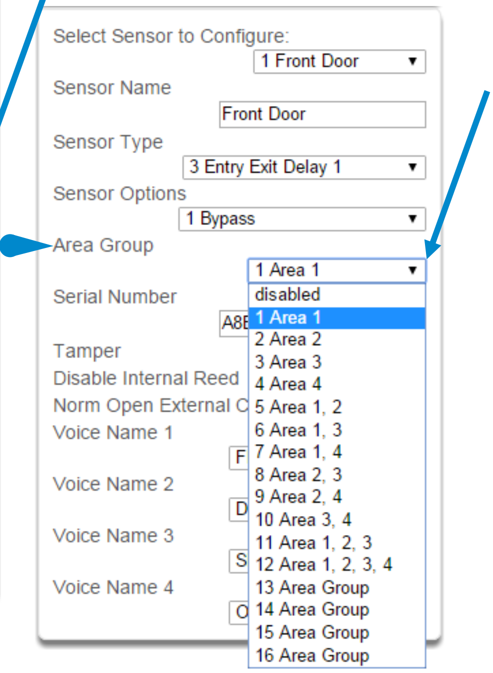
Sensor Type
3 Entry Exit Delay 1 ▾

Sensor Options
1 Bypass ▾

Area Group
Serial Number
Tamper
Disable Interna
Norm Open Ex
Voice Name 1
Voice Name 2
Voice Name 3
Voice Name 4

disabled
1 Bypass
2 Bypass Stay
3 Bypass - Forced Arm
4 Bypass - Cross Zone
5 Fire
6 Panic
7 Silent Panic
8 Normally Open no EOL
9 Normally Closed no EOL
10 Gas Detected
11 High Temp
12 Water Leakage
13 Low Temp
14 High Temp
15 Fire Alarm Pull Station
16 Sensor Options
17 Sensor Options
18 Sensor Options
19 Sensor Options

Sensor Area Group



Select Sensor to Configure:
1 Front Door ▾

Sensor Name
Front Door

Sensor Type
3 Entry Exit Delay 1 ▾

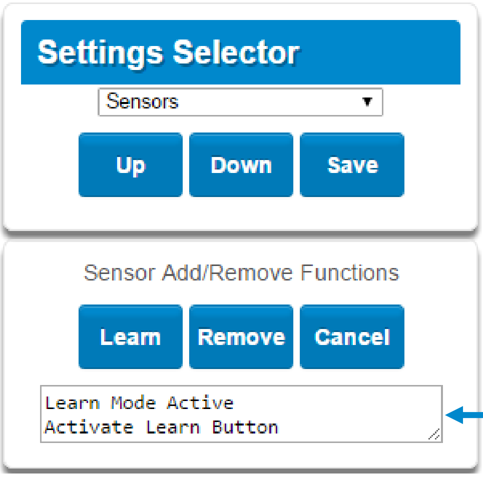
Sensor Options
1 Bypass ▾

Area Group
1 Area 1 ▾

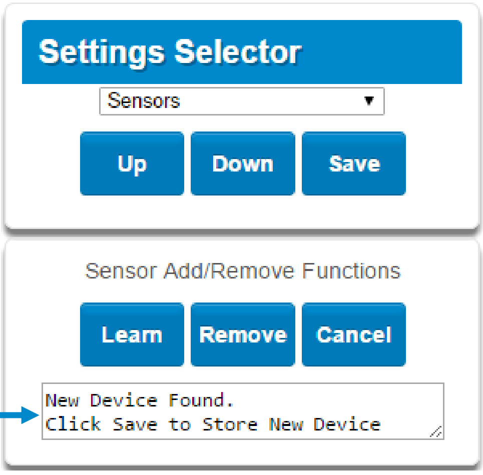
Serial Number
Tamper
Disable Internal Reed
Norm Open External C
Voice Name 1
Voice Name 2
Voice Name 3
Voice Name 4

disabled
1 Area 1
2 Area 2
3 Area 3
4 Area 4
5 Area 1, 2
6 Area 1, 3
7 Area 1, 4
8 Area 2, 3
9 Area 2, 4
10 Area 3, 4
11 Area 1, 2, 3
12 Area 1, 2, 3, 4
13 Area Group
14 Area Group
15 Area Group
16 Area Group

When all of your programming definition for the sensor is complete, press **Learn.** A notification box will appear below the learn button. Activate the sensor. Consult the sensor manual for instructions; generally this is performed by opening the case and manipulating the tamper activator. This will send a tamper signal to the panel. The notification box will alert you that a new device was found.



```
Learn Mode Active
Activate Learn Button
```

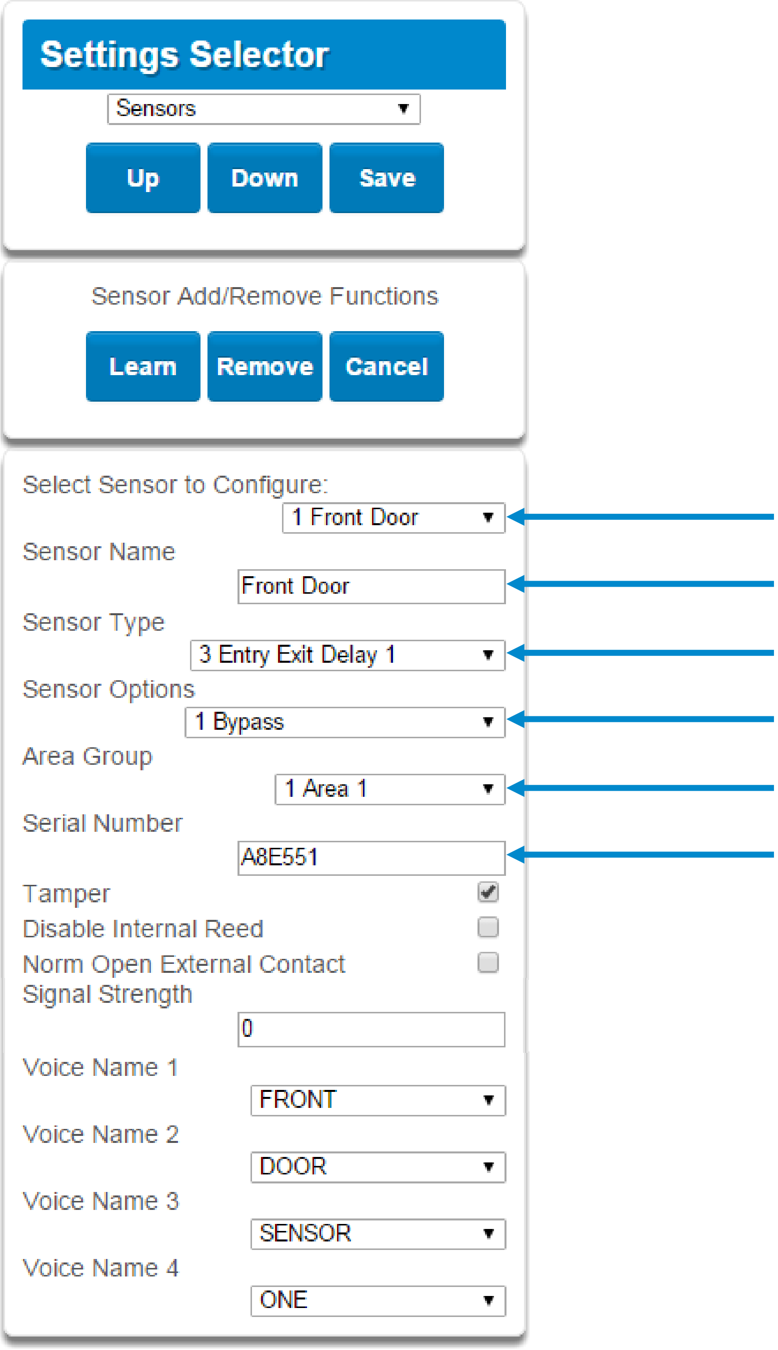


```
New Device Found.
Click Save to Store New Device
```

The screen below shows a sensor learned in.

Name:	Front Door
Type:	Entry Exit Delay 1
Option:	Bypass
Area Group:	Area 1
Serial Number:	A8E551

Note that the sensor Serial Number box has been populated after learning in the sensor.



Select Sensor to Configure: 1 Front Door

Sensor Name: Front Door

Sensor Type: 3 Entry Exit Delay 1

Sensor Options: 1 Bypass

Area Group: 1 Area 1

Serial Number: A8E551

Tamper ☑

Disable Internal Reed □

Norm Open External Contact □

Signal Strength: 0

Voice Name 1: FRONT

Voice Name 2: DOOR

Voice Name 3: SENSOR

Voice Name 4: ONE

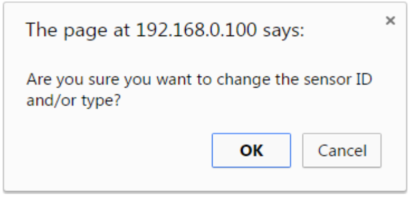
Explanations of the sensor configurations appear on the next page.

Also reference Advanced Programming, Sensors, Section 5.2.

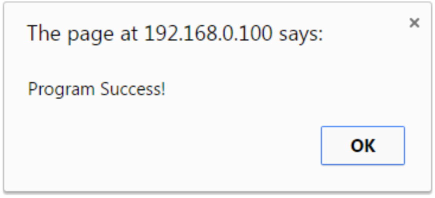
	Option	Default	Function
Sensor Configuration Menu	Select Sensor to Configure	1 Sensor	Choose among 64 sensors.
	Sensor Name	Blank	Custom 32 character name
	Sensor Type	3 Entry Exit Delay 1	Sensor types determine the sensor attributes such as entry/exit, instant, etc. Additionally sensor types determine the siren attributes.
	Sensor Option	1 Bypass	Sensor options determine the sensor attributes such as a sensor's ability to be bypassed, force arm, Cross Zone, stay mode, etc. Additionally sensor options determine the sensors reporting attributes.
	Area Group	1 Area 1	Assigning a sensor to an area will enable it to report.
	Serial Number	Blank	This is the TXID of the wireless sensor, it can be manual entered or the sensor can be "Learned" into panel.
	Tamper	On	Tamper switch on the wireless sensor is enabled or disabled.
	Disable Internal Reed	Off	The internal reed switch(es) on the wireless device can be disabled. Applies if the sensor is a device type 10.
	Norm Open External Contact	Off	The external input on wireless sensors can be enabled. Check this box when external contact is normally open. If the 60-362N-10-319.5 sensor is used the jumper pin does not have to be used. Applies if the sensor is a device type 10.
	Signal Strength	0	Shows the last signal strength received
	Voice Name 1	Blank	This feature uses the internal voice vocabulary to name the sensor. These names will be announced in sequence when the sensor is opened while in the Chime mode.
	Voice Name 2	Blank	
	Voice Name 3	Blank	
	Voice Name 4	Blank	

When you are finished programming the Sensor

Press the **Save** button.
A dialogue box appears.
Press the **OK** button.
A dialogue box appears.
Press the **OK** button.


The page at 192.168.0.100 says:

Are you sure you want to change the sensor ID and/or type?


The page at 192.168.0.100 says:

Program Success!

These dialogue boxes appear after any changes to the system are attempted/registered.

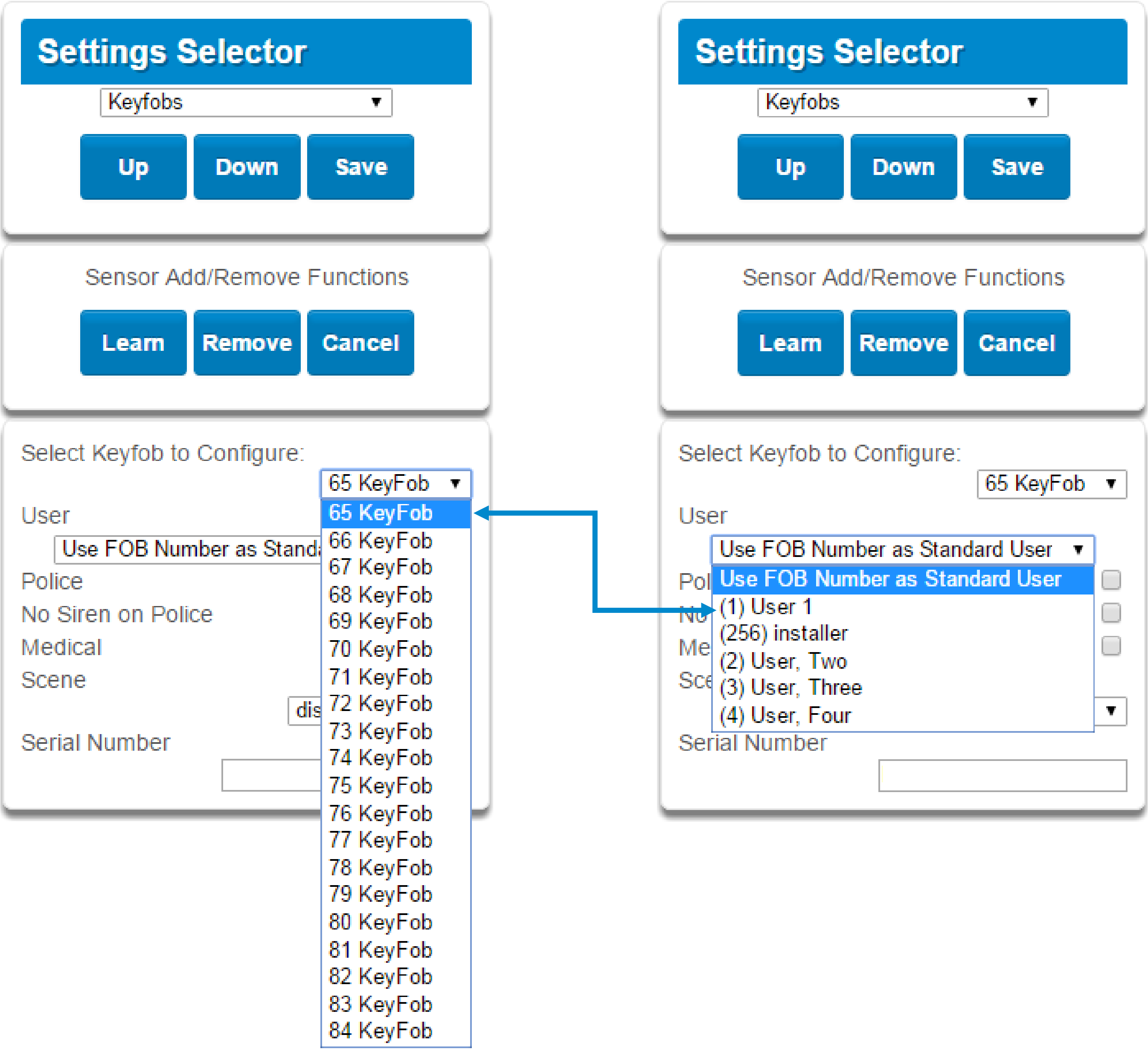
Note: After you have finished programming a sensor, be sure to advance the sensor number in the drop down menu when programming the next sensor. Otherwise you will over-write the sensor configuration you just programmed.

4.2 Learn in a Keyfob

Press ••• More then ⚙ Settings for the **SettingsSelector** page.

Select the drop down menu under **Sensors** to see the list of programmable items.
Select **Keyfobs**.

With the keyfobs screen selected you can choose the keyfob number to configure and select the user number to link to the keyfob.



Settings Selector

Keyfobs ▼

Up | Down | Save

Sensor Add/Remove Functions

Learn | Remove | Cancel

Select Keyfob to Configure: 65 KeyFob ▼

65 KeyFob
66 KeyFob
67 KeyFob
68 KeyFob
69 KeyFob
70 KeyFob
71 KeyFob
72 KeyFob
73 KeyFob
74 KeyFob
75 KeyFob
76 KeyFob
77 KeyFob
78 KeyFob
79 KeyFob
80 KeyFob
81 KeyFob
82 KeyFob
83 KeyFob
84 KeyFob

User

Use FOB Number as Standa

Police

No Siren on Police

Medical

Scene

dis

Serial Number

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 ▼

Use FOB Number as Standard User
(1) User 1
(256) installer
(2) User, Two
(3) User, Three
(4) User, Four

Pol □

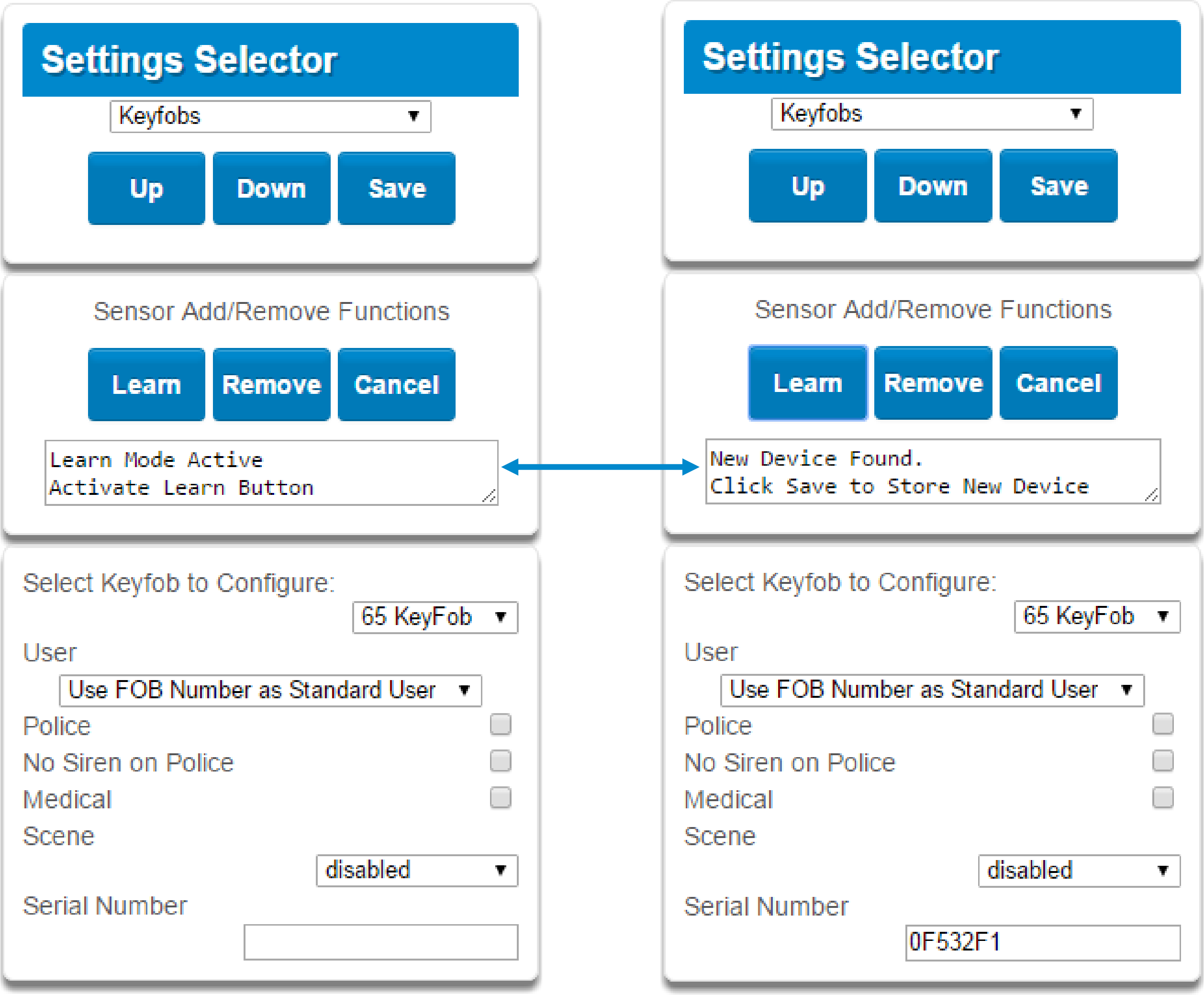
No □

Me □

Sce ▼

Serial Number

Give the keyfob a number (you are giving the keyfob a sensor number). Select the user and press **Learn**. A notification box will appear below the learn button. Activate the keyfob. Consult the keyfob manual for instructions; generally this is performed by simultaneously pressing the lock and unlock buttons. This will send a tamper signal to the panel.



Settings Selector: Keyfobs

```
Learn Mode Active
Activate Learn Button
```

```
New Device Found.
Click Save to Store New Device
```

Select Keyfob to Configure: 65 KeyFob

User: Use FOB Number as Standard User

Police □

No Siren on Police □

Medical □

Scene: disabled

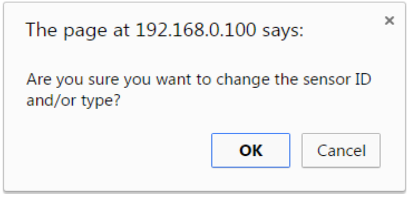
Serial Number: 0F532F1

The notification box will alert you that a new device (keyfob) was found. The keyfob Serial Number box will be populated. Explanations of the Keyfob configurations appear on the next page.

Keyfob Configuration Menu	Option	Default	Function
	Select Keyfob to Configure	65 Keyfob	This is the starting Sensor number for Keyfobs.
	User	Use FOB Number as Standard User	If "Use FOB Number as Standard User” is used, when there is an activation on that Fob the Central Station report will come in with that sensor number. If there is a user assigned to the fob that user number will come in on the Central Station Report. If no user is assigned it will show as user 999 in the Central Station Report.
	Police	Off	Enabling this will enable the Police / Panic on the Fob, this will also be audible at the panel (top 2 buttons press at the same time).
	No Siren on Police	Off	With this enabled it will make the Police / Panic silent at the panel.
	Medical	Off	Enabling this will enable the Medical / Aux on the Fob. This will be an audible alarm at the panel. (bottom 2 buttons pressed at the same time)
	Scene	Off	By using the drop down menu one of 16 scenes can be activated.
	Serial Number	Blank	This is the TXID of the Fob, it can be manually entered or the sensor can be "Learned" into panel.

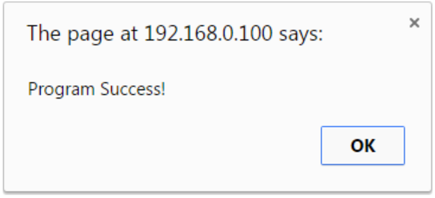
When you are finished programming the Keyfob,

Press the **Save** button.
A dialogue box appears.
Press the **OK** button.
A dialogue box appears.
Press the **OK** button.



The page at 192.168.0.100 says:

Are you sure you want to change the sensor ID and/or type?



The page at 192.168.0.100 says:

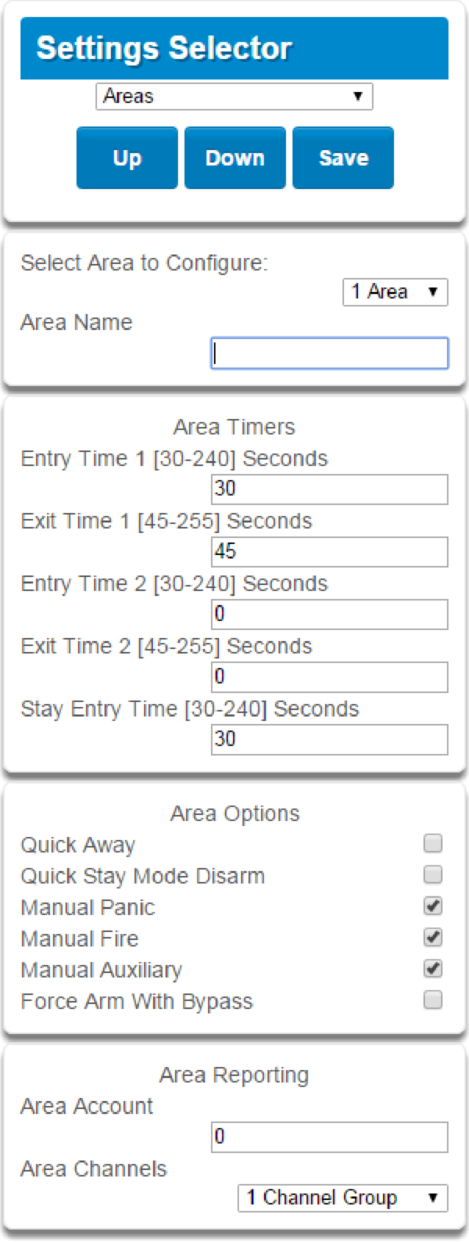
Program Success!

These dialogue boxes appear after any changes to the system are attempted/registered.

4.3 Programming Areas

Select **Areas** from the drop down menu.

With the Areas screen selected you can choose an Area number to configure, give the area a name, and define attributes for that area.
The hub can support a total of 4 areas; each area is configured with its entry and exit times, area options, area timers, area type and reporting characteristics.



Select Area to Configure: 1 Area ▾

Area Name

Area Timers

Entry Time 1 [30-240] Seconds: 30

Exit Time 1 [45-255] Seconds: 45

Entry Time 2 [30-240] Seconds: 0

Exit Time 2 [45-255] Seconds: 0

Stay Entry Time [30-240] Seconds: 30

Area Options

- Quick Away ☐
- Quick Stay Mode Disarm ☐
- Manual Panic ☑
- Manual Fire ☑
- Manual Auxiliary ☑
- Force Arm With Bypass ☐

Area Reporting

Area Account: 0

Area Channels: 1 Channel Group ▾

Explanations of the Area configurations appear on the following pages.

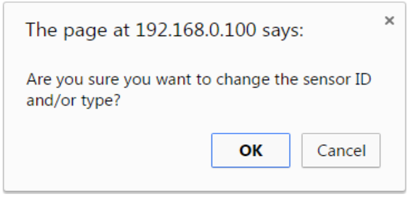
Also reference Advanced Programming, Areas, Section 5.3.

Areas Configuration Menu

	Option	Default	Function
	Select Area to Configure	Area 1	Use the drop down menu to select which of the 4 areas to program.
	Area Name	Blank	Each area can be configured with a custom 32 character name. The area name is displayed wherever an area is referenced on the system.
Area Timers	Entry Time 1 (30-240) Seconds	30	Provides time to enter into the premises to deactivate the alarm system.
	Exit Timer 1 (45 - 255) Seconds	45	Provides time to exit the premise without activating the alarm system.
	Entry Timer 2 (30 - 240) Seconds	0	If there is a second entry door that requires more time to deactivate the alarm system.
	Exit Timer 2 (45 -255) Seconds	0	If there is a second exit door that requires more time to leave.
	Stay Enter Timer (30 - 240) Seconds	30	When the system is armed to "STAY" this will be the entry time to deactivate the alarm system.
Area Options	Quick Away	Off	If enabled, the area can be armed in away mode with a single press. When area is armed via quick away mode, the closing user number is the default user of 999.
	Quick Stay Mode Disarm	Off	If enabled, this will allow the stay mode to be disarmed by pressing the stay key on the panel. If the system is in alarm a PIN must be used.
	Manual Panic	On	Enables or Disables the Keypad Panic
	Manual Fire	On	Enables or Disables the Keypad Fire
	Manual Auxiliary	On	Enables or Disables the Keypad Auxiliary
	Force Arm With Bypass	Off	If enabled, the area can be armed even if sensors are not ready. Any sensors 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 Auto-Bypass is enabled. Individual sensors can be made “force arm-able without auto-bypass” by leaving this area option off, then enabling Forced Arm Enable in Sensor options, and disabling Sensor Inhibit (Bypass) in the Sensor Type Profile.

Areas Configuration Menu	Area Reporting	Area Account	0	This account number is ONLY used when sending an email. This should be the same as the Central Station account number, however if it is not this will not affect the Central Station reporting
		Area Channels	1 Channel Group	This determines which channel will be used to report area events to the Central Station. The channel must be configured in the Channel option programming.

When you are finished programming the Area settings, remember to save your changes.



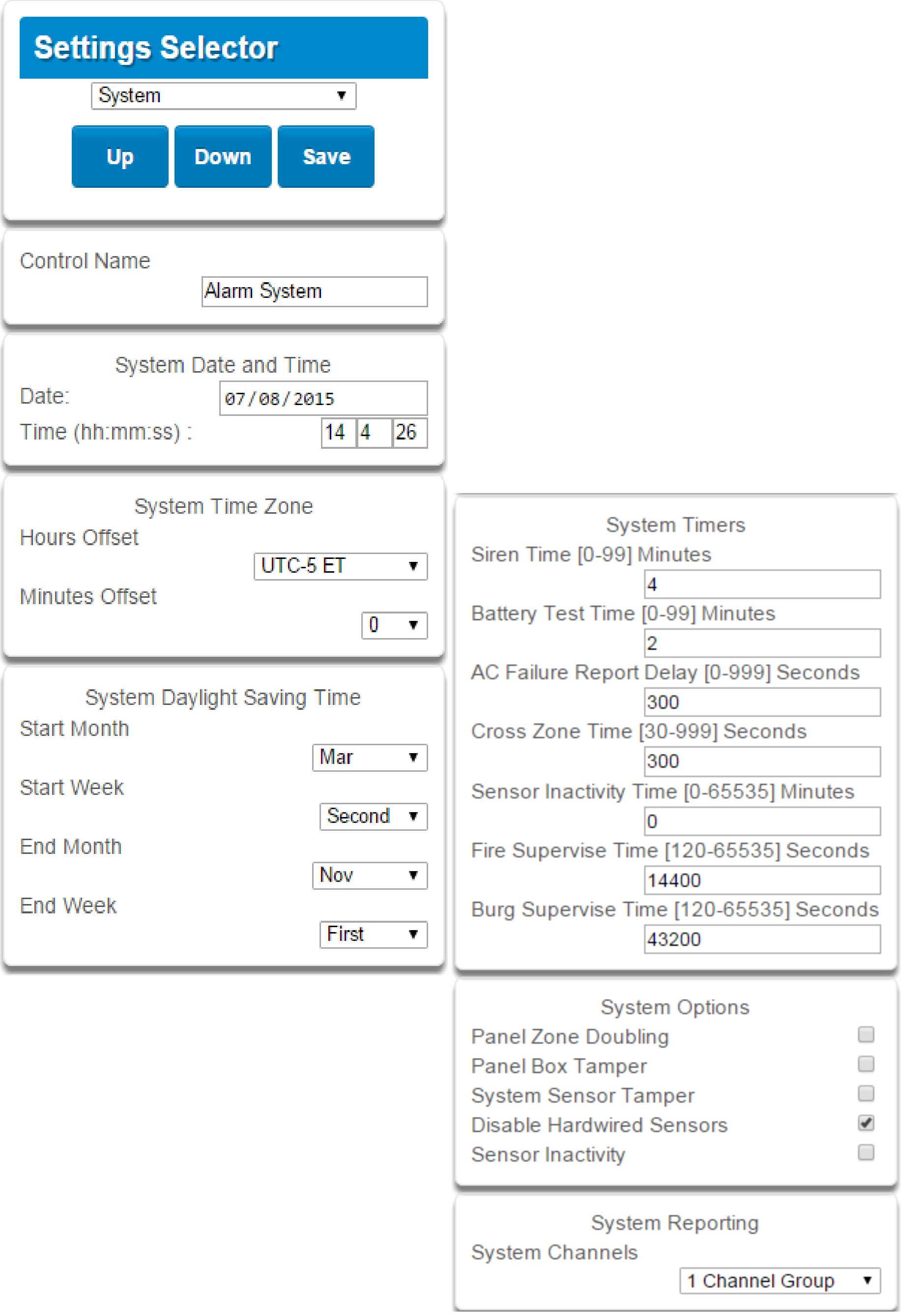
The page at 192.168.0.100 says:

Are you sure you want to change the sensor ID and/or type?

4.4 Programming the System

Select **System** from the drop down menu.

When the System screen is selected you can program several system wide settings, including the system clock and timers, as well as sensor options and reporting.



System ▾

Control Name: Alarm System

System Date and Time

Date: 07/08/2015

Time (hh:mm:ss) : 14 4 26

System Time Zone

Hours Offset: UTC-5 ET ▾

Minutes Offset: 0 ▾

System Daylight Saving Time

Start Month: Mar ▾

Start Week: Second ▾

End Month: Nov ▾

End Week: First ▾

System Timers

Siren Time [0-99] Minutes: 4

Battery Test Time [0-99] Minutes: 2

AC Failure Report Delay [0-999] Seconds: 300

Cross Zone Time [30-999] Seconds: 300

Sensor Inactivity Time [0-65535] Minutes: 0

Fire Supervise Time [120-65535] Seconds: 14400

Burg Supervise Time [120-65535] Seconds: 43200

System Options

Panel Zone Doubling □

Panel Box Tamper □

System Sensor Tamper □

Disable Hardwired Sensors ☑

Sensor Inactivity □

System Reporting

System Channels: 1 Channel Group ▾

When you are finished programming the System settings, remember to save your changes.

Explanations of the System configurations appear on the following pages.

Also reference Advanced Programming, System, Section 5.1.

System Configuration Menu

Option		Default	Function
Date &Time	Date		Once it is connected to UltraSync the Date and time are automatically synced.
	Time (hh:mm:ss)		Once it is connected to UltraSync the Date and time are automatically synced.
Time Zone	Hours Offset	UTC 5 ET	Starting with EST is UTC-5, CST is UTC-6, MT is UTC-6, PST is UTC-7.
	Minutes Offset	0	This is used in other locations throughout the world.
Daylight Saving Time	Start Month	Mar	Standard
	Start Week	Second	Standard
	End Month	Nov	Standard
	Start Month	First	Standard
System Timers	Siren Time (0-99) Minutes	4	The siren time sets the time in minutes that the siren output is active.
	Battery Test Time (0-99) Minutes	2	The battery test time sets the duration in minutes that the system will perform a dynamic battery test. The system will perform a dynamic battery test at the disarming of the first area or at midnight once each 24-hour cycle. Dynamic battery test is disabled when the test duration is set to 0. Dynamic battery test can also be run manually from a keypad.
	AC Failure Report Delay (0-999) Seconds	300	The AC fail 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.
	Cross Zone Time (30-999)	300	The Cross Zone time sets the duration in seconds whereby two or more sensors must trip before an alarm condition will be registered or the one sensor must trigger twice within this time period, or a continuous trip longer than 10 seconds. This feature only applies to sensors with the Cross Zone feature set in sensor options.
	Sensor Inactivity Time (0-65535) Minutes	0	Sensors programmed with Sensor Inactivity in the Sensor Options must be opened and closed within the time programmed here (in minutes). If they do not, a Sensor Inactivity will report. This feature can be enabled in the System Options menu. Default Sensor Inactivity option is off and this timer is set to 10080 minutes (7 days).

System Configuration Menu

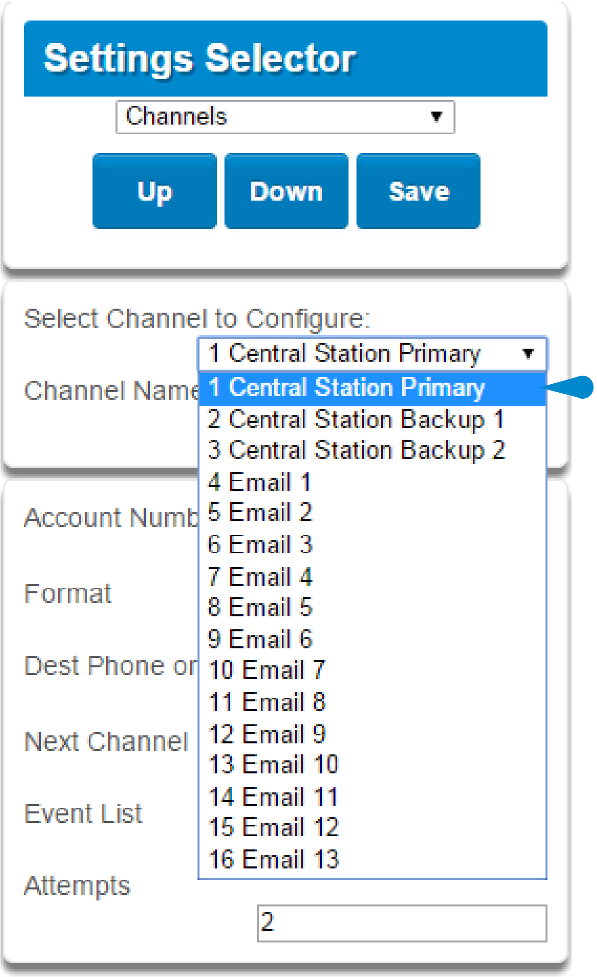
	Option	Default	Function
System Timers	Fire Supervise Time (120-65535) Seconds	14400	This applies only to wireless sensors programmed as fire type. Sensors send a reduced packet count supervisory signal every 60 minutes (check your sensor manual for most up to date details). If no supervisory signal is received by the panel within the time specified here then the sensor 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.
	Burg Supervise Time (120-65535) Seconds	14400	This applies only to wireless sensors programmed as non-fire type. Sensors send a reduced packet count supervisory signal every 60 minutes (check your sensor manual for most up to date details). If no supervisory signal is received by the panel within the time specified here then the sensor 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.
System Options	Panel Sensor Doubling	Off	If enabled, the two (2) hardwired sensor inputs will be doubled to support four (4) sensors. The terminals for Sensor 1 will represent sensors 1 and 3, and the terminals for sensor 2 will represent sensor 2 and 4. This option cannot be selected for sensors other than the two sensors on the main panel. This option cannot be used in conjunction with the DEOL option.
	Panel Box Tamper	Off	The panel has a built-in normally closed tamper switch that will sound the siren if the panel is removed from the wall. This option will enable or disable this tamper switch.
	System Sensor Tamper	Off	If enabled, the hub will monitor all sensors, except fire sensors, for Dual End of Line (DEOL). A short or open circuit on a DEOL will activate sensor tamper alarms. This feature cannot be used if Panel Sensor Doubling is enabled.
	Disable Hardwire Sensors	On	If enabled, the hub will disable all hardwired sensor inputs.
	Sensor Inactivity	Off	If enabled, the system will monitor each sensor for activations. If no activations occur within the sensor activity time then a failed sensor activity report may be reported via the selected communication channel and a failed sensor activity message set in the hub's event log. For a sensor to be eligible for activity monitoring, it must have "Sensor Activity" set in sensor options. Sensors programmed with Sensor Inactivity in the Sensor Options must be open and closed within the time programmed here (in minutes). If they do not, a Sensor Inactivity will report.
System Reporting	System Channel	1 Channel Group	The Channel Group that the hub will send system events to.

4.5 Programming Reporting and Notifications

Select **Channels** from the drop down menu.

With the Channels screen selected you can program a communication path for events to be sent from the panel to a selected destination.

The hub 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.



Choose a channel in the drop down menu and assign it attributes.
Explanations of the Channel Configuration menu appear on the following page.

Also reference Advanced Programming, Reporting and Notifications, Section 5.4.

When you are finished programming the Channel settings, remember to save your changes.

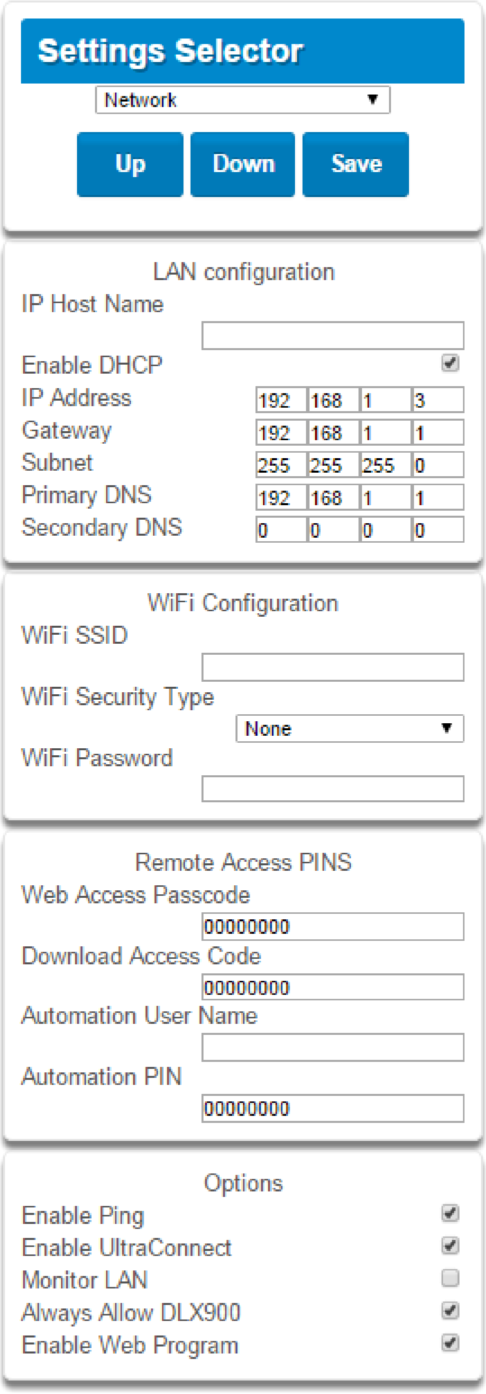
Channel Configuration Menu

Option	Default	Function
Select Channel to Configure	1 Central Station Primary	
Channel Name	Central Station Primary	Custom names of the selected channel can be created here.
Account Number	Blank	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	UltraSync	This is the communication format for the selected channel. Select from: UltraSync Email
Dest Phone or Email	Blank	The phone number or email address of the selected destination.
Next Channel	Central Station Backup 1 Central Station Backup 2 Email 1 Email 2 Email 3 Etc.	If the channel selected is unable to deliver the event to the selected destination, the system will use this backup channel if the primary channel fails. The Next Channel specified here must be greater than the Channel Number.
Event List	1 Event List	Select the pre-programmed list of events that will be sent via this channel. The specific event in each event list is programmed in Advanced Programming, Channels. See Channels Programming Event List.
Attempts	2	Enter the number of times the hub should try to send the events to the UltraSync server. After the number of attempts has been exhausted the hub will try the Next Channel if specified.

4.6 Programming the Network

Select **Network** from the drop down menu.

Enter your network settings on this page.



LAN configuration

IP Host Name				
Enable DHCP	☑			
IP Address	192	168	1	3
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: 00000000

Download Access Code: 00000000

Automation User Name

Automation PIN: 00000000

Options

Enable Ping	☑
Enable UltraConnect	☑
Monitor LAN	☐
Always Allow DLX900	☑
Enable Web Program	☑

Explanations of the Network Configuration Menu appear on the following pages. Remember to save your changes when you are finished programming the Network settings.

Option	Default	Function
LAN Configuration		
IP Host Name	-	A text label assigned to the hub's communicator so you do not have to remember the IP Address. **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.
Enable DHCP	Off	Allows the panel to be automatically assigned an IP address by the network.
IP Address	-	The IP address assigned to the hub which enables it to connect to the local LAN. This will allow you to access the embedded web server of the hub 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.
WI FI Configuration		
WI FI SSID	Blank	Wi Fi Network name the hub is connecting to
WI FI Security type	Blank	WEP/WEP-128bit/WPA2-Passphrase
WI FI Password	Blank	Network password, which must match the password assigned to the WIFI SSID (access point). There can be no special charterers, only Alphanumeric.
Remote Access PINS		
WEB Access Passcode	0	The UltraSync app requires the Web Access Code to get access to the panel. The default Web Access Passcode of 00000000 disables remote access. The system allows for an 8 digit numeric (only) code. Each owner should have a unique number.
Download Access Code	0	Enables remote access for DLX900. The default Download Access Passcode of 00000000 prevents remote access.
Automation User Name	Blank	Used when there is API integration
Automation PIN	Blank	Used when there is API integration
Options		
Enable Ping	On	Allows the panel to respond to the PING command.

Option	Default	Function
Enable UltraSync	On	This is an automatic feature of the UltraSync Self-Contained Hub. It is recommended you leave this setting on. Enable this option to allow the system 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 the hub will override ignore this setting and allow email reporting via UltraSync cloud servers. If you wish to prevent connections to the UltraSync cloud servers, then uncheck this option and do not use the UltraSync reporting format. Also reference table in submenu 16 of Advanced Programming, Communicator.
Monitor LAN	Off	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.
Always Allow DLX900	On	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 DLX900 access disabled until a user on site with physical access to the keypad enters program mode with a valid PIN code. The hub will be in program mode if a user gains authorized access to menu 5, 8, or 9 on the keypad.
Enable Web Programming	On	Enabling this option will cause the hub's Web Server and UltraSync app to always display Installer menus regardless of if the panel is in program mode or not. Disabling this option will hide the Installer menus on the hub's Web Server and UltraSync app unless program mode is active. This provides greater security by keeping web programming disabled unless a user on site with physical access to the keypad enters program mode with a valid PIN code. The hub will be in program mode if a user gains access to menu 5, 8, or 9. UltraSync app requires the Web Access Code to get access to the panel.

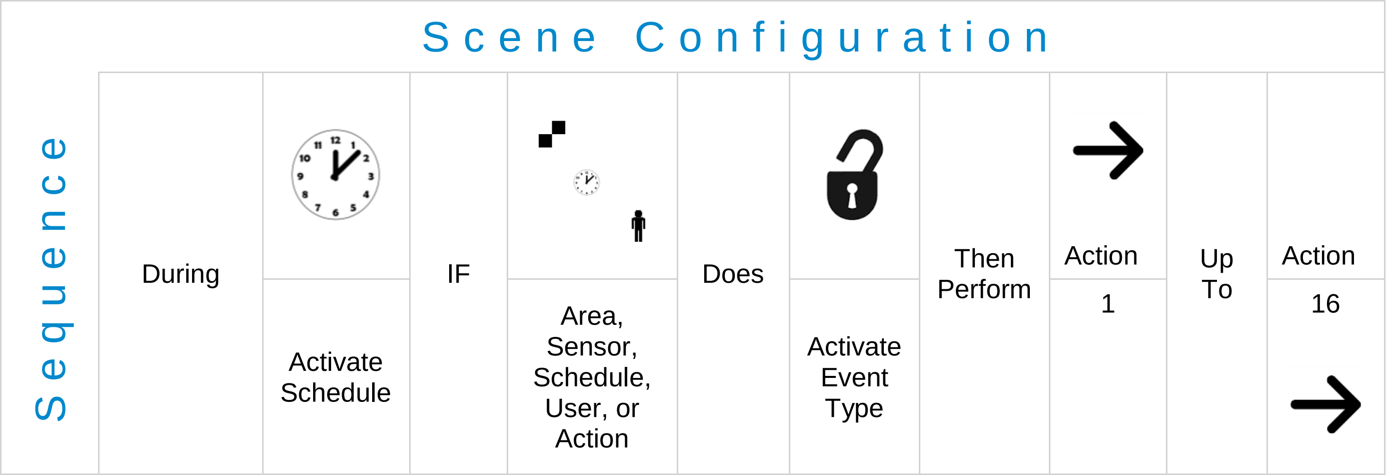
4.7 Programming Scenes

Select **Scenes** from the drop down menu.

With the Scenes screen selected you can create scenes on schedules and determine which event types and device triggers will activate them.

Each scene can trigger up to 16 consecutive scene actions when certain conditions are 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.

Remember to save your changes when you are finished programming the Scene settings.



Scene Configuration

Sequence

During

Activate Schedule

IF

Area, Sensor, Schedule, User, or Action

Does

Activate Event Type

Then Perform

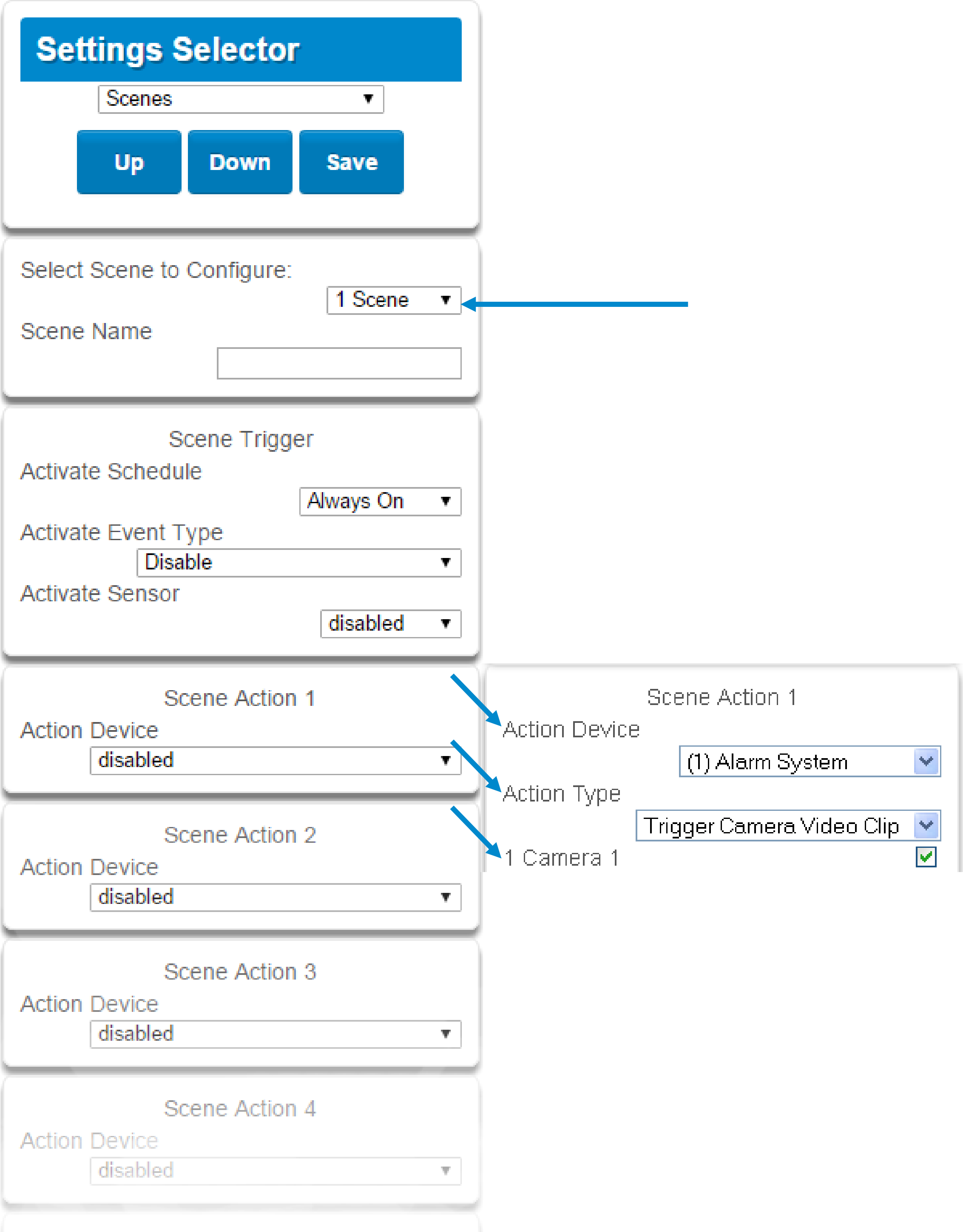
Action 1

Up To

Action 16

Explanations of the Scene Configuration Menu appear on the following pages.

Also reference Advanced Programming, Scenes, Section 5.18.



Scenes

Select Scene to Configure: 1 Scene

Scene Name

Scene Trigger

Activate Schedule: Always On

Activate Event Type: Disable

Activate Sensor: disabled

Scene Action 1

Action Device: disabled

Scene Action 2

Action Device: disabled

Scene Action 3

Action Device: disabled

Scene Action 4

Action Device: disabled

Scene Action 5

Scene Action 1

Action Device: (1) Alarm System

Action Type: Trigger Camera Video Clip

1 Camera 1 ☑

Example Scene

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

	Option		Default	Function
Scene Configuration Menu	Select Scene to Configure			The hub can support a total of 16 Scenes. Each Scene is identified by a unique number, which cannot be altered, and remains 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 system.
	Scene Trigger	Activate Schedule	Always On	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	Disable	Select the event that will trigger this Scene. You can reference Activate Events list in Advanced Programming, Scenes.
		Activate Sensor	Disabled	Select which Area \ Sensor \ Schedule \ User \ Action \ Device will provide the trigger for the Scene.
	Scene Action 1 Action Device		Disabled	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 **1.** Alarm System Action **2.** ZWave Device Action. Alarm System Action Result Type - The event of the Action Result to perform. See Advanced Programming, Scenes and the Scene Action and Scene Action Events Types for reference. Result Number - Select the area / scene / camera number to control: ZWave Device Action To display ZWave Action Types you must first learn in a ZWave device. The ZWave device name will then appear. Action Device – select the ZWave device you want to control ZWave Type 8 Setting 1 – depends on ZWave device. May include options such as On, Off, Heat, Cool, Auto, Up, Down, Lock, Unlock.
	Scene Action 2 Action Device		Disabled	
	Scene Action 3 Action Device		Disabled	
	Scene Action 4 Action Device		Disabled	
	Scene Action 5 Action Device		Disabled	
	Scene Action 6 Action Device		Disabled	
	Etc.		Etc.	
	Etc.		Etc.	

