xGen Lite Installation and Programming Guide

P/N 466-5545-EN • REV C • ISS 08OCT19

Trademarks and patents

Interlogix, xGen Lite name and logo are trademarks of UTC Fire & Security Americas Corporation, Inc.

IOS is the registered trademark of Cisco Technology, Inc.

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

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

App Store is a service mark of Apple Inc.

Amazon, Alexa and all related logos are trademarks of Amazon.com, Inc. or its affiliates.

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

Manufacturer

Placed on the market by:
UTC Fire & Security Americas Corporation, Inc.
3211 Progress Drive, Lincolnton, NC, 28092, USA

Authorized EU manufacturing representative:
UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Netherlands

Product warnings and disclaimers

THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. UTC FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY “AUTHORIZED DEALER” OR “AUTHORIZED RESELLER”, IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS.

For more information on warranty disclaimers and product safety information, please check https://firesecurityproducts.com/policy/product-warning/ or scan the QR code.

Version

This document applies to xGen Lite version 000000

EU compliance

CE

Certification

EN 50131-1:2006 System requirements
EN 50131-3:2009 Control and indicating equipment
EN 50131-6:2017 Power Supplies
Security Grade 2, Environmental class II

EN 50136-2:2013 / EN 50131-10:2014

SP3, SP4 (IP or cellular); DP2, DP3 (IP and cellular)

Tested and certified by Telefication B.V.

Compliance labelling should be removed or adjusted if non-compliant configurations are selected.

Important: This product has not been designed to comply to EN 50134 and EN 54 norms.

EU directives

UTC Fire & Security hereby declares that this device is in compliance with the applicable requirements and provisions of all applicable rules and regulations, including but not limited to the Directive 2014/53/EU. For more information see: www.utcfssecurityproducts.eu

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

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

Contact information

www.utcfireandsecurity.com or www.interlogix.com

Customer support

www.utcfssecurityproducts.eu

Content

Important information

Limitation of liability

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

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

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

Product Warnings

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

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

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

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

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

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

DO NOT CONNECT TO A RECEPTACLE CONTROLLED BY A SWITCH.

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

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

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

Warranty Disclaimers

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

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

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

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

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

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

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

Disclaimer

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

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

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

Intended Use

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

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

Advisory messages

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

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

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

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

Introduction

The xGenLite is an advanced intrusion panel for protecting your home, business, and assets.

With large expansion capabilities, multi-area mode, wireless expansion, advanced user permissions, advanced schedules, and home automation features, the xGenLite suits most residential and small commercial applications.

The system can be quickly programmed using drop-down menus with commonly used defaults. Advanced customization is possible using the web server or DLX900 desktop software.

All zones, partitions, lists, groups, outputs, schedules, permission profiles, and defaults can be assigned a text name to make it easy to program and maintain.

The advanced user management system can be linked to complex schedules and automation events that dynamically change what users have access to in real-time based on system conditions. Zones can also behave differently based on different conditions.

The xGenLite intrusion panel is designed to be operated from the NXG-1820 touchscreen keypad. All menus appear as plain text on a clear 3.5 inch screen allowing access to all programming features.

System Capacity

Feature	NXG-4	NXG-8	NXG-9
On-board zones	4	8	8
Max Zones	4 hardwired 16 wireless	48	48
Partitions	4	8	8
Users	40	100	100
Max Keyfobs	8	16	16
Max Tablets	4	4	4
Max keypads	16	24	24
Max Expander Modules incl Keypads and Tablets	24	32	32
On-board outputs	3 OC, BELL	4 OC, BELL, Smoke	4 OC, BELL, Smoke
Event log (Events)	1024	1024	1024

xGenLite Specifications

Product Codes

Product	Description	EN grade
NXG-4	xGen Lite panel, 4 zones, 4 partitions, max. 16 zones, with IP on-board	2
NXG-4-RF	xGen Lite panel, 4 zones, 4 partitions, max. 16 zones, with IP and LoNa Receiver on-board	2
NXG-4-RF-Z	xGen Lite panel, 4 zones, 4 partitions, max. 16 zones, with IP, Zwave and LoNa Receiver on-board	2
NXG-8	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP on-board	2
NXG-8-CB	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP on-board, large metal housing	2
NXG-8-Z	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP and Zwave on-board	2
NXG-8-Z-CB	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP and Zwave on-board, large metal housing	2
NXG-9-LB	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP on-board, large poly housing	2
NXG-9-RF	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP and LoNa Receiver on-board, small poly housing	2
NXG-9-RF-LB	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP and LoNa Receiver on-board, large poly housing	2
NXG-9-RF-Z	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP, Zwave and LoNa Receiver on-board, small poly housing	2
NXG-9-RF-Z-LB	xGen Lite panel, 8 zones, 8 partitions, max. 48 zones, with IP, Zwave and LoNa Receiver on-board, large poly housing	2
NXG-4-BO	xGen Lite board, 4 zones, 4 partitions, max. 16 zones, with IP on-board	2
NXG-4-RF-BO	xGen Lite board, 4 zones, 4 partitions, max. 16 zones, with IP and LoNa Receiver on-board	2
NXG-4-RF-Z-BO	xGen Lite board, 4 zones, 4 partitions, max. 16 zones, with IP, Zwave and LoNa Receiver on-board	2
NXG-8-BO	xGen Lite board, 8 zones, 8 partitions, max. 48 zones, with IP on-board	2
NXG-8-Z-BO	xGen Lite board, 8 zones, 8 partitions, max. 48 zones, with IP and Zwave on-board	2
NXG-9-BO	xGen Lite board, 8 zones, 8 partitions, max. 48 zones, with IP on-board, for poly housing	2
NXG-9-RF-BO	xGen Lite board, 8 zones, 8 partitions, max. 48 zones, with IP and LoNa Receiver on-board, for poly housing	2
NXG-9-RF-Z-BO	xGen Lite board, 8 zones, 8 partitions, max. 48 zones, with IP, Zwave and LoNa Receiver on-board, for poly housing	2

Product	Description	EN grade
NXG-1820	3.5 inch Touchscreen keypad, multilingual	2/3
NXG-208-G3	8 zone expander	2/