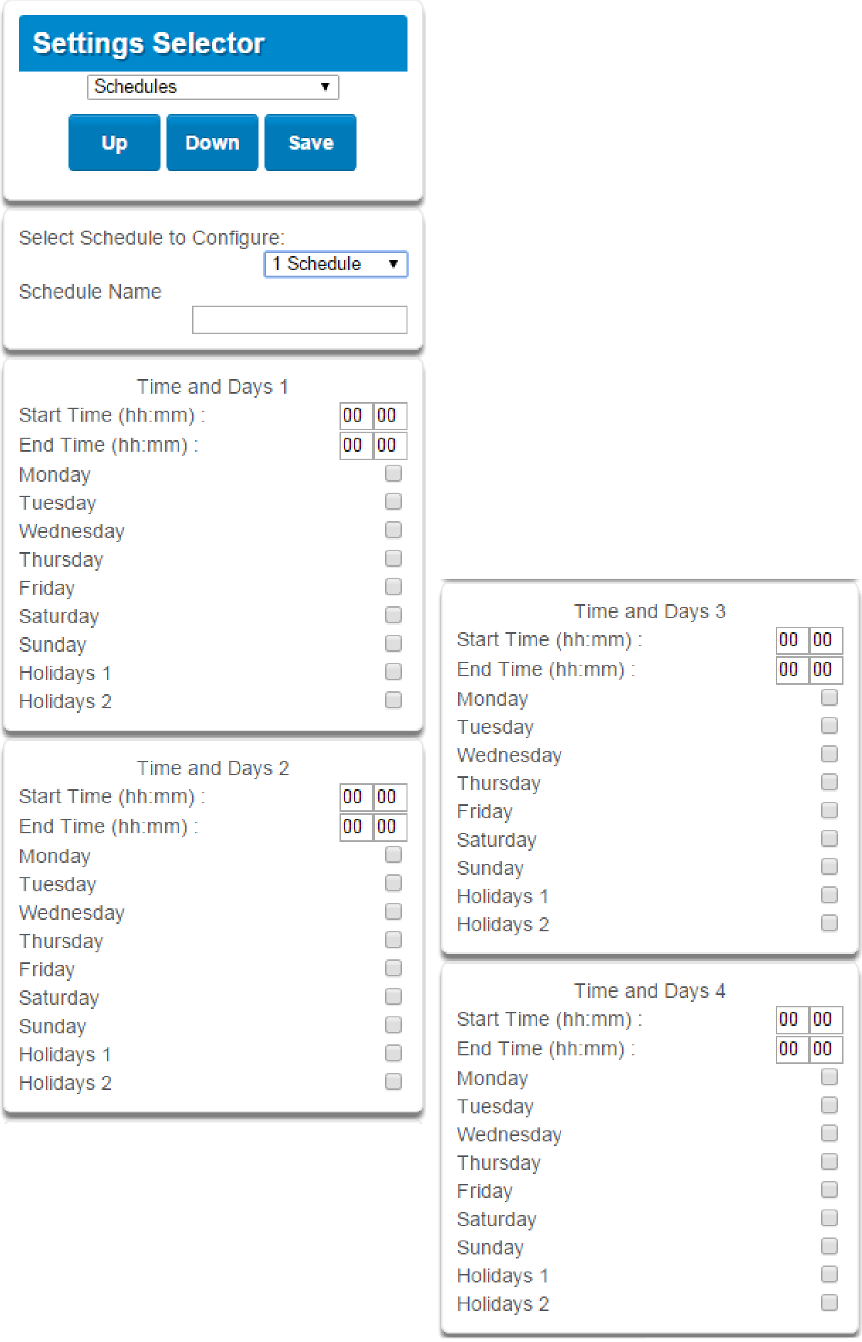
4.8 Programming Schedules

Select **Schedules** from the drop down menu.

With the Schedules screen selected you can create up to 16 schedules, each having four time and day periods.

Explanations of the Schedules Configuration menus appear on the following pages. Also reference Advanced Programming, Schedules, Section 5.6.

Remember to save your changes when you are finished programming the Schedules settings.



Settings Selector

Schedules ▾

Select Schedule to Configure: 1 Schedule ▾

Schedule Name

Time and Days 1

Start Time (hh:mm) : 00 00

End Time (hh:mm) : 00 00

Monday □
Tuesday □
Wednesday □
Thursday □
Friday □
Saturday □
Sunday □
Holidays 1 □
Holidays 2 □

Time and Days 2

Start Time (hh:mm) : 00 00

End Time (hh:mm) : 00 00

Monday □
Tuesday □
Wednesday □
Thursday □
Friday □
Saturday □
Sunday □
Holidays 1 □
Holidays 2 □

Time and Days 3

Start Time (hh:mm) : 00 00

End Time (hh:mm) : 00 00

Monday □
Tuesday □
Wednesday □
Thursday □
Friday □
Saturday □
Sunday □
Holidays 1 □
Holidays 2 □

Time and Days 4

Start Time (hh:mm) : 00 00

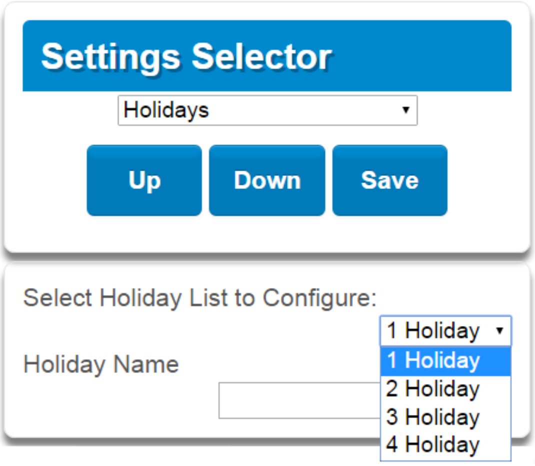
End Time (hh:mm) : 00 00

Monday □
Tuesday □
Wednesday □
Thursday □
Friday □
Saturday □
Sunday □
Holidays 1 □
Holidays 2 □

		Option	Default	Function
Schedules Configuration Menu		Select Schedule to Configure	1 Schedule 1	The hub 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	Schedule 1	Each schedule can be configured with a custom 32 character name. The area name is displayed wherever a schedule is referenced on the system.
	Time and Days 1 -16	Up to 16 Start and Stop times can be created. **Note**: The hub handles schedules that span midnight automatically		
		Start Time (hh:mm)	-	Enter in the start time
		End Time (hh:mm)	-	Enter in the stop time
		Monday	-	Enter in the days of the week the schedule is to be active
		Tuesday	-	
		Wednesday	-	
		Thursday	-	
		Friday	-	
		Saturday	-	
		Sunday	-	
		Holiday 1	-	Enter in the holiday that this schedule will be following. **Note**: When the holiday is enabled the schedule will not be active.
		Holiday 2	-	Same as Holiday 1
		Holiday 3	-	Same as Holiday 1
		Holiday 4	-	Same as Holiday 1

4.9 Programming Holidays

Select **Holidays** from the drop down menu.



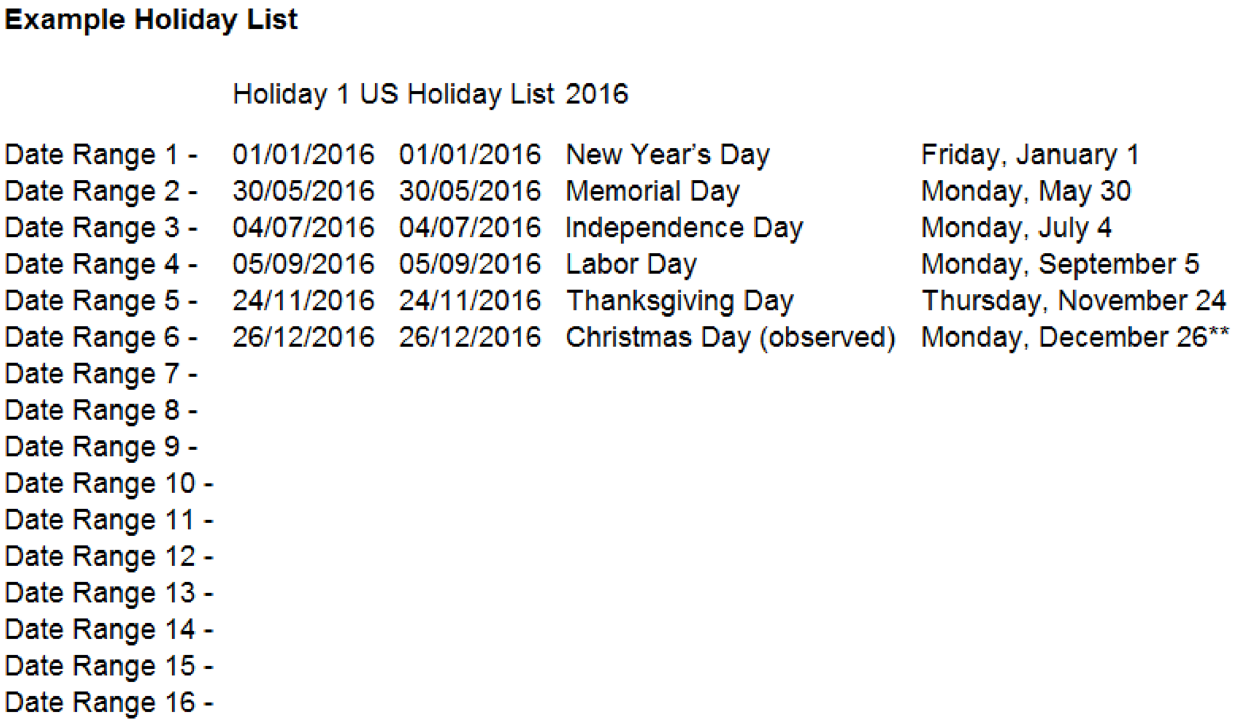
Select Holiday List to Configure: 1 Holiday

Holiday Name

With the Holidays screen selected you can create up to four sets of holiday dates for the system. Set the number, name and date range for each holiday. Holidays are then assigned to the schedules and used to deactivate the schedule while the holiday is active. Remember to save your changes when you are finished programming the Holidays settings.

Explanations of the Holiday configurations appear below.
Also reference Advanced Programming, Holidays, Section 5.13.

	Option		Default	Function
Holiday Configuration Menu	Select Holiday List to Configure		n/a	The hub 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 #	1 Holiday 2 Holiday 3 Holiday 4 Holiday	n/a	The hub can support a total of 4 Holiday Sets. Each set 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 system.
	Start -End	Start Date	n/a	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.
		End Date	n/a	



Example Holiday List

Holiday 1 US Holiday List 2016

Date Range 1 -	01/01/2016	01/01/2016	New Year's Day	Friday, January 1
Date Range 2 -	30/05/2016	30/05/2016	Memorial Day	Monday, May 30
Date Range 3 -	04/07/2016	04/07/2016	Independence Day	Monday, July 4
Date Range 4 -	05/09/2016	05/09/2016	Labor Day	Monday, September 5
Date Range 5 -	24/11/2016	24/11/2016	Thanksgiving Day	Thursday, November 24
Date Range 6 -	26/12/2016	26/12/2016	Christmas Day (observed)	Monday, December 26**
Date Range 7 -				
Date Range 8 -				
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 (checked)

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

4.10 Programming Zwave Devices

See the Zwave Configuration Menu later in this section.

Also reference Advanced Programming, Devices, section 5.9.

Zwave Room Names

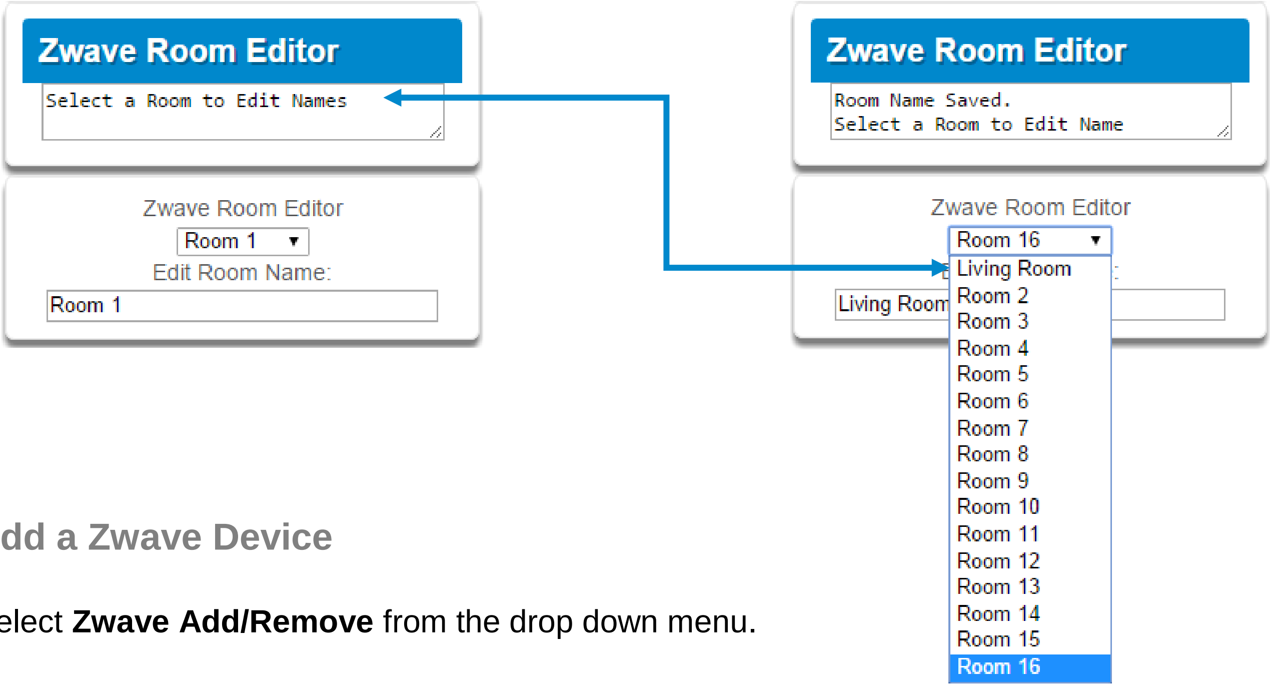
Select **Zwave Room Names** from the drop down menu.

From the drop down menu under **Zwave Room Editor** select a room to edit the name.

For this example we will change the name of Room 1 to Living Room.

Type Living Room in the form “Edit Room Name:” This can be a 32 character name.

Press **Save**. The notification box will alert you that the Room Name is Saved. The drop down list has been updated for Room 1.



Zwave Room Editor

Select a Room to Edit Names

Zwave Room Editor

Room 1

Edit Room Name:

Room 1

Zwave Room Editor

Room Name Saved.
Select a Room to Edit Name

Zwave Room Editor

Room 16

Living Room

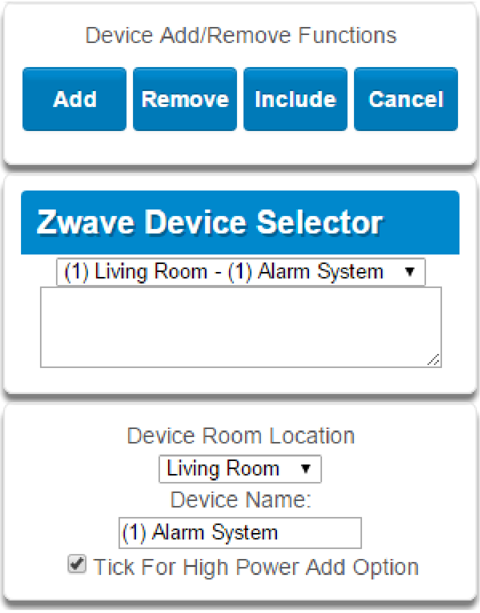
Add a Zwave Device

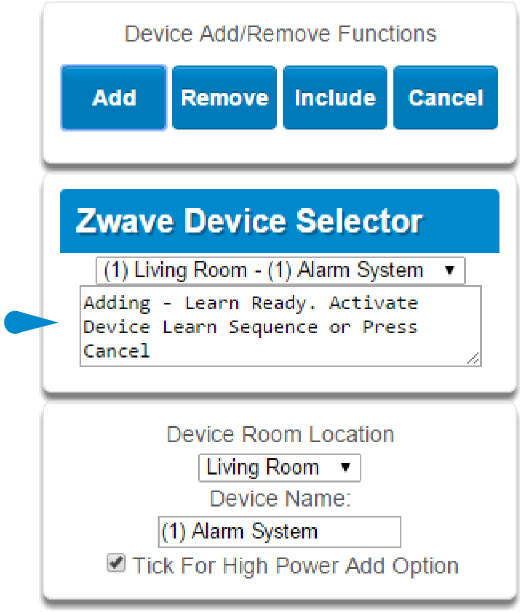
Select **Zwave Add/Remove** from the drop down menu.

1. Press **Add.**
2. Initiate ADD mode on ZWave device. See your ZWave device’s manual for instructions. The notification box will alert you that the Device is added.

Note: If a ZWave device has been added before or to another system, you must first remove it before adding it to this system. To do this, press **Remove**, then activate LINK or REMOVE mode on the device.

3. Press **Rooms**.
4. Check that you can see the device you just added. Press a button such as ON or OFF to verify that you can control the device.

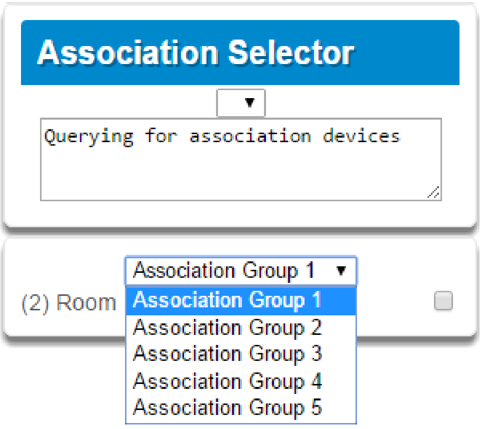




```
Adding - Learn Ready. Activate
Device Learn Sequence or Press
Cancel
```

Zwave Device Association

Select **Zwave Device Association** from the drop down menu.



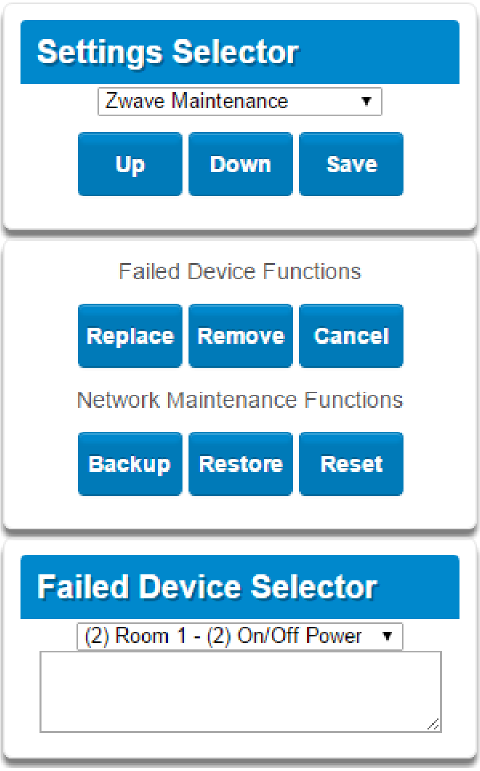
```
Querying for association devices
```

Zwave Maintenance

Select **Zwave Maintenance** from the drop down menu.
The Zwave Maintenance page main tile contains additional buttons from the settings tile.

Failed Device Functions:

REPLACE: This option is used when a Zwave device is defective, and it allows the replacement of the device while keeping the same Device number. The device number is what is used in Scenes association.
REMOVE: This option is used when a Zwave device is missing or is damaged to the point that it will not transmit signals.
BACKUP: This saves the Zwave programming to the panel.
RESTORE: This restores the Zwave programming to the last time is was saved.
RESET: This defaults all the Zwave programming in the panel.



Zwave Configuration Menus

	Option	Default	Function
Room Names	Zwave Room Editor	Drop down to select room to edit	Room Selection
	Edit Room Name	Room 1	Room Naming (up to 32 characters)
Device Selector	Device Room Location	Drop down to select the room location	
	Device Name	(1) Alarm	
	Check For High Power Add Option	On	
Device Association	Association Functions		
	Add		
	Remove		
	Query		
	Association Selector	Drop down list of all devices learned into the system	
	Association Group		
Maintenance	Failed Device Functions		
	Replace		
	Remove		
	Cancel		
	Network Maintenance Functions		
	Backup		
	Restore		
	Reset		
	Failed Device Selector	Drop down list of all the failed devices	

4.11 Wi Fi Setup

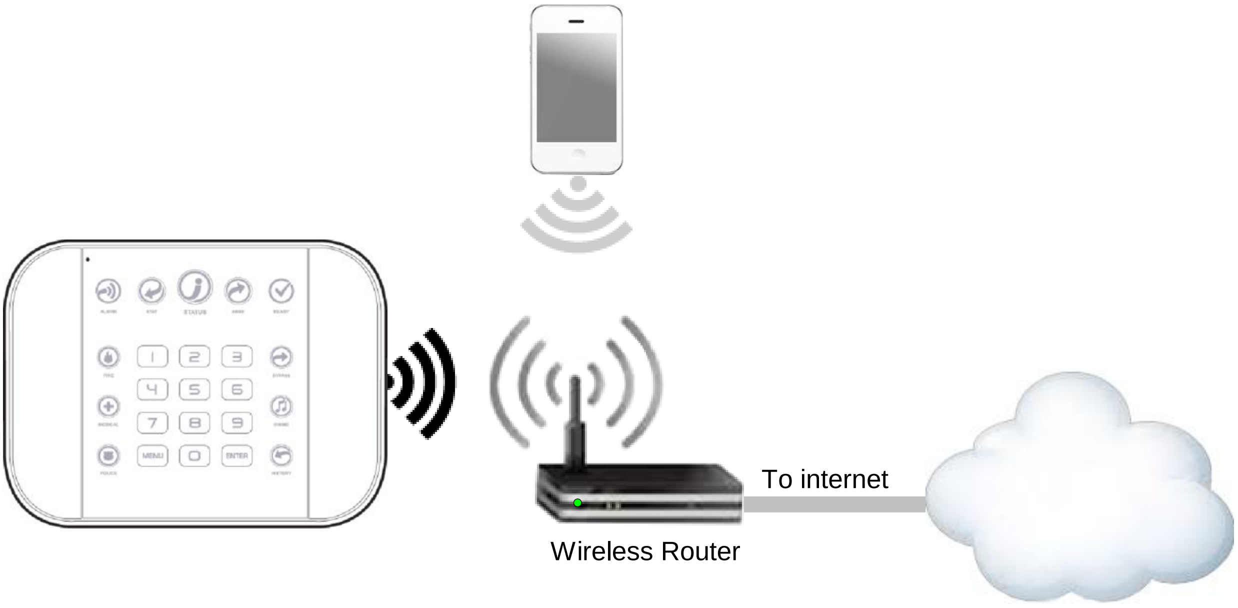
Turn on **Wi Fi Discovery Mode** on the panel – this provides direct access to the panel from a mobile device such as a smart phone, tablet, or laptop:

1.	MENU 9	Select main menu - Option 9, Advanced system configuration
2.	INSTALLER CODE ENTER	Enter Installer code
3.	8	Turn on WiFi Discovery Mode for 10 min
4.	MENU MENU	Exits from Advanced system configuration menu

Enable Wi Fi on your mobile device

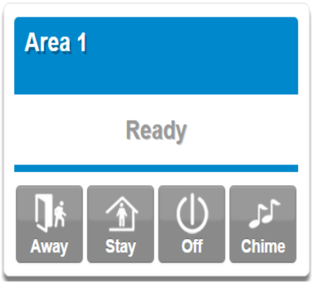
On your mobile device, browse for available Wi Fi networks and select the **ZeroWire_xxxx** network to connect to it. Only a single user can connect at any time and there is no Wi Fi password. Once connected the panel will be assigned a fixed IP address of 192.168.1.3.

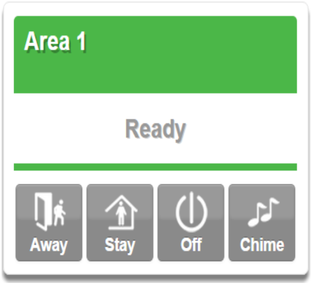
Use your device to connect to the panel. The wireless router must support 802.11 b or 802.11g.



Open your web browser and enter **192.168.1.3**. The login screen should appear.

Enter your username and password, by default this is: **installer** and **9-7-1-3**. Press **Sign In**. You should now see a screen similar to one of the below:



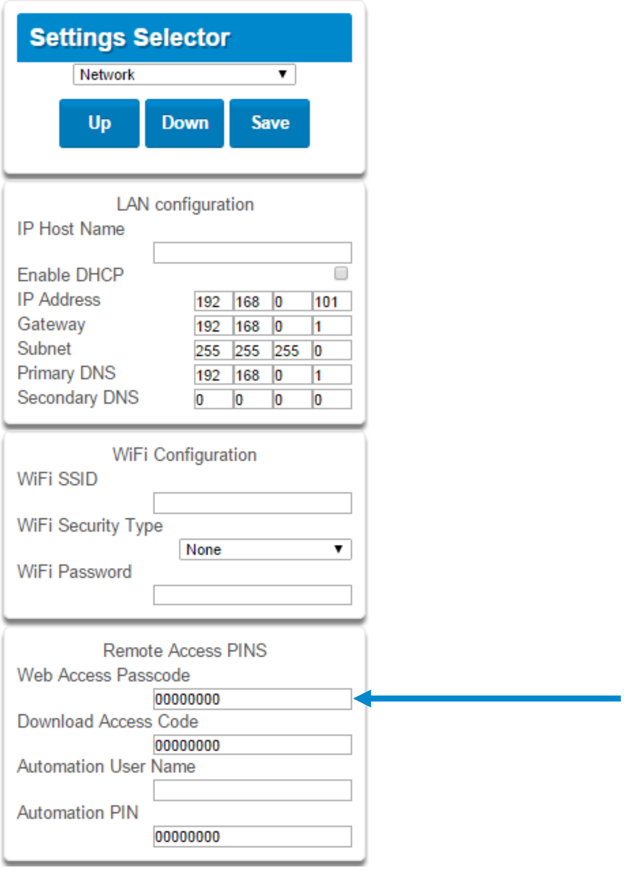


4.12 Set Up a Web Access Passcode for UltraSync

For security, the UltraSync app is disabled by default. Follow these steps to enable it:

Press ••• More then ⚙ Settings for the **SettingsSelector** page.

Select **Network** from the drop down menu.
Enter a Web Access Passcode:



LAN configuration

IP Host Name

Enable DHCP □

IP Address	192	168	0	101
Gateway	192	168	0	1
Subnet	255	255	255	0
Primary DNS	192	168	0	1
Secondary DNS	0	0	0	0

WiFi Configuration

WiFi SSID

WiFi Security Type: None ▼

WiFi Password

Remote Access PINS

Web Access Passcode: 00000000

Download Access Code: 00000000

Automation User Name

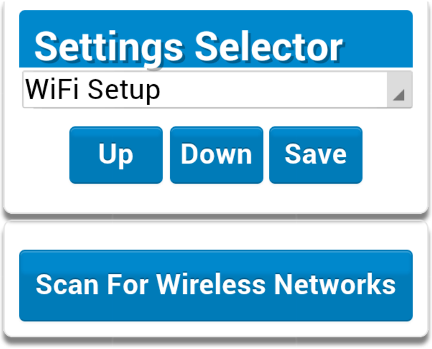
Automation PIN: 00000000

Press **Save**.

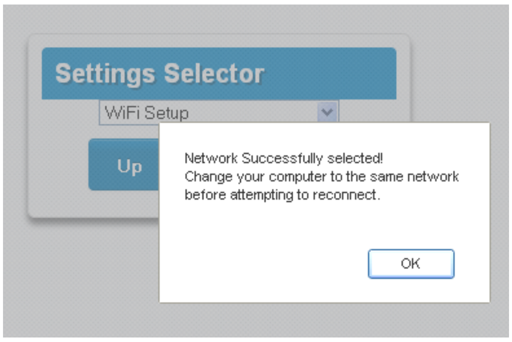
For a detailed explanation of function of the Web Access Passcode please see section 4.6 Programming the Network.

Scan for Wireless Networks

Select **Wi Fi Setup** from the drop down menu on the **SettingsSelector** page.
Press **Scan for Wireless Networks**:



Press the Wi Fi network name you wish to connect to.
Enter Wi Fi passcode then press **OK**. "Network Successfully selected" will appear as shown below. Your mobile device will be disconnected from the panel.

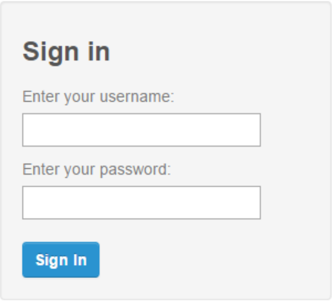


Network Successfully selected!
Change your computer to the same network before attempting to reconnect.

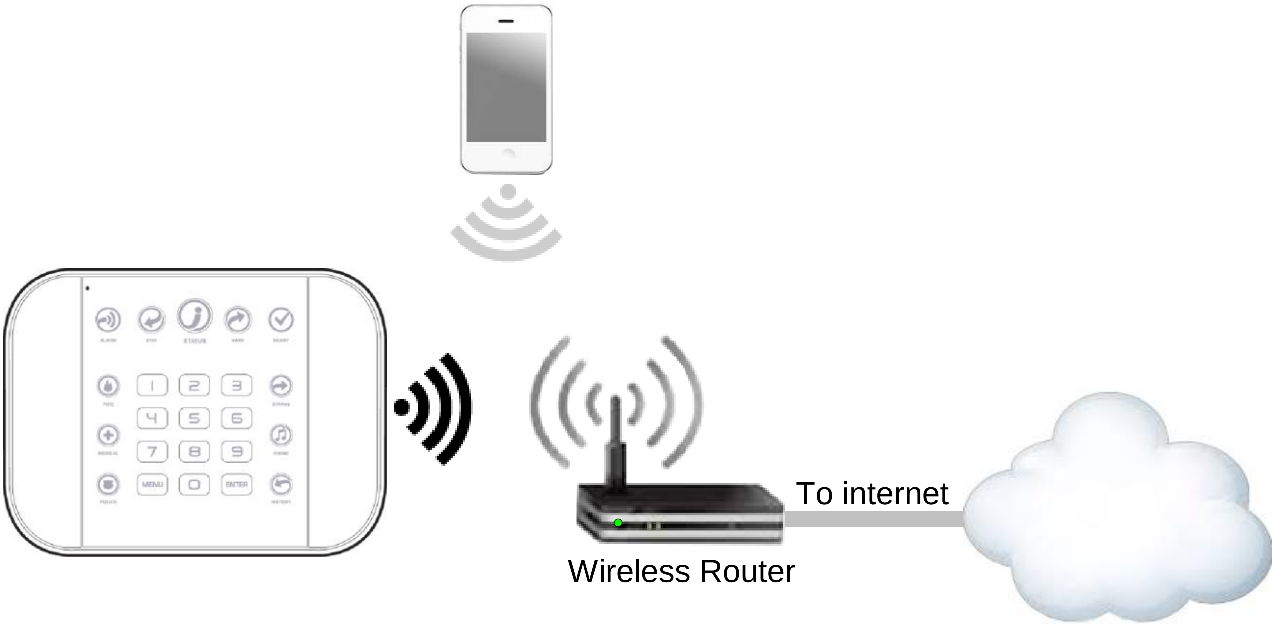
On your mobile device, connect to the same Wi Fi network found by the scan.
On the panel press **Menu – 8 – [PIN] – 6** and write down the IP address announced. This is the IP address of your panel. If you hear "IP address is not configured" then wait a further 30 seconds and repeat this step.

Open your web browser.

Enter announced **IP address**. The login screen should appear:



Your panel is now successfully connected to your Wi Fi network.



Troubleshooting Wi Fi Setup

1. Cannot get an IP address	
Cause	Solution
Connection does not work	*Close the web browser on your device, and restart your wireless router, and start again from step 1.*
The wireless/router may not be configured for automatic DHCP or certain security settings may be enabled.	*Check your router settings and try again.*

2. Network connections fail	
Cause	Solution
Some newer routers will have these off at factory default. Some 802.11n access points may not accept 802.11g connections.	*Check if Wi Fi router allows b and g connections.*
	Check if router is within range and has good signal, otherwise a Wi Fi range extender may help.
	Ensure auto-correct is turned off (when typing the pass phrase).
	Ensure wireless router has DHCP enabled.
	Ensure wireless router does not have firewall or security rules that prevent additional connections.
	Ensure IP addresses are available; for example connect a new device to it and verify it has an internet connection.

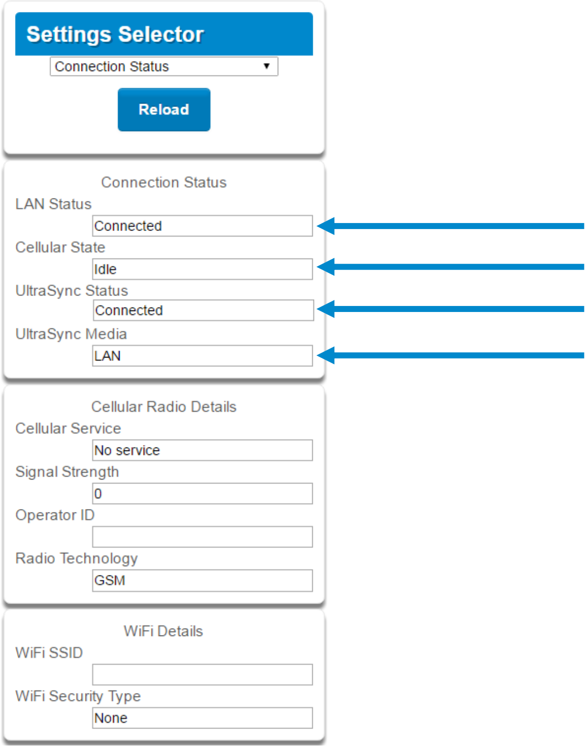
4.13 Check Wi Fi Connection to UltraSync

Login to the hub’s Web Server from your mobile device or computer using the IP address announced.

Press **Settings**.
Select or press **Connection Status** in the drop down menu.

Check that

a. LAN Status should display **Connected**.
b. LAN Media should display **Wi Fi**.
c. UltraSync Status should display **Connected**.
d. UltraSync Media should display **LAN**.



Connection Status

LAN Status: Connected
Cellular State: Idle
UltraSync Status: Connected
UltraSync Media: LAN

Cellular Radio Details

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

WiFi Details

WiFi SSID:
WiFi Security Type: None

If it does not:

e. Check cable connection.
f. Check router settings.

4.14 Programming Cameras

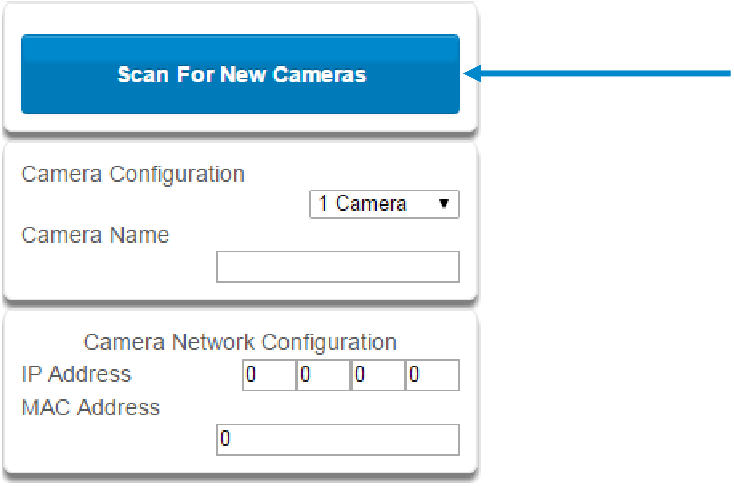
Select **Cameras** from the drop down menu.

The UltraSync Self-Contained Hub supports selected IP cameras. Contact your supplier for the correct model(s).
Install your camera according to the manual supplied with the camera. Once the camera has been connected to the same network as the panel, proceed with the scanning of the camera from the panel.

Also reference Camera Setup Instructions in section 8.

Add a Camera Method 1 – Automatic Discovery

Press **Scan For New Cameras**.



Camera Configuration
1 Camera ▼
Camera Name

Camera Network Configuration
IP Address 0 0 0 0
MAC Address 0

The scan results in an IP address and MAC address listing in the form fields shown.

Viewing Cameras in UltraSync

1. Log in to UltraSync app.
2. Press **Cameras**.
3. You will now be able to view the live camera feed.

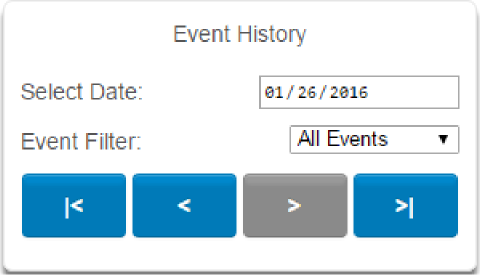
Add a Camera Method 2 – Manual Entry
Reference Advanced Programming, Cameras, Section 5.20.

Removing Cameras
Reference Advanced Programming, Cameras, Section 5.20.

	Option	Default	Function
Camera Menu	Scan For New Cameras	-	Finds cameras added to the same IP network as hub
	Camera Configuration		Notification
	Camera Name drop down (all cameras)	This name can be up to 32 characters. Make sure the name matches the name you have set up in the camera app.	
	Camera Network Configuration		
	IP Address	IP address assigned to the camera by the premises network	
	MAC address	MAC address assigned to the camera by the premises network	

4.15 Check Event History

The UltraSync Self-Contained Hub allows you to check the history of events that have occurred in the system. Press **History** and this menu will appear:

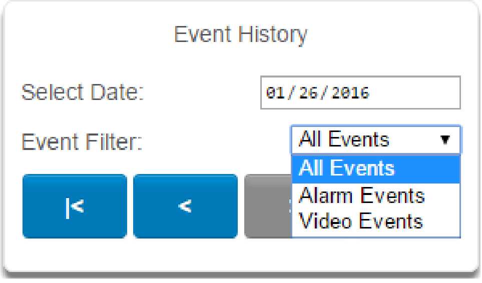


Event History

Select Date: 01/26/2016

Event Filter: All Events ▼

Navigate to events recorded in the system with the arrow buttons. You can select the date for finding events and use the Event Filter dropdown menus to select among alarm events or video events. The system stores 1024 alarm events and 1024 video events. The display shows 10 events at a time.



Event History

Select Date: 01/26/2016

Event Filter: All Events ▼

4.16 Check Connection Status

Select **Connection Status** from the drop down menu.

Also reference Advanced Programming, System, Section 5.1.

	Connections	Options	Function
Connection Status Menu	Connection Status		Notification - Diagnostic
	LAN Status	Not Linked, Configuring, Connected (system connection status)	
	Cellular State	1. Idle 2. Getting Details 3. Configuring Modem 4. Modem Connected 5. Configuring PPP 6. Authenticating 7. Configuring Protocol 8. Getting Echo 9. Connected 10. Terminating 11. Idle	
	UltraSync Status	1. Idle 2. Selecting Server 3. Making Connection 4. Disconnecting 5. Retry Delay 6. Getting Server Hello 7. Connected	
	UltraSync Path	IP, Cellular	
	Cellular Radio Details		
	Cell Service	No Service, Restricted Service, Valid Service	
	Signal Strength	-113 to -51	
	Operator ID		
	Radio Technology	GSM, UMTS	
	WI FI Details		
	WI FI SSID		
	WI FI Security Type	WPA2 + AES WPA + AES WPA + TKIP/AES WPA + TKIP WEP	

4.17 Check Details

Select **Details** from the drop down menu.

	Device Details	Detail
Detail Status	Control Name	
	Device UID (Serial)	Serial number of the panel
	Ethernet MAC Address	Ethernet MAC address assigned to the panel by the premises network
	WI FI MAC Address	WIFI MAC address assigned to the panel by the premises network
	Control Model	
	Firmware Version	of the panel
	Hardware Version	" " " "
	Bootloader	" " " "
	Voice Version	" " " "
	Website Version	" " " "
	Memory Map Version	" " " "
	Menu String Version	" " " "

5 Advanced Installation Using Web Server

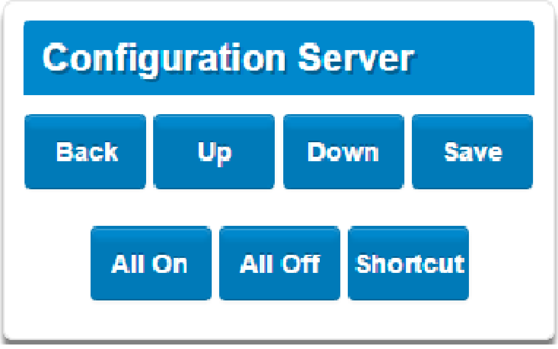
Advanced settings are only accessible via the hub’s Web Server, UltraSync app, or DLX900.

From the UltraSync app press the ••• More button then ⚙ Advanced

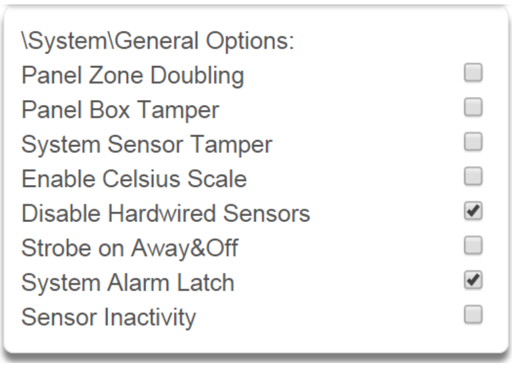
You are on the **Configuration Server** page.

The Configuration Server page main tile contains different buttons than the settings tile.

BACK: Moves you back to the main selection.
UP: Moves you up one option through the programming options.
DOWN: Moves you down one option through the programming options.



ALL ON / ALL OFF: Allow you to select or deselect all the check boxes in menus like below.

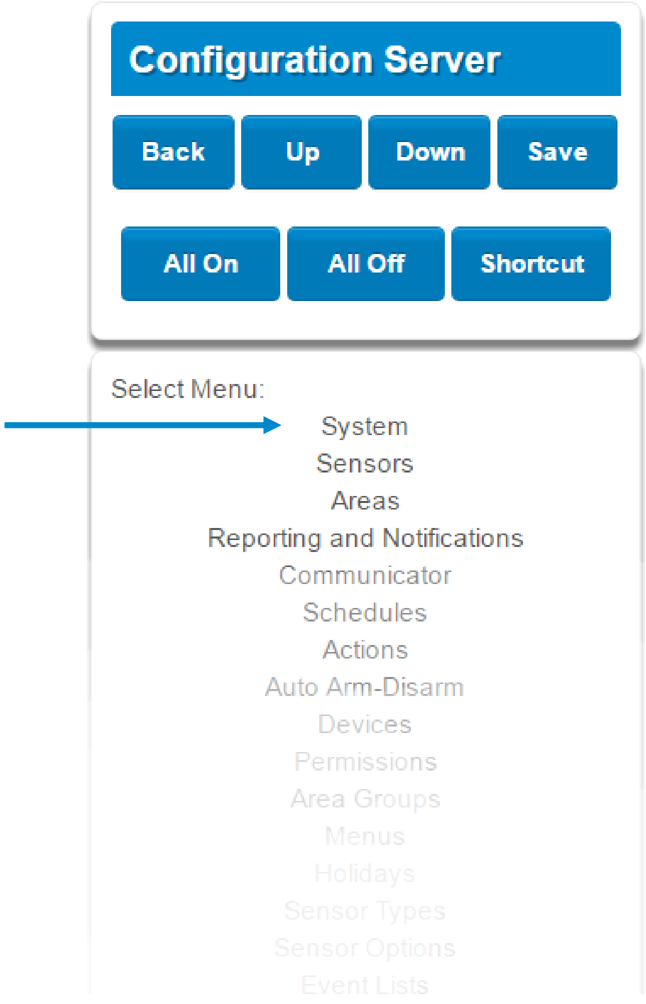


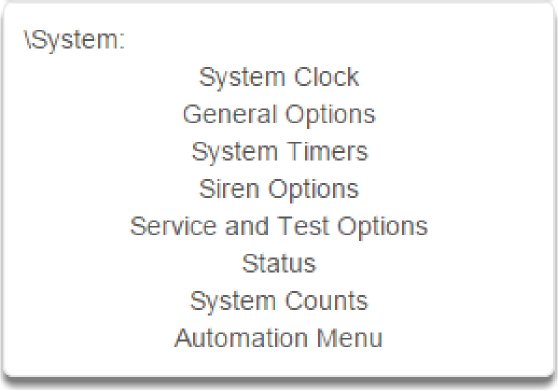
\System\General Options:
Panel Zone Doubling ☐
Panel Box Tamper ☐
System Sensor Tamper ☐
Enable Celsius Scale ☐
Disable Hardwired Sensors ☑
Strobe on Away&Off ☐
System Alarm Latch ☑
Sensor Inactivity ☐

5.1 Advanced Programming, System

Select **System** from the menu.

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

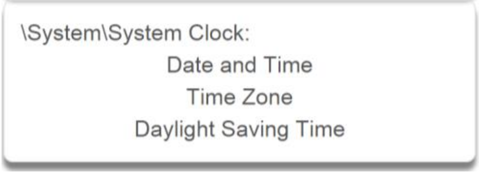




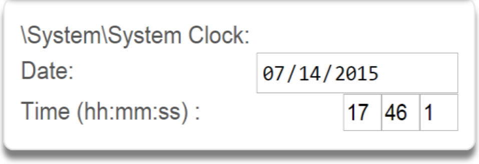
System Submenus

System Clock

1 System Clock



2 Clock Date and Time


\System\System Clock:

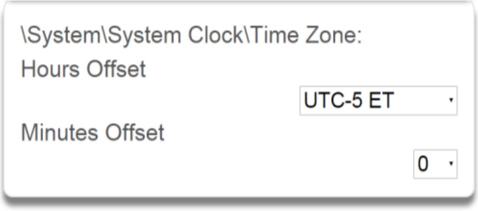
Date: 07/14/2015

Time (hh:mm:ss) : 17 46 1

When connected to an IP network the system clock synchronizes its time and date automatically with an Internet Time Server if configured in Advanced Programming, Communicator.

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

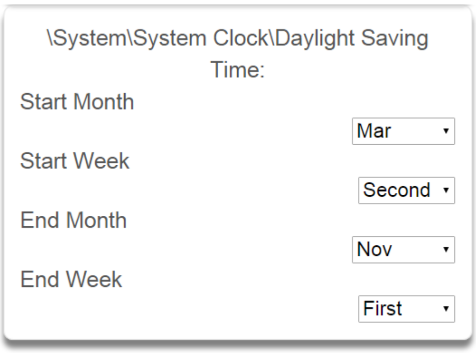
3 Time Zone Hours Offset / Minutes Offset


\System\System Clock\Time Zone:

Hours Offset: UTC-5 ET

Minutes Offset: 0

4 Daylight Saving Time


\System\System Clock\Daylight Saving Time:

Start Month: Mar

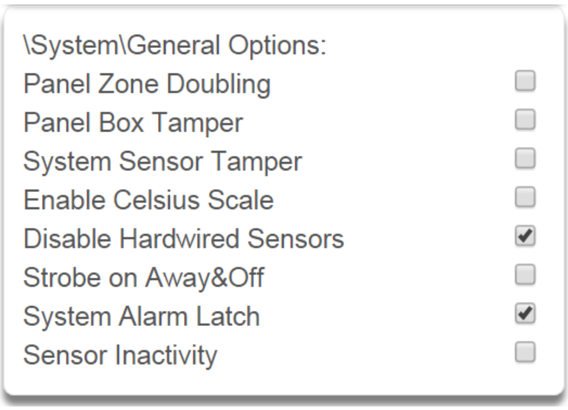
Start Week: Second

End Month: Nov

End Week: First

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

1 General Options

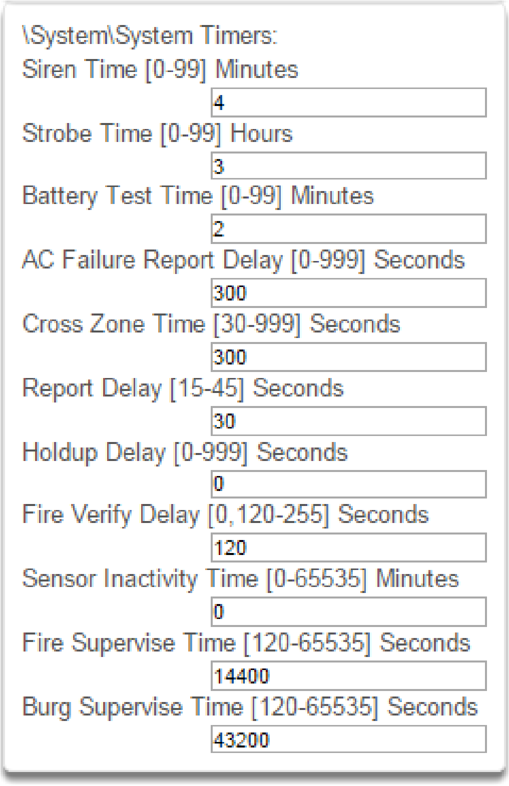


\System\General Options:

- Panel Zone Doubling □
- Panel Box Tamper □
- System Sensor Tamper □
- Enable Celsius Scale □
- Disable Hardwired Sensors ☑
- Strobe on Away&Off □
- System Alarm Latch ☑
- Sensor Inactivity □

Option	Default	Function
Panel Sensor Doubling	Off	If enabled, the two (2) hardwired sensor inputs will be doubled to support four (4) sensors. The terminals for Sensor 1 will represent sensors 1 and 3, and the terminals for sensor 2 will represent sensor 2 and 4. This option cannot be selected for sensors other than the two sensors on the main panel. This option cannot be used in conjunction with the DEOL option.
Panel Box Tamper	Off	The panel has a built-in normally closed tamper switch that will sound the siren if the panel is removed from the wall. This option will enable or disable this tamper switch.
System Sensor Tamper	Off	If enabled, the hub will monitor all sensors, except fire sensors, for Dual End of Line (DEOL). A short or open circuit on a DEOL will activate sensor tamper alarms. This feature cannot be used if Panel Sensor Doubling is enabled.
Enable Celsius Scale	Off	Enable Celsius vs. Fahrenheit Scale.
Disable Hardwire Sensors	On	If enabled, the hub will disable all hardwired sensor inputs. To utilize the hardwired sensors on the back of the panel you must disable this feature.
Strobe on Away	Off	If enabled, the system strobe will flash when an area is set in away mode. The strobe outputs must be configured follow the area alarm event condition. The strobe is not activated on Disarm or Stay.
System Alarm Latch	On	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.
Sensor Inactivity	Off	If enabled, the system will monitor each sensor for activations. If no activations occur within the sensor activity time then a failed sensor activity report may be reported via the selected communication channel and a failed sensor activity message set in the system event log. For a sensor to be eligible for activity monitoring, it must have “Sensor Activity” set in sensor options. Sensors programmed with Sensor Inactivity in the Sensor Options must be open and closed within the time programmed here (in minutes). If they do not, a Sensor Inactivity will report.

1 System Timers



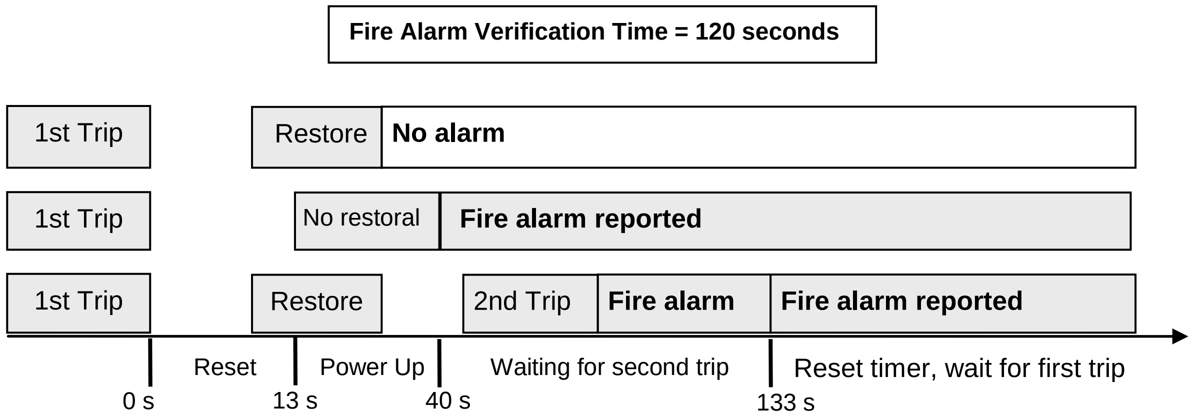
\System\System Timers:
Siren Time [0-99] Minutes
4
Strobe Time [0-99] Hours
3
Battery Test Time [0-99] Minutes
2
AC Failure Report Delay [0-999] Seconds
300
Cross Zone Time [30-999] Seconds
300
Report Delay [15-45] Seconds
30
Holdup Delay [0-999] Seconds
0
Fire Verify Delay [0,120-255] Seconds
120
Sensor Inactivity Time [0-65535] Minutes
0
Fire Supervise Time [120-65535] Seconds
14400
Burg Supervise Time [120-65535] Seconds
43200

Option	Default	Function
Siren Time (0-99) Minutes	4	The siren time sets the time in minutes that the siren output is active.
Strobe Time (0-99) Hours	3	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 (0-99) Minutes	2	The dynamic battery test time sets the duration in minutes that the system will perform a dynamic battery test. The system will perform a dynamic battery test at the disarming of the first area or at midnight once each 24-hour cycle. Dynamic battery test is disabled when the test duration is set to 0. Dynamic battery test can also be run manually from a keypad.
AC Failure Report Delay (0-999) Seconds	300	The AC fail 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.
Cross Zone Time (30-999)	300	The Cross Zone Time sets the duration in seconds whereby two or more sensors must trip before an alarm condition will be registered or the one sensor must trigger twice within this time period, or a continuous trip longer than 10 seconds. This feature only applies to sensors with the Cross Zone feature set in sensor options.
Report Delay (15-45) Seconds	30	The report delay is the duration in seconds that non-24 hour and non-fire type sensors will delay before reporting. This provides a valid user the opportunity to reset an unintended alarm condition before that event is reported.

System Timers

Option	Default	Function
Holdup Delay (0-999) Seconds	0	The holdup delay is the duration in second that a holdup delay sensor 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 sensor type is de-activated during the holdup delay period then the holdup alarm will reset and not activate.
Fire Verify Delay (0,120-255) Seconds	120	The fire alarm verification feature is designed to reduce false alarms reported by smoke detectors. The system will wait 40 seconds to allow the smoke sensor 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

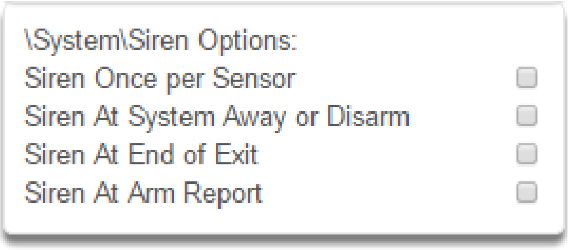
Here are some scenarios:



Sensor Inactivity Time (0-65535) Minutes	0	Sensors programmed with Sensor Inactivity in the Sensor Options must be open and closed within the time programmed here (in minutes). If they do not, a Sensor Inactivity will report. This feature can be enabled in “System Options”. See Section 4.4. Default Sensor Inactivity option is off and this timer is set to 10080 minutes (7 days).
Fire Supervise Time (120-65535) Seconds	14400	This applies only to wireless sensors programmed as fire type. Sensors send a reduced packet count supervisory signal every 60 minutes (check your sensor manual for most up to date details). If no supervisory signal is received by the panel within the time specified here then the sensor 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.
Burg Supervise Time (120-65535) Seconds	14400	This applies only to wireless sensors programmed as non-fire type. Sensors send a reduced packet count supervisory signal every 60 minutes (check your sensor manual for most up to date details). If no supervisory signal is received by the panel within the time specified here then the sensor 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.

System Siren Options

1 Siren Options

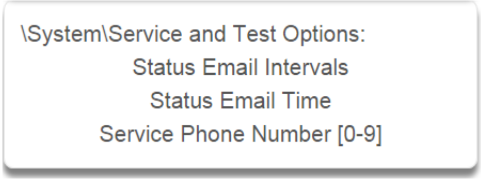


\System\Siren Options:

Siren Once per Sensor □
Siren At System Away or Disarm □
Siren At End of Exit □
Siren At Arm Report □

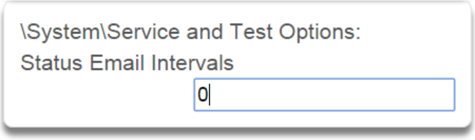
Siren Once Per Sensor	If enabled, the system will only activate the siren once per sensor in a given arm cycle and will not activate the siren again even if that siren time expires and that sensor reactivates. Every sensor will have one siren activation attempt before that sensor cannot reactivate the siren. If this option is not enabled, at the expiry of the siren time any sensor can reactivate the siren an unlimited number of times.
Siren At System Away/Disarm	If enabled, the system will activate the built-in siren briefly each time the last area in the system is set in away mode or when the first area is disarmed. To enable this function by area, leave this option disabled in this section, and enable the “Siren at System Away/Disarm” in section 5.3 Advanced Programming, Areas for the area(s) you require.
Siren At End Of Exit	If enabled, the system will activate the built-in siren briefly each time the system is set in away mode and the exit delay expires.
Siren At Arm Report	If enabled, the system will activate the built-in siren briefly every time the system is set in away mode, the exit delay expires and a successful system arm report is completed.

1 Service and Test Options



\System\Service and Test Options:
Status Email Intervals
Status Email Time
Service Phone Number [0-9]

2 Email Intervals

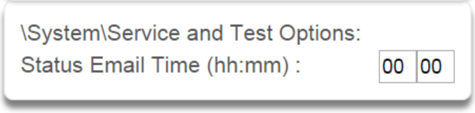


\System\Service and Test Options:
Status Email Intervals
0

If enabled, the system 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 a program interval is entered or when the system is powered up.

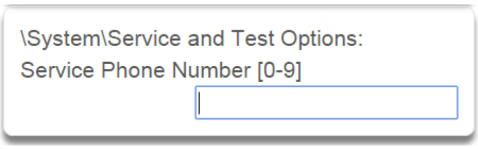
3 Email Time



\System\Service and Test Options:
Status Email Time (hh:mm) : 00 00

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.

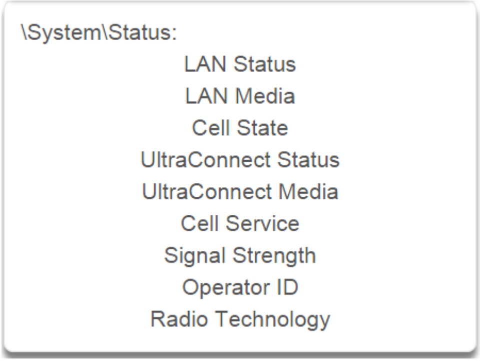
4 Service Phone number



\System\Service and Test Options:
Service Phone Number [0-9]

When a system condition needs repair, this number will be announced to the end-user. Typically this is the installation company.

1 Status

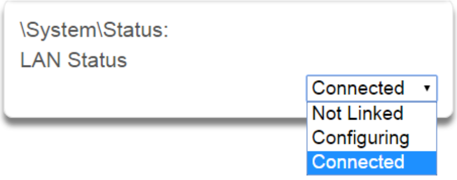


\System\Status:

LAN Status
LAN Media
Cell State
UltraConnect Status
UltraConnect Media
Cell Service
Signal Strength
Operator ID
Radio Technology

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

2 LAN Status

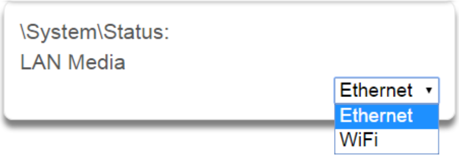


\System\Status:
LAN Status

Connected ▾
Not Linked
Configuring
Connected

Status of the connection to the Local Area Network.

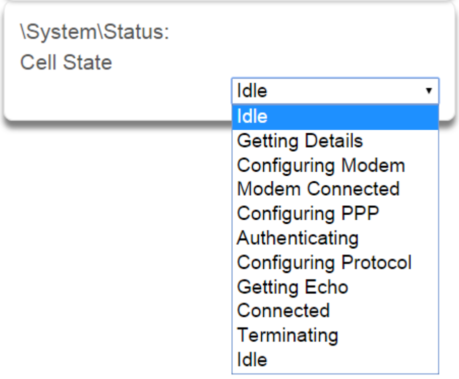
3 LAN Media



\System\Status:
LAN Media

Ethernet ▾
Ethernet
WiFi

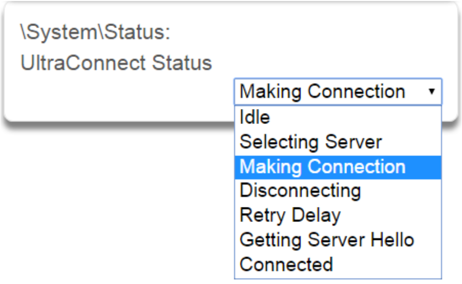
4 Cell State



\System\Status:
Cell State

Idle ▾
Idle
Getting Details
Configuring Modem
Modem Connected
Configuring PPP
Authenticating
Configuring Protocol
Getting Echo
Connected
Terminating
Idle

5 UltraSync Status

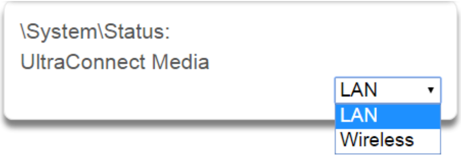


\System\Status:
UltraConnect Status

Making Connection ▾
Idle
Selecting Server
Making Connection
Disconnecting
Retry Delay
Getting Server Hello
Connected

Status of the connection to the cloud servers.

6 UltraSync Media

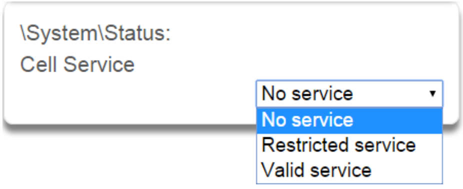


\System\Status:
UltraConnect Media

LAN ▾
LAN
Wireless

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

7 Cell Service

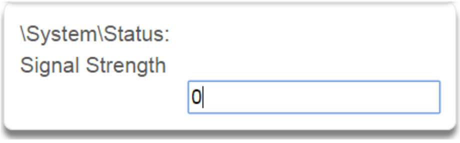


\System\Status:
Cell Service

No service ▾
No service
Restricted service
Valid 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.

8 Signal Strength



\System\Status:
Signal Strength

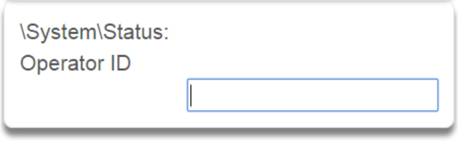
0

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

If the reported value is -113 to -89 then installing an external antenna is recommended.
If the reported value is -89 to -51 then the signal strength is OK.

System Status

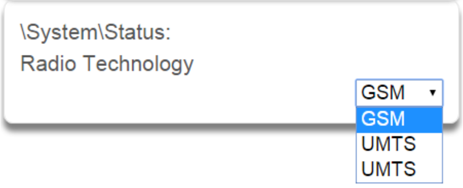
9 Operator ID



\System\Status:
Operator ID

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

10 Radio Technology



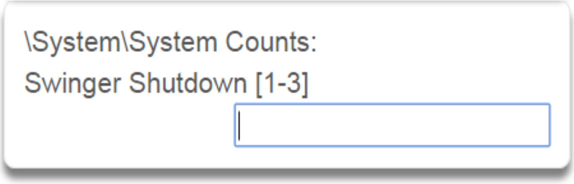
\System\Status:
Radio Technology

GSM

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

System Counts

1 Counts



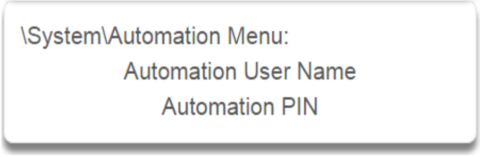
\System\System Counts:
Swinger Shutdown [1-3]

Swinger Shutdown is a false alarm prevention feature prevents a single sensor from activating more than a programmed number of times during a single arming period. After a certain number of alarms caused by the same sensor within the same arming period, the system will then shutdown that sensor for the remainder of that arming period. The sensor will be reactivated when the system is disarmed or rearmed to any security mode.

See SIA CP-01-2010 Programmable Features Table for reference.

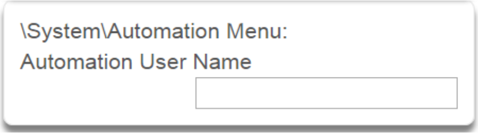
System Automation Menu

1 Automation Menu



\System\Automation Menu:
Automation User Name
Automation PIN

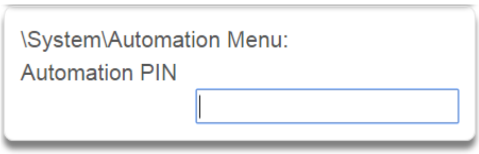
2 Automation User name



\System\Automation Menu:
Automation User Name

Used when there is API integration

3 Automation Pin



\System\Automation Menu:
Automation PIN

Used when there is API integration.

5.2 Advanced Programming, Sensors

Press ••• More then ⚙ Advanced for the **Configuration Server** page.

Select **Sensors** from the menu.

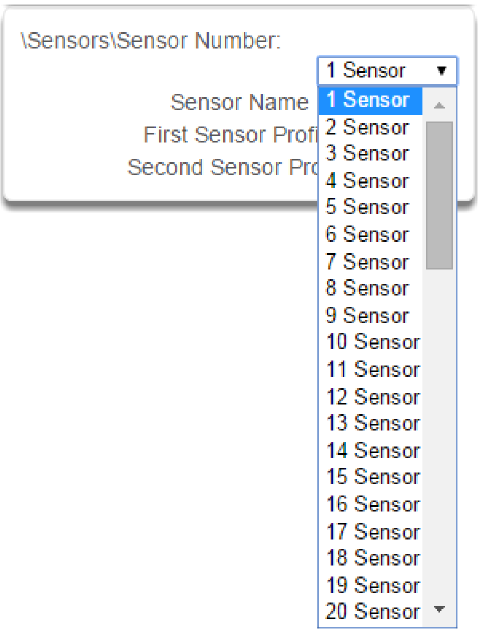
A sensor (sometime referred to as a zone or input) on the hub is a single physical hardwired connection or a non-physical wireless connection. Additionally sensors on the hub can be used as logic inputs within actions and / or be configured as one of many sensor types. See Advanced Programming, Actions.

Note: After you have finished programming a sensor, be sure to advance the sensor number in the drop down menu when programming the next sensor. Otherwise you will over-write the sensor configuration you just programmed.

Sensor Submenus

Sensor Submenus

1 Sensor Number



\Sensors\Sensor Number:

1 Sensor ▼

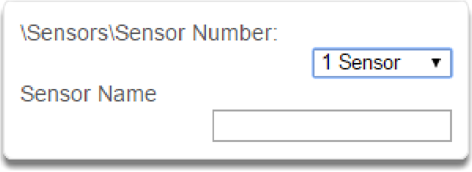
Sensor Name

First Sensor Profi

Second Sensor Pro

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

2 Sensor Name



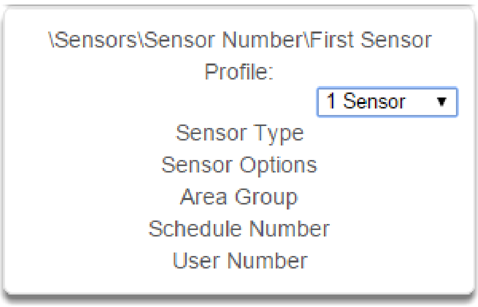
\Sensors\Sensor Number:

1 Sensor ▼

Sensor Name

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

3 First Sensor Profile



\Sensors\Sensor Number\First Sensor Profile:

1 Sensor ▼

Sensor Type

Sensor Options

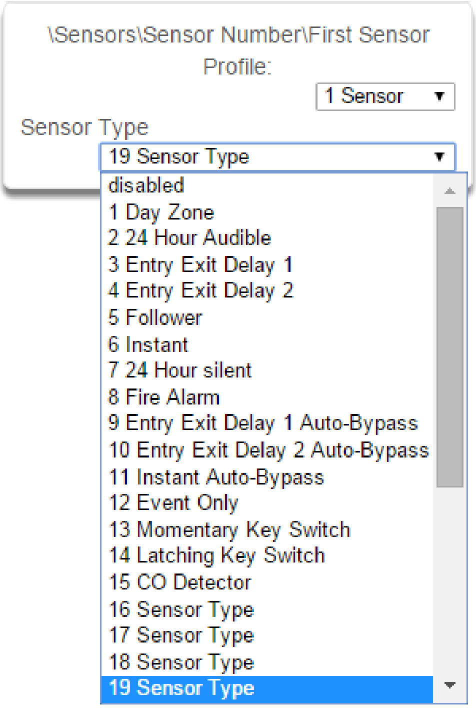
Area Group

Schedule Number

User Number

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

4 Sensor Type



\Sensors\Sensor Number\First Sensor

Profile: 1 Sensor

Sensor Type: 19 Sensor Type

- disabled
- 1 Day Zone
- 2 24 Hour Audible
- 3 Entry Exit Delay 1
- 4 Entry Exit Delay 2
- 5 Follower
- 6 Instant
- 7 24 Hour silent
- 8 Fire Alarm
- 9 Entry Exit Delay 1 Auto-Bypass
- 10 Entry Exit Delay 2 Auto-Bypass
- 11 Instant Auto-Bypass
- 12 Event Only
- 13 Momentary Key Switch
- 14 Latching Key Switch
- 15 CO Detector
- 16 Sensor Type
- 17 Sensor Type
- 18 Sensor Type
- 19 Sensor Type

One of 32 configurable sensor types may be allocated to any sensor's sensor type. Each sensor type can behave independently between an arm and disarmed state. Sensor types determine the sensor attributes, siren attributes, and sensor attribute options.

Here is an example of a preset sensor type:

Sensor Type – 1 – Day Sensor

Sensor Type Armed

Sensor Attribute - Instant

Siren Attribute - Yelping

Sensor Attribute Options:

Keypad Sounder	YES
Report Delay	NO
No Panel Display	NO
Momentary Switch	NO
Sensor Inhibit (Bypass)	NO

Sensor Type Disarmed

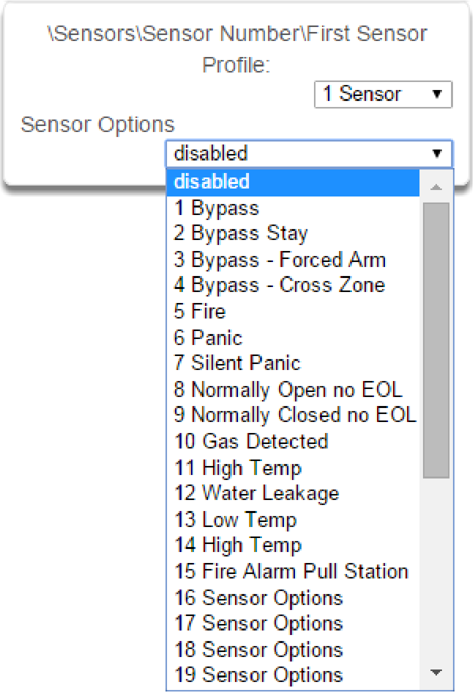
Sensor Attribute - Local

Siren Attribute - Silent

Sensor Attribute Options:

Keypad Sounder	YES
Report Delay	NO
No Panel Display	NO
Momentary Switch	NO
Sensor Inhibit (Bypass)	NO

5 Sensor Options

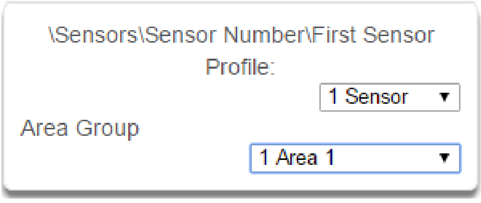


\Sensors\Sensor Number\First Sensor Profile: 1 Sensor

Sensor Options: disabled

One of 32 configurable sensor options may be allocated to any sensor. Sensor options determine the sensor attributes such as a sensor's ability to be bypassed, force arm, cross zone, stay mode, etc. Additionally sensor options determine the sensor's reporting attributes.

6 Area Group (1-16)



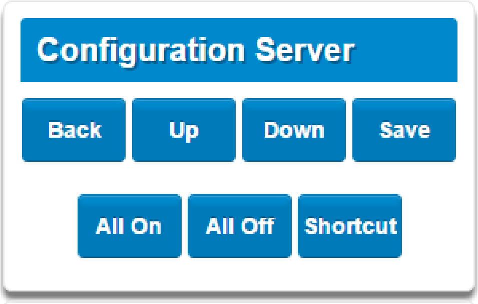
\Sensors\Sensor Number\First Sensor Profile: 1 Sensor

Area Group: 1 Area 1

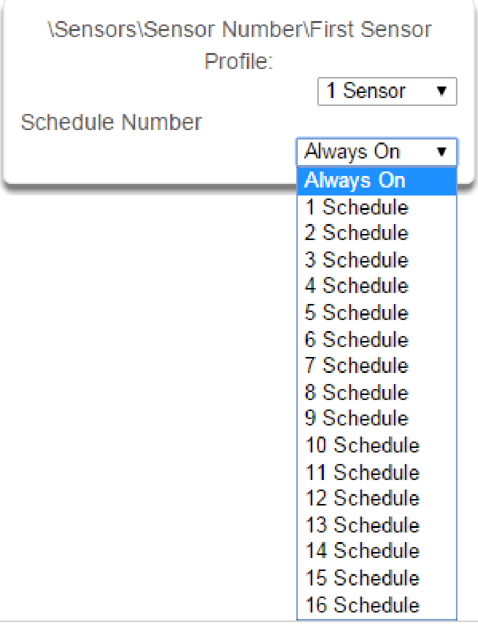
One of 16 configurable area groups can be allocated to any sensor's area group. Area groups are a list of the hub's areas. When an area group is allocated to a sensor, that sensor will then belong to all the areas in the area group. If a sensor is assigned to multiple areas it will not arm until the last area is armed. It will also be disarmed when the first area is disarmed.

Ensure the correct Area Group is assigned to a sensor. If an area Group with no areas is used, then the sensor will never report.

7 Schedule Number



Configuration Server



\Sensors\Sensor Number\First Sensor Profile: 1 Sensor

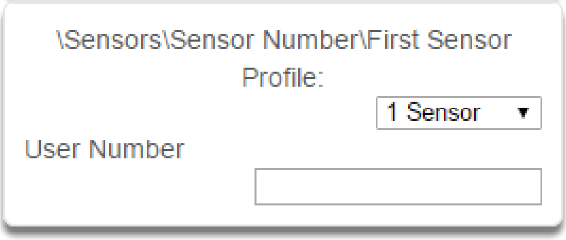
Schedule Number: Always On

One of 16 configurable schedules can be allocated to any sensor's schedule number. Sensor profile schedules determine when to allocate a sensor profile to a sensor. The first sensor profile has the highest priority and the second sensor profile has the lowest priority.

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

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

8 User Number



\Sensors\Sensor Number\First Sensor Profile:

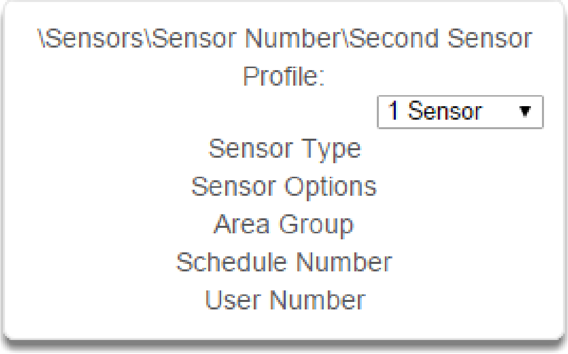
1 Sensor ▾

User Number

The sensor user number feature is used whenever the sensor type is set to “keyswitch”. Instructions for users configuration are in Section 6 – Users and Permissions. One of 40 configurable users can be allocated to any sensor’s user number. The hub’s sensor profile user number is a powerful feature that is used to apply the selected user’s attributes to a keyswitch operation. When the keyswitch sensor is activated, the system 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.

Note: If the user number is programmed to 0, the system will use a default User number of 999 and will operate on all areas in the sensors area group.

9 Second Sensor Profile (Refer to First Sensor Profile)



\Sensors\Sensor Number\Second Sensor Profile:

1 Sensor ▾

Sensor Type

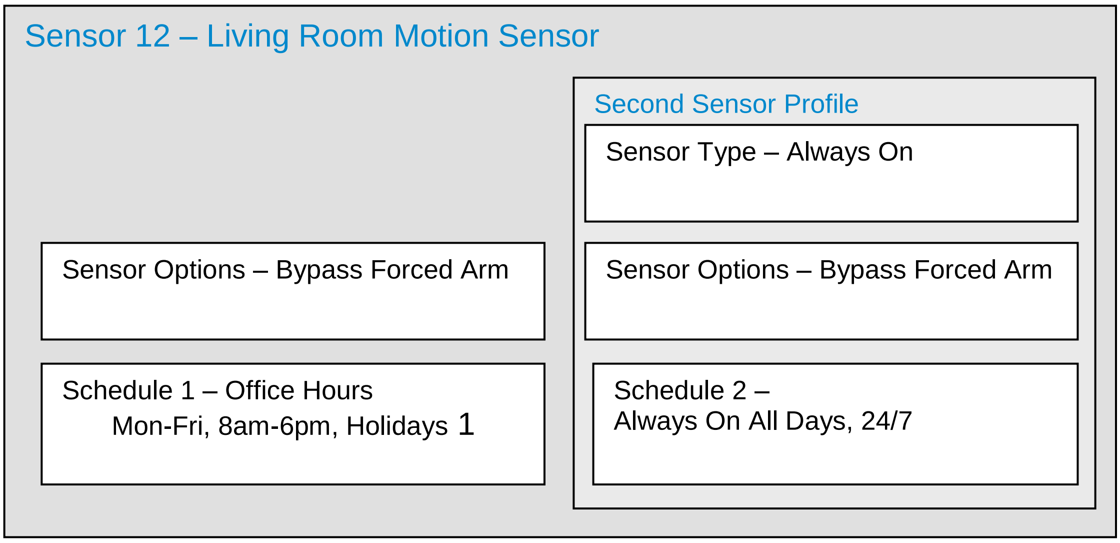
Sensor Options

Area Group

Schedule Number

User Number

Example Diagram



Sensor 12 – Living Room Motion Sensor

Sensor Options – Bypass Forced Arm

Schedule 1 – Office Hours Mon-Fri, 8am-6pm, Holidays 1

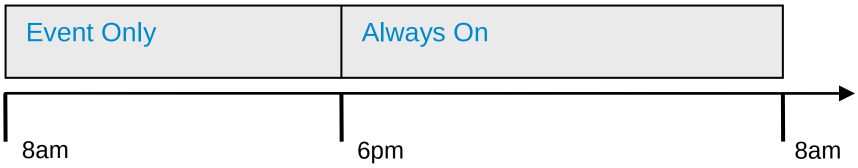
Second Sensor Profile

Sensor Type – Always On

Sensor Options – Bypass Forced Arm

Schedule 2 – Always On All Days, 24/7

Sensor Programming



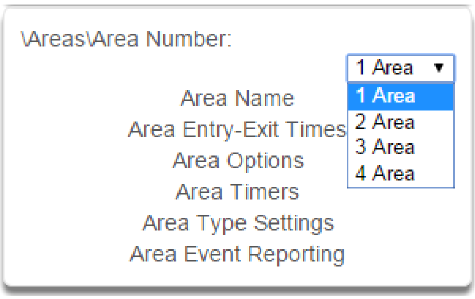
5.3 Advanced Programming, Areas

Select **Areas** from the drop down menu.

Areas Submenus

Areas Submenus

1 Area Number

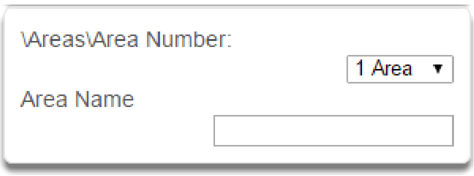


\Areas\Area Number:

1 Area

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

2 Area Name



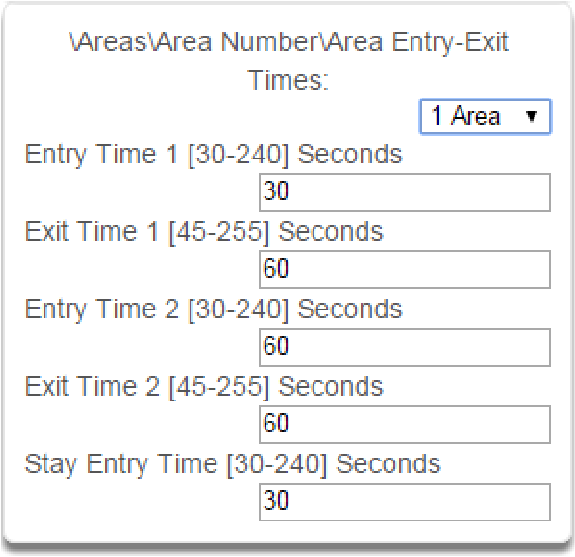
\Areas\Area Number:

1 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 system.

3 Area Entry-Exit times



\Areas\Area Number\Area Entry-Exit Times:

1 Area ▼

Entry Time 1 [30-240] Seconds: 30

Exit Time 1 [45-255] Seconds: 60

Entry Time 2 [30-240] Seconds: 60

Exit Time 2 [45-255] Seconds: 60

Stay Entry Time [30-240] Seconds: 30

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

When an area is turned on, it will start an Exit 1 timer. While an Exit 1 timer is running – Entry 1, Entry 2, and Follower sensor types will not create an alarm.

When the Exit 1 timer expires it will start the Exit 2 timer. While an Exit 2 timer is running – Entry 2 sensors will not create an alarm.

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

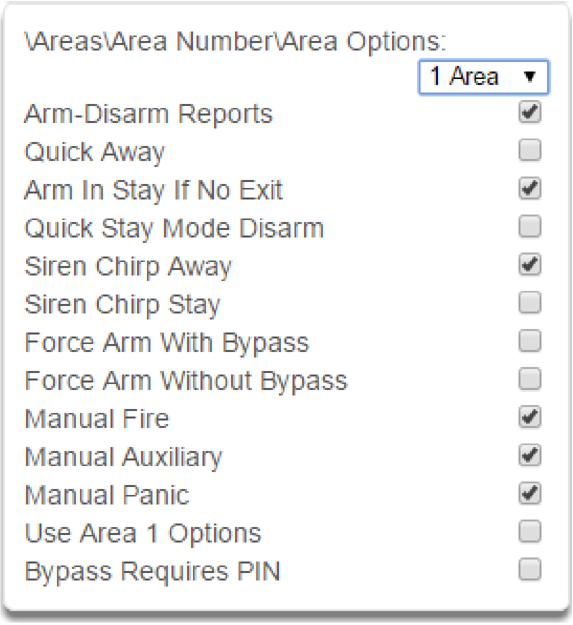
If an entry delay is running and a sensor is activated with an entry time that is less than the time remaining, the timer will be reduced to the time of that new sensor.

Activation of a Follower sensor while an entry timer is not running will create an instant alarm.

If a sensor is in more than 1 area, the sensor 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.

Stay Entry Time
The stay entry time is the entry warning time that applies to all sensors armed in the stay mode. Entry 2 sensors will follow Entry 2 time and will ignore this setting. This stay entry time does not apply to any 24 hour sensor types.

4 Area Options



\Areas\Area Number\Area Options:

1 Area ▼

Arm-Disarm Reports	☑
Quick Away	□
Arm In Stay If No Exit	☑
Quick Stay Mode Disarm	□
Siren Chirp Away	☑
Siren Chirp Stay	□
Force Arm With Bypass	□
Force Arm Without Bypass	□
Manual Fire	☑
Manual Auxiliary	☑
Manual Panic	☑
Use Area 1 Options	□
Bypass Requires PIN	□

1. Arm/Disarm Reports
If enabled, this area will send open and close reports via one or more appropriately configured channels.

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

3. Arm In Stay If No Exit
If enabled, Arm In Stay If No Exit will cause this area to arm in stay mode even when a user arms it in away mode, providing that an entry 1 or entry 2 sensor type is not triggered during the exit delay.

4. 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 currently running.

At the end of the stay entry delay or if there is an area alarm, the stay mode can only be disarmed via a valid user PIN.

5. Siren Chirp Away
If enabled, the panel will activate the built-in siren briefly each time this area is set in away mode or disarmed with a key-switch sensor or wireless keyfob.

6. Siren Chirp Stay

If enabled, the panel will activate the built-in siren briefly each time this area is set in stay mode with a key-switch sensor or wireless keyfob.

7. Force Arm With Bypass

If enabled, the area can be armed even if sensors are not ready. Any sensors that are not ready will automatically be bypassed. The bypass will be logged in the event history.

The automatic bypass will be applied when the sensor 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 sensor becomes ready after it is armed, that sensor will automatically remove the bypass, log the bypass restore, and optionally report the bypass restore.

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

8. Force Arm Without Bypass
If enabled, the area can be armed even if sensors are not ready. Any sensors 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 sensors can be made “force armable without auto-bypass” by leaving this area option off, then enabling Forced Arm Enable in Sensor options, and disabling Sensor Inhibit (Bypass) in the Sensor Type Profile.

9. 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 on.

10. 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 on.

11. 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 on.

12. Use Area 1 Options

If enabled, the selected area will use the options chosen for Area 1. The panel ignores all other selections made; it overrides them to instead use the options chosen for Area 1. Default is on.

13. Bypass Requires PIN

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

Notes on Force Arming, Bypass, and Auto-Bypass

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

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. This is not always user friendly or practical.

The term force arm refers to the ability to arm an area even though sensors are not ready. It is usually only used with motion sensors 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.)

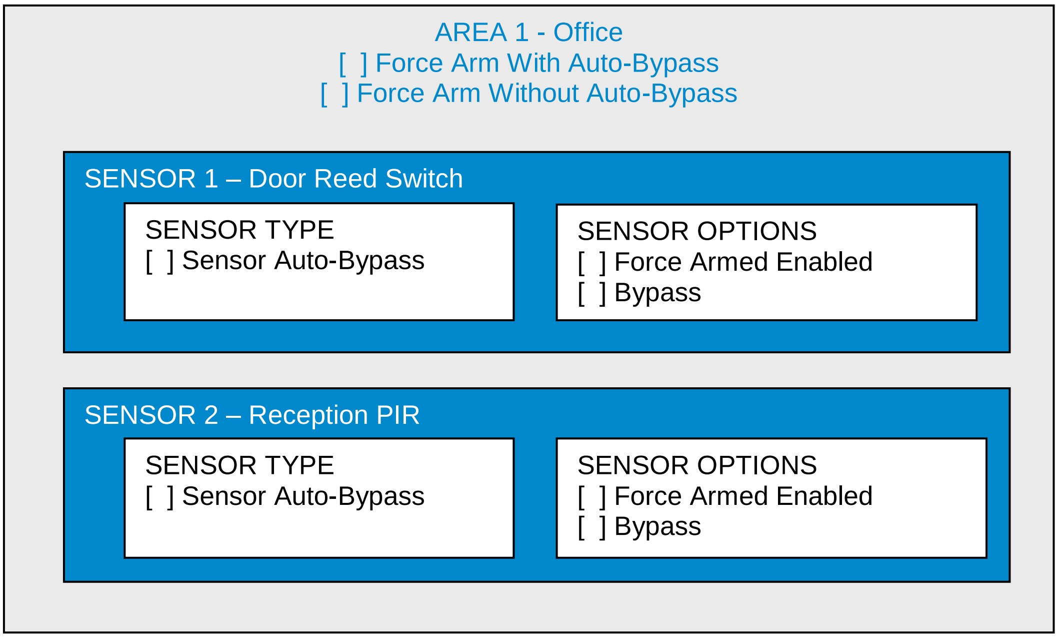
If the front door is not closed properly then Area 1 would go into alarm at the end of the Exit time. To avoid this false alarm we enable “**Force Arm With Auto-Bypass**” so all sensors that are not closed (i.e. not ready) by end of the exit time will be “Auto-Bypassed”.

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

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

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

In general disabling “Sensor 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 Auto-Bypass**” at the area level to prevent sensors from being auto-bypassed when Force Armed.



AREA 1 - Office
[ ] Force Arm With Auto-Bypass
[ ] Force Arm Without Auto-Bypass

SENSOR 1 – Door Reed Switch

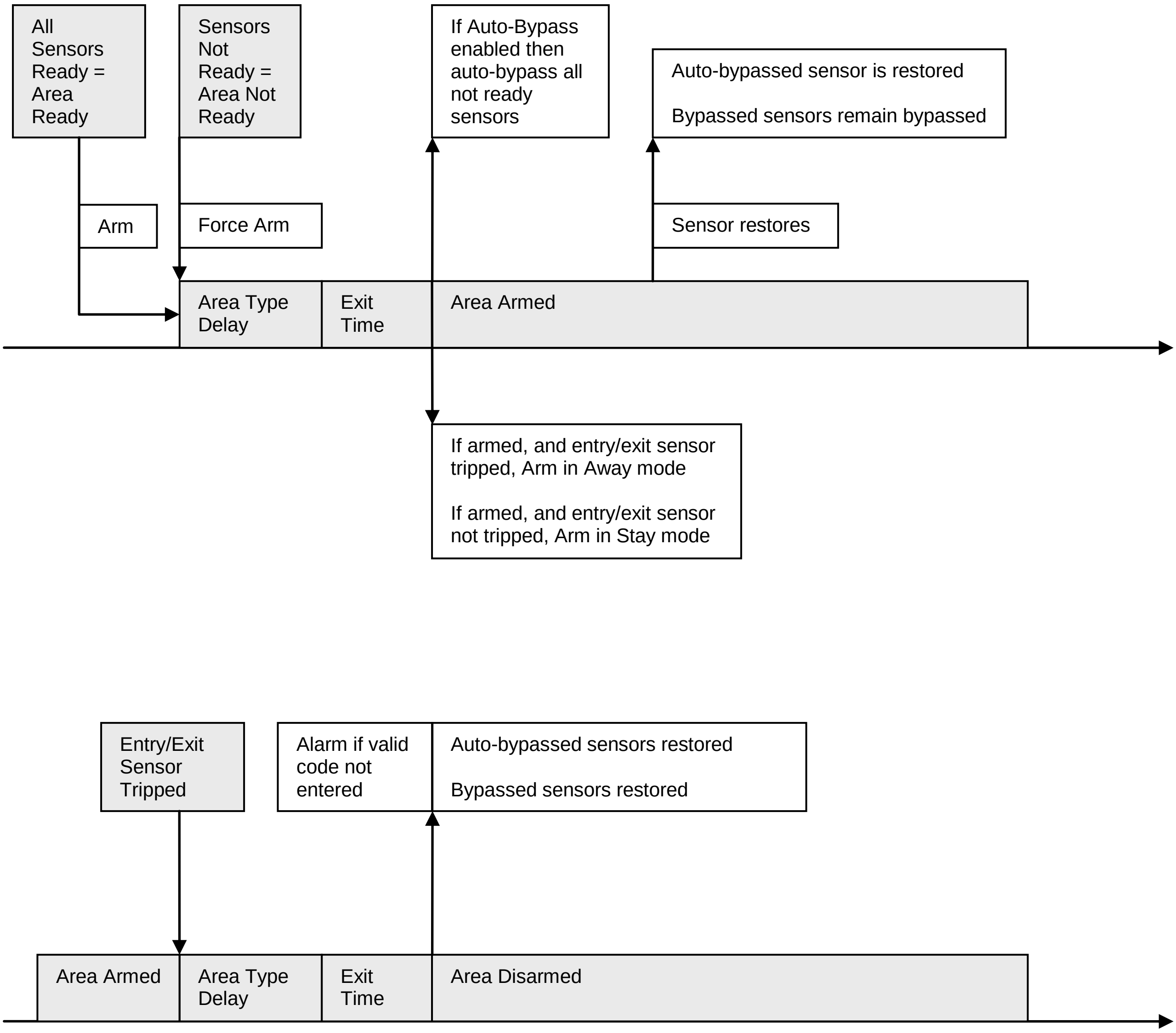
SENSOR TYPE
[ ] Sensor Auto-Bypass

SENSOR OPTIONS
[ ] Force Armed Enabled
[ ] Bypass

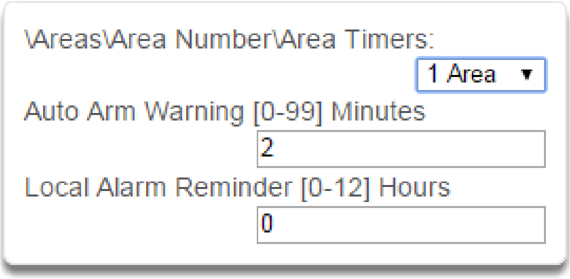
SENSOR 2 – Reception PIR

SENSOR TYPE
[ ] Sensor Auto-Bypass

SENSOR OPTIONS
[ ] Force Armed Enabled
[ ] Bypass


All Sensors Ready = Area Ready
Sensors Not Ready = Area Not Ready
If Auto-Bypass enabled then auto-bypass all not ready sensors
Auto-bypassed sensor is restored
Bypassed sensors remain bypassed
Arm
Force Arm
Sensor restores
Area Type Delay
Exit Time
Area Armed
If armed, and entry/exit sensor tripped, Arm in Away mode
If armed, and entry/exit sensor not tripped, Arm in Stay mode
Entry/Exit Sensor Tripped
Alarm if valid code not entered
Auto-bypassed sensors restored
Bypassed sensors restored
Area Armed
Area Type Delay
Exit Time
Area Disarmed

5 Area Timers



\Areas\Area Number\Area Timers: 1 Area

Auto Arm Warning [0-99] Minutes: 2

Local Alarm Reminder [0-12] Hours: 0

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 system will re-arm the area and send the appropriate event (closing, man down, guard tour fail).

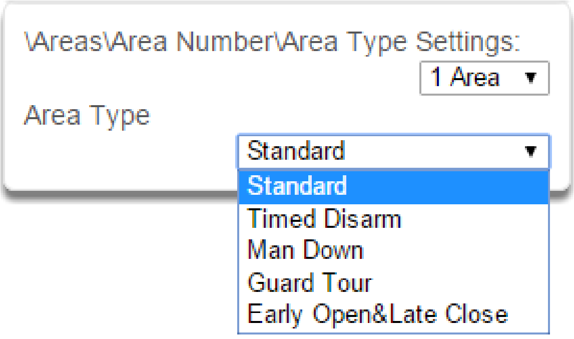
If the area type is Early Open & Late Close, this timer sets the period after the start (opening) and after the end (closing) of the area type schedule that the area can be disarmed or armed. Otherwise an early to open or late to close report will be sent if enabled in user permissions. Fail to open 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 minutes between 0 and 999 that may elapse between actioning a local alarm and the local alarm reactivating if that sensor has remained open.

For example if a smoke detector is removed to change the battery the tamper will trip; if a user resets the alarm on the panel but does not replace the smoke detector within the local alarm reminder time, then the fire alarm tamper will retrigger.

6 Area Type



\Areas\Area Number\Area Type Settings: 1 Area

Area Type: Standard

Standard
The area functions as normal.

Timed Disarm
Timed disarm is used when an authorised 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 accidently left disarmed.

The following conditions must be true before a timed area disarm function will occur.

a. The area type must be set to Timed Disarm.
b. The area type schedule must be active.
c. The users active profile's permission must have;
  i. This area set in the permission's timed disarm area group.
  ii. The permission must be in schedule.
  iii. The permission's Area Type Override must NOT be set.

At the end of the user's disarm time, the Area Type Delay will activate for the set period. At the end of the Area Type Delay 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.

At anytime during the timed disarm period, authorised 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 authorised 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 authorised 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.

a. The area type must be selected to man down.
b. The area type schedule must be active (after the start time and before the end time).
c. The uses active profile's permission must have;
  i. This area set in the permission's man down group.
  ii. The permission must be in schedule.
  iii. 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 Area Type Delay will activate for the set period. At the end of the Area Type Delay period the area will arm and if configured, report a man down alarm. At anytime during the man down period, authorised 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 authorised 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 authorised 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.
a. The area type must be selected to guard tour.
b. The area type schedule must be active (after the start time and before the end time).
c. The uses active profile's permission must have;
  i. This area set in the permission's guard tour group.
  ii. The permission must be in schedule.
  iii. The permission's Area Type Override must NOT be set.

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

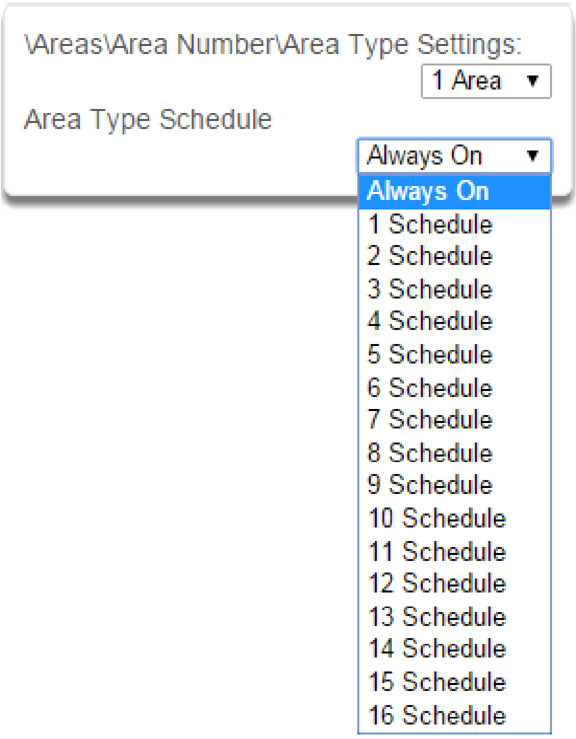
At the end of the user's guard tour time, the Area Type Delay will activate for the set period and keypad sounder will be active. At the end of the Area Type Delay period the area will arm and if configured, report a Guard Tour Fail alarm. At anytime during the guard tour period, authorised users with 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 Area Type Delay 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 Area Type Delay 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.

7 Area Type Schedule



\Areas\Area Number\Area Type Settings:

1 Area

Area Type Schedule

Always On

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.

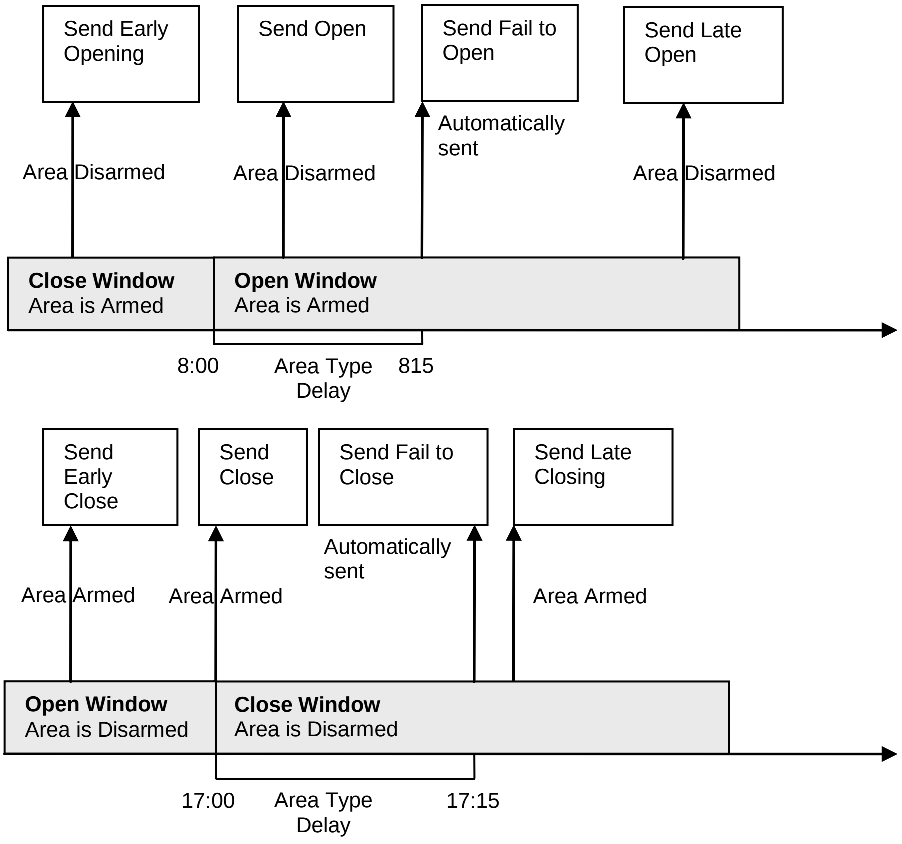
Area Type Delay

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

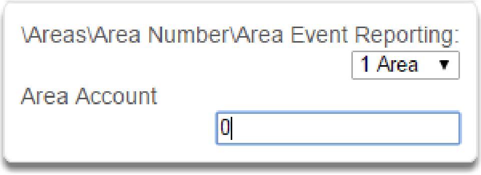
If the area type is Timed Disarm, Man Down, or Guard Tour, this setting is a warning time given to a user once the user's Disarm Time, Man Down Time, or Guard Tour Time has expired. During this warning time a user can cancel the automatic re-arming and event report by entering their code, this will also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

Example
Area Type – Early Open & Late Close
Area Type Schedule – 8:00 to 17:00
Area Type Delay – 15 min
User Permissions – Options – Open/close report, Early open report, Late close report
Area Options – Arm-Disarm Reports



8 Area Event Reporting/Account

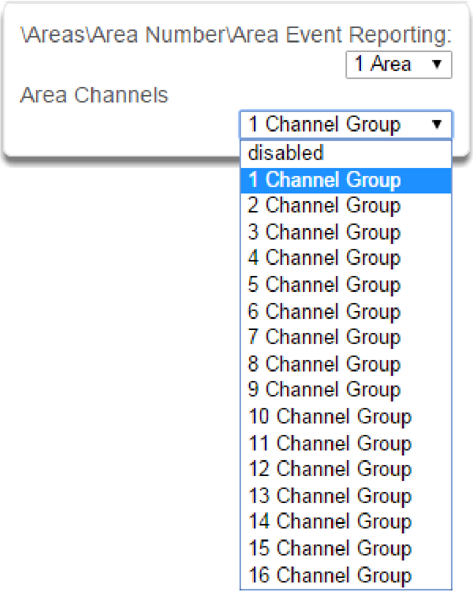


\Areas\Area Number\Area Event Reporting: 1 Area

Area Account: 0

If set, the area account code 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 code is equal to the default of 0, the channel account code will be used for this area's alarm reporting events. If the channel account code is equal to the default of 0, the channel 1 account code is used. If the channel 1 account code is 0 then the account will be sent as 0.

9 Area Event Reporting/Channels



\Areas\Area Number\Area Event Reporting: 1 Area

Area Channels: 1 Channel Group

The channel group determines which communicator channel(s) area events will be reported to. 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.

5.4 Advanced Programming, Reporting and Notifications

Select **Channels** from the drop down menu.

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

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

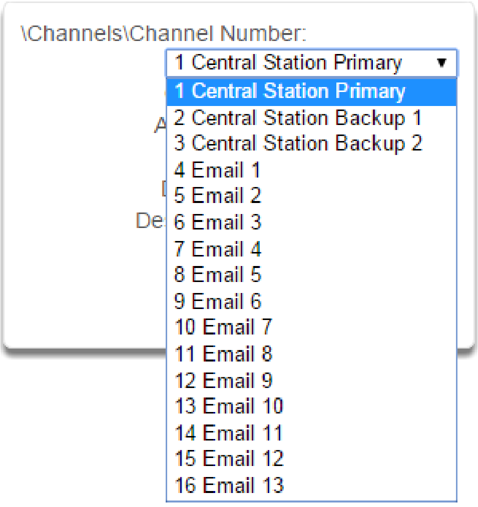
Email is a “best-effort” system and there is no guarantee messages will be delivered by the network. When the network is busy, messages can be dropped. Central control room monitoring is highly recommended as each event is acknowledged on receipt to ensure an appropriate response can be made.

Installers have access to setup/modify all channels (1-16). Master Users have access to channels 7-16, which are used for email notifications. Standard users do not have access to channels.

Channels Submenus

Channels Submenus

1 Channel Number

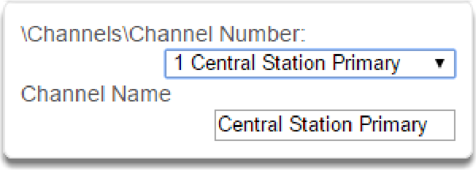


\Channels\Channel Number: 1 Central Station Primary

The system 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.

Channel 1 and channels 4-16 are configured as primary reporting paths by default. Channel 1 is disabled by default. Use as Backup as the Format selection has the effect of disabling reporting of a primary channel. The Format must be selected to a value *other* than Use as Backup to enable reporting. Channels 4-16 are configured as email reporting paths by default.

2 Channel Name

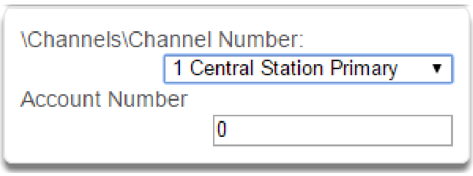


\Channels\Channel Number: 1 Central Station Primary

Channel Name: Central Station Primary

Custom names of the selected channel can be created here.

3 Account Number



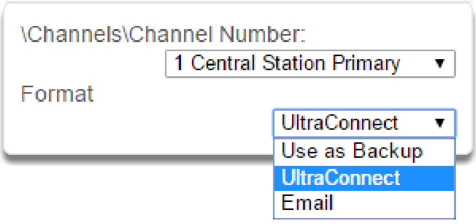
\Channels\Channel Number: 1 Central Station Primary

Account Number: 0

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.

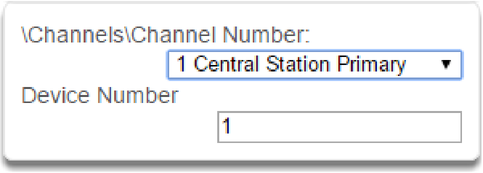
Channels 2 and 3 are configured as backup reporting paths by default. Channel 2 is set to backup channel 1 and channel 3 is set to back up channel 2 by default. Note that the primary channel must set the Next Channel for back up reporting to function.

4 Format


\Channels\Channel Number: 1 Central Station Primary

Format: UltraConnect

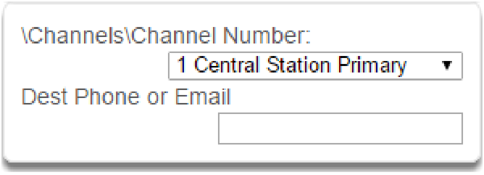
5 Device Number


\Channels\Channel Number: 1 Central Station Primary

Device Number: 1

This is the communication format for the selected channel. When Use as Backup is selected, the backup path will utilize the primary channel's format. Note that the primary channel must set the Next Channel for back up reporting to function.

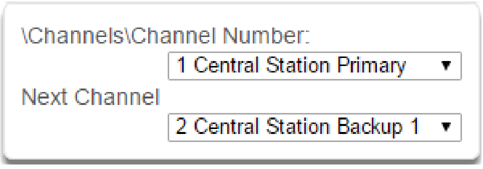
6 Destination Phone/Email


\Channels\Channel Number: 1 Central Station Primary

Dest Phone or Email:

The email address or mobile device name (push notification) of the selected destination.
When enabling push notifiactions in the UltraSync application, the device name will automatically be set in destination phone or email.

7 Next Channel 1-16

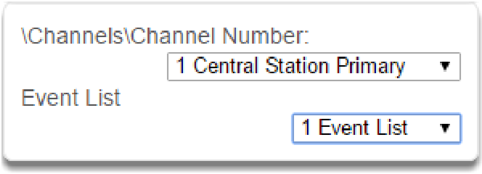

\Channels\Channel Number: 1 Central Station Primary

Next Channel: 2 Central Station Backup 1

If the channel selected is unable to deliver the event to the selected destination, the system 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.

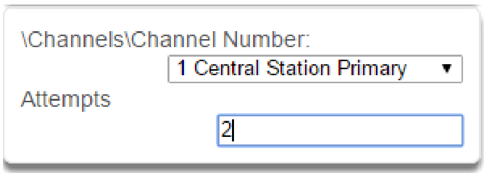
8 Event List 1-16


\Channels\Channel Number: 1 Central Station Primary

Event List: 1 Event List

Select the pre-programmed list of events that will be sent via this channel. The specific events in each event list are programmed.

9 Attempts

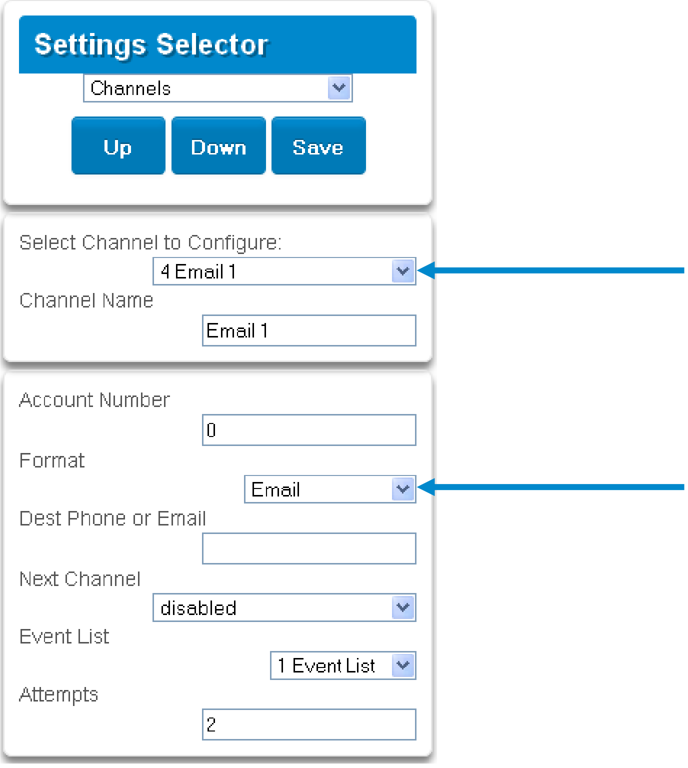

\Channels\Channel Number: 1 Central Station Primary

Attempts: 2

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

Configure Email Reporting

1. Login to Web Server or UltraSync app. Use an Installer or Master user account.
2. Press **Settings**.
3. Select Channels in the drop down menu.
4. Press **Select Channel to Configure** where the Format is already set to Email.



Channels

Select Channel to Configure: 4 Email 1

Channel Name: Email 1

Account Number: 0

Format: Email

Dest Phone or Email:

Next Channel: disabled

Event List: 1 Event List

Attempts: 2

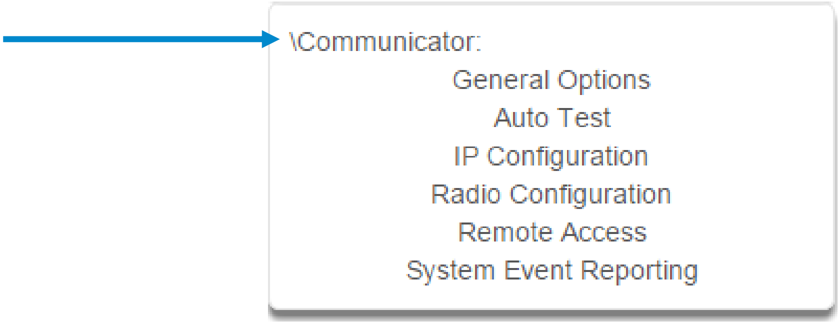
5. Enter an email address.
6. Select an **Event List**.
7. Enter a Channel Name for future reference.
8. Press **Save**.

Installer and Master User types can customize Event Lists for selective reporting.

5.5 Advanced Programming, Communicator

Select **Communicator** from the drop down menu.

The Communicator is a core component of the 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.



\Communicator:

General Options

Auto Test

IP Configuration

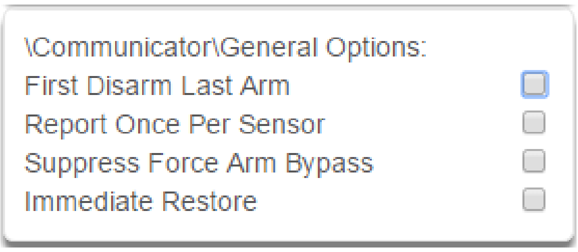
Radio Configuration

Remote Access

System Event Reporting

Communicator Submenus

1 General Options



\Communicator\General Options:

- First Disarm Last Arm □
- Report Once Per Sensor □
- Suppress Force Arm Bypass □
- Immediate Restore □

1. First Disarm Last Arm

If enabled, the system 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 system 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

2. Report Once Per Sensor

If enabled, this will limit reporting to only once per sensor 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 sensor is being activated (for example the intruder may be moving around and is being picked up by the sensor on that sensor).

3. Suppress Force Arm Bypass

If enabled, the system does not send bypass reports when a sensor is forced armed.

If not enabled, when a sensor 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 open at the end of the exit time, or due to change of sensor type caused by a schedule.

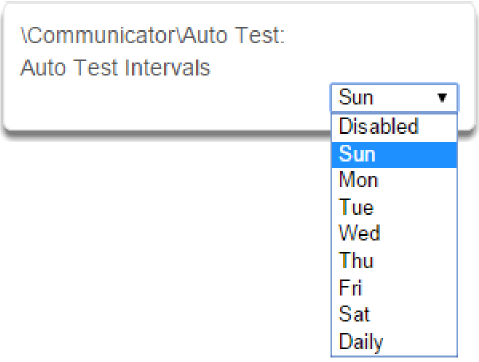
If forced armed sensors re-close during the armed period, bypass restores are sent.

4. Immediate Restore

If enabled, the system will immediately send all restorals as the sensor reports the event.

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

2 Auto Test/Intervals

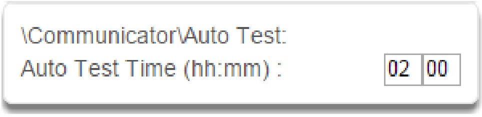


\Communicator\Auto Test:

Auto Test Intervals: Sun

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.

3 Auto Test/Time

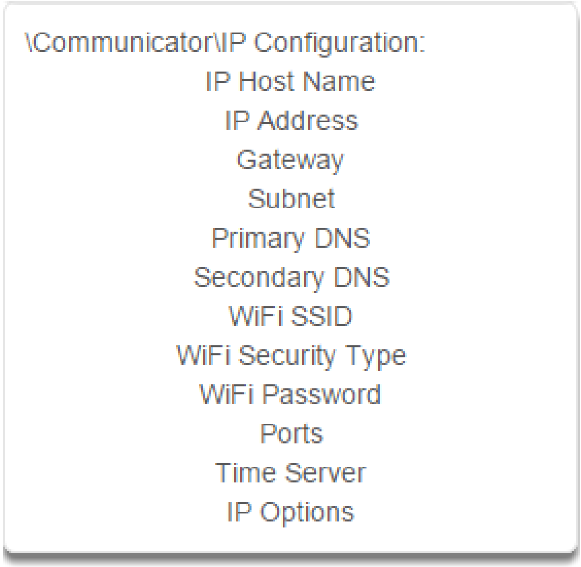


\Communicator\Auto Test:

Auto Test Time (hh:mm) : 02 00

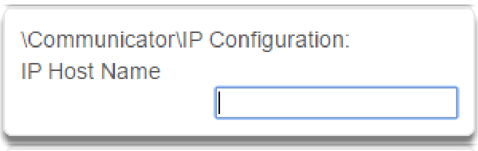
Enter the time at which the automatic test report should be sent. This should be in 24-hour format. For example 18:00.

4 IP Configuration

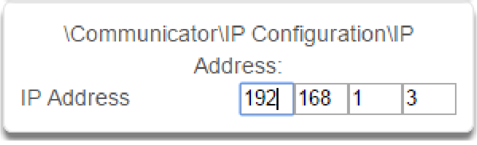


\Communicator\IP Configuration:
IP Host Name
IP Address
Gateway
Subnet
Primary DNS
Secondary DNS
WiFi SSID
WiFi Security Type
WiFi Password
Ports
Time Server
IP Options

5-6 IP Config Detail



\Communicator\IP Configuration:
IP Host Name



\Communicator\IP Configuration\IP Address:
IP Address 192 168 1 3

Host Name

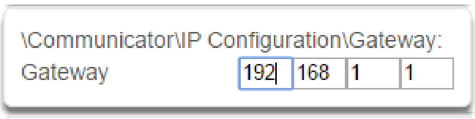
This is a text label assigned to the communicator so you do not have to remember the IP Address.

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.

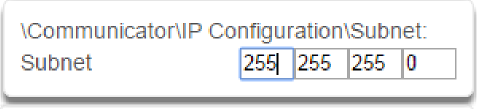
IP Address

The IP address assigned to the communicator to enable it to connect on to the local LAN. This will allow you access to 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.

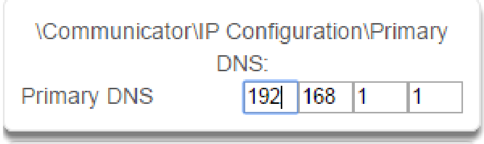
7-10 IP Config Detail



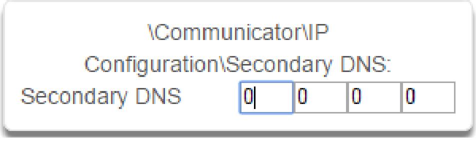
\Communicator\IP Configuration\Gateway:
Gateway 192 168 1 1



\Communicator\IP Configuration\Subnet:
Subnet 255 255 255 0



\Communicator\IP Configuration\Primary DNS:
Primary DNS 192 168 1 1



\Communicator\IP Configuration\Secondary DNS:
Secondary DNS 0 0 0 0

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

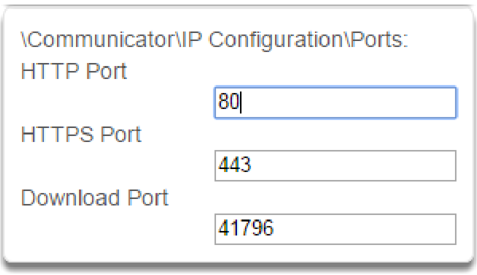
Subnet
The subnet mask for the network.

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.

11 Ports



\Communicator\IP Configuration\Ports:

HTTP Port: 80

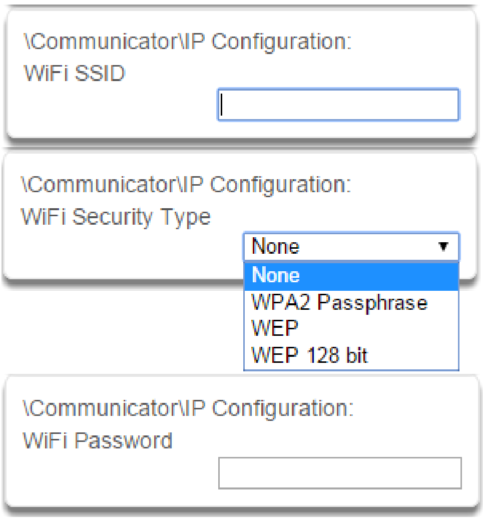
HTTPS Port: 443

Download Port: 41796

The ports that the computer needs to communicate with the system.

Defaults:
HTTP Port = 80
HTTPS Port = 443
Download Port = 41796

12-14 IP Config Detail

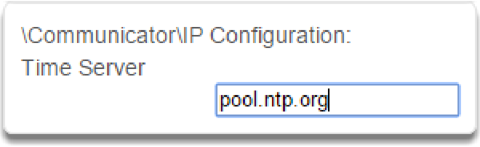


\Communicator\IP Configuration:
WiFi SSID

\Communicator\IP Configuration:
WiFi Security Type: None

\Communicator\IP Configuration:
WiFi Password

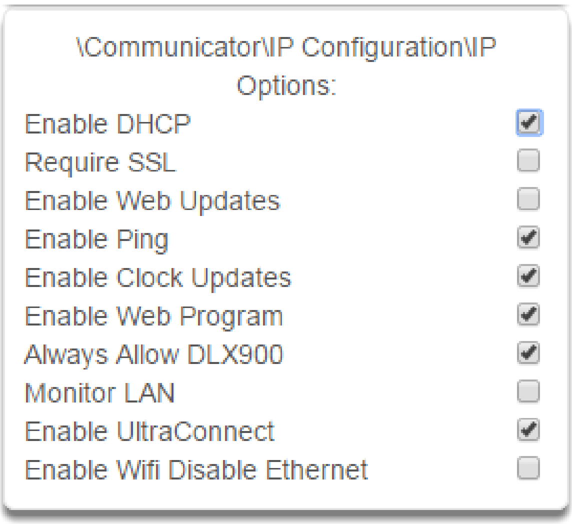
15 Time Server



\Communicator\IP Configuration:
Time Server: pool.ntp.org

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

16 IP Options



\Communicator\IP Configuration\IP Options:

- Enable DHCP ☑
- Require SSL ☐
- Enable Web Updates ☐
- Enable Ping ☑
- Enable Clock Updates ☑
- Enable Web Program ☑
- Always Allow DLX900 ☑
- Monitor LAN ☐
- Enable UltraConnect ☑
- Enable Wifi Disable Ethernet ☐

1. Enable DHCP
Allow the panel to be automatically assigned an IP address by the network.

2. Require SSL
Feature no longer supported. Leave unchecked.

3. Enable Web Updates - RESERVED
Allows the panel to update the web pages via a network. Go to Hostname/mpfsupload to update the web pages served by the panel. Does not update firmware.

4. Enable Ping

Allows the hub to respond to the PING command.

5. Enable Clock Updates

Allows the hub’s internal clock to synchronise with the internet time server specified .

6. Enable Web Program

Enabling this option will cause the Web Server and UltraSync app to always display Installer menus regardless of if the panel is in program mode or not.

Disabling this option will hide the Installer menus on the Web Server and UltraSync app unless program mode is active. This provides greater security by keeping web programming disabled unless a user on site with physical access to the keypad enters program mode with a valid PIN code.

The hub will be in program mode if a user gains access to menu 5, 8, or 9.
UltraSync app requires the Web Access Code to get access to the panel.

7. 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.

The hub will be in program mode if a user gains authorised access to menu 5, 8, or 9 on the keypad.

8. 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.

9. Enable UltraSync

This is an automatic feature. It is recommended you leave this setting on.

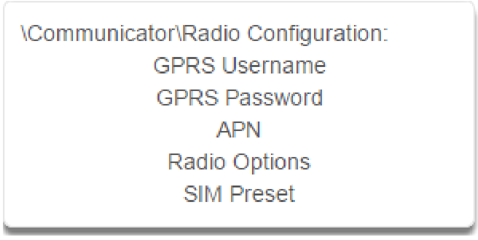
Enable this option to allow the system to send email reports via the UltraSync servers. This is independent of the Web Access Passcode which when set to 00000000 will prevent the UltraSync app from connecting.

If any channel is set to Email format reporting, then system will override this setting and allow email reporting via UltraSync cloud servers.

If you wish to prevent connections to the 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

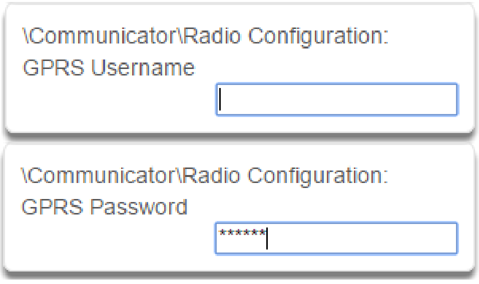
17 Radio Configuration



\Communicator\Radio Configuration:

GPRS Username
GPRS Password
APN
Radio Options
SIM Preset

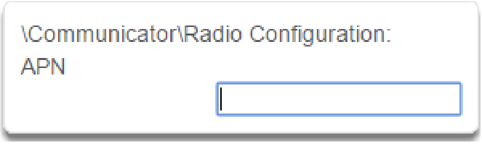
18 GPRS Username/Password



\Communicator\Radio Configuration:
GPRS Username

\Communicator\Radio Configuration:
GPRS Password
******

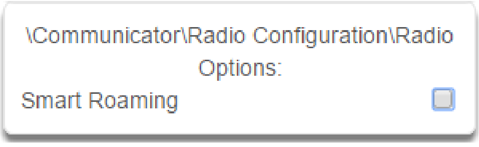
19 APN



\Communicator\Radio Configuration:
APN

Access Point Name (APN) for the settings to set up a connection to the gateway between the cellular network and the public Internet.

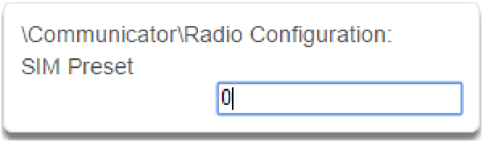
20 Radio Options



\Communicator\Radio Configuration\Radio Options:

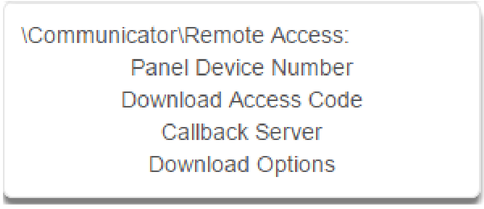
Smart Roaming □

21 SIM Preset



\Communicator\Radio Configuration:
SIM Preset
0

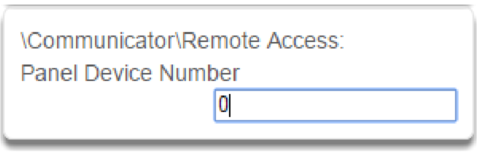
22 Remote Access



\Communicator\Remote Access:

Panel Device Number
Download Access Code
Callback Server
Download Options

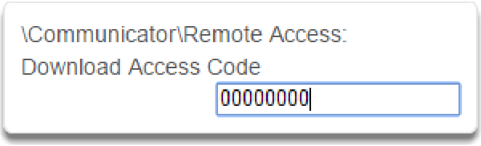
23 Panel Device Number



\Communicator\Remote Access:
Panel Device Number
0

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

24 Download Access Code



\Communicator\Remote Access:
Download Access Code
00000000

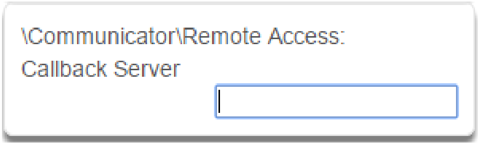
A variable length code for the computer user. This code gives the software complete authority over all menus including those that are locked. For convenience DLX900 will also try **installer** and **9-7-1-3** to allow a connection for first time set up if the Download Access Code does not work This is why changing the default code is important.

The default Download Access Passcode of 00000000 prevents remote access.

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.

25 Callback Server

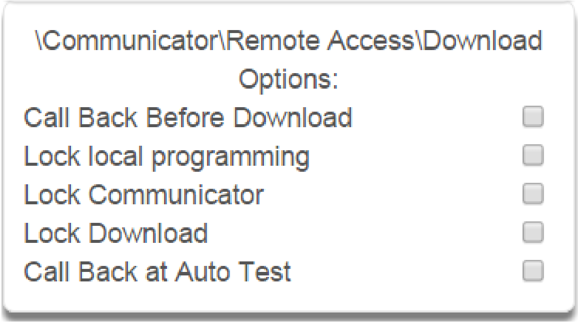


\Communicator\Remote Access:
Callback Server

If an IP address or host name is programmed into this feature, and “Call Back Before Download Session” is enabled, the hub 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 panel.

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

26 Download Options



\Communicator\Remote Access\Download Options:

Call Back Before Download □
Lock local programming □
Lock Communicator □
Lock Download □
Call Back at Auto Test □

1. Call Back Before Download
If a download is requested the hub will hang up and make a call to the Call Back Number. This is to increase the security of remote access.

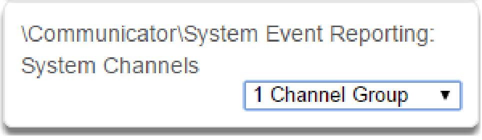
2. Lock local Programming
Prevent changes to the system via a keypad, all changes MUST be made using the remote access software.

3. Lock Communicator
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.

4. Lock Download
Prevents the programming of the Remote Access Menu without using the Download Access PIN.

5. Call Back at Auto Test
When an auto test is initiated, perform a call back to the number specified.

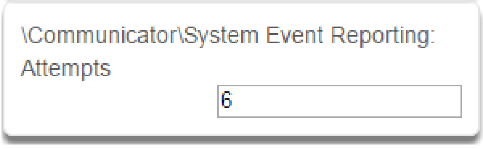
27 Event Reporting /Channels



\Communicator\System Event Reporting: System Channels
1 Channel Group ▼

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

28 Event Reporting /Attempts



\Communicator\System Event Reporting: Attempts
6

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

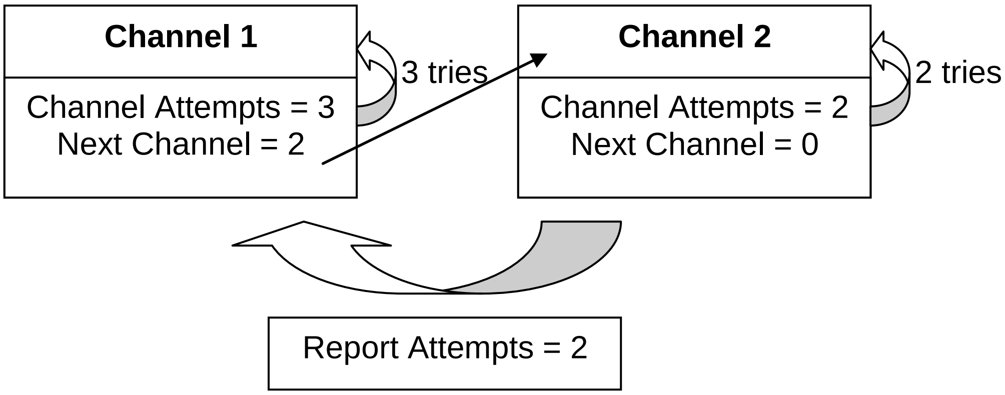
Example

If Channel 1 is the primary, and Channel 2 is the backup for Channel 1, then when both channels fail it will go back to Channel 1. This setting controls how many times the system cycles back to Channel 1 before it gives up.

The Channel Attempts setting controls how many times the system stays on the channel before switching to the backup.

Always check the max. number of attempts on all channels to avoid unexpectedly high communication charges.

In the diagram below, the system will try Channel 1 3 times, switch to Channel 2 and try 2 times, then go back to Channel 1. This sequence is repeated 2 times in total. In total there will be 10 attempts.



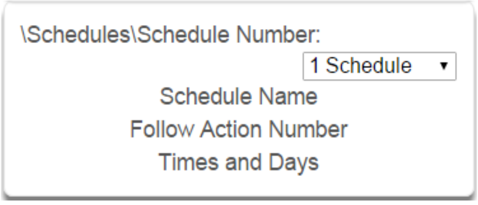
5.6 Advanced Programming, Schedules

Select **Schedules** from the drop down menu.

Schedules Submenus

Schedules Submenus

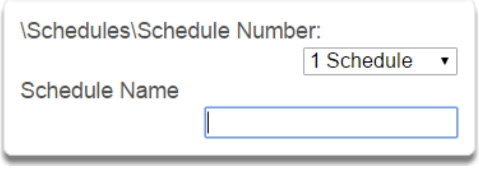
1 Schedule Number



\Schedules\Schedule Number: 1 Schedule

The system can support a total of 96 schedules. Each schedule is identified by a unique schedule number, which cannot be altered, and remains as the key reference for each schedule.

2 Schedule Name

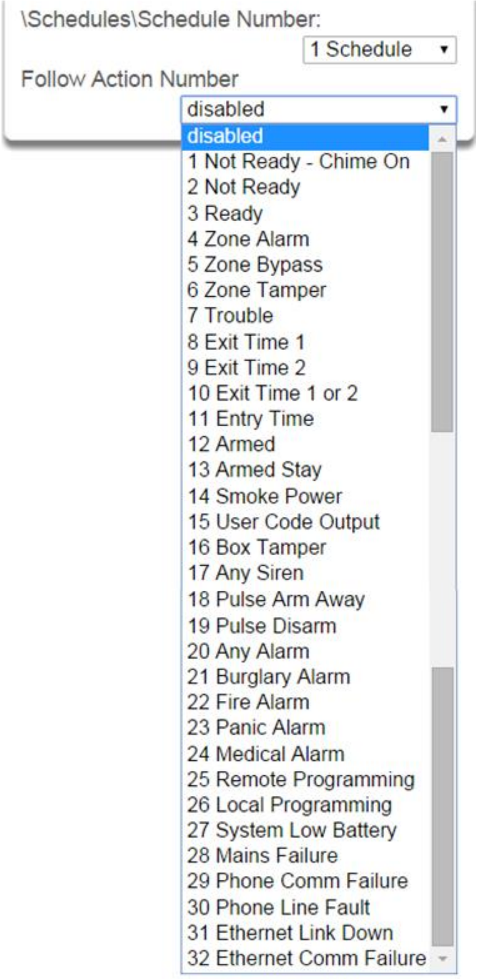


\Schedules\Schedule Number: 1 Schedule

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 system.

3 Follow Action Number



\Schedules\Schedule Number: 1 Schedule

Follow Action Number: disabled

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, sensor behaviors, 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.

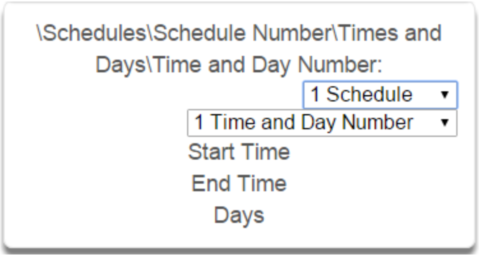
Follow Action

Action controls Schedule controls

Permissions
(users and devices)
Area Types
Sensor Profiles
Arm-Disarm
Scenes

Schedules Submenus

4 Times and Days


\Schedules\Schedule Number\Times and Days\Time and Day Number:

1 Schedule ▾

1 Time and Day Number ▾

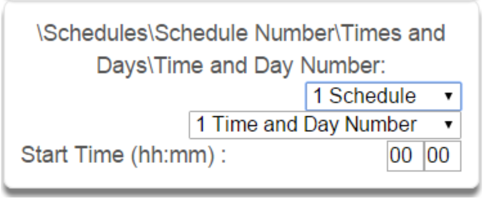
Start Time

End Time

Days

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

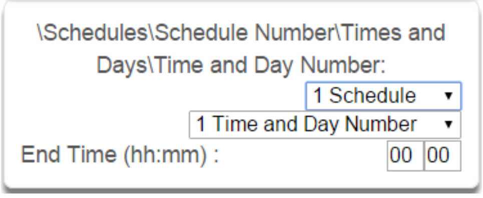
5 Start Time / End Time


\Schedules\Schedule Number\Times and Days\Time and Day Number:

1 Schedule ▾

1 Time and Day Number ▾

Start Time (hh:mm) : 00 00

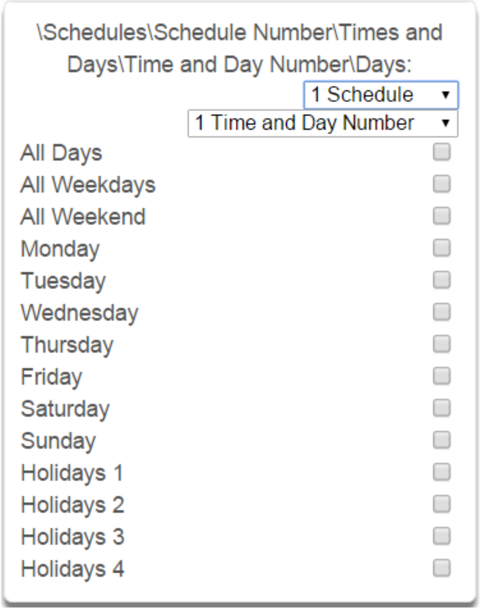

\Schedules\Schedule Number\Times and Days\Time and Day Number:

1 Schedule ▾

1 Time and Day Number ▾

End Time (hh:mm) : 00 00

6 Days / Holidays

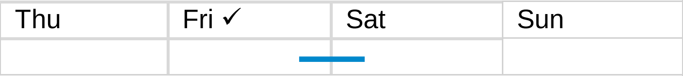

\Schedules\Schedule Number\Times and Days\Time and Day Number\Days:

1 Schedule ▾

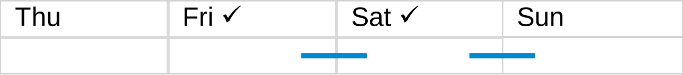
1 Time and Day Number ▾

All Days	□
All Weekdays	□
All Weekend	□
Monday	□
Tuesday	□
Wednesday	□
Thursday	□
Friday	□
Saturday	□
Sunday	□
Holidays 1	□
Holidays 2	□
Holidays 3	□
Holidays 4	□

The hub handles schedules that span midnight automatically. For example, if a schedule is to cover Fri 8:00pm to Sat 6:00am, *only check Friday* and the hub will automatically manage the time after midnight.



If you *check Friday and Saturday*, the schedule will cover Fri 8:00pm – Sat 6:00am and Sat 8:00pm – Sun 6:00am.



Note: Holidays 1-4: If checked, it means the item assigned this schedule will NOT have access during the specified holiday dates.

See Advanced Programming,Holidays to program these dates.

5.7 Advanced Programming, Actions

The system 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.

These features are considered advanced programming and should only be changed by an installer with a thorough understanding of the features.

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 Event Sequence										
Event 1	and or	**Event 2**	and or	**Event 3**	and or	**Event 4**	=	**Action State (trigger)**	+	**Action Result**

When all 4 Action Events are met, then the Action State (trigger) will be set. The Action State can be monitored by the Main 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.

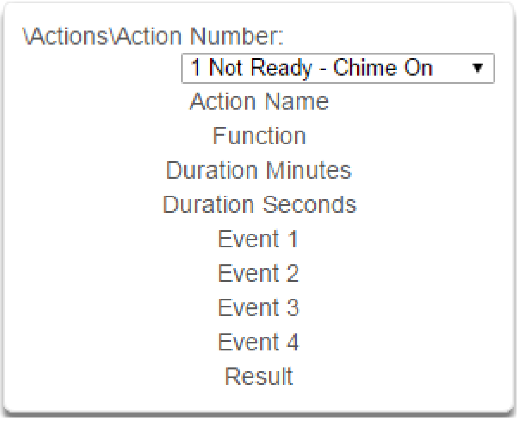
Strobe Action Sequence				
Areas 1 – 8 All Armed	=	**Action 1 True**	+	**Activate Strobe**

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

For example, when all areas are armed and there is activity on Sensor 1, activate a camera recording.

Camera Action Sequence						
Areas 1 – 8 Armed	and	**Sensor 1 Faulted**	=	**Action 1 True**	+	**Activate Camera**

Select **Actions** from the drop down menu.

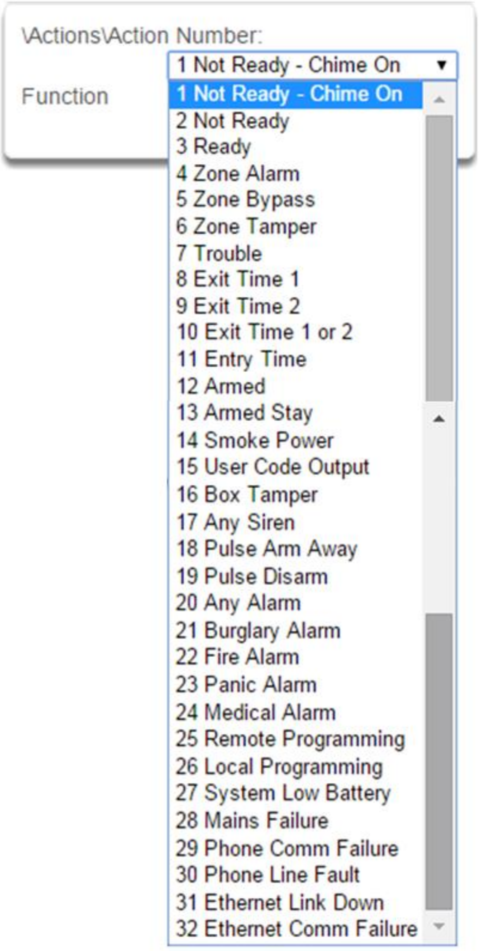


\Actions\Action Number: 1 Not Ready - Chime On

Actions Submenus

Actions Submenus

1 Action Number

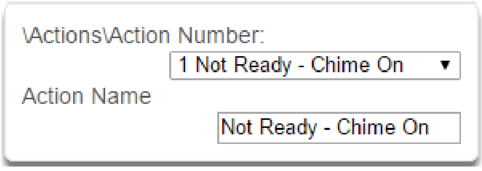


\Actions\Action Number: 1 Not Ready - Chime On

The system 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.

Note: All 32 actions are pre-programmed with the specified trigger. To create a new action, you need to modify one of these actions.

2 Action Name

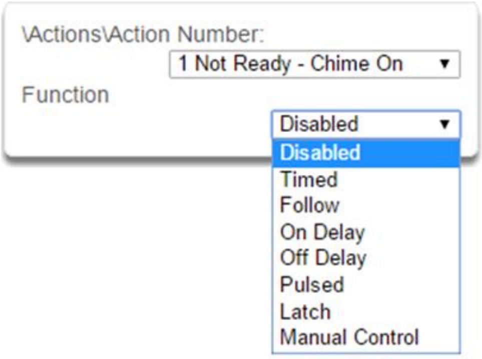


\Actions\Action Number: 1 Not Ready - Chime On

Action Name: Not Ready - Chime On

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

3 Function

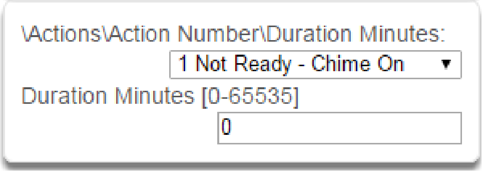


\Actions\Action Number: 1 Not Ready - Chime On

Function: Disabled

- Timed – The action state turns **on** for the time specified.
- **Follow** (Recommended) – 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 the 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.
- On Pulse – 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.

4 Duration: Minutes



\Actions\Action Number\Duration Minutes:

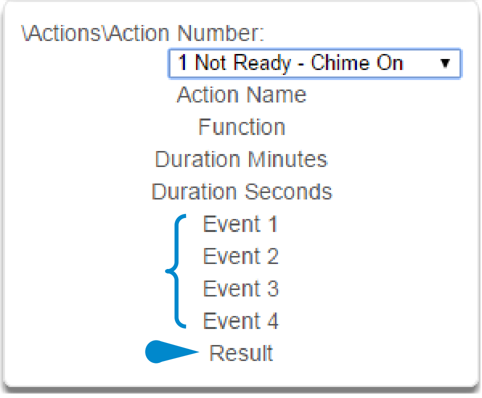
1 Not Ready - Chime On ▼

Duration Minutes [0-65535]

0

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

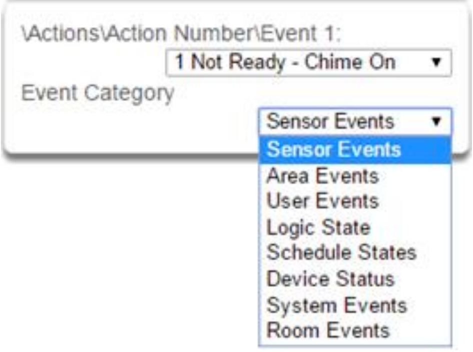
6 Event(s) 1-4 and Results



\Actions\Action Number:

1 Not Ready - Chime On ▼

8 Event Category



\Actions\Action Number\Event 1:

1 Not Ready - Chime On ▼

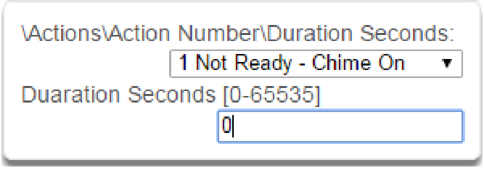
Event Category

Sensor Events ▼

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

See the Action Events Category and Action Event Types table in section A.10 for reference.

5 Duration: Seconds



\Actions\Action Number\Duration Seconds:

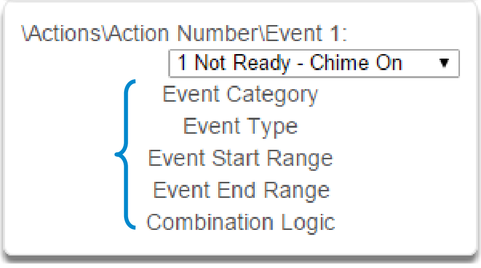
1 Not Ready - Chime On ▼

Duaration Seconds [0-65535]

0

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

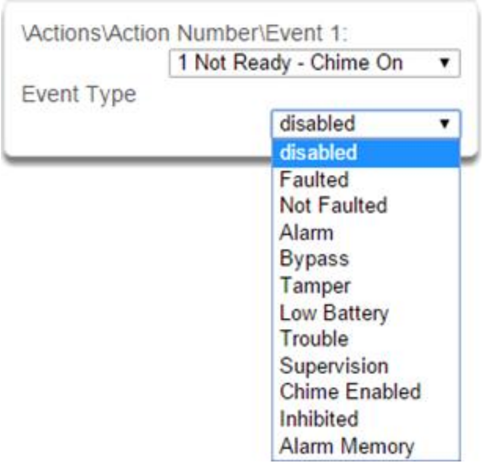
7 Event Attributes



\Actions\Action Number\Event 1:

1 Not Ready - Chime On ▼

9 Event Type



\Actions\Action Number\Event 1:

1 Not Ready - Chime On ▼

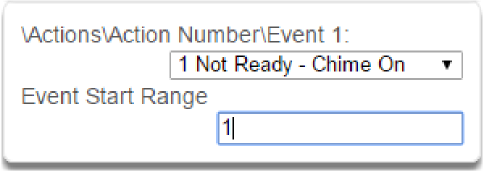
Event Type

disabled ▼

Select the event that you want the Action to monitor.

See the Action Events Category and Action Event Types table in section A.10 for reference.

10 Event Start Range



\Actions\Action Number\Event 1:

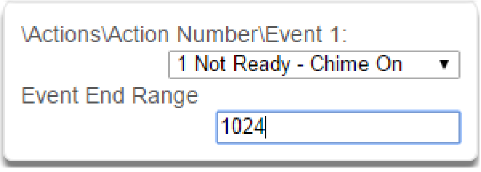
1 Not Ready - Chime On ▾

Event Start Range

1

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 sensor number.

11 Event End Range



\Actions\Action Number\Event 1:

1 Not Ready - Chime On ▾

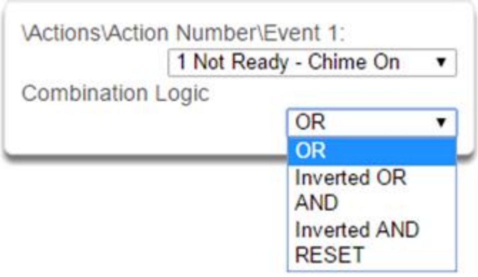
Event End Range

1024

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 sensor 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.

12 Event Combination Logic



\Actions\Action Number\Event 1:

1 Not Ready - Chime On ▾

Combination Logic

OR ▾

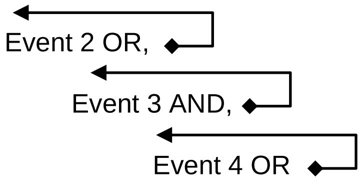
The logic condition to apply to Event 1

• OR	e.g. Area 1 Armed Away **OR** Area 2 Armed Away
• Inverted OR	e.g. **NOT** Sensor 1 Bypass **OR** Sensor 2 Bypass
• AND	e.g. Area 1 Armed Away **AND** Area 2 Armed Away
• Inverted AND	e.g. **NOT** Sensor 1 Bypass **AND** Sensor 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,



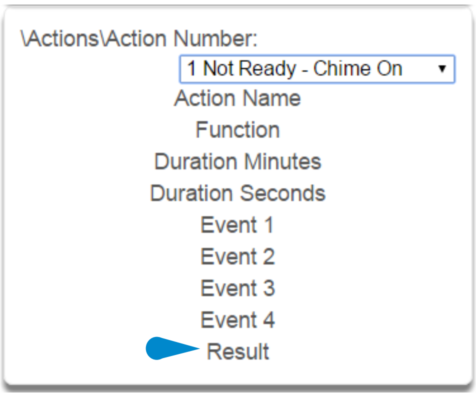
Event 2 OR,

Event 3 AND,

Event 4 OR

produces a logic equation of:
(**NOT** Event 1 **OR** Event 2) **AND** (Event 3 **OR** Event 4)

13 Result

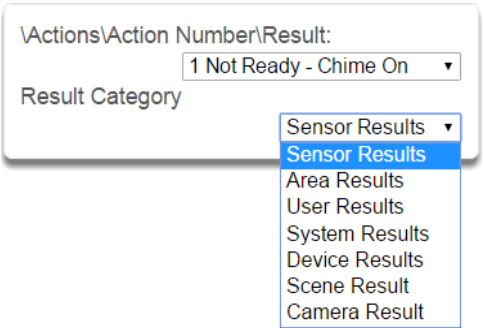


\Actions\Action Number: 1 Not Ready - Chime On

The system 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 1-50 to prevent them from being able to control the alarm system.

14 Result Category



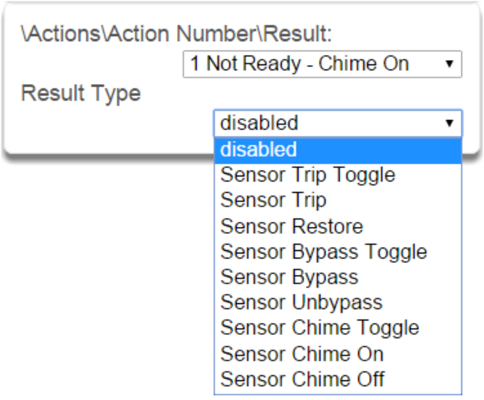
\Actions\Action Number\Result: 1 Not Ready - Chime On

Result Category: Sensor Results

Result Category: The category of the Action Result to perform.

See the Action Results Category and Action Results Event Types table in section A.11 for reference.

15 Result Type

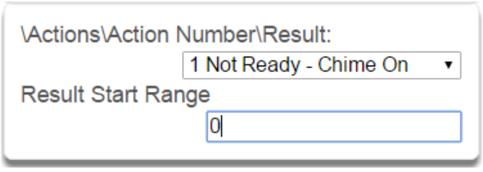


\Actions\Action Number\Result: 1 Not Ready - Chime On

Result Type: disabled

The event of the Action Result to perform
See the Action Results Category and Action Results Event Types table in section A.11 for reference.

16 Result Start Range

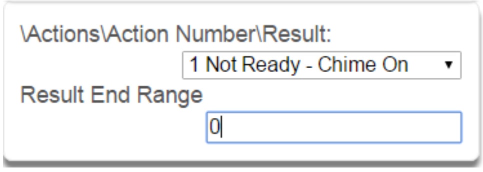


\Actions\Action Number\Result: 1 Not Ready - Chime On

Result Start Range: 0

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

17 Result End Range

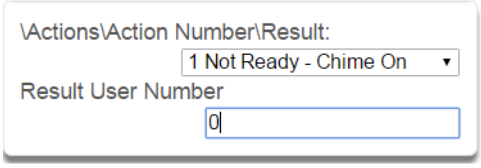


\Actions\Action Number\Result: 1 Not Ready - Chime On

Result End Range: 0

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

18 Result User Number



\Actions\Action Number\Result: 1 Not Ready - Chime On

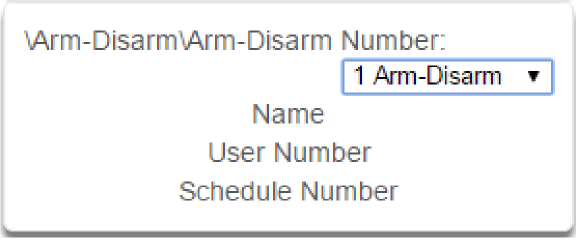
Result User Number: 0

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.

5.8 Advanced Programming, Auto Arm-Disarm

Advanced Arm-Disarm programming allows the system to automate arming and disarming according to a specified schedule.

Select **Arm-Disarm** from the drop down menu.



\Arm-Disarm\Arm-Disarm Number: 1 Arm-Disarm ▼

Name

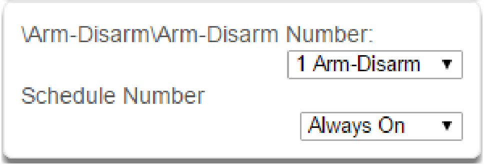
User Number

Schedule Number

Arm-Disarm Submenus

Arm-Disarm Submenus

1 Number (1-8)

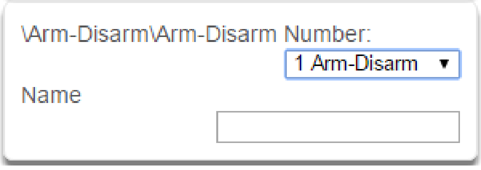


\Arm-Disarm\Arm-Disarm Number: 1 Arm-Disarm ▼

Schedule Number: Always On ▼

The system can support a total of 8 automated Arm-Disarm scenarios. Each scenario is identified by a unique number, which cannot be altered, and remains as the key reference for each function.

2 Name

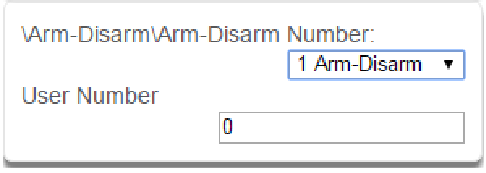


\Arm-Disarm\Arm-Disarm Number: 1 Arm-Disarm ▼

Name

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

3 User Number

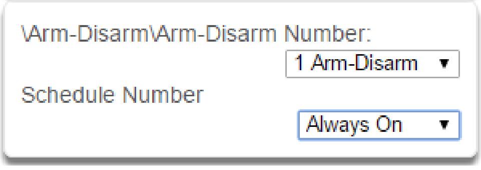


\Arm-Disarm\Arm-Disarm Number: 1 Arm-Disarm ▼

User Number: 0

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.

4 Schedule Number



\Arm-Disarm\Arm-Disarm Number: 1 Arm-Disarm ▼

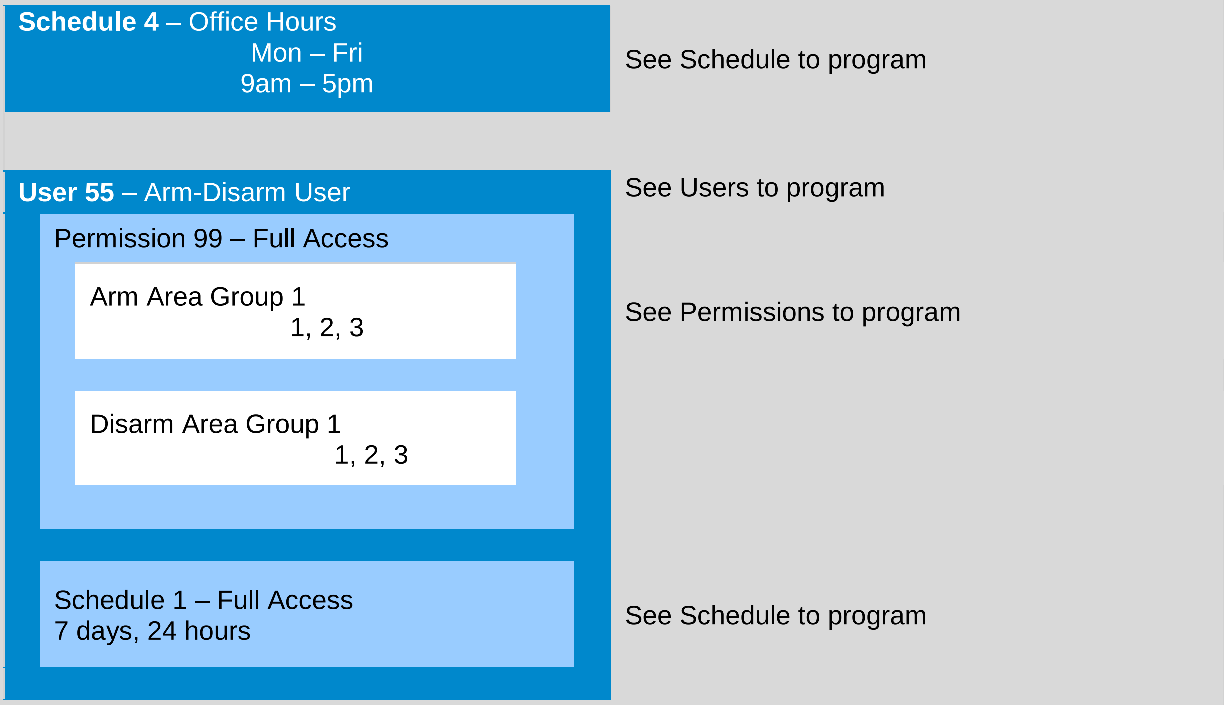
Schedule Number: Always On ▼

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.

When a Schedule becomes valid (inside valid time sensor) the system will disarm all Areas that are in the User's - Active Profile - Disarm Area Group. When the Schedule becomes invalid (out of time sensor) then system 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.

Arm Disarm Number 1 – Arm-Disarm Example



Schedule 4 – Office Hours
Mon – Fri
9am – 5pm

See Schedule to program

User 55 – Arm-Disarm User

See Users to program

Permission 99 – Full Access

Arm Area Group 1
1, 2, 3

Disarm Area Group 1
1, 2, 3

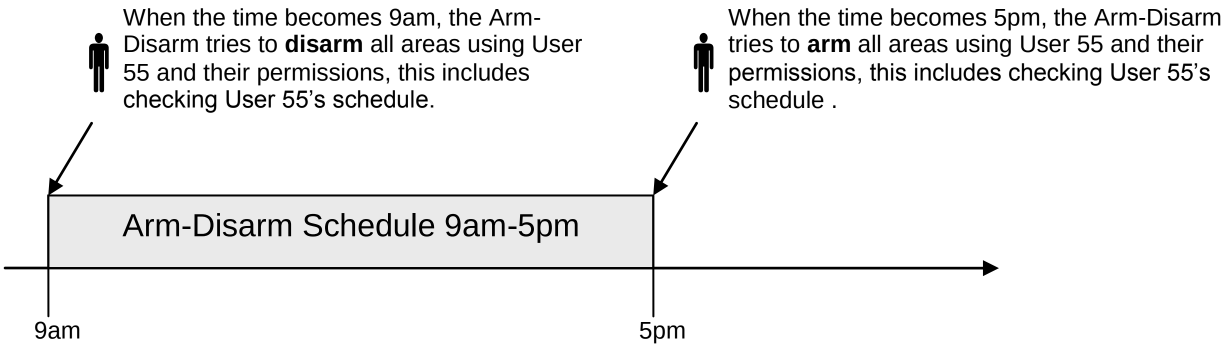
See Permissions to program

Schedule 1 – Full Access
7 days, 24 hours

See Schedule to program

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.



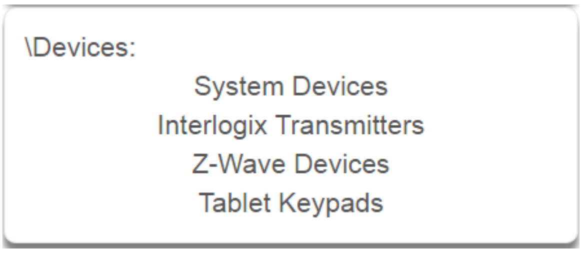
When the time becomes 9am, the Arm-Disarm tries to **disarm** all areas using User 55 and their permissions, this includes checking User 55's schedule.

When the time becomes 5pm, the Arm-Disarm tries to **arm** all areas using User 55 and their permissions, this includes checking User 55's schedule .

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.

5.9 Advanced Programming, Devices

Select **Devices** from the drop down menu.

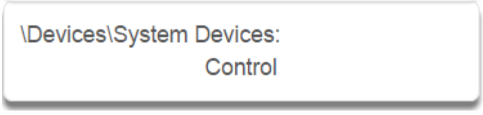


This menu allows you to program devices connected to the system.

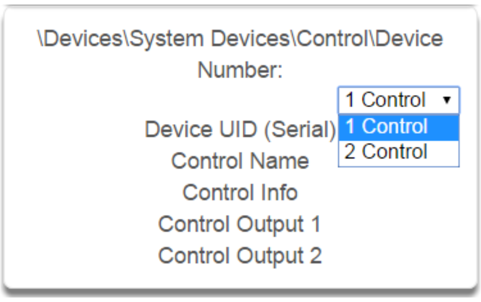
Devices Submenus

Devices Submenus

1 System Devices Control

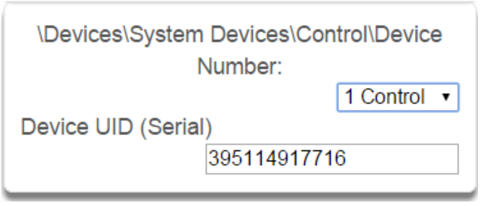


2 System Devices Control Device Number


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

Select among control devices to program them.

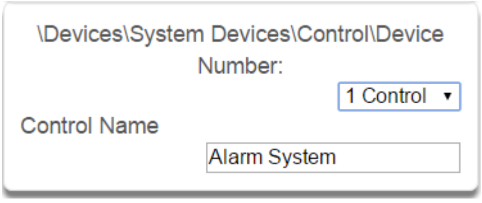
3 Device UID


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

Device UID (Serial) 395114917716

Serial number of the hub.

4 Control Name

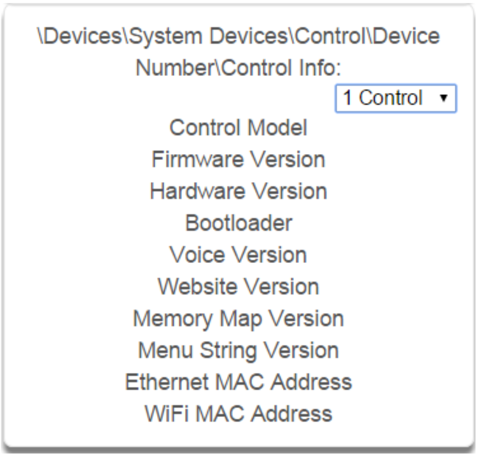

\Devices\System Devices\Control\Device Number: 1 Control ▾

Control Name Alarm System

The name of the system.

Devices Submenus

5 Control Info



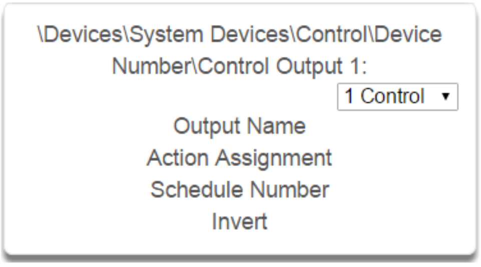
\Devices\System Devices\Control\Device Number\Control Info:

1 Control ▾

Control Model
Firmware Version
Hardware Version
Bootloader
Voice Version
Website Version
Memory Map Version
Menu String Version
Ethernet MAC Address
WiFi MAC Address

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

6 Control Output 1



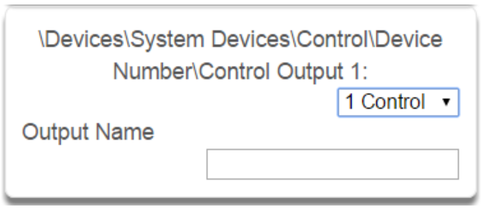
\Devices\System Devices\Control\Device Number\Control Output 1:

1 Control ▾

Output Name
Action Assignment
Schedule Number
Invert

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

7 Control Output 1 Output Name



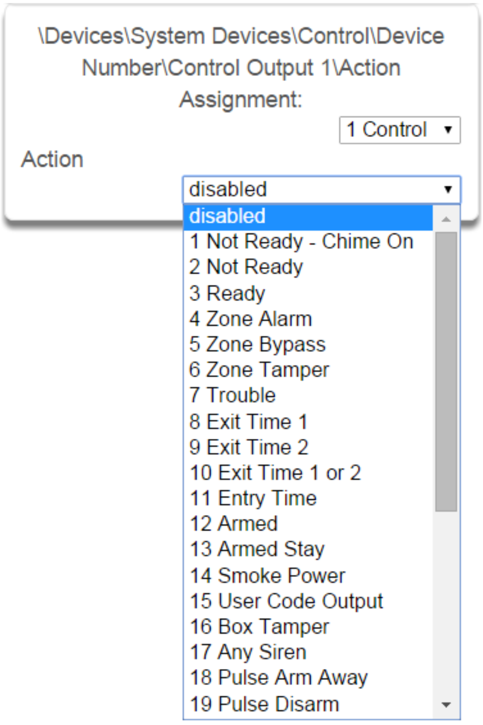
\Devices\System Devices\Control\Device Number\Control Output 1:

1 Control ▾

Output Name

Each output can be configured with a custom 32 character name.

8 Control Output 1 Action Assignment



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

1 Control ▾

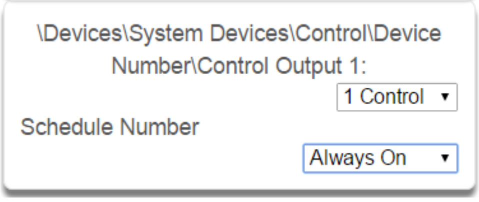
Action

disabled ▾

disabled
1 Not Ready - Chime On
2 Not Ready
3 Ready
4 Zone Alarm
5 Zone Bypass
6 Zone Tamper
7 Trouble
8 Exit Time 1
9 Exit Time 2
10 Exit Time 1 or 2
11 Entry Time
12 Armed
13 Armed Stay
14 Smoke Power
15 User Code Output
16 Box Tamper
17 Any Siren
18 Pulse Arm Away
19 Pulse Disarm

The output will activate while the selected action state is true. If the action state becomes false then the output will deactivate.

9 Control Output 1 Schedule Number


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

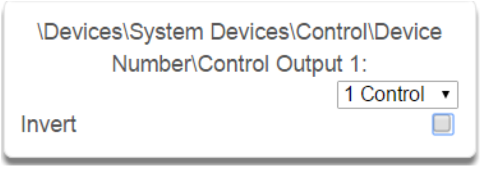
1 Control ▾

Schedule Number

Always On ▾

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.

10 Control Output 1 Invert

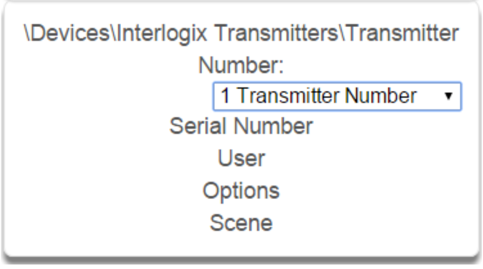

\Devices\System Devices\Control\Device Number\Control Output 1:

1 Control ▾

Invert □

Invert the Output

11 Interlogix Transmitters


\Devices\Interlogix Transmitters\Transmitter Number:

1 Transmitter Number ▾

Serial Number

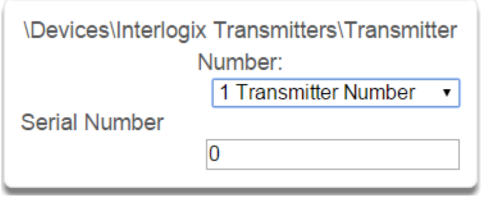
User

Options

Scene

Number of the Interlogix Transmitter

12 Serial Number


\Devices\Interlogix Transmitters\Transmitter Number:

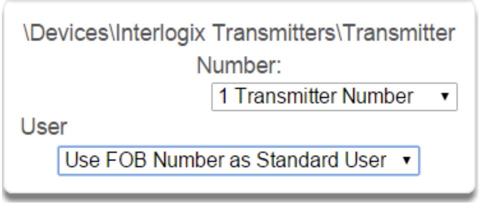
1 Transmitter Number ▾

Serial Number

0

Serial number of the Interlogix Device

13 User


\Devices\Interlogix Transmitters\Transmitter Number:

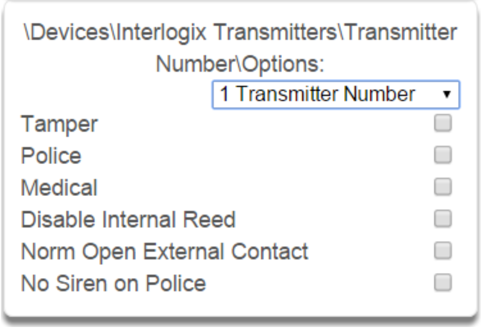
1 Transmitter Number ▾

User

Use FOB Number as Standard User ▾

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

14 Transmitter Options


\Devices\Interlogix Transmitters\Transmitter Number\Options:

1 Transmitter Number ▾

Tamper □

Police □

Medical □

Disable Internal Reed □

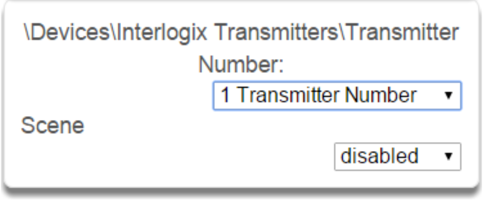
Norm Open External Contact □

No Siren on Police □

Allows the Installer to configure options for wireless transmitters including:

- Tamper
- Police
- Medical
- Disable Internal Reed – this applies to transmitters with an internal reed switch
- Norm Open External Contact
- No Siren on Police

15 Scene

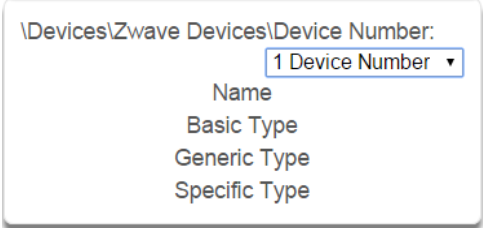


\Devices\Interlogix Transmitters\Transmitter Number: 1 Transmitter Number ▾

Scene: disabled ▾

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

16 Zwave Devices



\Devices\Zwave Devices\Device Number: 1 Device Number ▾

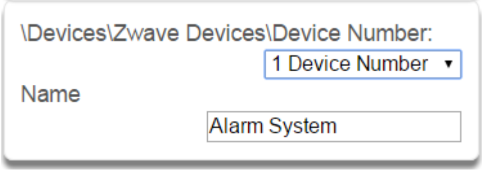
Name

Basic Type

Generic Type

Specific Type

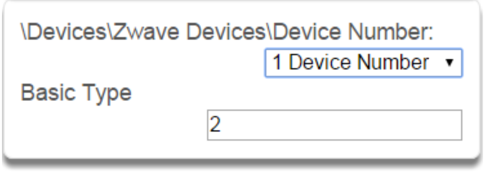
17 Zwave Devices Name



\Devices\Zwave Devices\Device Number: 1 Device Number ▾

Name: Alarm System

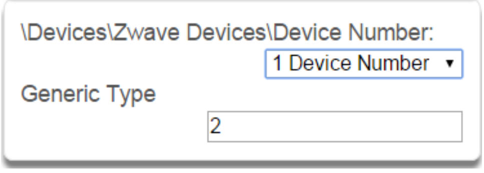
18 Zwave Devices Basic Type



\Devices\Zwave Devices\Device Number: 1 Device Number ▾

Basic Type: 2

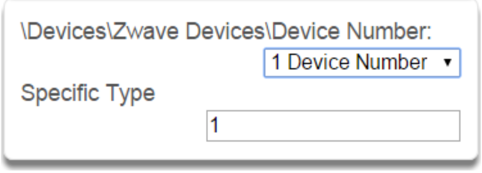
19 Zwave Devices Generic Type



\Devices\Zwave Devices\Device Number: 1 Device Number ▾

Generic Type: 2

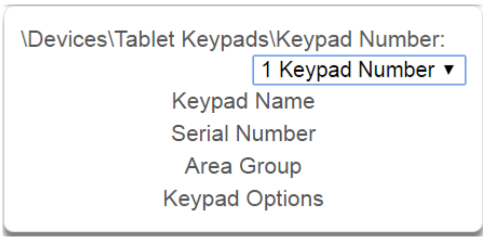
20 Zwave Devices Specific Type



\Devices\Zwave Devices\Device Number: 1 Device Number ▾

Specific Type: 1

21 Tablet Keypads



\Devices\Tablet Keypads\Keypad Number: 1 Keypad Number ▾

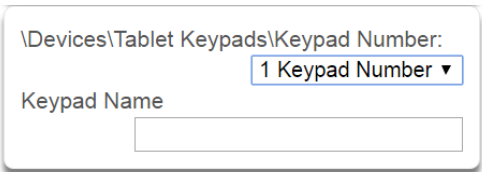
Keypad Name

Serial Number

Area Group

Keypad Options

22 Keypad Name

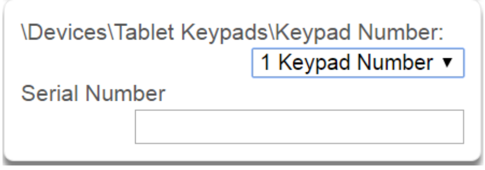


\Devices\Tablet Keypads\Keypad Number: 1 Keypad Number ▾

Keypad Name:

The name of the Tablet Keypad

23 Serial Number

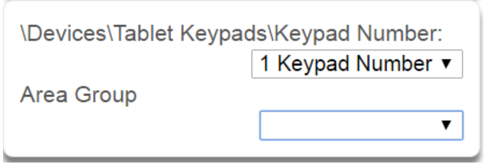


\Devices\Tablet Keypads\Keypad Number: 1 Keypad Number ▾

Serial Number:

The serial number of the Tablet Keypad

24 Area Group

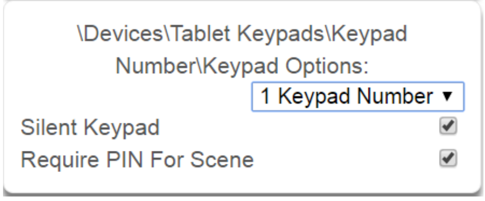


\Devices\Tablet Keypads\Keypad Number: 1 Keypad Number ▾

Area Group: ▾

The area the tablet Keypad is assigned to.

25 Keypad Options



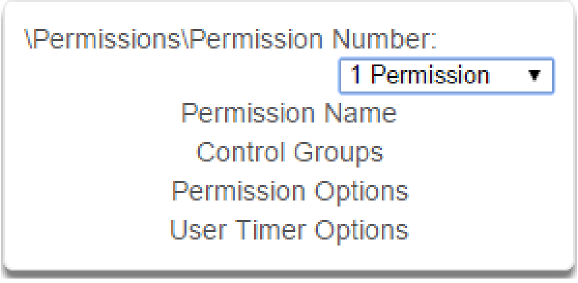
\Devices\Tablet Keypads\Keypad Number\Keypad Options: 1 Keypad Number ▾

Silent Keypad ☑

Require PIN For Scene ☑

5.10 Advanced Programming, Permissions

Select **Permissions** from the drop down menu.



\Permissions\Permission Number:

1 Permission ▼

Permission Name

Control Groups

Permission Options

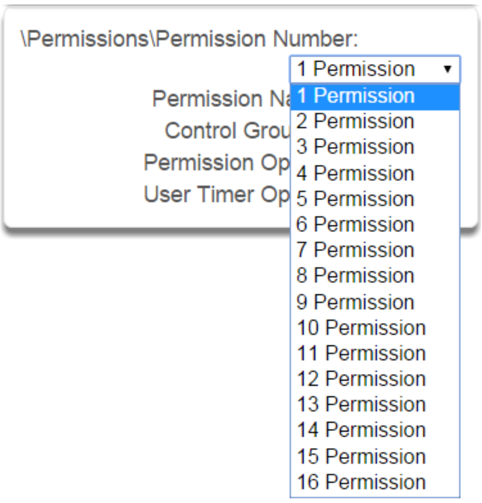
User Timer Options

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

Permissions Submenus

Permissions Submenus

1 Permission Number



\Permissions\Permission Number:

1 Permission ▾

Permission Na

Control Grou

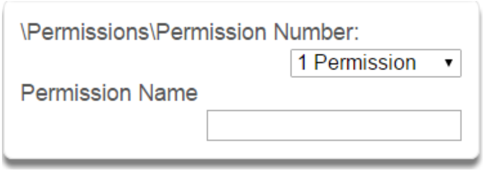
Permission Op

User Timer Op

1 Permission
2 Permission
3 Permission
4 Permission
5 Permission
6 Permission
7 Permission
8 Permission
9 Permission
10 Permission
11 Permission
12 Permission
13 Permission
14 Permission
15 Permission
16 Permission

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

2 Permission Name



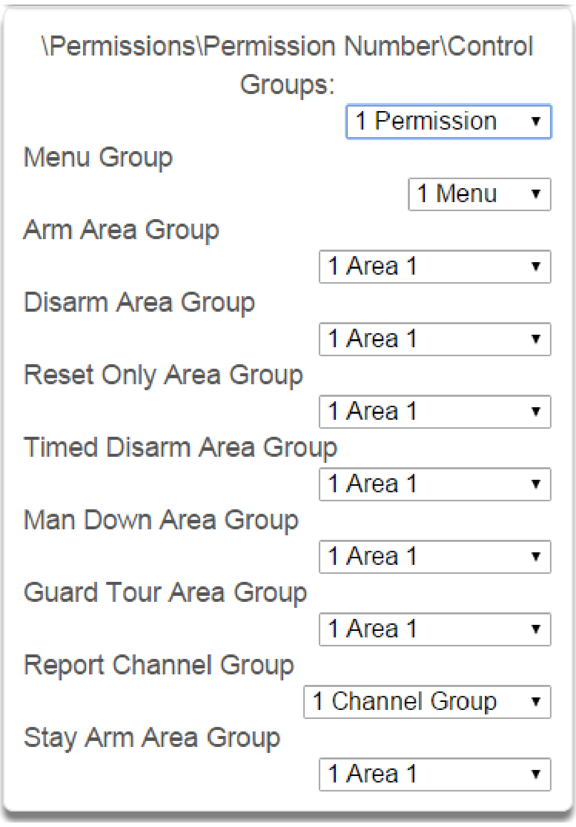
\Permissions\Permission Number:

1 Permission ▾

Permission Name

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

3 Control Groups



\Permissions\Permission Number\Control Groups:

1 Permission

Menu Group: 1 Menu

Arm Area Group: 1 Area 1

Disarm Area Group: 1 Area 1

Reset Only Area Group: 1 Area 1

Timed Disarm Area Group: 1 Area 1

Man Down Area Group: 1 Area 1

Guard Tour Area Group: 1 Area 1

Report Channel Group: 1 Channel Group

Stay Arm Area Group: 1 Area 1

1. Menu Group
This controls what menus the user or device can access

2. Arm Area Group
This controls which areas can be armed.

3. Disarm Area Group
This controls which areas can be disarmed.

4. 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.

5. Timed Disarm Area Group
This controls which areas can be timed disarm.

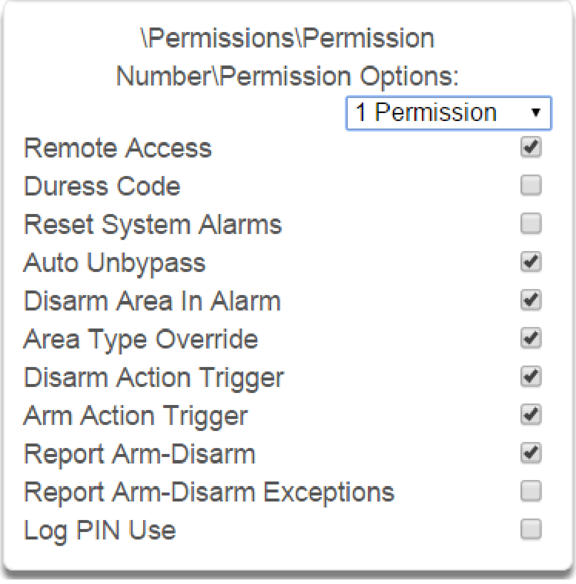
6. Man Down Area Group
This controls which areas will have man down monitoring.

7. Guard Tour Area Group
This controls which areas are a part of the guard tour.

8. Report Channel Group
This controls what channels the user can modify.

9. Stay Arm Area Group
This controls what areas can be stay armed.

4 Permission Options



\Permissions\Permission Number\Permission Options:

1 Permission ▾

Remote Access	☑
Duress Code	□
Reset System Alarms	□
Auto Unbypass	☑
Disarm Area In Alarm	☑
Area Type Override	☑
Disarm Action Trigger	☑
Arm Action Trigger	☑
Report Arm-Disarm	☑
Report Arm-Disarm Exceptions	□
Log PIN Use	□

1. 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.

2. Duress Code - designates this user as a duress code, whenever this code is used a duress message is sent.

3. 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.

4. Auto Un-Bypass - When enabled, a bypassed sensor will be reset when disarming. When disabled, the Sensor will remain bypassed even after the system has been disarmed.

5. 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.

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

7. Disarm Action Trigger - When enabled, this users will trigger the Action trigger event “User Disarm Trigger” when disarming an area, used in conjunction with for programming actions.

8. Arm Action Trigger - When enabled, this user will trigger the Action trigger event “User Arm Trigger” when arming an area, used in conjunction with for programming actions.

9. 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.

10. Report Arm-Disarm Exceptions –
Report Arm-Disarm Exceptions = ON:

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’

Report Arm-Disarm Exceptions = OFF:

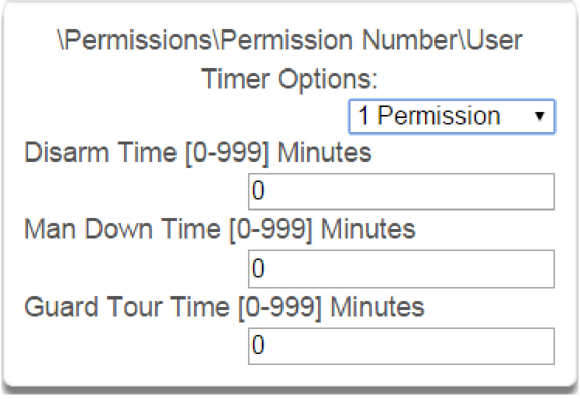
As expected only reports were the ‘Fail To Open’ and ‘Fail To Close’ reports with their respective resets ‘Late Open’ and ‘Late Close’. Both the ‘Early Open’ and ‘Early Close’ reports were suppressed.

‘Fail To Open’ and the reset report ‘Late Open’
‘Fail To Close’ and the reset report ‘Late Closing’

See Area Type for more details.

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

5 User Timer Options



\Permissions\Permission Number\User Timer Options:

1 Permission ▾

Disarm Time [0-999] Minutes

0

Man Down Time [0-999] Minutes

0

Guard Tour Time [0-999] Minutes

0

1. Disarm Time
2. Man Down Time
3. 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 Area Type Settings for a more detailed description on these features.

5.11 Advanced Programming, Area Groups

Select **Area Groups** from the drop down menu.

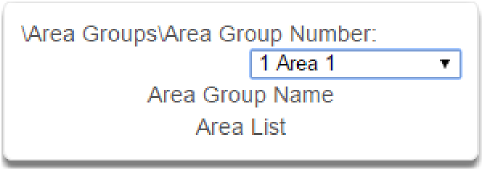
The system can support a total of 16 Area Groups. Each Area Group is identified by a unique number, which cannot be altered, and remains as the key reference for each area.

When assigned to a user, an Area Group controls what areas the user can see and control. When assigned to a sensor or device, an Area Group determines what Areas that sensor/device will report and display in.

Area Groups Submenus

Area Groups Submenus

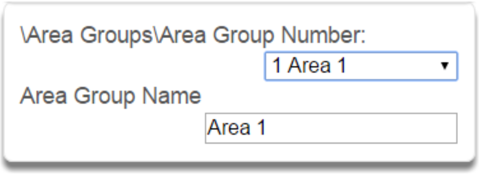
1 Area Group Number



\Area Groups\Area Group Number:
1 Area 1 ▾
Area Group Name
Area List

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

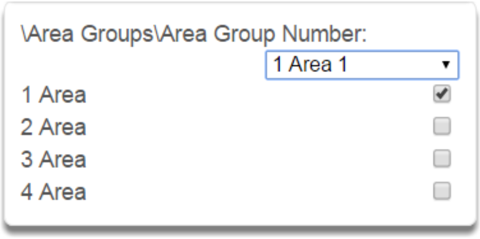
2 Area Group Name



\Area Groups\Area Group Number:
1 Area 1 ▾
Area Group Name
Area 1

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

3 Area List



\Area Groups\Area Group Number:
1 Area 1 ▾

1 Area ☑
2 Area □
3 Area □
4 Area □

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

5.12 Advanced Programming, Menus

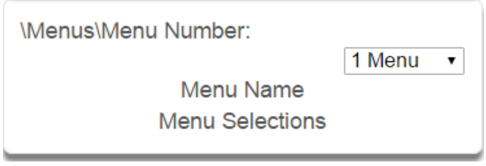
Select **Menus** from the drop down menu.

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

Menus Submenus

Menus Submenus

1 Menu Number (1 – 16)



\Menus\Menu Number:

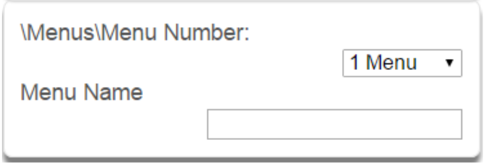
1 Menu ▾

Menu Name

Menu Selections

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

2 Menu Name



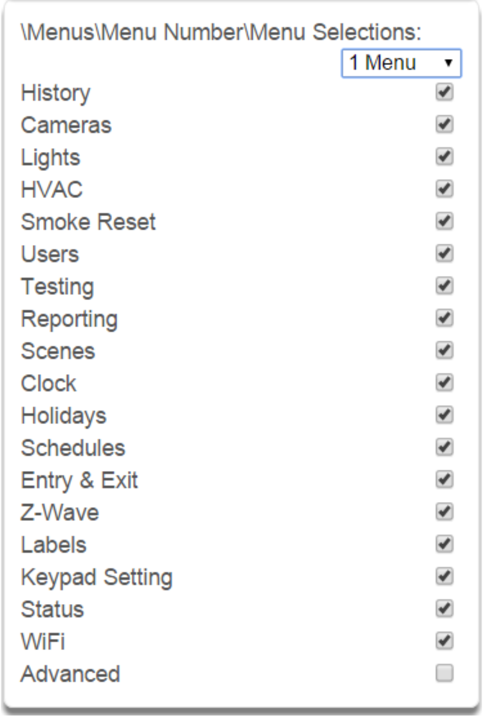
\Menus\Menu Number:

1 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 system.

3 Menu Selections



\Menus\Menu Number\Menu Selections:

1 Menu ▾

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

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

5.13 Advanced Programming, Holidays

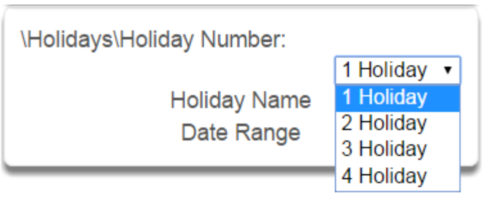
Select **Holidays** from the drop down menu.

Also reference Section 4.9 Programming Holidays

Holidays Submenus

Holidays Submenus

1 Holiday Number (1 – 4)



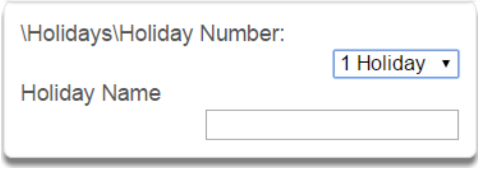
\Holidays\Holiday Number:

Holiday Name

Date Range

The system supports up to 4 sets of Holiday Sets. 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.

2 Holiday Name

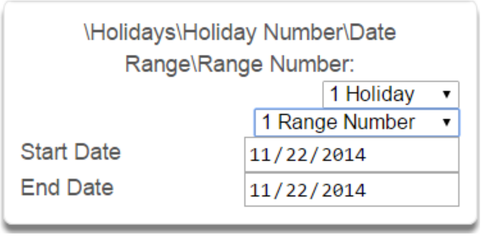


\Holidays\Holiday Number: 1 Holiday ▾

Holiday Name

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

3 Holiday Date Range



\Holidays\Holiday Number\Date Range\Range Number:

1 Holiday ▾

1 Range Number ▾

Start Date 11/22/2014

End Date 11/22/2014

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.

5.14 Advanced Programming, Sensor Types

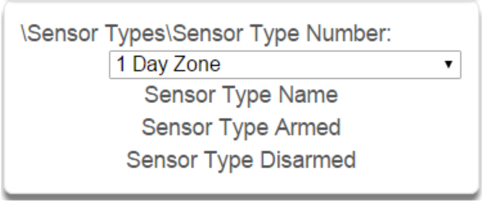
Select **Sensor Types** from the drop down menu.

Sensors can be programmed to be one of 32 different sensor configurations (sensor type profiles). Sensors are fully configurable in the panel. These features are considered advanced programming and should only be changed by an installer with a thorough understanding of the features.

Sensor Types Submenus

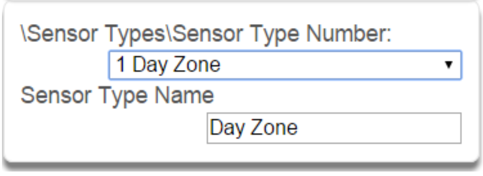
Sensor Types Submenus

1 Sensor Type Number (1 – 32)


\Sensor Types\Sensor Type Number:
1 Day Zone ▾
Sensor Type Name
Sensor Type Armed
Sensor Type Disarmed

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

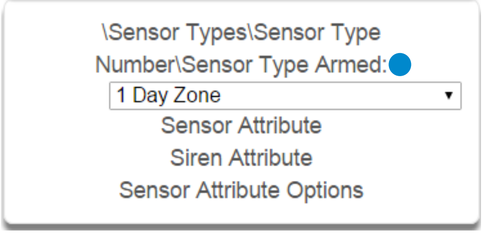
2 Sensor Type Name


\Sensor Types\Sensor Type Number:
1 Day Zone ▾
Sensor Type Name
Day Zone

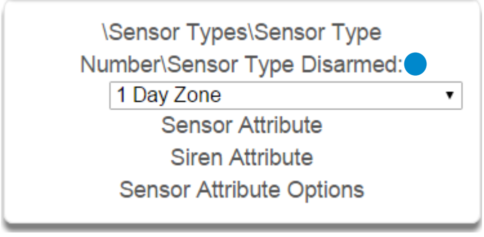
Each Sensor Type can be configured with a custom 32 character name. The name is displayed wherever a Sensor Type is referenced on the system.

Sensor type profiles can also change depending on whether the areas they are in are armed or disarmed. This provides a new level of flexibility in panel programming.

Armed


\Sensor Types\Sensor Type Number\Sensor Type Armed:●
1 Day Zone ▾
Sensor Attribute
Siren Attribute
Sensor Attribute Options

Disarmed


\Sensor Types\Sensor Type Number\Sensor Type Disarmed:●
1 Day Zone ▾
Sensor Attribute
Siren Attribute
Sensor Attribute Options

3 Sensor Type Profile / Armed

Sensor Attribute
This is how the sensor will behave when the area it is in is armed.

- Disabled – sensor is disabled.
- Entry 1 – sensor will follow area entry/exit timer 1.
- Entry 2 – sensor will follow area entry/exit timer 2.
- Handover – instant alarm type unless an entry sensor is tripped first.
- Instant – sensor goes into alarm as soon as it is tripped.
- Local – sensor only triggers a local alarm and keypad sounder but does not report when tripped.
- Trouble Sensor – typically used on fire doors to the exterior of a building. When the system is disarmed they report trouble and sound a buzzer. When the system is armed they are instant burg alarms.
- Fire – smoke detectors must be wired Normally Open. A short on a fire sensor 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 sensor type, regardless of the Sensor Trouble reporting option. Keypad sensor LED is steady for fire condition and flashing for trouble condition. After fire activation, use the keypad to clear & reset fire sensor by pressing Sensor Reset.
- Holdup delay – when tripped, starts the hold up timer, if the timer is reached then a hold up alarm is sent.
- Holdup reset – when this sensor is tripped, the hold up timer is stopped.
- Keyswitch – A momentary key switch can be used to arm/disarm the panel when it is momentarily shorted from a closed condition. Use a 3.3K resister for this sensor type. Or if DEOL monitoring is enabled in System Options, use two 3.3K resistors to allow full line monitoring.
- Event Only – this sensor 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 sensor goes into alarm.

- Silent – siren makes no sound
- Fire – temporal three pulse siren
- Yelping – siren makes a yelping sound
- Four Pulse – temporal four pulse siren

4 Sensor Type Profile / Disarmed

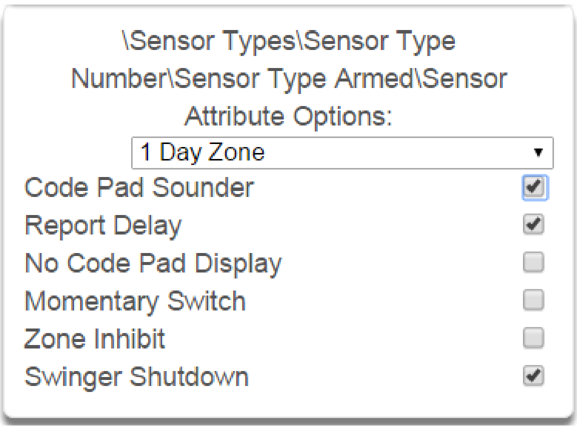
This is how the sensor will behave when the area it is in is disarmed.

- Disabled – sensor is disabled.
- Instant – sensor goes into alarm as soon as it is tripped.
- Local – sensor only triggers a local alarm and keypad sounder but does not report when tripped.
- Fire – smoke detectors must be wired Normally Open. A short on a fire sensor 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 sensor type, regardless of the Sensor Trouble reporting option. Keypad sensor LED is steady for fire condition and flashing for trouble condition. After fire activation, use the keypad to clear & reset fire sensor by pressing Sensor Reset.
- Holdup delay – when tripped, starts the hold up timer, if the timer is reached then a hold up alarm is sent.
- Holdup reset – when this sensor is tripped, the hold up timer is stopped.
- Keyswitch – A momentary key switch can be used to arm/disarm the panel when it is momentarily shorted from a closed condition. Use a 3.3K resister for this sensor type. Or if DEOL monitoring is enabled in System Options, use two 3.3K resistors to allow full line monitoring.
- Event Only – this sensor only creates an event when tripped and is stored in the event log.

Siren Attribute

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

5 Sensor Attribute Options (Armed or Disarmed)



\Sensor Types\Sensor Type Number\Sensor Type Armed\Sensor Attribute Options:

1 Day Zone ▾

Code Pad Sounder	☑
Report Delay	☑
No Code Pad Display	□
Momentary Switch	□
Zone Inhibit	□
Swinger Shutdown	☑

- Code Pad Sounder – If enabled, the panel will announce alarm, tamper, or trouble conditions. Default is on.

- Report Delay – if enabled, the system will delay reporting sensor activations until the next scheduled report. This setting is ignored if the sensor is a Fire type and sensor activations are reported immediately. When disabled sensor activations (trip, bypass and restorals) are reported immediately. Default is off.

- No Keypad Display – if enabled, any sensor 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 sensor will not latch. If it is triggered again then it will send another report immediately. Default is off.

- Sensor Inhibit (Bypass) – This feature is designed to reduce false alarms at arming/disarming. If enabled, a sensor 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 sensor is open, or when a schedule change occurs that changes the sensor type. The bypass will be applied to the sensor if it remains open at the end of the exit timer. Default is off.

- Swinger Shutdown

Swinger Shutdown is a false alarm prevention feature that counts the number of alarms caused by a specific sensor.

Sensor Types Table

Preset Number	Preset Name	Sensor Attribute	Siren Attribute	Panel Sounder	Report delay	No Panel Display	Momentary	Sensor Inhibit (Bypass)
		Armed						
1	Day Sensor	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 Sensor	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

5.15 Advanced Programming, Sensor Options

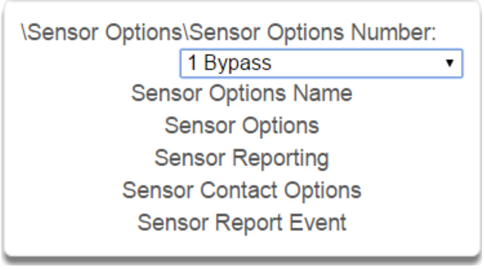
Select **Sensor Options** from the drop down menu.

Sensors are fully configurable in the panel. These features are considered advanced programming and should only be changed by an installer with a thorough understanding of the features.

Sensor Options Submenus

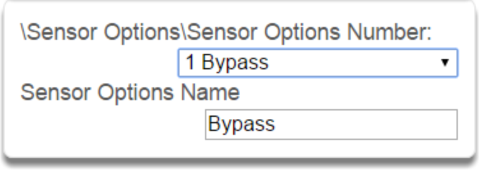
Sensor Options Submenus

1 Sensor Options Number (1 – 32)


\Sensor Options\Sensor Options Number:
1 Bypass ▾

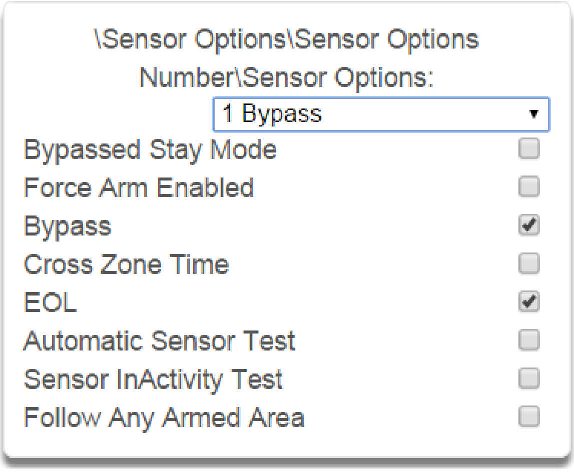
The system can support a total of 32 Sensor Options. Each Sensor Option is identified by a unique number, which cannot be altered, and remains as the key reference for each Sensor Option.

2 Sensor Options Name


\Sensor Options\Sensor Options Number:
1 Bypass ▾
Sensor Options Name
Bypass

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

3 Sensor Options



\Sensor Options\Sensor Options Number\Sensor Options:

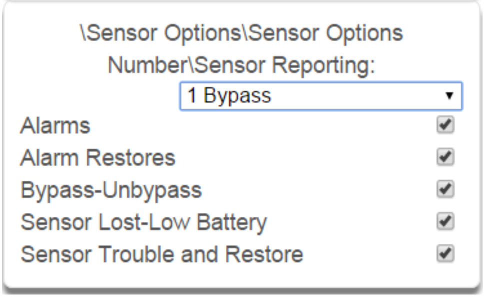
1 Bypass ▾

Bypassed Stay Mode	☐
Force Arm Enabled	☐
Bypass	☑
Cross Zone Time	☐
EOL	☑
Automatic Sensor Test	☐
Sensor InActivity Test	☐
Follow Any Armed Area	☐

Also see the Sensor Options table for reference.

- Bypassed Stay Mode – if enabled, this sensor is automatically bypassed when the area is armed in stay mode. For example, it is an interior sensor.
- Force Arm Enabled – if enabled, this sensor type may be open while arming if forced arming is enabled in the area options. Normally all sensors in an area must be closed before a user can attempt to arm that area.
- Bypass – if enabled, this sensor may be bypassed.
- Cross Zone– This sensor type will require two triggers or another sensor would have to have been trigged before it will activate an alarm.
- EOL – Enable End Of Line resistor tamper monitoring
- Automatic Sensor Test – if enabled, this test is controlled by action results automatic test on and off.
- Sensor Inactivity Test – if enabled, this sensor will check for Sensor Inactivity. The Sensor Inactivity setting must be enabled in General Options. The time is programmed in Sensor Inactivity Time. See Programming the System, section 4.4.
- Follow Any Armed Area – If enabled, and a sensor 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 sensor will become active.

4 Sensor Reporting



\Sensor Options\Sensor Options Number\Sensor Reporting:

1 Bypass ▾

Alarms ☑

Alarm Restores ☑

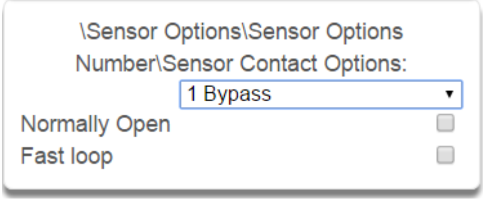
Bypass-Unbypass ☑

Sensor Lost-Low Battery ☑

Sensor Trouble and Restore ☑

- Alarms Reporting – if enabled, this sensor will report alarms.
- Alarm Restores Reporting – if enabled, this sensor will report alarms.
- Bypass-Unbypass Reporting – if enabled, this sensor will report bypasses and unbypass restorals.
- Sensor Lost-Low Battery Reporting – if enabled, this sensor will report loss of wireless supervision and low battery faults.
- Sensor Trouble and Restore – if enabled, this sensor will report sensor trouble and restorals. Fire type sensors will always report regardless of this option.

5 Sensor Contact Options



\Sensor Options\Sensor Options Number\Sensor Contact Options:

1 Bypass ▾

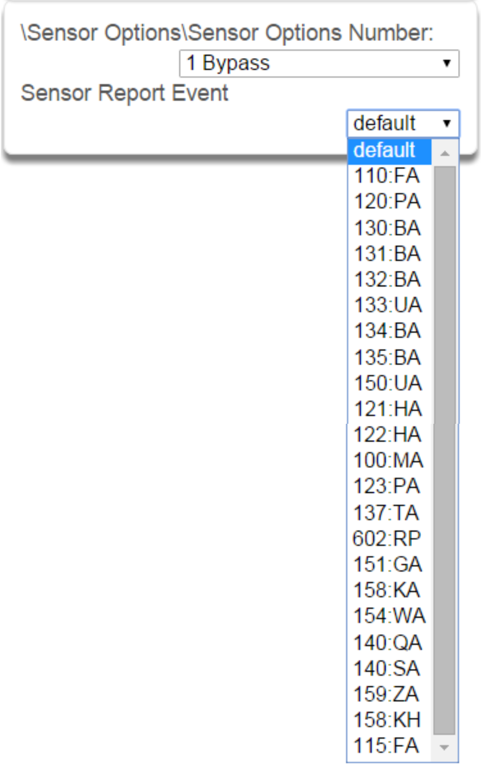
Normally Open □

Fast loop □

(Applies to the hardwire inputs, not wireless sensors.)

- Normally Open no EOL – if enabled, the sensor circuit is normally open. Default is off.
- Fast Loop – if enabled, the system will be more sensitive and respond quicker to a change in state to the sensor. 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 sensor is used for intrusion detection.

6 Sensor Report Event



\Sensor Options\Sensor Options Number:

1 Bypass ▾

Sensor Report Event

default ▾

From the drop down menu, select the CID and SIA event code to report when this sensor is tripped.

Sensor Options Table

Preset Number	Preset Name	Bypassed Stay Mode	Forced Arm Enabled	Bypass	Cross Zone Time	EOL	Automatic Sensor Test	Sensor Inactivity Test	Follow Any Armed Area	Alarms reporting	Alarm restore reporting	Bypass-Unbypass reporting	Sensor reporting Lost-Low Battery	Sensor reporting Trouble and Restore	Normally Open	Fast Loop	Sensor 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 – Cross Zone**			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

5.16 Advanced Programming, Event Lists

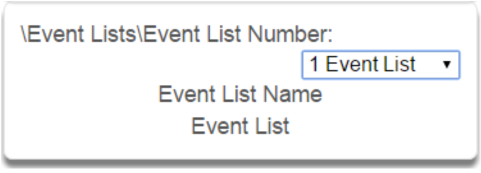
Select **Event Lists** from the drop down menu.

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 Lists Submenus

Event Lists Submenus

1 Event List Number (1 – 16)



\Event Lists\Event List Number:

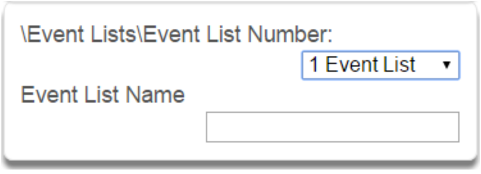
1 Event List ▾

Event List Name

Event List

The system 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.

2 Event List Name



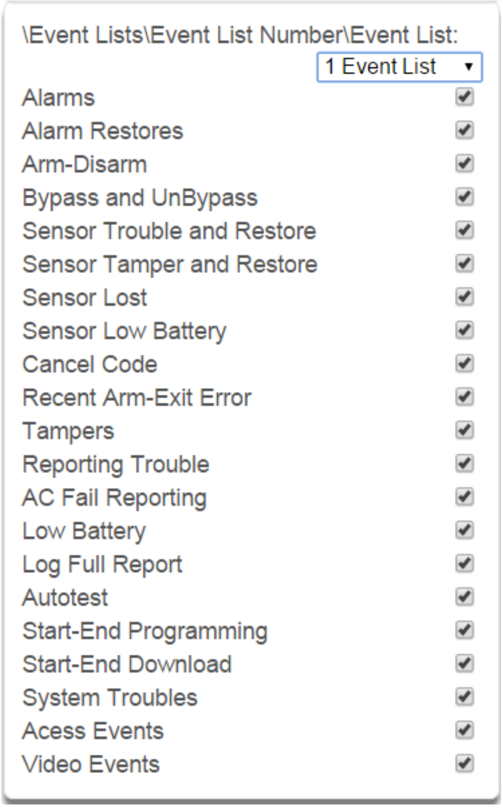
\Event Lists\Event List Number:

1 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 system.

3 Event List



\Event Lists\Event List Number\Event List:

1 Event List ▾

Alarms	☑
Alarm Restores	☑
Arm-Disarm	☑
Bypass and UnBypass	☑
Sensor Trouble and Restore	☑
Sensor Tamper and Restore	☑
Sensor Lost	☑
Sensor Low Battery	☑
Cancel Code	☑
Recent Arm-Exit Error	☑
Tampers	☑
Reporting Trouble	☑
AC Fail Reporting	☑
Low Battery	☑
Log Full Report	☑
Autotest	☑
Start-End Programming	☑
Start-End Download	☑
System Troubles	☑
Acess Events	☑
Video Events	☑

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

5.17 Advanced Programming, Channel Groups

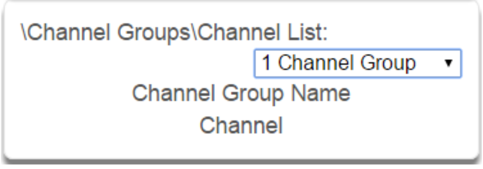
Select **Channel Groups** from the drop down menu.

The hub 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.

Channel Groups Submenus

Channel Groups Submenus

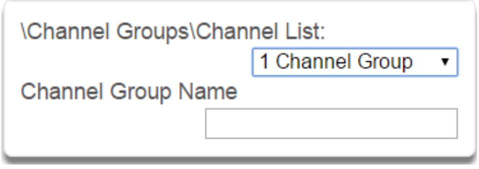
1 Channel Group Number (1 – 16)



\Channel Groups\Channel List:
1 Channel Group ▾
Channel Group Name
Channel

The system 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.

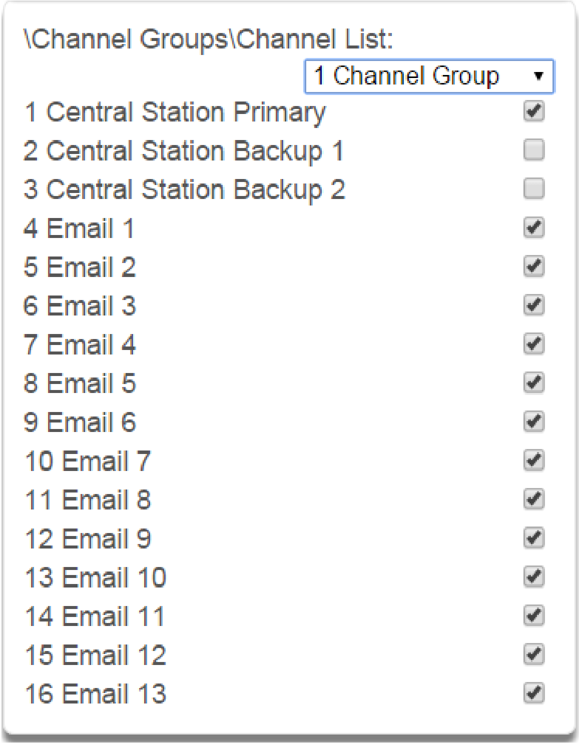
2 Channel Group Name



\Channel Groups\Channel List:
1 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 system.

3 Channel List



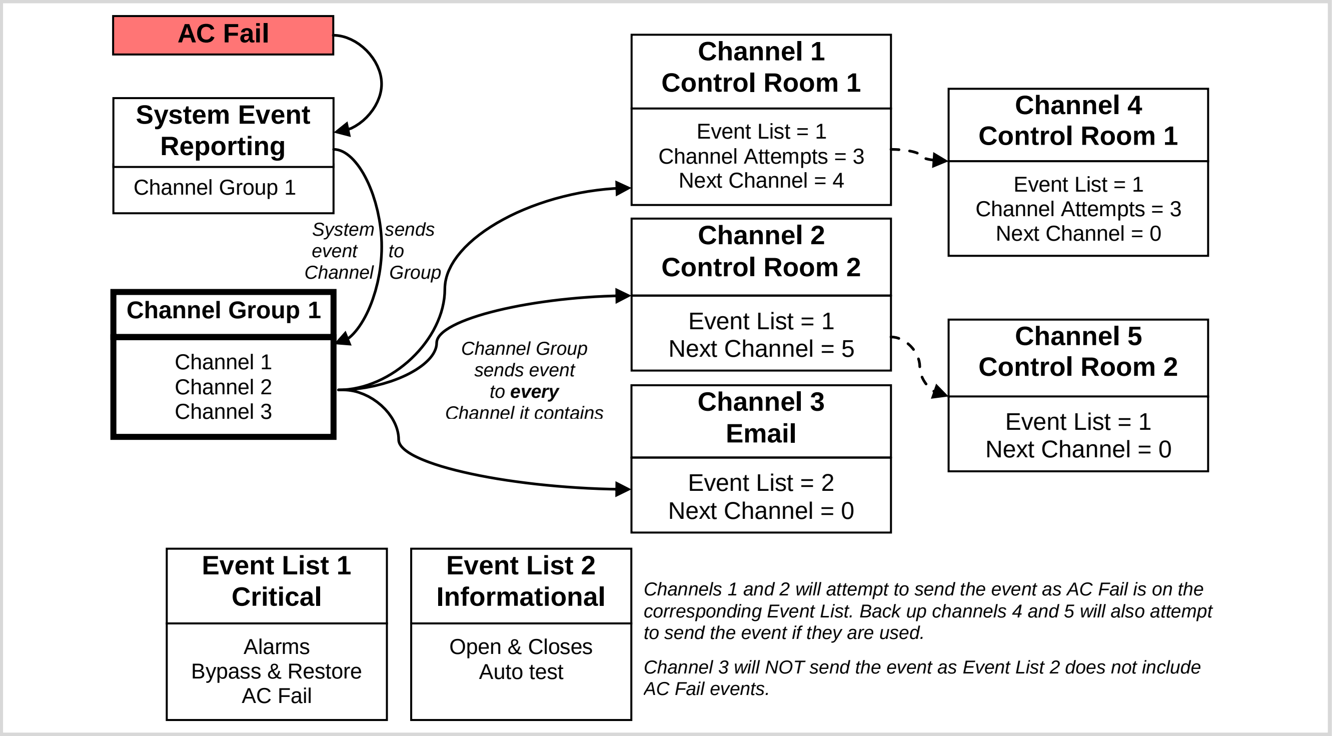
\Channel Groups\Channel List:
1 Channel Group ▾

1 Central Station Primary ☑
2 Central Station Backup 1 ☐
3 Central Station Backup 2 ☐
4 Email 1 ☑
5 Email 2 ☑
6 Email 3 ☑
7 Email 4 ☑
8 Email 5 ☑
9 Email 6 ☑
10 Email 7 ☑
11 Email 8 ☑
12 Email 9 ☑
13 Email 10 ☑
14 Email 11 ☑
15 Email 12 ☑
16 Email 13 ☑

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

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 **System** Event

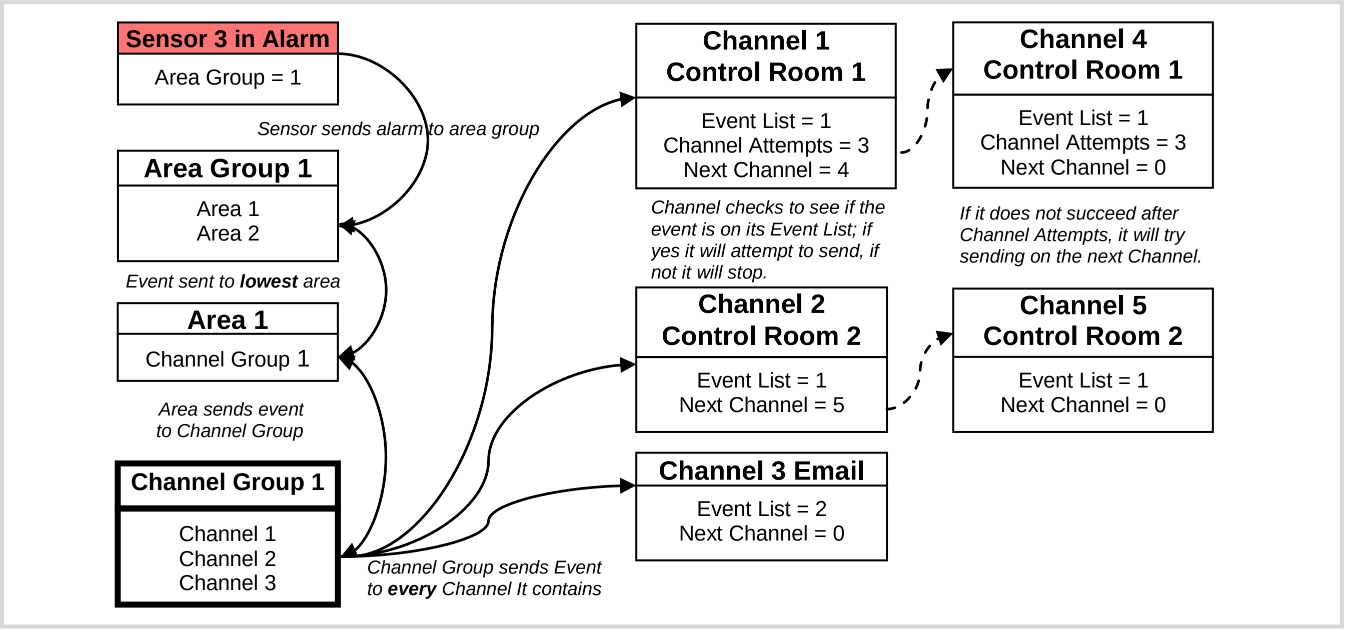


Channels 1 and 2 will attempt to send the event as AC Fail is on the corresponding Event List. Back up channels 4 and 5 will also attempt to send the event if they are used.

Channel 3 will NOT send the event as Event List 2 does not include AC Fail events.

If a **sensor or area event is generated**, then the event is sent to the Channel Group specified (Area – Channel Group) in the lowest area the sensor 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 **Sensor or Area** Event



Channel checks to see if the event is on its Event List; if yes it will attempt to send, if not it will stop.

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

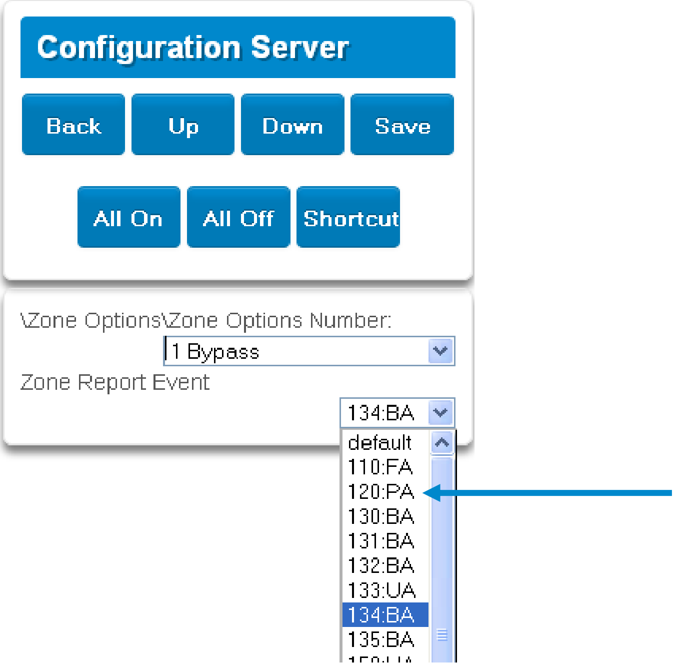
Customize Reporting Codes

The hub 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 sensor I.D. generating the alarm.

Programmed Event Code	Contact I.D. Code	SIA Event Code	Description
0	Use default code for Sensor Type	Use default code for Sensor 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	Medical 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

Customize the code reported by following these steps:

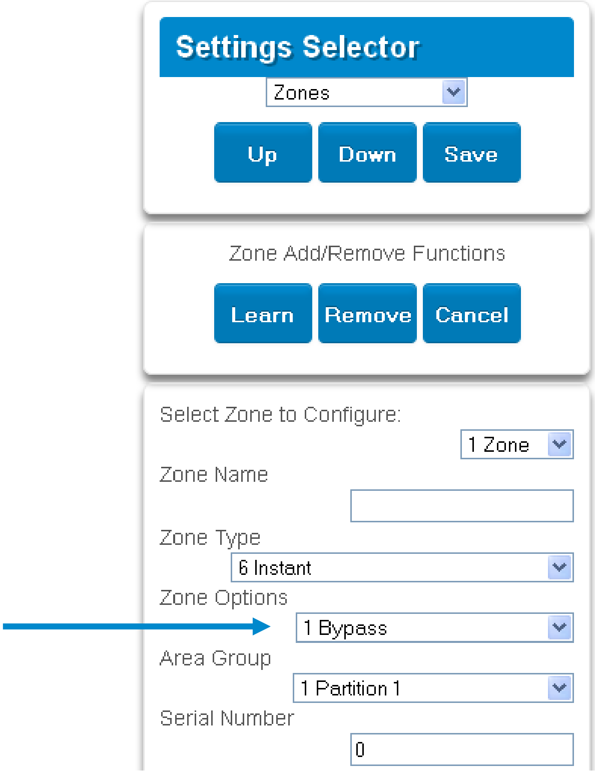
1. Login to the Web Server
2. Press **Advanced\Sensor Options**.
3. Select the Sensor Options you want to change.
4. Press **Sensor Report Event**.
5. Select the desired Contact I.D.\SIA Event Code pair from the drop down menu.



\Zone Options\Zone Options Number: 1 Bypass

Zone Report Event: 134:BA

6. Press **Save**.
7. Press **Settings** and Sensors should appear.
8. Assign the customized Sensor Options to the Sensor.



Select Zone to Configure: 1 Zone

Zone Name

Zone Type: 6 Instant

Zone Options: 1 Bypass

Area Group: 1 Partition 1

Serial Number: 0

9. Press **Save**.

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 sensor number if extended Contact I.D. is enabled in the system options. Otherwise sensor ‘0’ will always be reported. If there are no parentheses, the sensor will be reported as ‘0’.

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

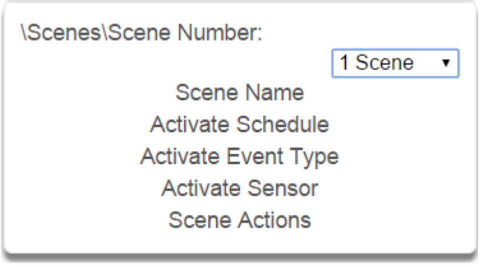
5.18 Advanced Programming, Scenes

Select **Scenes** from the drop down menu.

Scenes Submenus

Scenes Submenus

1 Scene Number (1 – 16)



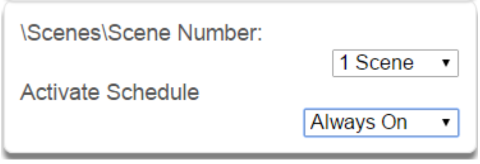
\Scenes\Scene Number: 1 Scene ▾

Scene Name
Activate Schedule
Activate Event Type
Activate Sensor
Scene Actions

The system can support a total of 16 Scenes.

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

3 Activate Schedule

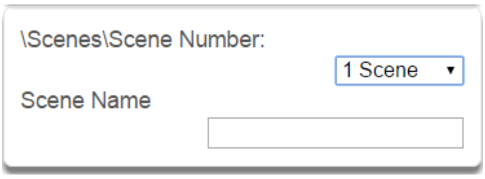


\Scenes\Scene Number: 1 Scene ▾

Activate Schedule: Always On ▾

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.

2 Scene Name

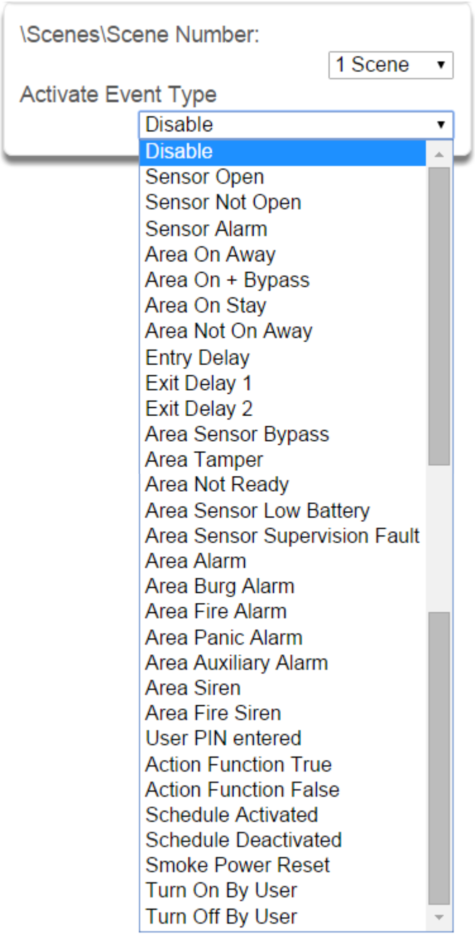


\Scenes\Scene Number: 1 Scene ▾

Scene Name

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

4 Activate Event Type List



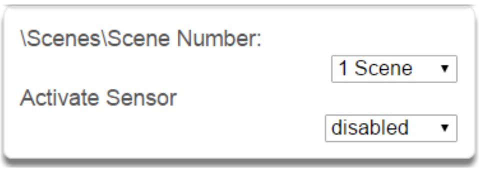
\Scenes\Scene Number: 1 Scene ▾

Activate Event Type: Disable ▾

Disable
Sensor Open
Sensor Not Open
Sensor Alarm
Area On Away
Area On + Bypass
Area On Stay
Area Not On Away
Entry Delay
Exit Delay 1
Exit Delay 2
Area Sensor Bypass
Area Tamper
Area Not Ready
Area Sensor Low Battery
Area Sensor Supervision Fault
Area Alarm
Area Burg Alarm
Area Fire Alarm
Area Panic Alarm
Area Auxiliary Alarm
Area Siren
Area Fire Siren
User PIN entered
Action Function True
Action Function False
Schedule Activated
Schedule Deactivated
Smoke Power Reset
Turn On By User
Turn Off By User

Select the event that will trigger the Scene.

5 Activate Sensor

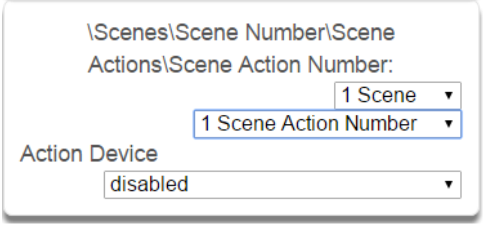


\Scenes\Scene Number: 1 Scene

Activate Sensor: disabled

Select which Area \ Sensor \ Schedule \ User \ Action \ Device will provide the trigger for the Scene.

6 Scene Action Number/Action Device



\Scenes\Scene Number\Scene Actions\Scene Action Number: 1 Scene, 1 Scene Action Number

Action Device: disabled

Each scene can trigger up to 16 scene actions when a certain condition is met. A scene can be triggered manually, through a schedule, or via a system event. These are simplified actions that allow you to control devices on your system. There are two types of Scene Action - Alarm System Action and ZWave Device Action.

1. Alarm System Action

2. Result Type - The event of the Action Result to perform. Reference the Scene Action and Scene Action Events Types table below.

3. Result Number - Select the area / scene / camera number to control.

1. ZWave Device Action
To display ZWave Action Types you must first learn in a ZWave device. The ZWave device name will then appear.

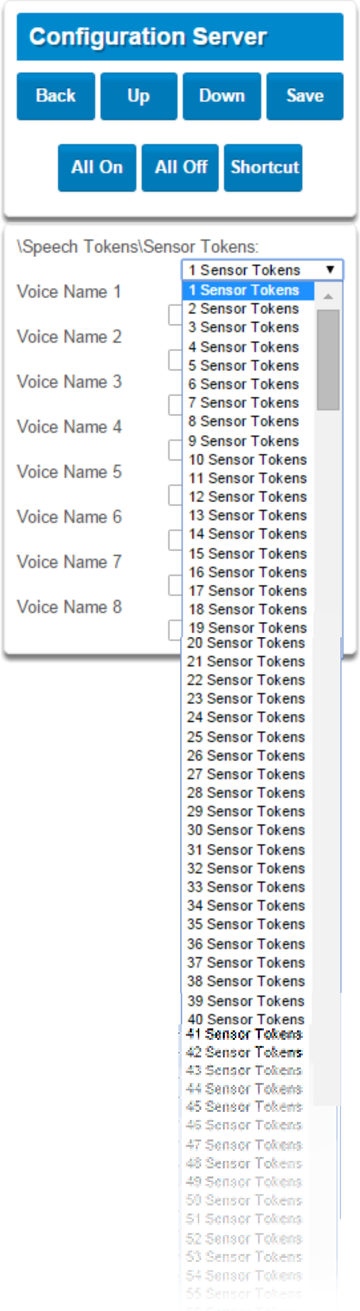
2. Action Device – select the ZWave device you want to control.

3. ZWave Type 8 Setting 1 – depends on ZWave device. May include options such as On, Off, Heat, Cool, Auto, Up, Down, Lock, Unlock.

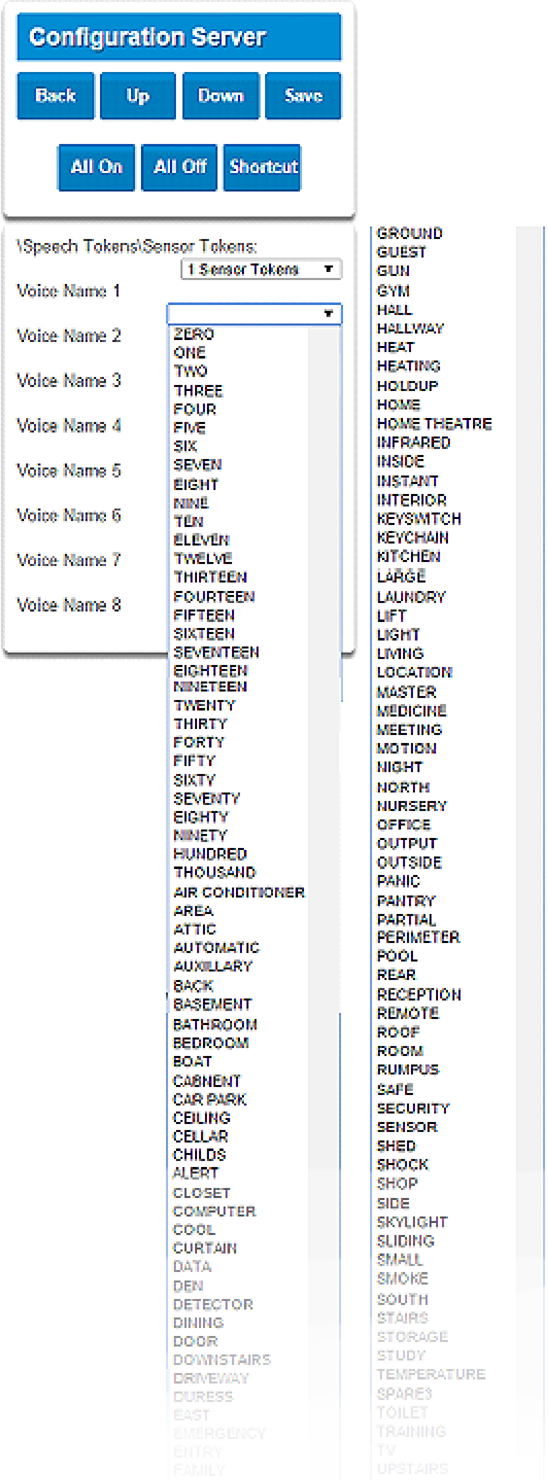
Scene Action	Action Event Type
Alarm System Action	Disabled Sensor Bypass Turn On Away Turn Off Turn On Stay Reset AutoArm Timer Turn On Away, No Auto Stay Chime On Chime Off Activate Scene Trigger Camera Video Clip
ZWave Device Action	The available functions depend on the ZWave device(s) installed. Here are some examples: Disabled On Off Heat Cool Auto Cool Set Point Heat Set Point Lock Unlock

5.19 Advanced Programming, Speech Tokens

Select **Speech Tokens** from the drop down menu, and select a sensor token from the sub menu. Select a **Voice Name** from the drop down menu.



\Speech Tokens\Sensor Tokens: 1 Sensor Tokens

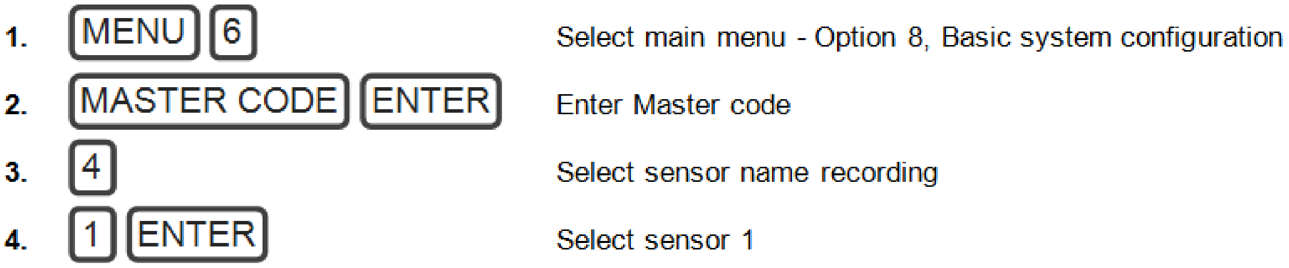


\Speech Tokens\Sensor Tokens: 1 Sensor Tokens

For each sensor, you can select up to eight names from the drop down list of voice names. You may also view the list of sensor names available in the Voice Library.

You may check the results of your speech token programming using the panel.

See section 9.3 Configure Sensor Names. Use the first four steps to listen to the voice names you have selected. The example below illustrates how to listen to the voice name for sensor 1.



1. MENU 6 — Select main menu - Option 8, Basic system configuration
2. MASTER CODE ENTER — Enter Master code
3. 4 — Select sensor name recording
4. 1 ENTER — Select sensor 1

5.20 Advanced Programming, Cameras

Select **Cameras** from the drop down menu.

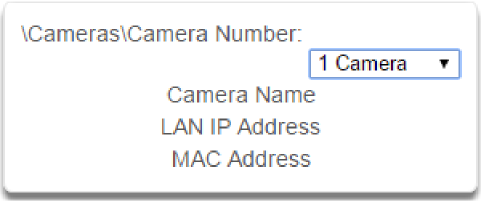
Add a Camera Method 2 – Manual Entry

1. Enter a name for the camera.
2. Enter the IP address and MAC address (Submenu 3,4 below).
3. Press **Save.**
4. Your camera will now be viewable from the Web Server and UltraSync app.

Cameras Submenus

Cameras Submenus

1 Camera Number (1-16)

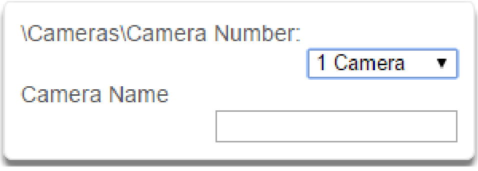


\Cameras\Camera Number: 1 Camera ▼

Camera Name
LAN IP Address
MAC Address

Choose the Camera Number

2 Camera Name

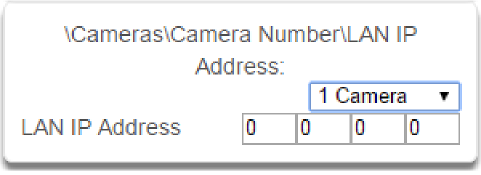


\Cameras\Camera Number: 1 Camera ▼

Camera Name

Assign Camera Number a Name

3 Camera LAN IP Address

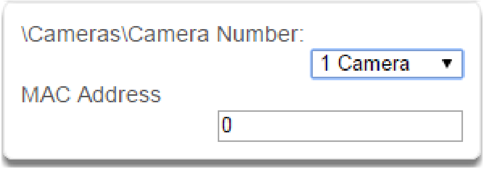


\Cameras\Camera Number\LAN IP Address: 1 Camera ▼

LAN IP Address 0 0 0 0

Assign a Camera a LAN IP address

4 Camera MAC Address



\Cameras\Camera Number: 1 Camera ▼

MAC Address 0

Assign a Camera a MAC address

Removing a Camera

1. Select the camera you wish to remove.
2. Delete the IP address and MAC address (Submenu 3,4 above).
3. Press **Save**.
4. Your camera will no longer be accessible from the system.

5.21 Advanced Programming, Network Servers

Select **Network Servers** from the drop down menu.

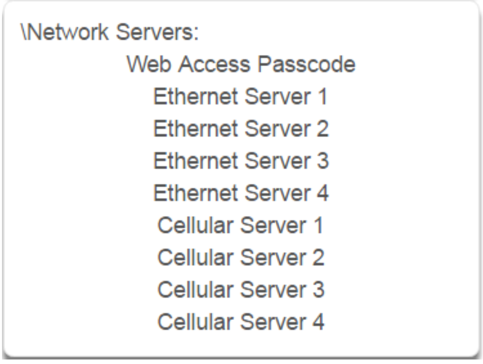
The system can establish a secure VPN connection to Network Servers to allow simplified set up and configuration of email reporting and remote access features.

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

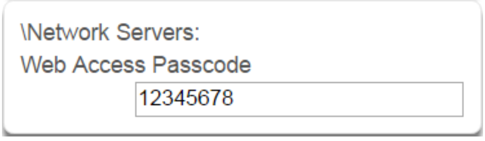
Network Servers Submenus

Network Servers Submenus

1 Passcode and Servers

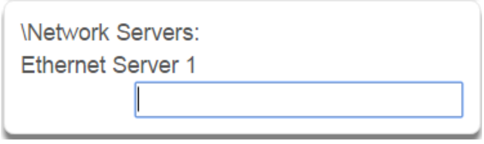


2 Web Access Passcode


\Network Servers:
Web Access Passcode
12345678

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

3 Ethernet Servers (1-4)


\Network Servers:
Ethernet Server 1

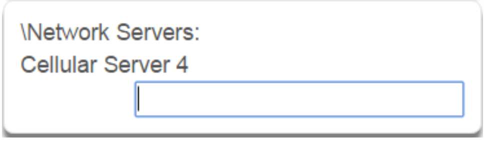
Ethernet Server 1 -

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

Ethernet Servers 2 - 4

The IP address or server names of the backup Ethernet servers.

4 Cellular Servers


\Network Servers:
Cellular Server 4

Cellular Server 1 -

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

Cellular Servers 2 - 4

The IP address or server names of the backup cellular servers.

6 Users and Permissions

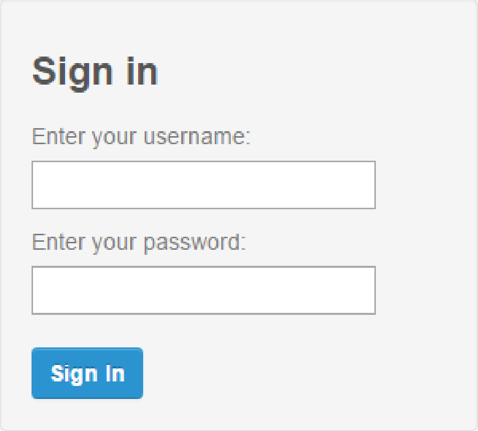
A user is an operator that is granted the authority to control and or configure the system. The Users menu is where you add, delete or modify one of the 40 users. Each user is assigned a PIN code and a user number. This allows them to interact with the system.

Users will typically interact with the system via a keypad or wireless (s) for tasks such as arming and disarming an area, bypassing a sensor. Permissions can be granted to a user to perform tasks such as adding sensors, 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 system will deny access.

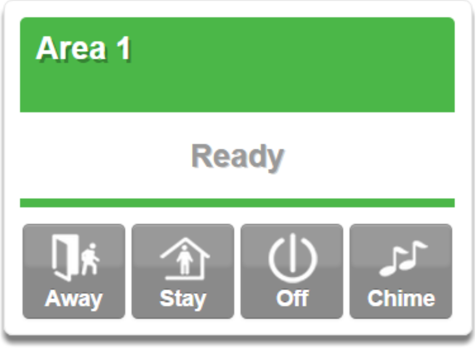
6.1 Add Users

Connect to the Web Server (either via Wi Fi Discovery Mode, Wi Fi, Ethernet LAN, or the UltraSync app). The login screen should appear:

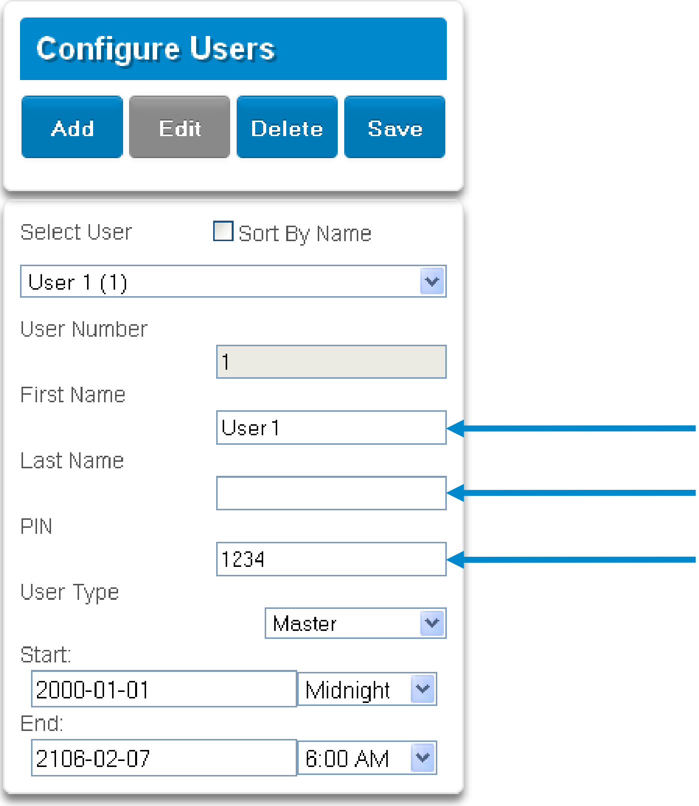


Enter your username and password. A master code is required to add users, by default this is “**User 1”** and “**1-2-3-4**”, then press **Sign In**.

You should see a screen similar to below. Press **Users**.



User Menu:



Select User □ Sort By Name

User 1 (1)

User Number: 1

First Name: User 1

Last Name:

PIN: 1234

User Type: Master

Start: 2000-01-01 Midnight

End: 2106-02-07 6:00 AM

Enter a First and/or Last Name.

Enter a unique PIN code between 4 and 8 digits.

Select a User Type:

- **Standard users** can arm and disarm areas; they cannot create users or review event history.
- **Master users** can arm and disarm areas. They can create, delete, or modify user codes. They can also change system settings.
- **Arm Only users** can only turn on the security system; they cannot disarm, or dismiss any system conditions.
- **Duress users** will send a duress event when they are used to arm or disarm the system.
- **Custom users** can have additional permissions and settings configured.

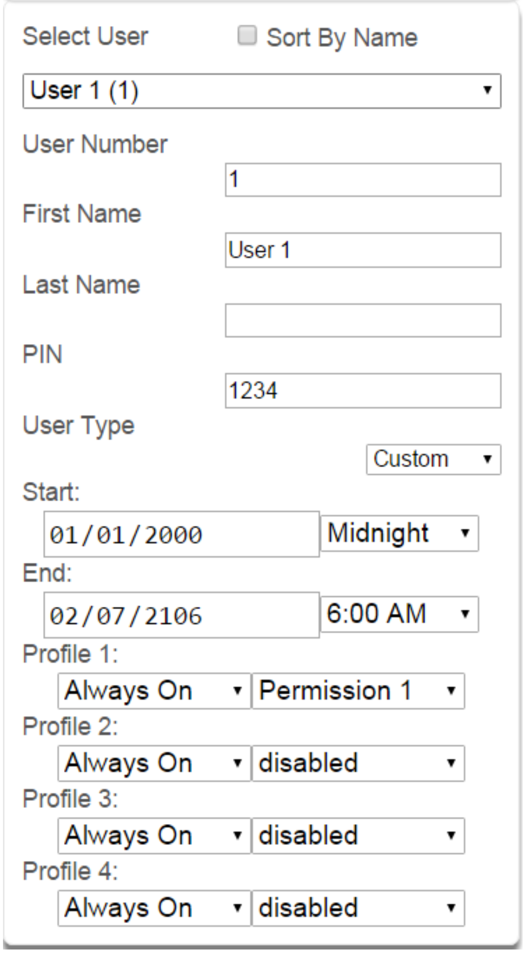
Press **Save**.

6.2 Users Submenus

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

User Submenus

User Submenus



Select User □ Sort By Name

User 1 (1) ▾

User Number: 1

First Name: User 1

Last Name:

PIN: 1234

User Type: Custom ▾

Start: 01/01/2000 Midnight ▾

End: 02/07/2106 6:00 AM ▾

Profile 1: Always On ▾ Permission 1 ▾

Profile 2: Always On ▾ disabled ▾

Profile 3: Always On ▾ disabled ▾

Profile 4: Always On ▾ disabled ▾

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 system 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 system via the management software.

User Number

The system will store a number of users relative to the model type and the amount of memory installed. Unlike other systems, user numbers are not predefined and can be configured from user number 1 to 1000 as long as user numbers are not duplicated and do not exceed the total number of users that can fit the allocated memory.

User PIN

Users can be configured with 4 to 8 digit PIN. The user PIN is required by the 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.

User Submenus

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 to which they have access.

Master – Master users can change Standard user PIN codes and Master user PIN codes, and can access all menus except installation programming.

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 – The hub will apply user permissions and user permission schedules. This requires advanced programming. 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.

6.3 Permissions

There are a total 128 unique permissions that can be configured in the Permissions menu. Once configured any permission number from 1 to 16 can be allocated in this feature (user permissions 1).

User permissions determine what level of access and functionality a user has when interacting with the 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.

Combining a user permission with a user permission schedule will determine when that user has that level of access and functionality. The system 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.

When any user permission is active, it overrides any user type. This means a permission can increase or decrease access when it is active. If a user is not assigned any permissions (i.e. permission set to "Disabled"), then the User Type setting is used to determine what the user can do.

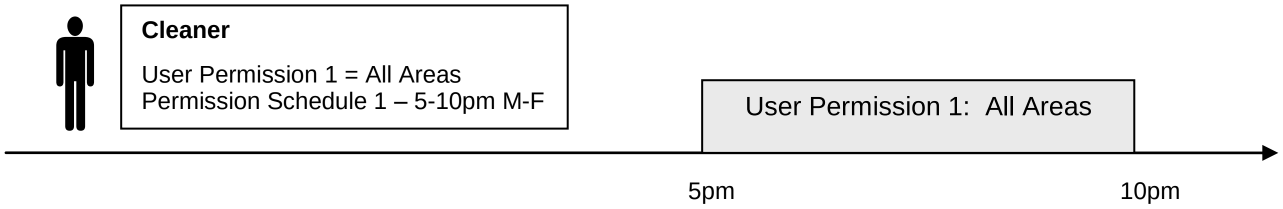
Permission Schedule 1

Permission schedules determine when to allocate user permissions to a user.

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.

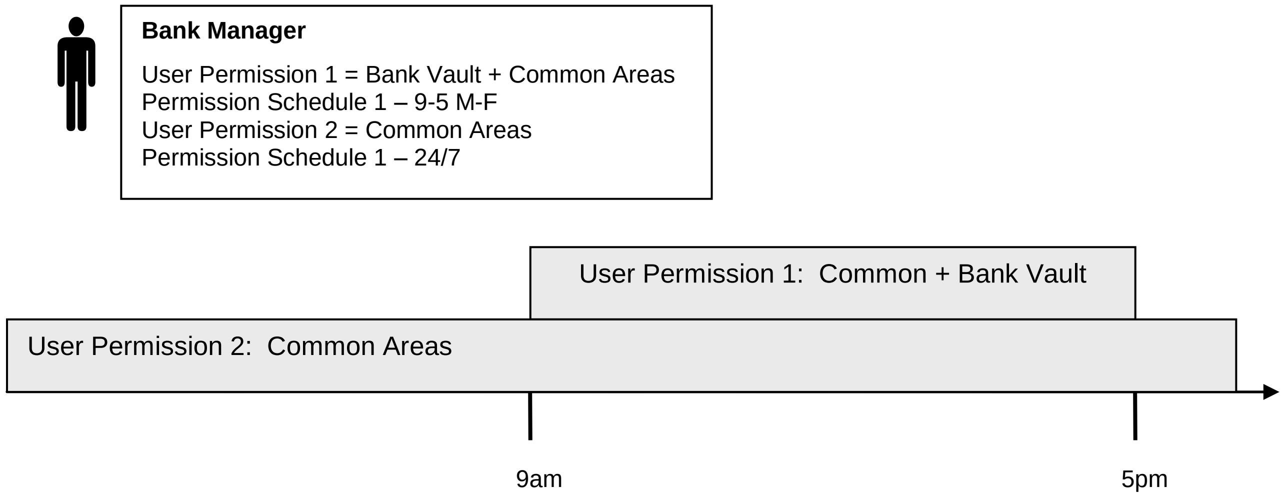
IMPORTANT: If permission 1 is active due to a valid schedule, permission 2 will never become active. Make sure to assign/program permissions in the right order.



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.



Bank Manager

User Permission 1 = Bank Vault + Common Areas
Permission Schedule 1 – 9-5 M-F
User Permission 2 = Common Areas
Permission Schedule 1 – 24/7

User Permission 1: Common + Bank Vault
User Permission 2: Common Areas
9am
5pm

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 become active again.

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.

	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 installation settings				X	X	**Custom**
Can create and modify Engineer users					X	

Area Group

When a non-Custom User Type is selected, this setting determines what areas that user has access to.

When a Custom User Type is selected, permissions will be used instead of this Area Group setting.

Start Date

The first date when this 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

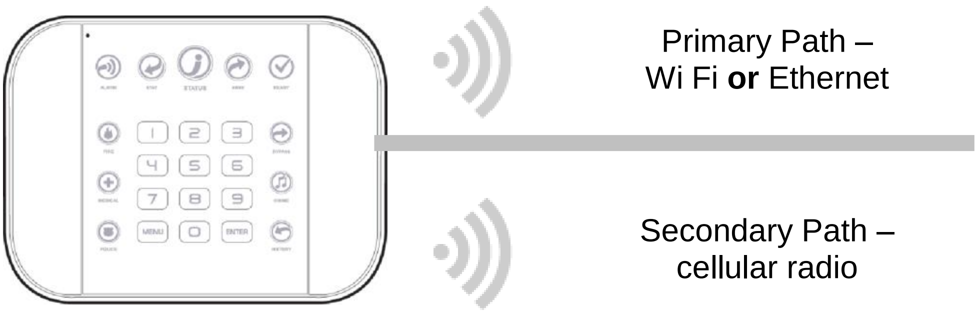
The last date when this user can interact with the system. Future end dates can also be set here. The user will only be able to interact with the system between the start date and end date.

Language

The hub Supports Selectable Languages
English (US)
French (CA)
Spanish (MX)

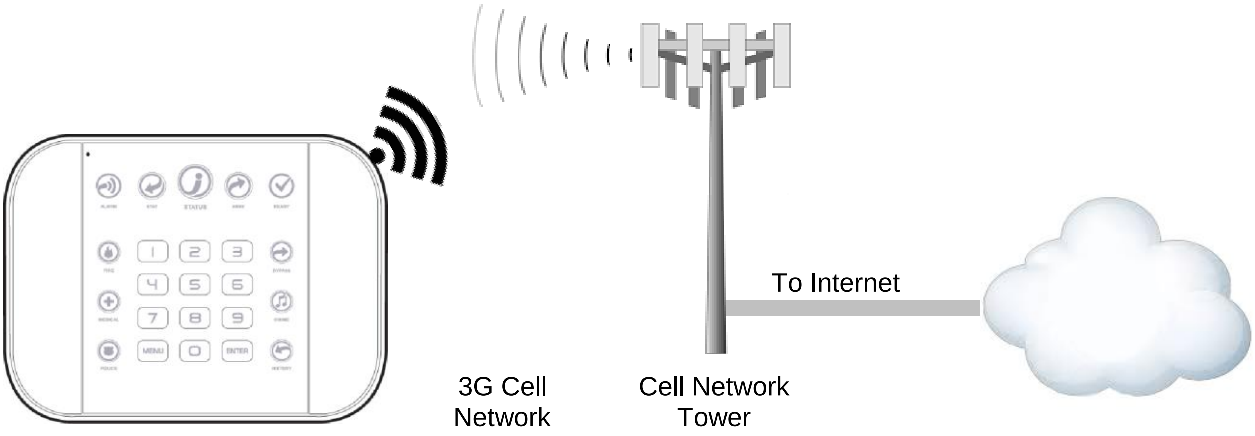
7 Cellular Radio Setup

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



This provides a plug and play connection to UltraSync servers for secure reporting with no configuration needed in most cases. The only requirement is good mobile device reception. To connect via Cellular Radio you only need to plug in the cellular radio module.

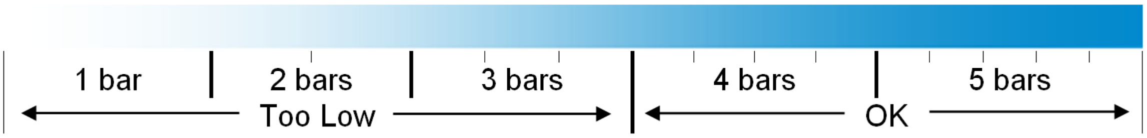
Your cellular radio module should be pre-configured and function once plugged in to the hub. If not, please refer the manual that comes with the cellular radio for instructions on how to install it.



7.1 Install Optional Cellular Radio

A mobile device can provide general guidance on mobile network coverage.

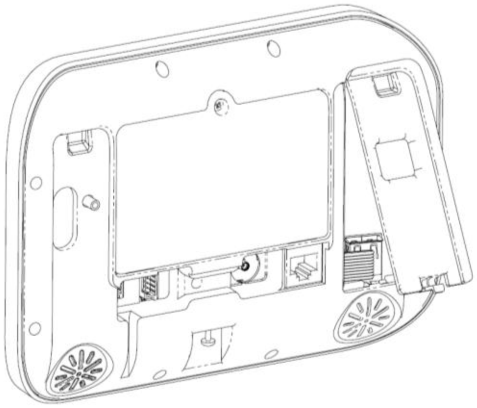
Look at the signal strength on a mobile device to verify there are 4/5 to 5/5 bars of reception in the location where you will install the hub.



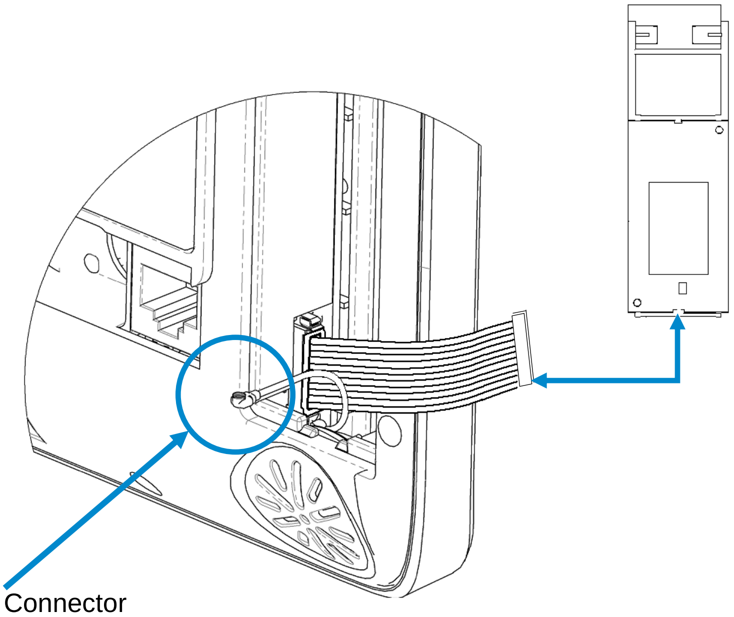
If the signal strength is low, find another location which has stronger signal strength.

Note: Actual signal strength can only be determined using the hub which will connect to a specific network which may be different than your device.

To install, remove the cover on the right.

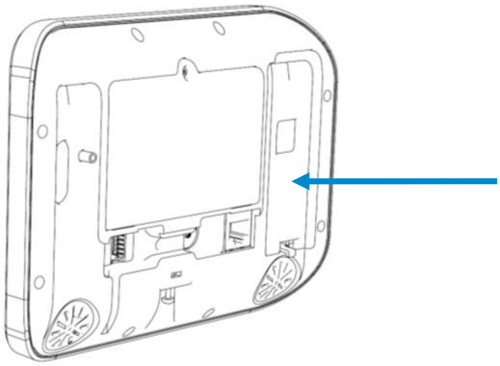


Locate the 10-pin lead inside the hub and connect this to the radio module.



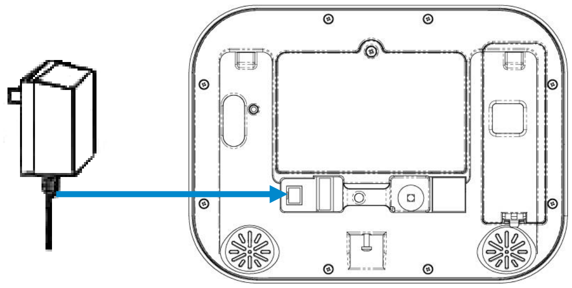
External Antenna Connector
Use ONLY with external antenna

Insert the whole radio module in to the hub taking care not to crimp any cables.
Replace the cover.



7.2 Connect Power

Connect power lead from power supply to the back of the hub. The connector is keyed and fits only one way.



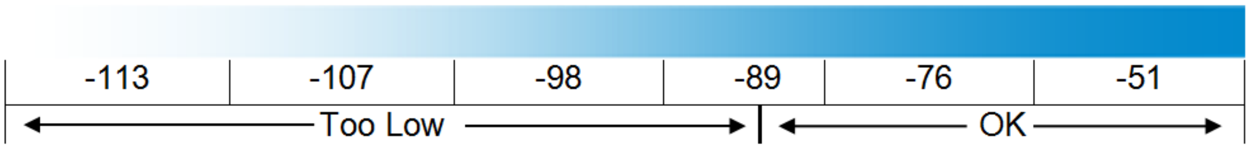
Connect the power supply to receptacle.

Warning: Do not connect to a receptacle controlled by a switch

7.3 Check Signal Strength

On the hub’s key pad:

1.	MENU 4	Select Main Menu - Option 4, System Test
2.	MASTER CODE ENTER	Enter Master Code
3.	5	Check cellular signal strength
4.	MENU MENU	Exits from Advanced system configuration menu

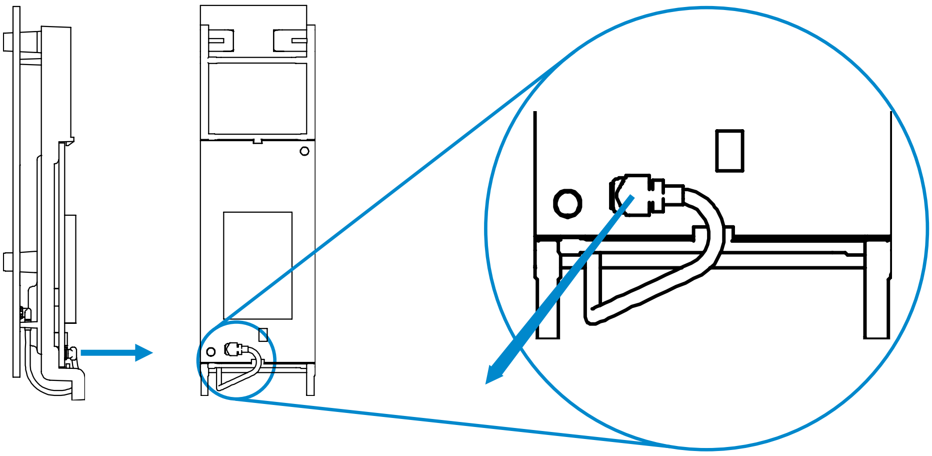


- If the reported value is -113 to -89 then installing an external antenna is recommended.
- If the reported value is -89 to -51 then the signal strength is OK.

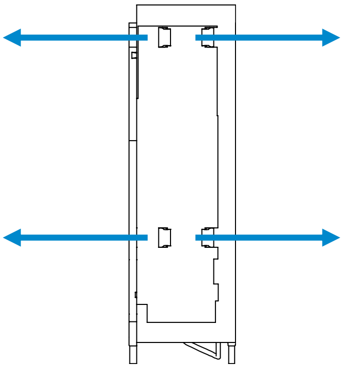
7.4 Install External Antenna – Optional

Complete this section only if signal strength is between -121 to -89.

Unplug power supply from receptacle and remove battery from hub.
Disconnect the antenna cable from the radio module.

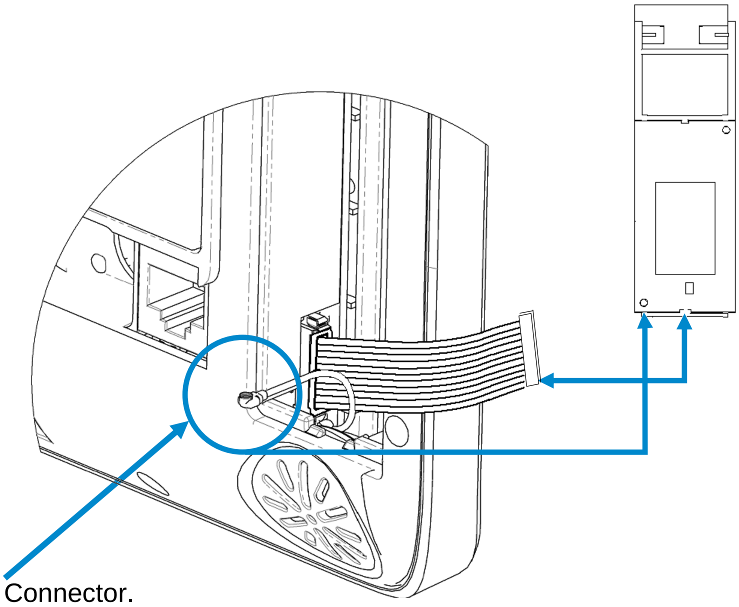


Gently pull retaining clips outwards and remove the rear circuit board. This is the internal antenna which will no longer be needed.



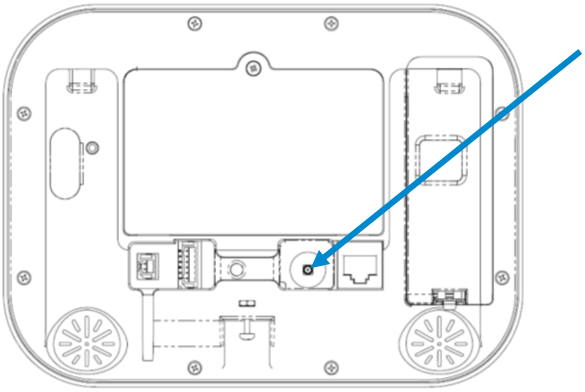
Back View

Connect the internal antenna cable from the hub to the radio module.



External Antenna Connector.
Use ONLY with external antenna

Connect an external antenna to the antenna connector on the rear of the hub. To obtain maximum signal strength the external antenna must be fully extended. Re-check signal strength following steps in section 7.3.



Move the hub or the antenna to another location if the signal is still too low.
Place the external antenna to optimize signal strength.

Note: The external antenna can be used wherever the panel is installed. The antenna can be mounted in a wall for that kind of installation, or extended from the panel in a table mount installation.

7.5 Check Cellular Connection to UltraSync

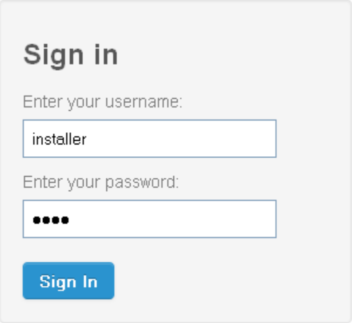
Turn on **Wi Fi Discovery Mode** – this provides direct access to the hub from a mobile device such as a smart phone, tablet, or laptop:

1.	MENU 9	Select main menu - Option 9, Advanced system configuration
2.	INSTALLER CODE ENTER	Enter Installer code
3.	8	Turn on WiFi Discovery Mode for 10 min
4.	MENU MENU	Exits from Advanced system configuration menu

Enable Wi Fi on your mobile device

On your mobile device, browse for available Wi Fi networks and select the **ZeroWire_xxxx** network to connect to it. Only a single user can connect at any time and there is no Wi Fi password. Once connected the hub will be assigned a fixed IP address of 192.168.1.3.

Open your web browser and enter **192.168.1.3**. The login screen should appear:



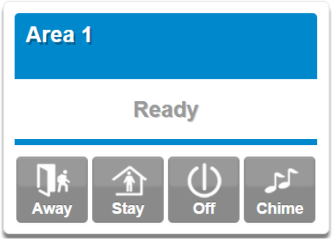
Sign in

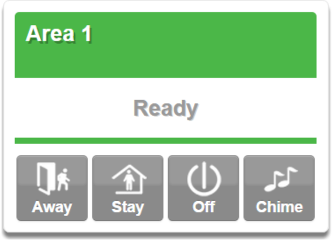
Enter your username: installer

Enter your password: ••••

Enter your username and password. By default this is **installer** and **9-7-1-3**.

Press **Sign In**. you should now see a screen similar to one of the below:





Press **Settings**.

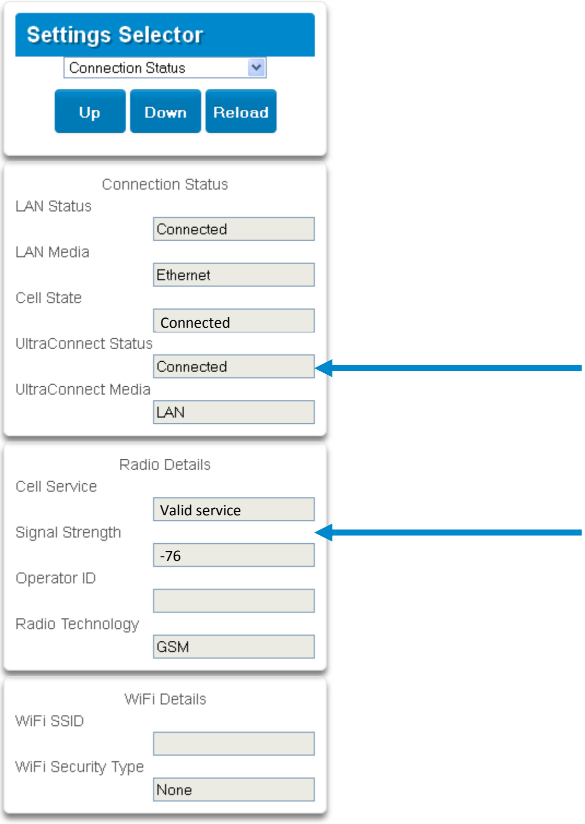
Press **Connection Status** in the drop down menu.

Check that

a. UltraSync Status should display **Connected**.

b. Cell Service should display **Valid service**.

c. Signal Strength should display a value between -**89 to** -**51**.



Connection Status

Connection Status

LAN Status: Connected

LAN Media: Ethernet

Cell State: Connected

UltraConnect Status: Connected

UltraConnect Media: LAN

Radio Details

Cell Service: Valid service

Signal Strength: -76

Operator ID:

Radio Technology: GSM

WiFi Details

WiFi SSID:

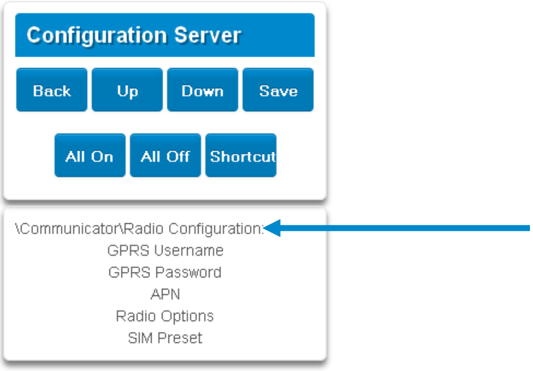
WiFi Security Type: None

If it does not:

Check cellular connection:

a. Look at cell state, it should display **Connected**.
b. Wait until cell state displays **Connected**, press **Reload** to refresh the status.
c. Check signal strength – signal strength should be between -91 to -51.
d. Contact Tech Support for assistance.
e. Check that radio is correctly installed and firmly connected to the 10 pin cable.
f. Check if antenna is correctly installed or move antenna to a higher location.

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



\Communicator\Radio Configuration:

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

8 Camera Setup Instructions

8.1 Quick Setup

Note: If the light source where the camera is installed experiences rapid, wide variations in lighting, the camera may not operate as intended.

To quickly put the camera into operation:

1. Prepare the mounting surface.
2 Mount the camera using the appropriate fasteners.
3. Connect the camera to the local network via Ethernet cable or Wi Fi.
4. Learn the camera into the UltraSync App using the “Scan for New Cameras” button in Section 4.14 Camera Configuration

8.2 Setting up Ethernet/Wi Fi transmission

Wi Fi transmission distance

The Wi Fi transmission distance/range of the camera is approximately 50 m (164 ft.) in open air applications.

Note: The transmission distance may vary due to the presence of physical obstacles, such as trees, walls, elevators, fire doors, furniture, etc. Avoid very solid walls and metallic objects in the transmission path. Other Wi Fi networks (for example Wi Fi, WiMAX) operating on 2.4 GHz and certain types of devices (e.g., microwave oven point-to-point Wi Fi transmission) can cause interference with your network. The result would lead to a reduction in transmission distance/range.

Devices Supported For Ad Hoc Installation
Apple iOS, PC – Windows XP, 7, 8

Devices NOT Supported For Ad Hoc Installation
Android, Windows Mobile, Blackberry

8.3 Wi Fi Signal Strength

Wi Fi signal strength can be checked in the Network section of the TruVision Browser. Use the scale below to measure if actions are needed to improve performance.

>65	65-75	75-85	85+
Poor	Good	Very Good	Excellent

85+ – Excellent:

No additional actions needed and default video resolutions settings may be increased if desired.

75-85 – Very Good:

No additional actions needed to increase signal strength. It is not recommended to increase video resolution settings.

65-75 – Good:

It is recommended to use a Wi Fi repeater or Powerline adapter to increase signal strength. Alternatively, video resolutions settings may be reduced to minimize poor video quality.

Below 65 – Poor:

It is not recommended to use the camera with a signal strength below 65. Video streams will likely not work below this level. A Wi Fi repeater or Powerline adapter should be used to increase signal strength.

8.4 Add Camera via Wi Fi for iOS Device

1. Power up the camera. (Boot up may take 1-2 minutes)
2. From your iOS device, go to **Settings**, then **Wi Fi**.
3. Find and select TVW-xxxxx. (Listed under Devices)
4. Once connected, press the info circle on the right of TVW-xxxxx.
5. Under IP Address, press **Static** and enter the info below.
   a) IP Address **192.168.1.71**
   b) Subnet Mask **255.255.255.0**
6. Open Mobile Browser. (Safari)
7. Enter the camera's default IP Address into the address bar.
   a) **192.168.1.70**
8. TruVision Configurator will appear. Enter Credentials below.
   a) User Name: **admin**
   b) Password: **1234**
9. Press **Configuration** on the top menu.
10. Press **Network** on the left menu.
11. Press **Wi Fi** on the middle tab.
12. Select your network from the Wireless List.
13. Enter Wi Fi Network Passphrase in **Key 1** Section**.**
14. Press **Save** on the bottom of the screen.

You are now connected to the network via Wi Fi!

8.5 Add Camera via Wi Fi for Windows PC

1. Power up the camera. (Boot up may take 1-2 minutes)
2. From your Windows PC, Find and connect to T**VW-xxxxx** in Wi Fi network list.
3. Go to **Network and Sharing Center**.
   Control Panel > Network and Internet > Network and Sharing Center
4. Press Change Adapter Settings on left.
5. Right click **Wireless Network Connection** and select **Properties.**
6. Click Internet Protocol Version 4 (TCP/IPv4) and click Properties.
7. Click "Use the following IP address", enter the info below, and then click OK.
   a) IP address: **192.168.1.71**
   b) Subnet mask: **255.255.255.0**
8. Open Browser (Firefox, Chrome, IE8) and enter the camera's IP Address into the browser's address bar.
   a) Camera's Default IP Address is **192.168.1.70.**
9. TruVision Configurator will appear. Enter Credentials below.
   a) User Name: **admin**
   b) Password: **1234**
10. Click **Configuration** on the top menu.
11. Click **Network** on the left menu.
12. Click **Wi Fi** on the middle tab.
13. Select your network from the **Wireless List**.
14. Enter Wi Fi Network Passphrase in **Key 1** Section.
15. Click **Save** on the bottom of the screen.

You are now connected to the network via Wi Fi!

8.6 Add Camera via Ethernet for iOS Device (non DHCP)

1. Power up the camera. (Boot up may take 1-2 minutes)
2. From your iOS device, go to **Settings**, then **Wi Fi**.
3. Find and select TVW-xxxxx. (Listed under Devices)
4. Once connected, press the info circle on the right of TVW-xxxxx.
5. Under IP Address, press **Static** and enter the info below.
    a) IP Address **192.168.1.71**
    b) Subnet Mask **255.255.255.0**
6. Open Mobile Browser. (Safari)
7. Enter the camera's default IP Address into the address bar.
    a) **192.168.1.70**
8. TruVision Configurator will appear. Enter Credentials below.
    a) User Name: **admin**
    b) Password: **1234**
9. Press **Configuration** on the top menu.
10. Press **Network** on the left menu.
11. Change LAN settings to desired configuration.
    a) Change the **IPv4 Address** and **IPv4 Subnet Mask** to match the router if a static IP Address is desired.
        i. You must change the static IP address to something different than the default 192.168.1.70 if more than one camera is used on the network.
        ii. Make sure to use the Test button to validate IP Address is not already assigned to another device in the network.
12. Press **Save** on the bottom of the screen.

You are now connected to the network via Ethernet!

8.7 Add Camera via Ethernet for Windows PC (non DHCP)

1. Power up the camera. (Boot up may take 1-2 minutes)
2. From your Windows PC, Find and connect to T**VW-xxxxx** in Wi Fi network list.
3. Go to **Network and Sharing Center**.
   Control Panel > Network and Internet > Network and Sharing Center
4. Click Change Adapter Settings on left.
5. Right click **Wireless Network Connection** and select **Properties.**
6. Click Internet Protocol Version 4 (TCP/IPv4) and click Properties.
7. Click "Use the following IP address", enter the info below, and then click OK.
   a) IP address: 192.168.1.71
   b) Subnet mask: 255.255.255.0
8. Open Browser (Firefox, Chrome, IE8) and enter the camera's IP Address into the browser's address bar.
   a) Camera's Default IP Address is **192.168.1.70.**
9. TruVision Configurator will appear. Enter Credentials below.
   a) User Name: **admin**
   b) Password: **1234**
10. Click **Configuration** on the top menu.
11. Click **Network** on the left menu.
12. Change LAN settings to desired configuration.
    a) Change the **IPv4 Address** and **IPv4 Subnet Mask** to match the router if a static IP Address is desired.
       i. You must change the static IP address to something different than the default 192.168.1.70 if more than one camera is used on the network.
       ii. Make sure to use the Test button to validate IP Address is not already assigned to another device in the network.
13. Click **Save** on the bottom of the screen.

You are now connected to the network via Wi Fi!

8.8 Add Camera via Ethernet (DHCP)

1. Power up the camera. (Boot up may take 1-2 minutes)
2. Connect router and camera with Ethernet cable.

You are now connected to the network via Ethernet!

8.9 Add Camera to UltraSync

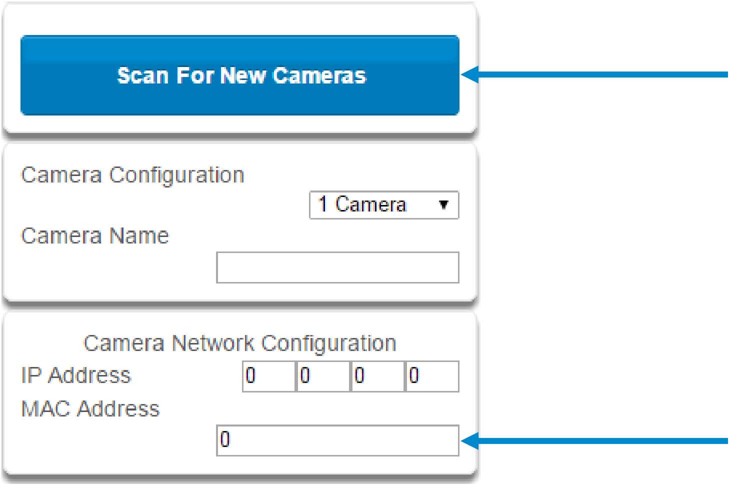
Ensure proper installation of camera hardware before proceeding to camera setup.
Make sure camera and UltraSecure intrusion panel are on the same local area network.
Applications were the Intrusion panels uses cellular only are not compatible with this camera.

Note: For detailed information on how to setup the UltraSync app, add locations, and login as an Installer, reference the intrusion panel installation guide.

Press ••• More then ⚙ Settings for the **Settings Selector** page.

Select **Cameras** from the drop down menu.

Press **Scan for New Cameras**. "Success!" message will pop-up after a few moments.
The scan results in an IP address and MAC address listing in the form fields shown.



Scan For New Cameras

Camera Configuration: 1 Camera ▾

Camera Name:

Camera Network Configuration

IP Address: 0 . 0 . 0 . 0

MAC Address: 0

Make sure the MAC ID that is automatically populated in the **MAC Address** field matches the MAC Address printed on the back of the camera. If not, change in the MAC Address to the one listed on the back of the Camera.

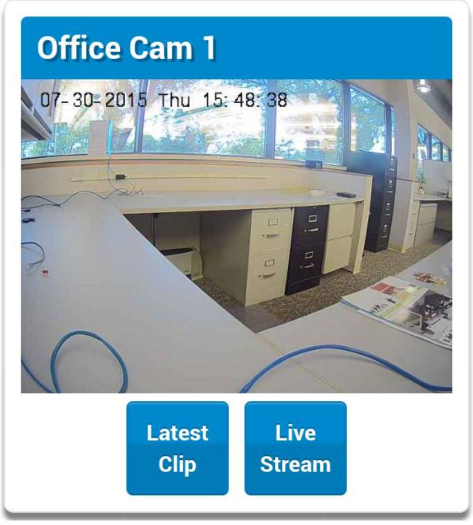
Press **Save**.

Note: Camera may take up to 1-2 minutes to finalize association with intrusion panel and show in cameras tab.

CONGRATULATIONS! You have now added the camera to UltraSync!

8.10 View Live Stream and Latest Clip

Press Cameras tab on bottom of the screen. All available cameras will be shown.



Press Latest Clip to view a live feed of a specific camera.

Press Live Stream to view the last recorded clip from a specific camera.

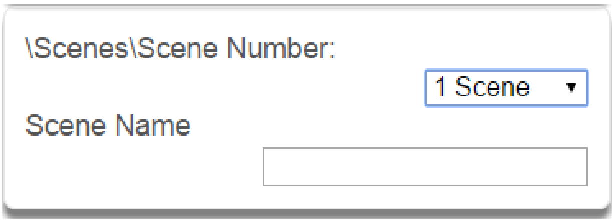
8.11 Program event triggered camera clips

Cameras can be programmed to automatically record when selected events occur. This is achieved by creating a scene.

Press ••• More then Settings for the **Settings Selector** page.

Select **Scenes** from the drop down menu.

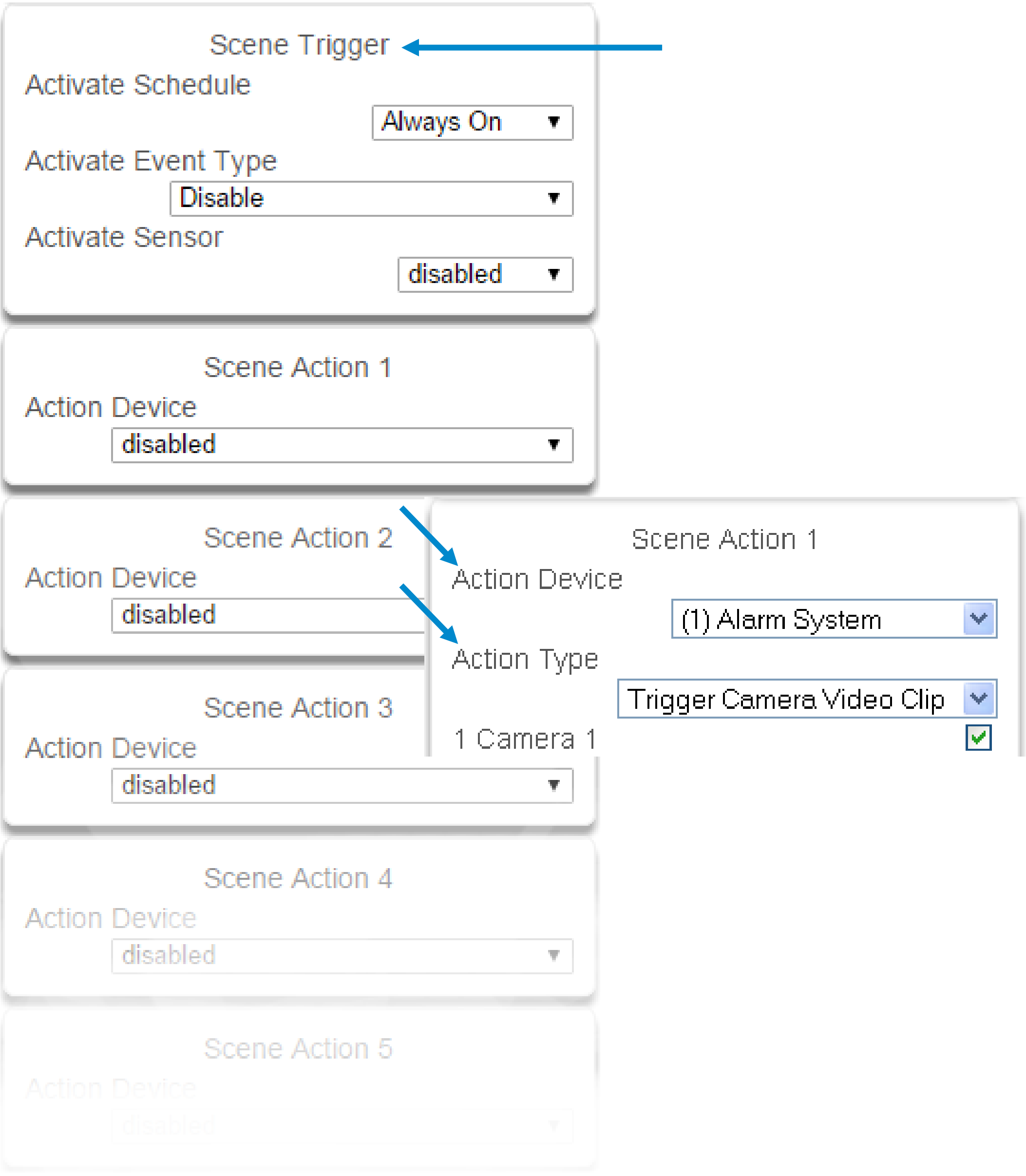
Select the **Scene to Configure** and type **Scene Name**.



\Scenes\Scene Number: 1 Scene ▾

Scene Name

Select the **Scene Trigger**.



Scene Trigger

Activate Schedule: Always On

Activate Event Type: Disable

Activate Sensor: disabled

Scene Action 1

Action Device: disabled

Scene Action 2

Action Device: disabled

Scene Action 3

Action Device: disabled

Scene Action 4

Action Device: disabled

Scene Action 5

Action Device: disabled

Scene Action 1

Action Device: (1) Alarm System

Action Type: Trigger Camera Video Clip

1 Camera 1 ☑

Select **Action Device (1) Alarm System**. This enables another drop down menu for Action Type. Choose the Action Type “Trigger Camera Video Clip”, then the cameras you wish to record a video clip when the event is triggered.

Press **Save**.

Clips are recorded on the Micro SD card installed in the camera and are linked to events in History.

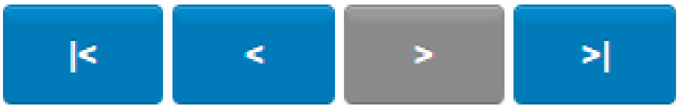
See the following page to see how to view event triggered clips.

8.12 View event triggered clips in History

Press on bottom of the screen.

Press

Find the Event you wish to view using **Oldest, Prev, Next,** *and* **Latest** buttons.



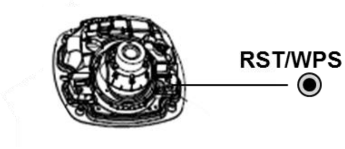
Once you find the clip you wish to view, press **Play Video Clip*.***

Remove Camera from UltraSync (if needed)

1. Press the **More** tab on the bottom of the Screen.
2. Press **Settings**.
3. Select **Cameras** under Settings Selector.
4. Select the camera you with to remove.
5. Delete text in Camera **Name, IP Address** and **MAC Address**.
6. Press **Save**.

Remove All Cameras Shortcut: To remove all cameras from UltraSync, go to Advanced Settings and use **SHORTCUT 910.22**.

Reset Camera to Factory Default (if needed)
If needed, the camera can be reset to factory default. Remove the camera cover, then press and hold the RST/WPS button for 20 Seconds.



8.13 Change Default Camera Settings (Via TruVision Navigator)

1. From a computer or mobile device that is connected on the same network as the camera, type in the IP address of the camera into the devices browser.
2. Login using default login.
   a. Login: admin
   b. Password: 1234
3. Change settings as desired such as video quality, frame rate, pre and post recording times.
4. For detailed instructions on using TruVision Navigator, go to *www.interlogix.com/video.*

8.14 Camera Troubleshooting

1. Camera is not showing in list of Wi Fi networks.	
Cause	Solution
The camera takes up to 90 seconds to boot up.	*It will not show in Wi Fi Networks until this is complete.*
The camera has previously been setup and ad hoc mode was turned off.	*Perform a factory reset to broadcast the camera again.*
Certain mobile devices do not support ad hoc mode. iOS and Windows devices are known to support ad hoc, Android and Windows Mobile devices typically do not support ad hoc mode.	*If your device does not support ad hoc mode, install the camera using a Windows PC.*

2. The camera does not add to the UltraSync network when I perform the "Scan for Cameras" Function	
Cause	Solution
Older firmware versions do not support cameras.	*Make sure your panel is updated to the XXXXXX-04 Firmware or new.*
The camera will not work if the devices are not on the same network.	*Make sure your camera and panel are on the same network.*
The hub must be using IP to work with the cameras.	*Make sure your panel is not installed using a cellular radio only.*
Make sure you are not adding cameras on a network that already has a high number of cameras installed on the same network. This is unusual, but may be common in testing environments.	*Put the hub and the cameras on their own router and this should solve the problem.*

3. The camera was added in the setup process, but the video doesn't show in the Cameras tab.	
Cause	Solution
After completing the setup process, the camera may take up to 2 minutes to full sync and show in the UltraSync App.	*Wait for the process to complete*
	Make sure your camera is still connected to the network.
	If video still doesn't show, go back into setup and perform the "Scan for Cameras" function again.

4. Live Video isn't giving good quality. It is choppy, shows gray, etc.	
Cause	Solution
Check to make sure your camera's Wi Fi and/or Ethernet connection speeds are not poor.	*If Wi Fi connection speeds are poor. It is recommended to use a Wi Fi repeater to increase signal strength.*
The cameras default settings are setup to work on a strong home network.	*In some cases, low video settings may be required to achieve a smooth video. Use the TruVision Browser to change the cameras video settings.*

5. Video Clips take a long time to load.	
Cause	Solution
The cameras default settings are setup to have video clips start playing in the UltraSync App within 15 seconds (On a strong network). If default settings were changed to longer clip times or higher video quality, the amount of time needed to pull the clip will be higher.	*Lower the quality or length of clips to shorten load times.*

9 Installation Using Keypad

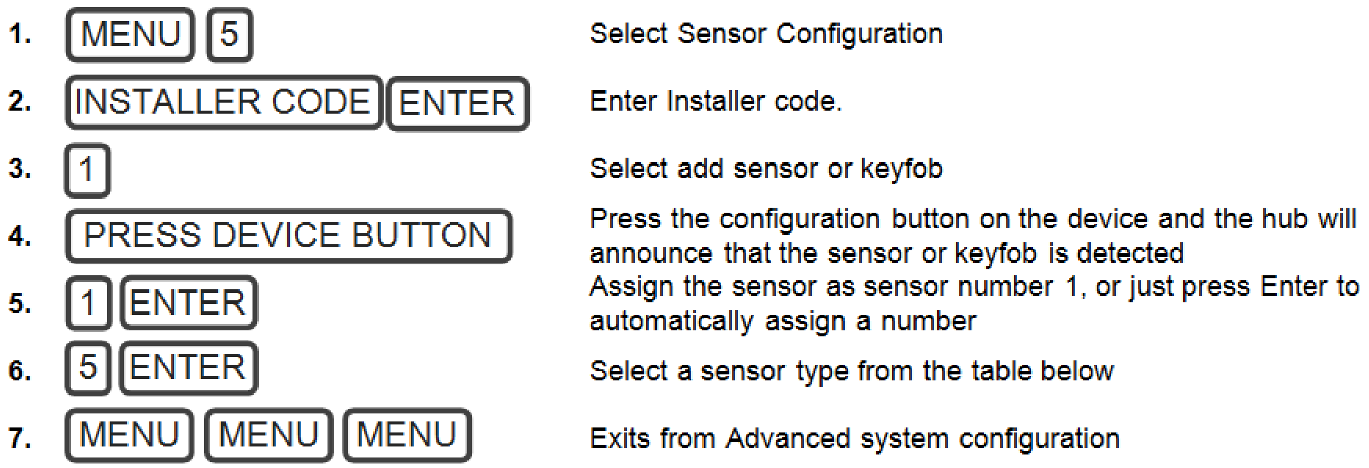
9.1 Basic Installation

It is possible to quickly install and test sensors using only the hub’s keypad, the voice guide will walk you through each option that requires programming.

Additional sensor settings can be accessed via the Web Server, UltraSync app, or DLX900.

9.2 Learning Sensors into the System

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



1.	MENU 5	Select Sensor Configuration
2.	INSTALLER CODE ENTER	Enter Installer code.
3.	1	Select add sensor or keyfob
4.	PRESS DEVICE BUTTON	Press the configuration button on the device and the hub will announce that the sensor or keyfob is detected
5.	1 ENTER	Assign the sensor as sensor number 1, or just press Enter to automatically assign a number
6.	5 ENTER	Select a sensor type from the table below
7.	MENU MENU MENU	Exits from Advanced system configuration

Sensor Types Presets

The sensor type can be changed using the keypad to one of the following presets. If you require further customization please use the Web Server, UltraSync app, or DLX900 to access more advanced settings.

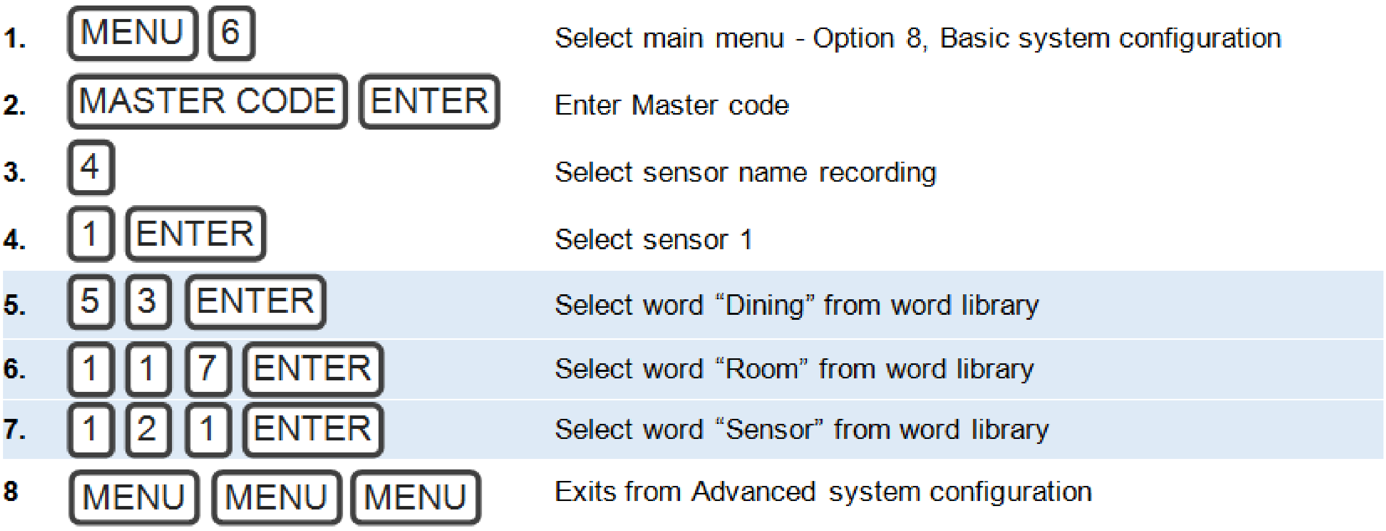
Option	Voice	Sensor Type	Sensor Options
1	Delay Sensor Type	3 Entry Exit Delay 1	1 Bypass
2	Delay Sensor Type with Bypass in Stay Mode	5 Follower	2 Bypass Stay
3	No Delay Sensor Type	6 Instant	1 Bypass
4	No Delay Sensor Type with Bypass in Stay Mode	6 Instant	2 Bypass Stay
5	24 Hour Sensor Type	2 24 Hour Audible	6 Panic
6	24 Hour Silent Sensor Type	7 24 Hour Silent	7 Silent Panic
Smoke Sensors	Smoke Sensor	8 Fire Alarm	5 Fire

9.3 Configure Sensor Names (optional)

All sensors can be named; see the Voice Library table for reference.

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 6	Select main menu - Option 8, Basic system configuration
2.	MASTER CODE ENTER	Enter Master code
3.	4	Select sensor name recording
4.	1 ENTER	Select sensor 1
5.	5 3 ENTER	Select word “Dining” from word library
6.	1 1 7 ENTER	Select word “Room” from word library
7.	1 2 1 ENTER	Select word “Sensor” from word library
8	MENU MENU MENU	Exits from Advanced system configuration

If you require less than eight words, press **MENU** (as in step 6) after you have entered the last word number.

The voice library can be set up to use English, Spanish or French.

Voice Library, English

These words can be used to customize your sensor names.

0	zero	**46**	closet	**92**	kitchen	**138**	training
1	one	**47**	computer	**93**	lounge	**139**	T V
2	two	**48**	cool	**94**	laundry	**140**	upstairs
3	three	**49**	curtain	**95**	lift	**141**	user
4	four	**50**	data	**96**	light	**142**	utility
5	five	**51**	den	**97**	living	**143**	volt
6	six	**52**	detector	**98**	location	**144**	veranda
7	seven	**53**	dining	**99**	master	**145**	wall
8	eight	**54**	door	**100**	medicine	**146**	warehouse
9	nine	**55**	downstairs	**101**	meeting	**147**	water
10	ten	**56**	driveway	**102**	motion	**148**	west
11	eleven	**57**	duress	**103**	night	**149**	window
12	twelve	**58**	east	**104**	north	**150**	windows
13	thirteen	**59**	emergency	**105**	nursery	**151**	wireless
14	fourteen	**60**	entry	**106**	office	**152**	yard
15	fifteen	**61**	family	**107**	output		
16	sixteen	**62**	fan	**108**	outside		
17	seventeen	**63**	fence	**109**	panic		
18	eighteen	**64**	fire	**110**	pantry		
19	nineteen	**65**	forced arm	**111**	partial		
20	twenty	**66**	foyer	**112**	perimeter		
21	thirty	**67**	freezer	**113**	pool		
22	forty	**68**	front	**114**	rear		
23	fifty	**69**	games	**115**	reception		
24	sixty	**70**	garage	**116**	remote		
25	seventy	**71**	gas	**117**	roof		
26	eighty	**72**	gate	**118**	room		
27	ninety	**73**	glass	**119**	rumpus		
28	hundred	**74**	glass break	**120**	safe		
29	thousand	**75**	ground	**121**	security		
30	air conditioner	**76**	guest	**122**	sensor		
31	partition	**77**	gun	**123**	shed		
32	attic	**78**	gym	**124**	shock		
33	automatic	**79**	hall	**125**	shop		
34	auxiliary	**80**	hallway	**126**	side		
35	back	**81**	heat	**127**	skylight		
36	basement	**82**	heating	**128**	sliding		
37	bathroom	**83**	hold-up	**129**	small		
38	bedroom	**84**	home	**130**	smoke		
39	boat	**85**	home theatre	**131**	south		
40	cabinet	**86**	infra-red	**132**	stairs		
41	car park	**87**	inside	**133**	storage		
42	ceiling	**88**	instant	**134**	study		
43	cellar	**89**	interior	**135**	temperature		
44	child’s	**90**	key switch	**136**	spare		
45	alert	**91**	Keychain	**137**	toilet		

9.4 Record Sensor Names (optional)

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

Example: Record user name for sensor 1.

1.	MENU 6	Select main menu - Option 6, Voice message recording
2.	MASTER CODE ENTER	Enter your Master code
3.	4	Select sensor name recording
4.	1 ENTER	Select sensor 1
5.	HOLD DOWN HISTORY	Activate recording mode
6.	((SPEAK NAME))	Record voice, maximum 2 seconds
7.	RELEASE HISTORY	Stop recording mode
8.	MENU MENU MENU	Exits from Advanced system configuration

9.5 Test Sensor Signal Strength

It is highly recommended you check the signal strength of each sensor once installed.

Test the signal strength:

1.	MENU 4	Select Main Menu - Option 4 – System Test
2.	MASTER CODE ENTER	Enter Master code
3.	4	Select sensor walk test
4.	TRIP SENSOR	Trip each sensor and listen to the voice feedback on the panel
6.	MENU MENU MENU	Exits from sensor walk test

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

9.6 Remove a Sensor

Example: Remove sensor 8.

1.	MENU 5	Select Sensor Configuration
2.	MASTER CODE ENTER	Enter your Master Code
3.	2	Select remove sensor or keyfob
4.	2	Select remove sensor
5.	8 ENTER	Select sensor 8
6.	MENU MENU MENU	Exits from Advanced system configuration

9.7 Change the User Type (optional)

The user type determines what that user can do:

Master users can arm and disarm areas. They can create, delete, or modify user codes. They can also change system settings.
Standard users can arm and disarm areas; they cannot create users or review event history.
Arm only users can only turn on the security system; they cannot disarm, or dismiss any system conditions.

9.8 Add a User / Keyfob

The hub allows you to add up to 40 users. Each user is assigned a PIN code and a user number between 1 and 1000. This allows them to interact with the system   Advanced user settings are only accessible via the Web Server, UltraSync app, or DLX900.

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

1.	MENU 3	Selects User Configuration menu
2.	MASTER CODE ENTER	**Note:** Installer account does NOT have access to users, must use a master code
3.	1	Selects configure user PIN
4.	4 ENTER	Select user 4
5.	2 5 8 0 ENTER	Sets user 4 PIN code as 2580
6.	MENU MENU MENU	Exits from Advanced system configuration

Example: Change user 6 to a master user to allow them to add/remove users.

1.	MENU 3	Selects User Configuration menu
2.	MASTER CODE ENTER	Enter Master code
3.	2	Selects configure user type
4.	6 ENTER	Select user 6
5.	2	Sets master user type
6.	MENU MENU MENU	Exits from Advanced system configuration

9.9 Record User Names (optional)

You can also record the names of the first 40 users using your voice.
Example: Record user name 1.

1.	MENU 6	Select main menu - Option 6, Voice message recording
2.	MASTER CODE ENTER	Enter Master code
3.	3	Select user name recording
4.	1 ENTER	Select user 1
5.	HOLD DOWN HISTORY	Activate recording mode
6.	((SPEAK NAME))	Record voice, maximum 2 seconds
7.	RELEASE HISTORY	Stop recording mode
8.	MENU MENU MENU	Exits from Advanced system configuration

9.10 Remove a User

Example: Remove user 4 from your system.

1.	MENU 3	Selects User Configuration menu
2.	MASTER CODE ENTER	Enter Master code
3.	1	Selects configure user PIN
4.	4 ENTER	Select user 4
5.	BYPASS	Disables the user PIN
6.	MENU MENU MENU	Exits from Advanced system configuration

9.11 Add a Keyfob

Example: Add a new keyfob and assign it as user 65

1.	MENU 5	Select Sensor Configuration
2.	MASTER CODE ENTER	Enter Master Code
3.	1	Select add sensor or keyfob
4.	PRESS DEVICE BUTTON	Press the configuration button on the device and the hub will announce that the sensor or keyfob is detected
5.	6 5 ENTER	Assign the keyfob to user 65
6.	MENU MENU MENU	Exits from Advanced system configuration

9.12 Remove a Keyfob

Example: Remove keyfob 65.

1.	MENU 5	Select Sensor Configuration
2.	MASTER CODE ENTER	Enter Master Code
3.	2	Select remove sensor or keyfob
4.	2	Select remove keyfob
5.	6 5 ENTER	Select the keyfob number
6.	MENU MENU MENU	Exits from Advanced system configuration

Personalize Your System

9.13 Volume Level

Example: Set volume level to 6.

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

9.14 Voice Annunciation

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

1.	MENU 8	Select main menu - Option 8, Basic system configuration
2.	MASTER CODE ENTER	Enter Master Code
3.	4 5	[4] Toggles voice annunciation on / off [5] Toggles full menu annunciation on / off
4.	MENU MENU	Exits from Advanced system configuration

9.15 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.	MENU 8	Select main menu-Option 8, Basic system configuration
2.	MASTER CODE ENTER	Enter Master Code
3.	4 5	[4] Toggles voice annunciation on/off [5] Toggles full menu annunciation on/off
4.	MENU MENU	Exits from Advanced system configuration

9.16 Backlight Level

Set Run Mode or Idle Mode brightness.
Example: Set run mode brightness level to 8.

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

Idle mode is when your systm is not being used. The lights on the screen dim for your comfort at night and to save power. All security functions work normally.

Example: Set idle mode brightness level to 1.

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

9.17 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 19.6.2016.

1.	MENU 8		Select main menu - Option 8, Basic system configuration
2.	MASTER CODE ENTER		
3.	1		Select time and date configuration
4.	1	[1] To configure the time and date 2	[2] To configure the date
5.	9 ENTER		Enter the hours value
6.	3 0 ENTER		Enter the minutes value
7.	1		Select AM time
8.	1 ENTER		Enter the day
9.	6 ENTER		Enter the month
10.	2 0 1 6 ENTER		Enter the year, must be 4 digits
11.	MENU MENU MENU		Exits from Advanced system configuration

9.18 Adjust Area Entry or Exit Times

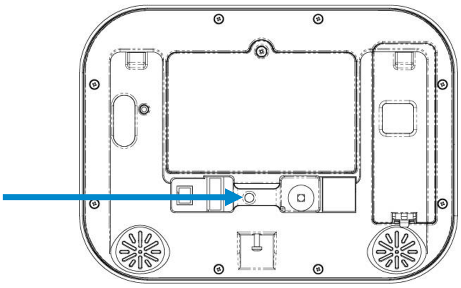
Example: Setting the entry time as 90 seconds.

1.	MENU 8		Select main menu - Option 8, Basic system configuration
2.	MASTER CODE ENTER		Enter Master Code
3.	2	[2] Select area entry time 3	[3] Select area exit time
4.	9 0 ENTER		Enter the new entry time
5.	MENU MENU MENU		Exits from Advanced system configuration

9.19 Reset Installer Account

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

1. Unplug the power supply and remove the backup battery.
2. Use a small screwdriver to hold down the reset button **before** you turn on power.



3. Wait 3 seconds after turning on the power. This will reset user 40 to PIN **9-7-1-3** and username **installer**.
4. Release the reset button.

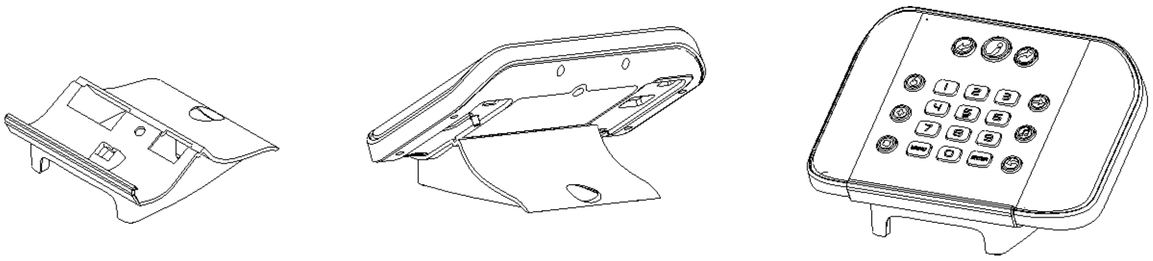
9.20 Reset to Factory Default (optional)

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

1.	MENU 9	Press Menu - 9
2.	INSTALLER CODE ENTER	Enter Installer Code
3.	0	Press 0
4.	➦	Press Bypass key
5.	Wait	Wait 10 seconds for the panel to start talking

9.21 Table Mount (Optional)

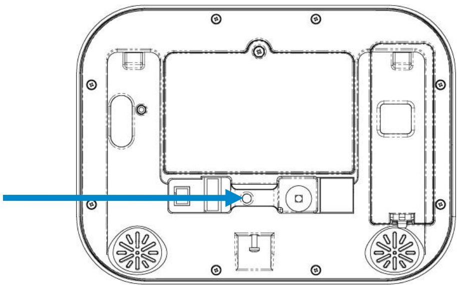
Alternatively, you may use the optional table mount to place the hub on a secure flat surface. Ensure the box tamper is **off**.



9.22 Wall Tamper Option

1. CAUTION: Wall tamper is an optional security feature that is disabled by default. When enabled, the siren will make a very loud alarm sound when power is connected.
   Press **9-7-1-3 Enter** to turn the siren off. If this does not work, reset the Installer account:

   a. Disconnect power.
   b. Use a small screwdriver to hold down the reset button.



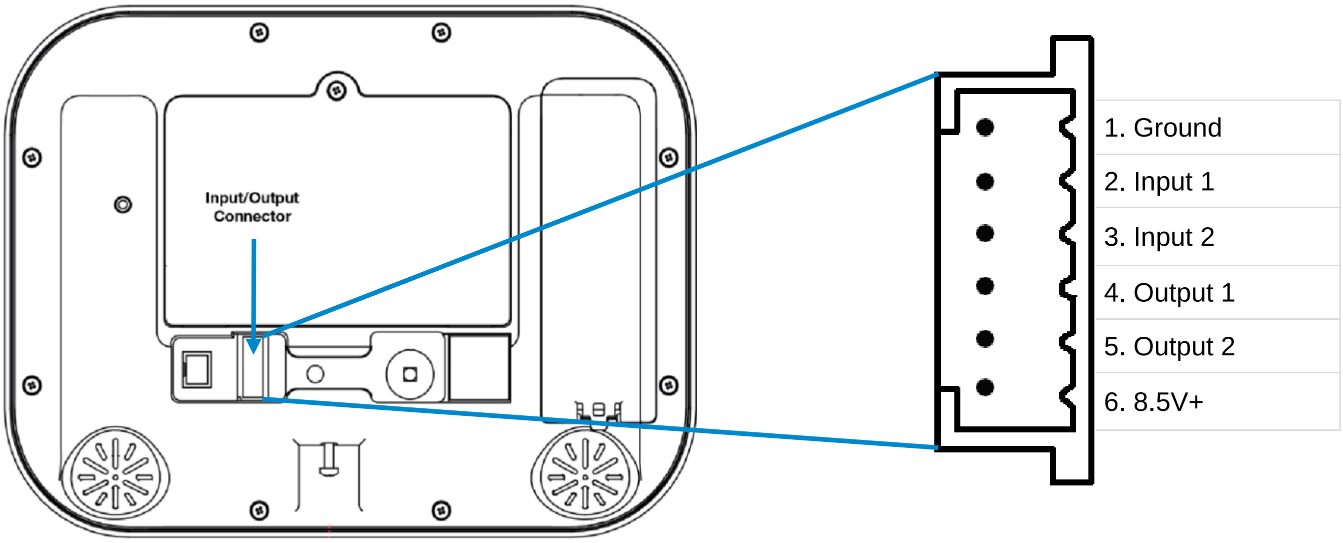
   c. Turn on power and keep holding down reset button for 3 seconds, then release the reset button. This will reset user number 256 to PIN **9-7-1-3** and username to **installer**.

2. Lights should be lit on the hub when the power is turned on. If not check that the power lead is connected securely to the rear of the hub.

Avoid using multiple power adapters and power boards. The hub is designed to be connected at all times to a power source; it is NOT designed to run from the battery pack.

9.23 Connecting Inputs

The hub has two general purpose inputs located on the rear of the unit. These can be connected to up to 4 devices when Sensor 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 sensors = OFF
- Set System Menu -> General Options -> Panel Sensor Doubling = OFF
- Set System Menu -> General Options -> Double EOL = ON for tamper monitoring, or OFF for no tamper

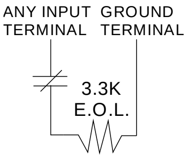
To enable 4 inputs without tamper monitoring:

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

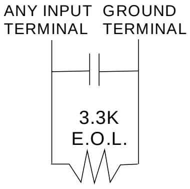
IMPORTANT NOTES:

- 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 Sensor Options -> Options
- Sensor Doubling can only be used with Normally Closed devices

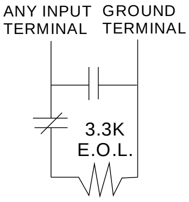
End-Of-Line Resistors for Non-Sensor Double (2 inputs):



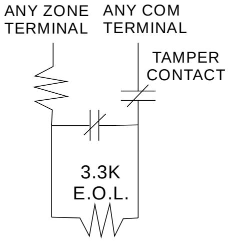
N.C. CONTACT WITH EOL RESISTOR



N.O. CONTACT WITH EOL RESISTOR

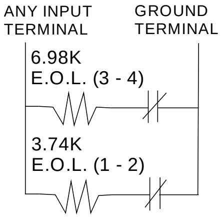


ONE N.O. CONTACT & ONE N.C. CONTACT WITH EOL RESISTOR

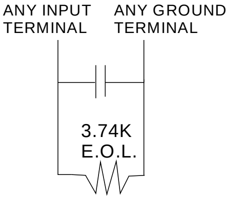


ZONE TAMPER EOL RESISTOR

End-Of-Line Resistors for Sensor Double (4 inputs):



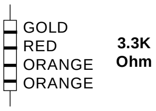
3.74K RESISTOR FOR ZONES 1 - 2 6.98K RESISTOR FOR ZONES 3 - 4



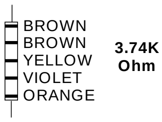
ZONE DOUBLED CONFIGURATION USED AS A FIRE ZONE, UPPER ZONE (3 - 4) IS NOT USEABLE

Resistor Diagram

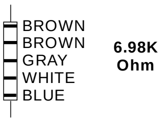
SINGLE ZONE E.O.L.



ZONE DOUBLE E.O.L. ZONES 1 - 2



ZONE DOUBLE E.O.L. ZONES 3 - 4



9.24 Connecting Outputs

The hub has two general purpose outputs located on the rear of the unit. See illustration in section 9.23, Connecting Inputs. These can be connected to up to 2 devices. Use the supplied header cable.
Outputs are controlled by Actions in the panel.

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

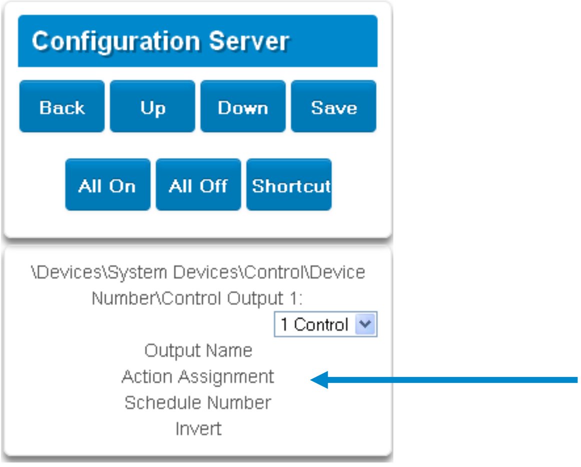
- When the action logic is true, the output will be on
- When the action is false, the output will be off

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

- Output 1 = Siren
- Output 2 = Strobe

To program outputs from the Web Server:

1. Press **Advanced** – Actions.
2. Create an Action – refer to Advanced Programming, Actions for more help.
3. Press **Advanced** – Devices – System Devices – Control.
4. Press **Control Output 1** or Control Output 2.
5. Press **Action Assignment**.

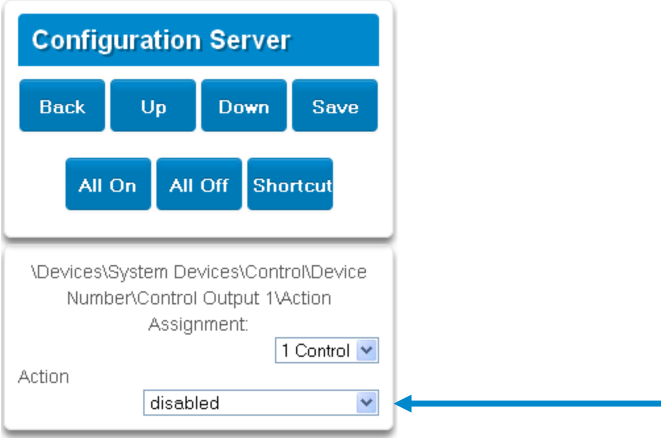


\Devices\System Devices\Control\Device Number\Control Output 1:

1 Control

Output Name
Action Assignment
Schedule Number
Invert

6. Press the drop down action menu and select the action you want to control the output. The output will now be controlled by the state of the selected action.



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

1 Control

Action: disabled

10 Testing the System

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

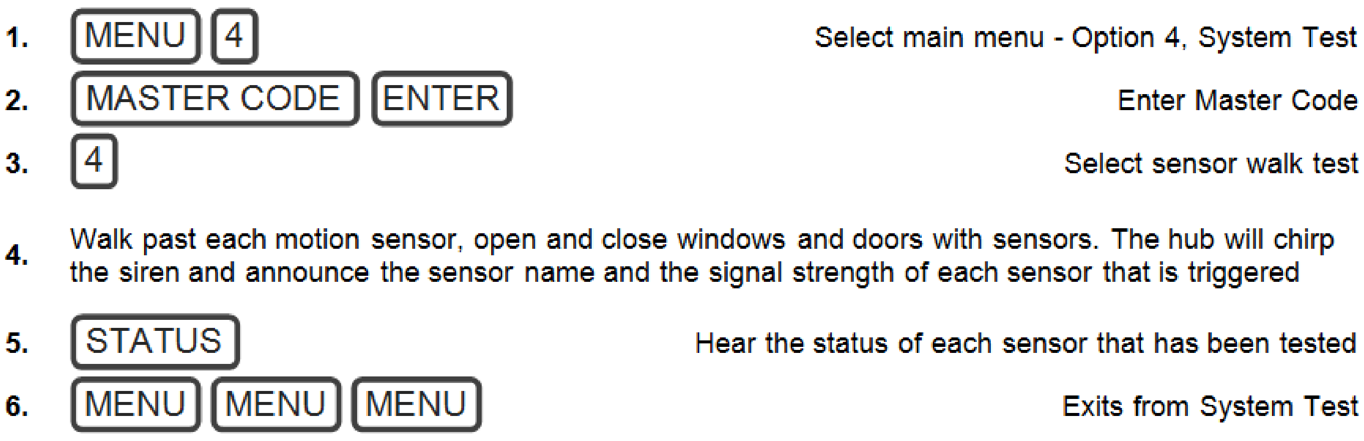
Each of these should be tested at least once per week and maintained to provide the highest level of security. Failure to conduct regular testing can result in system failure when most required.

The four system tests to perform are:

10.1 Perform a Walk Test

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

How to perform a sensor walk test:



1.	[MENU] [4]	Select main menu - Option 4, System Test
2.	[MASTER CODE] [ENTER]	Enter Master Code
3.	[4]	Select sensor walk test
4.	Walk past each motion sensor, open and close windows and doors with sensors. The hub will chirp the siren and announce the sensor name and the signal strength of each sensor that is triggered	
5.	[STATUS]	Hear the status of each sensor that has been tested
6.	[MENU] [MENU] [MENU]	Exits from System Test

10.2 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.

How to perform a siren test:

1.	MENU 4	Select main menu - Option 4, System Test
2.	MASTER CODE ENTER	Enter Master Code
3.	1	Select siren test
4.	MUTE	To stop sirens (Within 30 seconds)
5.	MENU MENU	Exits from System Test

10.3 Perform a Battery Test

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

The hub 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 or when the battery test fails (whichever is sooner). Contact your service provider for replacement parts.

How to perform a battery test:

1.	MENU 4	Select main menu - Option 4, System Test
2.	MASTER CODE ENTER	Enter Master Code
3.	3	Select battery test
4.	MENU MENU MENU	Exits from System Test

10.4 Perform a Communicator Test

The communicator is a part of the system 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.

How to perform a communicator test:

1. Call your central monitoring station and tell them you are performing a communicator test
2. MENU 8 Select main menu - Option 4, System Test
3. MASTER CODE ENTER Enter Master Code
4. 2 Select communicator test
5. The central monitoring station will confirm the test message was received
6. MENU MENU MENU Exits from System Test
7. If communicator test fails, notify your service provider

10.5 Event History

The Event History menu is used to listen to events that occurred in your security system. These events include arming, disarming, system faults and alarmed sensors. Ensure your clock is set correctly as all events are time stamped.

“Alarm Memory” will announce the last sensor(s) that caused your security system to go into an alarm condition:

1. ↺ Select History Menu
2. MASTER CODE ENTER Enter Master Code
3. 1 Listen to the last alarm memory event
4. MENU Exits from History Menu

It is recommended you record user names, sensor names, and outputs names to make reviewing any events much clearer as the hub will announce the recorded name.

You may also review all events recorded by your security system:
Reference the Event ID Table for events that can appear in the event log.

1. ↺ Select History Menu
2. MASTER CODE ENTER Enter Master Code
3. 2 Listen to history events
4. ENTER Press ENTER for next event 0 Press 0 for previous event
5. MENU Exits from History Menu

11 Glossary

Action	An action allows the system 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	Sensors are grouped in to 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	Sensors 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 sensors are not capable of activating an alarm. Sensors will return to normal operation when the system is armed then disarmed. This prevents unintentional permanent disabling of a sensor.
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 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 the system.
Chime Group	All the sensors 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 sensors are activated.
Closed	A sensor in a normal state is “closed”. The security system monitors each sensor for changes in state from closed to open and can respond with certain actions such as sounding the siren. For example, a reed switch on a front door may change from a closed state to an open state when the door opens.
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 Sensor 2 in Area 1 at 3:00am on 5/5/2014 from Account 1234. The system 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 while 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 panel due to system or area conditions. These include areas in alarm, opening and closing, sensor 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 open pre-selected sensors. Generally assigned to sensors that cover the panel (e.g.; motion sensors, front door reed switches), allowing the user to arm the security system without the need to wait for those sensors to be closed. A security system that is ready to be “force armed” will flash the ready light.
Handover	An instant alarm type, unless an entry sensor is tripped first.
Hub/Panel	The main controller for the security system. It stores all programming, provides network and other connectivity options for reporting, and provides physical terminals for connecting power, backup battery, sensors, and outputs.
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	The hub has a large range of features sorted into various menus such as Users, System, and Sensors. Each menu item can be seen when using the 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.

Open	A sensor in an abnormal state is “open”. The security system monitors each sensor for changes in state from closed to open and can respond with certain actions such as sounding the siren. For example, when a PIR sensor detects movement it will change from a closed state to an open state
Output	Outputs on the panel can be connected to a siren and strobe when an alarm condition occurs on the system.
Area	One or more sensors form an area which can be independently armed and disarmed. For example your system can be divided into an upstairs area and downstairs area.
Perimeter	Typically this refers to sensors located around the boundary of the protected area such as sensors on doors and windows, and excludes interior motion sensors.
Permission	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 pressing 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.
Sensor	A detection device such as a Passive Infrared motion sensor (PIR), reed switch, smoke detector, panic button, etc. Sensors may be physically wired to the system. Also known as an input or sensor on other security panels.
Service Provider	The installation / maintenance company servicing your security system.
Stay Modes	To turn your security system on when you are staying in the premises, this will automatically bypass pre-programmed sensors and arm others. Often used to arm only the perimeter while allowing movement inside the premises. Press STAY once for Arming with Entry Delay Press STAY a second time for Arm Stay – Instant. This removes the

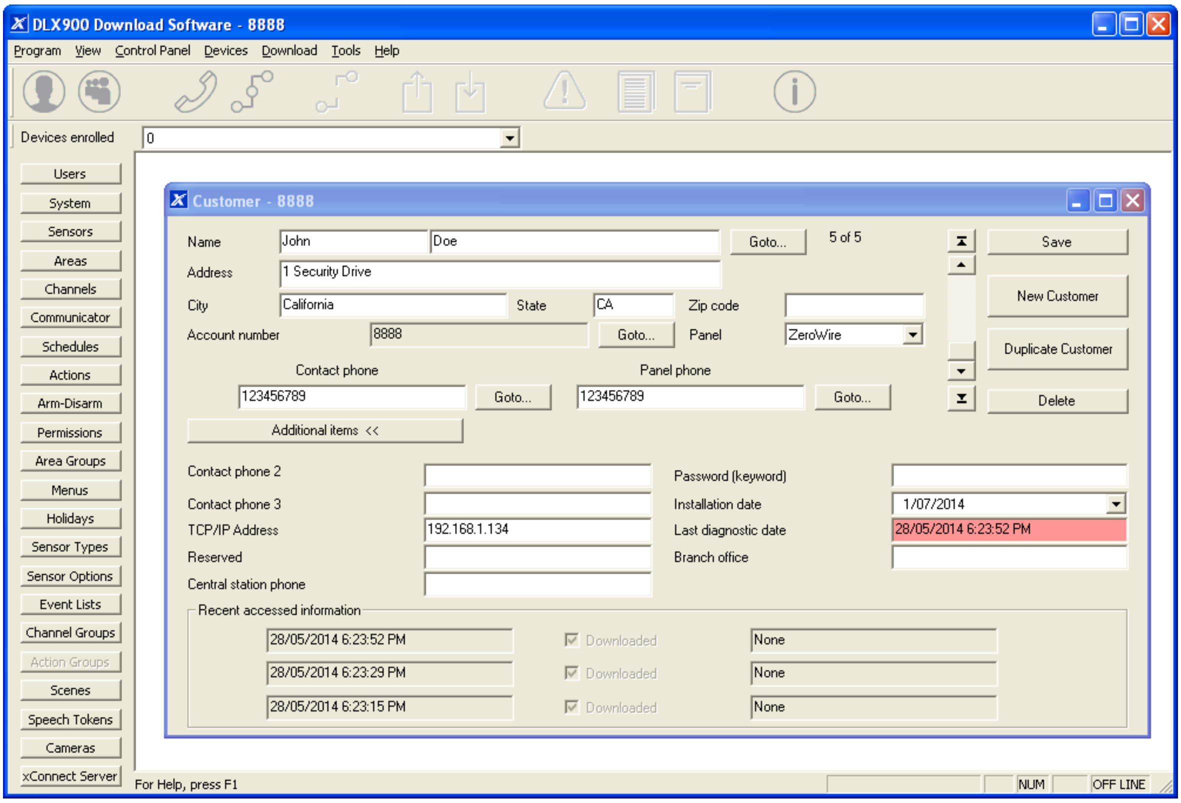
	entry delay and will immediately alarm the system when a sensor is faulted. Press STAY a third time for Arm Stay – Night. Removes the bypass state of selected zones and the entry delay from all delay zone types.
Tamper	A physical switch on a device that detects unauthorised access to the unit. For example opening the case of a sensor 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 sensor to detect removal from a surface.
Token	Each token is a pre-recorded word or phrase that can be used to name sensors, areas, outputs, and rooms.
UltraSync	Mobile app for smartphones to access the Web Server which provides access to view the status of a system, control sensors and outputs, program users and other features. Available to download for Apple^{TM} iPhone^{TM} and Google^{TM} Android^{TM} from the respective app store. The UltraSync app connects to the UltraSync server which will then connect to your system.
User	An authorised person who can interact with the security system and perform various tasks according to the permissions assigned to them. Each 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, the system 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.
Web Server	The hub has a built-in web server which provides access to system 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 hub keypad.

Appendices

A.1 DLX900 Software

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 www.interlogix.com.

In order for DLX900 to connect to the panel you will need:
- The IP address of the hub (or use the Discover feature for LAN connections)
- To know the Download Access Code (see Troubleshooting section, A.2) 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 panel into program mode, this can be changed in Settings-Network.



Devices enrolled: 0

Name: John Doe
5 of 5
Address: 1 Security Drive
City: California
State: CA
Zip code:
Account number: 8888
Panel: ZeroWire
Contact phone: 123456789
Panel phone: 123456789

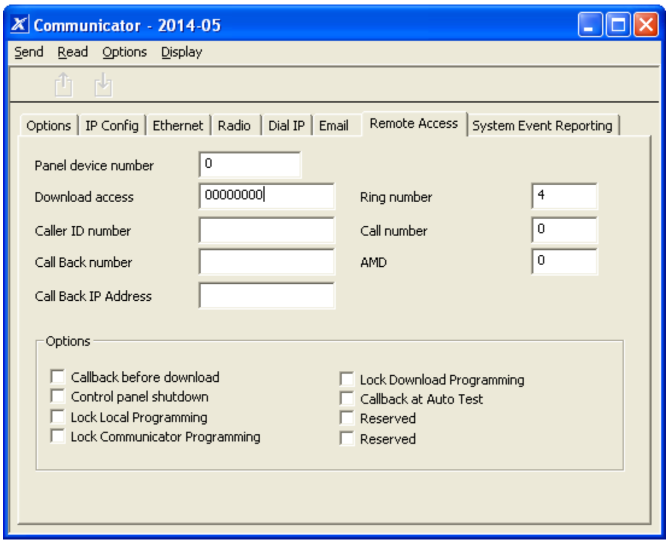
Contact phone 2:
Contact phone 3:
TCP/IP Address: 192.168.1.134
Reserved:
Central station phone:
Password (keyword):
Installation date: 1/07/2014
Last diagnostic date: 28/05/2014 6:23:52 PM
Branch office:

Recent accessed information

28/05/2014 6:23:52 PM	☑ Downloaded	None
28/05/2014 6:23:29 PM	☑ Downloaded	None
28/05/2014 6:23:15 PM	☑ Downloaded	None

For Help, press F1
NUM
OFF LINE

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 hub, press **Save**.
4. Go to Communicator – Remote Access.



Panel device number 0

Download access 00000000

Caller ID number

Call Back number

Call Back IP Address

Ring number 4

Call number 0

AMD 0

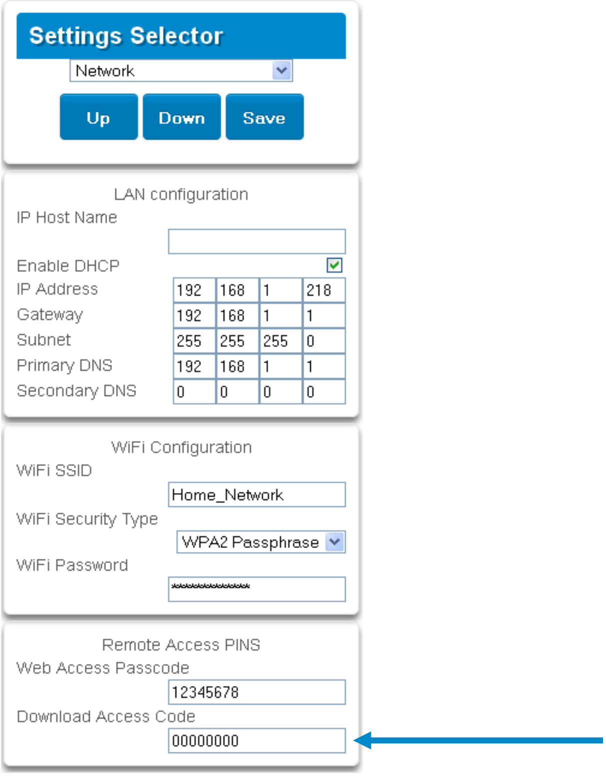
Options

□ Callback before download
□ Control panel shutdown
□ Lock Local Programming
□ Lock Communicator Programming
□ Lock Download Programming
□ Callback at Auto Test
□ Reserved
□ Reserved

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

To enable remote access for DLX900 in UltraSync, change the Download Access Code. The default Download Access Passcode of 00000000 prevents remote access. Login to the hub's Web Server and go to Settings – Network then change the code.

Note: DLX900 will attempt to connect using the default **installer** / **9**-**7**-**1**-**3** account. To disable DLX900 access, change the Installer PIN code and set the Download Access Code to 00000000.



Network

LAN configuration

IP Host Name

Enable DHCP ☑

IP Address 192 168 1 218

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 Home_Network

WiFi Security Type WPA2 Passphrase

WiFi Password ************

Remote Access PINS

Web Access Passcode 12345678

Download Access Code 00000000

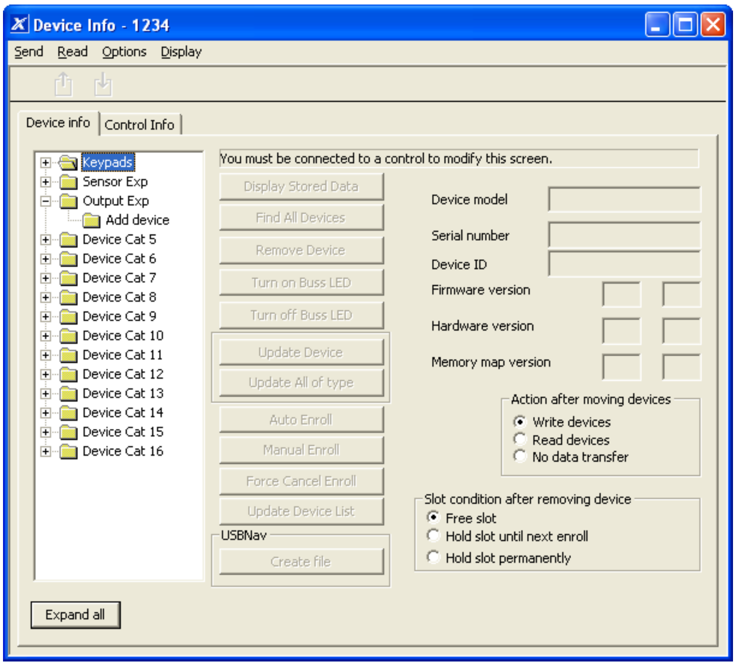
A.2 Troubleshooting DLX900

Problem	Solution
Cannot connect over TCP/IP	Check you can ping the hub. Check the Download Access Code. Check that remote access is enabled on the hub. 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 hub 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 the hub's 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 **9**-**7**-**1**-**3** 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.

A.3 Firmware Upgrade 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**:



You must be connected to a control to modify this screen.

Action after moving devices
● Write devices
○ Read devices
○ No data transfer

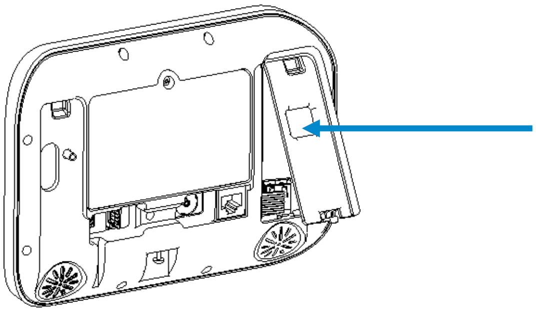
Slot condition after removing device
● Free slot
○ Hold slot until next enroll
○ Hold slot permanently

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

A.4 Firmware upgrade using USBUP

Upgrading firmware on your hub 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 hub 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 hub but leave it connected.
6. The USBUP header is inside the 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.

A.5 System Status Messages

Various messages may appear on the Status screen of the Web Server and UltraSync 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 communication channel
- Fire alarm – A fire alarm has been activated from the hub
- Panic – A panic alarm has been activated from the hub
- Medical – A medical alarm has been activated from the hub

Area Number / Area Name

- Is On in the away mode – This area is armed in the away mode.
- Is On in the stay mode – This area is armed in the stay mode.
- Is ready – This area is secure and ready to be armed.
- Is not ready – This area is NOT ready to be armed, a sensor is not secure.
- All areas are on in the away mode – All areas in this multi area system are armed in the away mode.
- All areas are on in the stay mode – All areas in this multi area system are armed in the stay mode.
- All areas are ready – All areas in this multi area system are secure and ready to be armed.

Sensor Number / Sensor Name

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

A.6 App and Web Error Messages

Various error messages may appear on the 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"

Sensors Page

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

Wi Fi

- "Connection Was lost before a response was received" – Sent when No response received on a Wi Fi 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 []"

A.7 Zwave Messages

Zwave Messages

- "Unavailable – Failed Device Function in progress" – An Attempt was made to enter an add remove mode when failed device mode is active.
- "Unavailable – Add mode active" – Attempt was made to enter an add remove mode when add mode is active.
- "Unavailable – Remove mode active" – An Attempt was made to enter an add remove mode when remove mode is active.
- "Unavailable – Resetting Network" – An Attempt was made to enter an add remove mode when resetting mode is active.
- "Unavailable – Backing Up Network" – An Attempt was made to enter an add remove mode when backup mode is active.
- "Unavailable – Restoring Network" – An Attempt was made to enter an add remove mode when restore mode is active.
- "Busy, Try Again Momentarily" – This message is received when the ZWave module is attempting 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 remove mode when remove mode is active.
- "Replace Device failed – already in process" – An Attempt was made to enter Replace mode when 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 ZWave module is still initializing
- "Command Failed" – A ZWave 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.

A.8 History Events

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

Event ID Table

Event Name	Description
24 Hour Alarm	
24 Hour Alarm Restore	
Abort	
Activity Monitor fail	
Alarm Aborted	Alarm was aborted
Automatic Test	
Battery Low Event	
Battery Low Event Restore	
Box Tamper	
Box Tamper Restore	
Burg Alarm	
Burg Alarm Restore	
Bypass	
Bypass Restore	
Cancel	
Checksum Fault	
Checksum Fault Restore	
Clock Changed	
Close	
Communication Failure	
Communication Failure Restore	
Cross Zone initial trip	
Cross Zone initial trip Restore	
Device Enrolled	
Device Failure	
Device Failure Restore	
Door Access	
Door Access Denied	
Door Forced	
Door Forced	
Door Propped	
Door Propped	
Duress	
Early Opening	
Early Opening	
End Listen In	
End Local Program	
End Remote Program	
End Walk Test Mode	
End Sensor Test	
Exit Error	
Expander DC Loss	
Expander DC Loss Restore	
Expander Low Battery	
Expander Low Battery Restore	
Fail To Close	
Fail to Open	
Fire Alarm	
Fire Alarm Restore	
Fire Maintenance Alarm	

Fire Maintenance Alarm Restore	
Fire Supervision	
Fire Supervision Restore	
First Open	
Ground Fault	
Ground Fault Restore	
Guard Tour Fail	
Keypad Lockout	
Last Close	
Late Closing	
Late Opening	
Mains Fail Event	
Mains Fail Event Restore	
Man Down	
Manual Audible Panic	
Manual Fire	
Manual Medical	
Manual Silent Panic	
Manual Test	
Manual Test Restore	
Open	
Output Activated	
Output Restored	
Over Current	
Over Current Restore	
Partial Close	
Partial Open	Opening from Partial Arm
Power Up	
Power Up Restore	
Recent Close	
Remote Program Fail	
Reserved	
Reserved Sensor Event Types/Restores	
Sensor Low Battery	
Sensor Low Battery Restore	
Serial Bus Expansion Event	
Siren Tamper	
Siren Tamper Restore	
Start Listen In	
Start Local Program	
Start Remote Program	
Start Walk Test Mode	
Start Sensor Test	
System Device Bypassed	
System Device Un-bypassed	
System Shut Down	
System Turn On	Restore from system shutdown
Tamper	
Tamper Restore	
Technician Arrival	
Technician Left	
Telephone Fault	
Telephone Fault Restore	
Trouble	
Trouble Restore	
User Activated Output	
Valid Code Entered	
Valid Code expired	
Valid Code lost	
Valid Code out of Schedule	

Valid Code Void	
Walk Test Fail	
Walk Test Pass	
Watchdog Reset	
Wireless Jam	
Wireless Jam Restore	
Wireless Supervision	
Wireless Supervision Restore	
Sensor Activity Supervision	
Sensor Activity Supervision Restore	

A.9 Event Reporting Class Table

Class Name	Description
Bypass/Bypass Restore	Sensor has been isolated
Cancel	
Communication Failures	
Don’t care	Used for devices that do not classify events.
Fire Alarm	A fire device created an alarm
Fire Restore	A fire device restored from Alarm
Log Only	
Non-Fire Alarm	A non-fire device created an alarm. This includes medical, panic, and burg.
Non-Fire Restore	A non-fire device restored from alarm.
Open/Close	An area turn on turn off
Power Trouble	Mains and battery trouble
Program Mode	Local or remote programming
Recent Close/Abort	
Reserved	
Sensor Trouble/restore	Low battery or wireless supervision
System trouble/Restore	A system trouble event or restore.
Tampers/Tamper Restore	A tamper alarm or tamper restore.
Test Reports	Manual or automatic test event
Sensor Trouble/Restore	A fire sensor or day sensor is in trouble or restored from trouble.

A.10 Action Events: Category and Types

Action Events Category	Action Event Type
Sensor Events	Disabled Faulted Not Faulted Alarm Bypass Tamper Low Battery Trouble Supervision Chime Enabled Inhibited (Bypassed) 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 Sensor Cross Zone Timing Sensor Bypass Sensor Tamper Sensor Not Ready Sensor Low Battery Sensor Supervision Fault Chime On (from sensor) Walk Test (from sensor) Trouble (from sensor) 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

Action Events Category	Action Event Type
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
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 Remote Program Fail Watchdog Reset
Room Events	Disabled Connected To Pending Connection To Privacy Talking Using Channel 1 Using Channel 2

A.11 Action Results Category and Action Results Event Types

Action Results Category	Action Results Event Type
Sensor Results	Sensor Trip Toggle Sensor Trip Sensor Restore Sensor Bypass Toggle Sensor Bypass Sensor Unbypass Sensor Chime Toggle Sensor Chime On Sensor Chime Off
Area Results	Arm Away Turn Off Silence Arm Stay Toggle Arm Stay Arm Away No Auto Stay Chime Toggle Chime On Chime Off Automatic Sensor Test Toggle Automatic Sensor Test On Automatic Sensor 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
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
User Results	User Expire or Activate User Activate User Deactivate
System Results	Disabled Detector Reset Communicator Test
Device Results	Disabled Battery Test Start Siren Device Bypass Device Unbypass
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 Camera 16

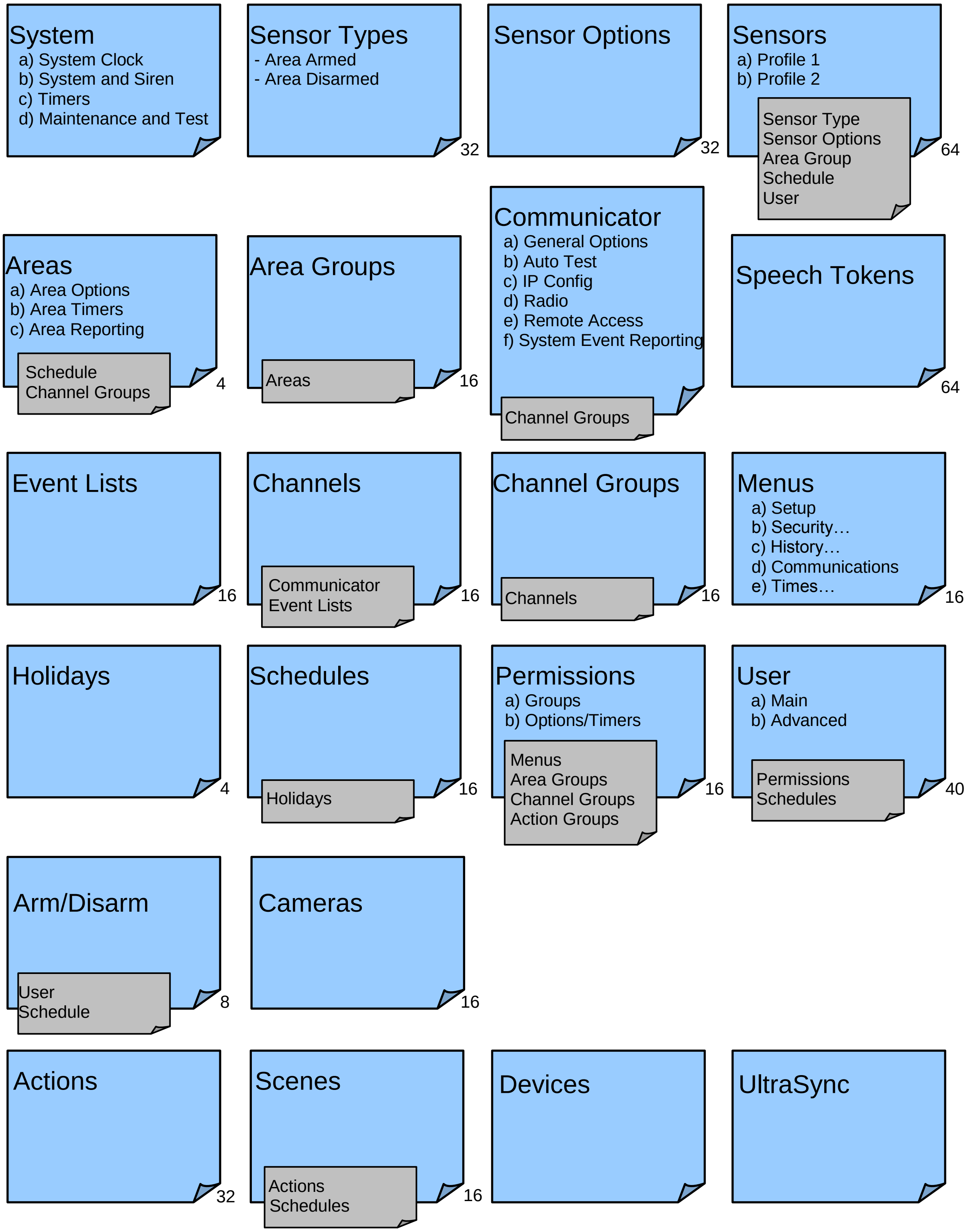
A.12 Building Blocks

Below is the system diagram showing all the different building blocks that can be used to create a security system.

You have full flexibility to customise your system. Program each building block in turn to complete your system. We suggest left to right, top to bottom. Refine blocks as you go or use pre-sets to save you time.

The smaller grey blocks indicate related blocks that are used by the larger blue block.

The number on the bottom right of each block indicates the capacity of the system.



System
a) System Clock
b) System and Siren
c) Timers
d) Maintenance and Test

Sensor Types
- Area Armed
- Area Disarmed
32

Sensor Options
32

Sensors
a) Profile 1
b) Profile 2
Sensor Type
Sensor Options
Area Group
Schedule
User
64

Areas
a) Area Options
b) Area Timers
c) Area Reporting
Schedule
Channel Groups
4

Area Groups
Areas
16

Communicator
a) General Options
b) Auto Test
c) IP Config
d) Radio
e) Remote Access
f) System Event Reporting
Channel Groups

Speech Tokens
64

Event Lists
16

Channels
Communicator
Event Lists
16

Channel Groups
Channels
16

Menus
a) Setup
b) Security…
c) History…
d) Communications
e) Times…
16

Holidays
4

Schedules
Holidays
16

Permissions
a) Groups
b) Options/Timers
Menus
Area Groups
Channel Groups
Action Groups
16

User
a) Main
b) Advanced
Permissions
Schedules
40

Arm/Disarm
User
Schedule
8

Cameras
16

Actions
32

Scenes
Actions
Schedules
16

Devices

UltraSync

A.13 Menu Tree

The menu structure as seen from the Advanced menu in the 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. **Sensors**
    1. Sensor Number
    2. Sensor Name
    3. First Sensor Profile
    4. Second Sensor 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. Wi Fi SSID
        8. Wi Fi Security Type
        9. Wi Fi Password
        10. Ports
        11. Time Server
        12. IP Options
    4. Radio Configuration
    5. Remote Access
        1. Panel Device Number
        2. Download Access Code
        3. Callback 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. ZWave 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. **Sensor Types**
    1. Sensor Type Number
    2. Sensor Type Name
    3. Sensor Type Armed
    4. Sensor Type Disarmed
16. **Sensor Options**
    1. Sensor Options Number
    2. Sensor Options Name
    3. Sensor Options
    4. Sensor Reporting
    5. Sensor Contact Options
    6. Sensor 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 Sensor
    6. Scene Actions
20. **Speech Tokens**
    1. Sensor 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

Specifications

Circuit	Primary
Voltage	9 VDC Regulated
Current	210 mA maximum 165 mA without voice
Operating Temperature	0 to 50 Degrees Celsius
Back Up Battery	Rechargeable Ni-MH battery pack
Inputs	2x sensor inputs up to 6.6V, close with 3.3k EOL
Outputs	2x open collector outputs at 100mA 30V (max)
Dimensions (W x H x D)	190 mm x 140 mm x 32 mm
Shipping Weight	1 Kg

UL SPECIFICATION

General: The UL Listed system consists of the following features and compatible devices:

Electrical:

9VDC Power Supply:
UL Listed (E365620) Huizhou Zhongbang Electronic Co Ltd, Model ZB-A090020A-J.
Input: 100-240VAC 50/60 Hz, 0.6A max
Output: 9 VDC, 2A

Backup Battery Pack:
Golden Power, Model 6MR2300AAH4A
7.2 VDC, 2300 mAh, Ni-MH

Software Version:

1.x

Installation Notes:

The system shall not be programmed to add input from the Web Server, UltraSync App, and Wi Fi to smartphone.

The chime feature is only to be used in the disarm stage. It is not to be used as the main audible alarm.

During the test mode, test AC and Battery every week by disconnecting AC power and verifying 5 minutes of emergency signaling. Reinstall restraining means of power plug.

Replace the battery pack every three (3) years.

The RF jamming signal is announced by the voice message “RF signal blocked” repeats until code is entered.

Compatible Receivers:

Operation has been verified with industry standard SIA Contact ID format. It is the Installer’s responsibility to verify compatibility between the panel and the receiver used during installation. The Installer shall verify the compatibility of the receiver and the system on a yearly basis.

Listings and Approvals:

UL:

ANSI/UL 985	Household Fire Warning
ANSI/UL 1023	Household Burglar
ANSI/UL 1637	Home Health Care Signaling

cUL:
ULC S545 – Residential Fire Warning System Control Units
ULC/ORD-C1023 – Preliminary Standard for Household Burglar Alarm System Units

SIA:

ANSI/SIA CP-01-2010	False Alarm Reduction

Minimum System Configuration:

Control Panel Model ZW-6400 for use with the following UL Listed accessories manufactured by UTC:
TX-1012-01-1, TX-1012-01-3 DOOR CONTACT
60-362N-10-319.5 DOOR CONTACT
TX-6010-01-1 SMOKE DETECTOR
60-848-02-95 SMOKE DETECTOR
60-703-95 PIR
60-639-95R PIR

Abort:

Consult with your Installer to determine if your system is configured with a communicator delay. A communicator delay will prevent a report to the central station if the control panel is disarmed within 30-45 seconds after an intrusion alarm is triggered. **Note:** Fire-type alarms are normally reported without a delay.

Quick exit:

Use the quick exit feature when someone wants to briefly leave while the home is still armed (for instance to get the newspaper). This feature needs to be enabled by your Installer. When you press the **DISARM** button, the display shows *Exit Time is On*. This allows a designated exit door to be open for up to two minutes without triggering an alarm.
Note: The designated door may be opened and closed only once. If you close the designated door behind you when you exit, you will have to disarm the system upon reentering. Leave the designated door open while using the quick exit feature.

Note: The designated door may be opened and closed only once. If you close the designated door behind you when you exit you will have to disarm the system upon reentering. Leave the designated door open while using the quick exit feature.

Exit delay extension:

If enabled by your Installer, the *Exit Delay extension* feature will recognize when you arm the system, leave your house and then quickly re-enter your house (such as you would if you forgot your car keys.) In such a case ZX-6400 will restart your exit delay to give you the full exit delay again.

Exit Progress Annunciation:

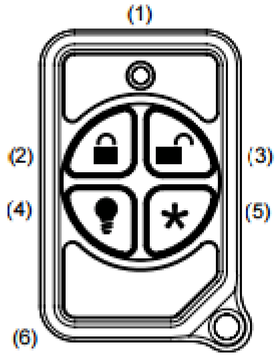
A pulsating audible sounds throughout the duration of the Exit Time to indicate that the exit period is in process. A rapid pulsating audible sounds during the last ten (10) seconds of the Exit Time to indicate that the Exit Time is running out.

Entry Progress Annunciation:

A pulsating audible sounds upon entry to indicate that the Entry Delay has begun.

Remote Control Devices: UTC model 6001064-95R

Figure 1: Micro Keyfob



(1) LED
(2) Lock button
(3) Unlock button
(4) Light button
(5) Star button
(6) Cover slot

Keyfob operation / System Acknowledgement:

Unlock button. Disarm the system. LED light momentary on and two squawks from the control panel
Lock button. Arm the system. LED light momentary on and two squawks from the control panel
Light button. Toggle system-controlled lights on/off (if programmed).
Star button. As programmed in the system.
When the battery is low, the LED light will not turn on when buttons are pressed, and the keyfob will not operate.

Canceling and preventing accidental alarms:

One of the biggest concerns you might have regarding your security system is causing an accidental alarm. Most accidental alarms occur when leaving the residence after arming the system or before disarming the system upon your return.

Alarms are canceled by entering a valid master or user code within the minimum cancel window of five (5) minutes. After alarms are canceled, the system will be disarmed.

Recent Closing:

Enabled (2-minute window)

Sensor Tripping Instructions:

Sensor	Action
Door/window	*Open the secured door or window.*
Carbon monoxide alarm	*Press and hold the **Test/Hush** button (approximately 5 seconds) until the unit beeps two times, and then release the button.*
Glass break	*Test with an appropriate glass break sensor tester.*
Motion sensor	*Avoid the motion sensor field of view for 5 minutes, and then enter its view.*
Smoke	*Press and hold the test button until the system sounds transmission beeps.*
Keyfob	*Press and hold the **Lock** and **Unlock** buttons simultaneously for 3 seconds.*
Remote touchpad	*Press and hold the two **Emergency** buttons simultaneously for 3 seconds.*

SIA CP-01-2010 Programmable Features

Your panel is shipped with preset defaults to comply with the Security Industry Association CP-01 Standard. The relevant settings are listed below and should not be changed to maintain CP-01 compliance.

FEATURE	REQUIREMENT	RANGE	SHIPPING DEFAULT
Exit Time	Required (programmable)	For full or auto arming: 45 sec. - 2 min. (255 sec. max.)	60 Seconds
Progress Annunciation / Disable - for Silent Exit	Allowed	Individual keypads may be disabled	All annunciators enabled
Exit Time Restart	Required Option	For re-entry during exit time	Enabled
Auto Stay Arm on Unvacated Premises	Required Option (except for remote arm)	If no exit after full arm	Enabled
Exit Time and Progress Annunciation / Disable - for Remote Arm	Allowed Option (for remote arm)	May be disabled - for remote arming	Enabled
Entry Delay(s)	Required (programmable)	30 sec. - 4 min. **	30 Seconds
Abort Window – for Non-Fire Sensors	Required Option	May be disabled - by sensor or sensor type	Enabled
Abort Window Time – for Non-Fire Sensors	Required (programmable)	0 sec. - 45 sec. **	30 Seconds
Abort annunciation	Required Option	Annunciate that no alarm was transmitted	Enabled
Cancel Window	Required	Minimum duration of the window shall be five (5) minutes.	
Cancel Annunciation	Required Option	Annunciate that a Cancel was transmitted	Enabled
Duress Feature	Allowed Option	No automatic derivative of another user code No duplicates with other user codes	Disabled
Cross Zoning	Required Option	Programming needed	Disabled
Programmable Cross Zoning Time	Allowed	May Program	Per manufacturer
Swinger Shutdown	Required (programmable)	For all non-fire sensors, shut down at 1 to 6 trips	Two trips
Swinger Shutdown Disable	Allowed	For non- police response sensors	Enabled
Fire Alarm Verification	Required Option	Depends on panel and sensors	Disabled
Call Waiting Cancel	Required Option	Depends on user phone line	Disabled

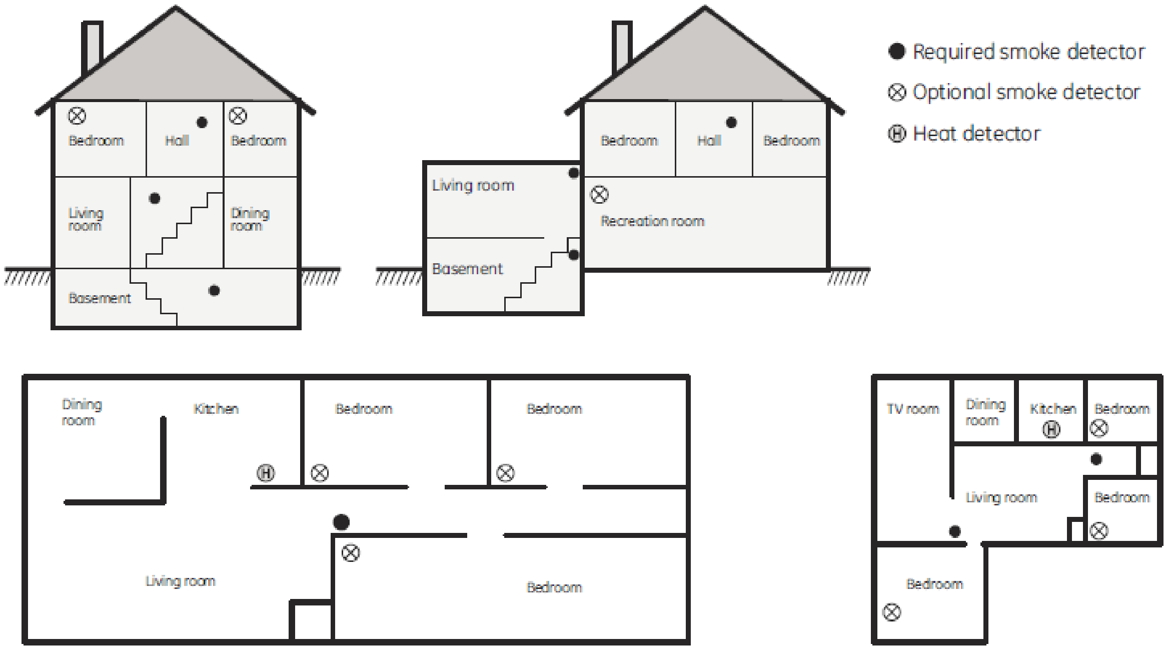
Smoke and heat detector locations:

Selecting a suitable location is critical to the operation of smoke alarms. *Figure 2* shows some typical floorplans with recommended smoke and heat detector locations. Use these location guidelines to optimize performance and reduce the chance of false alarms:

- Before mounting alarms, program (learn) them into memory and do a sensor test from the alarm's intended location to ensure good RF communication to the panel.
- Locate the alarm in environmentally controlled areas where the temperature range is between 40 and 100°F (5 and 38°C) and the humidity is between 0 and 90% noncondensing.
- Locate alarms away from ventilation sources that can prevent smoke from reaching the alarm.
- Locate ceiling mounted alarms in the center of the room or hallway, at least 4 in. (10 cm) away from any walls or areas.
- Locate wall mounted alarms so the top of the alarm is 4 to 12 in. (10 to 31 cm) below the ceiling.
- In rooms with sloped, peaked, or gabled ceilings, locate alarms 3 ft. (0.9 m) down or away from the highest point of the ceiling.
- When mounting to suspended ceiling tile, the tile must be secured with the appropriate fasteners to prevent tile removal.

Note: Do not mount the alarm to the metal runners of suspended ceiling grids. The metal runners can draw the magnet's field away from the alarm's reed switch and cause a false tamper alarm.

Figure 2. Smoke and Heat Detector Locations:



PRODUCT WARNINGS

A PROPERLY INSTALLED AND MAINTAINED ALARM/SECURITY SYSTEM MAY ONLY REDUCE THE RISK OF EVENTS SUCH AS BREAK-INS, BURGLARY, ROBBERY OR FIRE; IT IS NOT INSURANCE OR A GUARANTEE THAT SUCH EVENTS WILL NOT OCCUR, THAT ADEQUATE WARNING OR PROTECTION WILL BE PROVIDED, OR THAT THERE WILL BE NO DEATH, PERSONAL INJURY, AND/OR PROPERTY DAMAGE AS A RESULT.

WHILE INTERLOGIX UNDERTAKES TO REDUCE THE PROBABILITY THAT A THIRD PARTY MAY HACK, COMPROMISE OR CIRCUMVENT ITS SECURITY PRODUCTS OR RELATED SOFTWARE, ANY SECURITY PRODUCT OR SOFTWARE MANUFACTURED, SOLD OR LICENSED BY INTERLOGIX, MAY STILL BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

INTERLOGIX DOES NOT ENCRYPT COMMUNICATIONS BETWEEN ITS ALARM OR SECURITY PANELS AND THEIR 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.

WARRANTY DISCLAIMERS

INTERLOGIX HEREBY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING (BUT NOT LIMITED TO) ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO ITS SECURITY PRODUCTS AND RELATED SOFTWARE. INTERLOGIX FURTHER DISCLAIMS ANY OTHER IMPLIED WARRANTY UNDER THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT OR SIMILAR LAW AS ENACTED BY ANY STATE.

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

INTERLOGIX MAKES NO REPRESENTATION, WARRANTY, COVENANT OR PROMISE THAT ITS SECURITY PRODUCTS AND/OR RELATED SOFTWARE (I) WILL NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED; (II) WILL PREVENT, OR PROVIDE ADEQUATE WARNING OR PROTECTION FROM, BREAK-INS, BURGLARY, ROBBERY, FIRE; OR (III) WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS.

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.INTERLOGIX.COM/ZEROWIRE

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 the system 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.interlogix.com/zerowire

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

Copyright

Trademarks and Patents

Regulatory Notices for USA

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance to this equipment would void the user's authority to operate this device.

FCC Radiation Exposure Statement: This product complies with FCC radiation exposure limits set for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the device and your body.

Tested To Comply
With FCC Standards
For Home or Office Use

FCC ID: 2ADG2ZW-6400H
Contains FCC ID: W7OMRF24WG0MAMB

DESTINATION CONTROL STATEMENT – These commodities, technology, or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to United States law is prohibited.

This equipment should be installed in accordance with Chapter 2 of the National Fire Alarm Code, ANSI/NFPA 72, (National Fire Protection Association, Batterymarch Park, Quincy, MA 02269). Printed information describing proper installation, operation, testing, maintenance, evacuation planning, and repair service is to be provided with this equipment.

Regulatory Notices for Canada

Model / Modèle: ZW-6400

IC: 12545A-ZW6400H

Contains / Contient IC: 7693A-24WG0MAMB

CAN ICES-3 (B)/NMB-3(B)

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1) l'appareil ne doit pas produire de brouillage;

2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This Device complies with IC radiation exposure limits. It is desirable that the device shall be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter

Index

Click on entries to navigate

A

Action Events Category and Types 204
Action Results Category and Event Types........205
Actions Submenus......................................108–11
Add a Camera, Automatic Discovery..................65
Add a Keyfob 177
Add a User on the keypad 175
Add a Zwave Device...57
Add Camera to UltraSync 166
Add Users 147
Adding Cameras to the Network..................163–65
Adjust Area Entry or Exit Times........................179
Advanced Installation Using Web Server 69
Advanced Programming, Actions 107
Advanced Programming, Area Groups.............122
Advanced Programming, Areas...........................83
Advanced Programming, Arm-Disarm...............112
Advanced Programming, Cameras 143
Advanced Programming, Channel Groups........134
Advanced Pro, Reporting and Notifications.........94
Advanced Programming, Communicator.............97
Advanced Programming, Devices 114
Advanced Programming, Event Lists 133
Advanced Programming, Holidays 124
Advanced Programming, Menus 123
Advanced Programming, Network Servers 145
Advanced Programming, Permissions 118
Advanced Programming, Scenes......................139
Advanced Programming, Schedules 105
Advanced Programming, Sensor Options 129
Advanced Programming, Sensor Types...........125
Advanced Programming, Sensors......................79
Advanced Programming, Speech Tokens.........141
Advanced Programming, System 70
Appendices 193
Area Groups Submenus 122
Areas Configuration menu 40
Areas Submenus 83–93
Arm Disarm Submenus...............................112–13

B

Back of Panel...10
Backlight Level...178

C

Camera Setup Instructions 161
Camera Wi Fi Signal Strength 162
Cameras Submenus 143
Cellular Radio Setup...153
Change Default Camera Settings......................169
Change the User Type (optional) 175
Channel Configuration Menu...............................46
Channel Groups Submenus 134
Channels Submenus 94–95
Check Cell Radio Signal Strength 155
Check Cellular Connection to UltraSync 158
Check Ethernet Connection to UltraSync 17
Check Event History 67
Check System Connection Status 66
Check Wi Fi Connection to UltraSync 22, 64
Choose a Location...11
Communicator Submenus 97–104
Configure Sensor Names (optional) 172
Connecting Inputs...181
Connecting Outputs..183
Customize Reporting Codes.............................136

D

Devices Submenus 114–17
DLX900 Software..193

E

Email Reporting 96
Enable Wi Fi on your mobile device 18, 60
Ethernet Setup 16
Event History...187
Event ID Table 201
Event Lists Submenus 133
Event Reporting Class Table 203
Example Sensor or Area Event 135
Example System Event.....................................135

F

Features & Benefits 7
Firmware upgrade using DLX900 196
Firmware upgrade using USBUP......................197
Force Arming, Bypass, and Auto-Bypass............87
Front of Panel 9
Full Menu Annunciation 178

G

Glossary...189

H

Hardware Installation 11
History Events...201
Holiday Configuration Menu 55
Holidays Submenus..124

I

Included In Box 8
Install External Antenna....................................156
Install Optional Cellular Radio 154
Install the Battery 12
Install UltraSync App 23
Install the Hub 12
Installation Using Keypad 171
Installer Code..27
Installer Phone Number 27

K

Key Fob Configuration Menu...............................38

L

Learn in a Keyfob..36
Learn Sensors into the system 31
Learn Sensors into panel with the keypad.........171
Live Stream and Latest Clip..............................167

M

Menus Submenus...123
Menu Tree 207
Messages, App and Web Error 199
Messages, System Status 198
Messages, Zwave...200

N

Network Configuration Menu 48

O

Optional Accessories...8

P

Permanent Connection Mode 15
Permissions 150
Permissions Submenus...............................118–21
Personalize Your System 177
Power Connection 13
Program event triggered camera clips...............167
Programming Areas...39
Programming Cameras.......................................65
Programming Reporting and Notifications...........45
Programming Holidays 55
Programming Scenes 50
Programming Schedules 53
Programming the Network..................................47
Programming the System 42
Programming Zwave Devices.............................57

R

Recommended Items to Change.........................27
Record Sensor Names (optional) 174
Record User Names (optional) 176
Remove a Keyfob 177
Remove a Sensor 175
Remove a User..176
Remove a Camera..144
Reporting Fixed Codes in Contact I.D. 138
Reset Installer Account......................................180
Reset to Factory Default....................................180

S

Scan for Wireless Networks...........................19, 61
Scene Action Event Type 140
Scene Configuration Menu 52
Scene Configuration Sequence...........................50
Scenes Submenus......................................139–40
Schedules Configuration Menu 54
Schedules Submenus...................................105–6
Sensor Configuration Menu 35
Sensor Options Submenus................................129
Sensor Options Table..132
Sensor Submenus 79–82
Sensor Types Presets Table 171
Sensor Types Submenus 125–27
Sensor Types Table...128
Set Up a Web Access Passcode...................19, 61
Set up Camera Ethernet/Wi Fi...........................161
Set Up Connections...15
SIA CP-01-2010 Programmable Features.........213
Specifications..208
Switch between Wi Fi or Ethernet modes............15
Switch connection to Ethernet 16
System Clock 71
System Configuration Menu 44
System Counts..78
System General Options.....................................72
System Service and Test Options 76
System Settings 31
System Siren Options 75
System Status...77
System Submenus..71–78
System Timers...73

T

Table Mount (Optional) 180
Test Sensor Signal Strength..............................174
Test the Battery...186
Test the Communicator 186
Test the Siren..186
Test, Walk Through 185
Testing the System 185
The UltraSync App..23
Time and Date 179
Troubleshooting Camera 170
Troubleshooting DLX900 195
Troubleshooting UltraSync Setup........................28
Troubleshooting WiFi Setup 21, 63

U

UL SPECIFICATION..209
UltraSync Color Codes 29
UltraSync Submenus...145
Use your device to connect to the panel 18, 60
User 1 Name...27
User 1 PIN 27
User Submenus 149–50
Users and Permissions......................................147
Using the UltraSync App.....................................24

V

View event triggered clips in History..................169
Viewing Cameras in UltraSync 65
Voice Annunciation 178
Voice Library Table..173
Volume Level 177

W

Wall Tamper Option...181
Warning on power connection 13
Web Access Passcode 27
Wi Fi Setup 18, 60

Z

Zwave Configuration Menu..................................59
Zwave Device Association...................................58
Zwave Maintenance...58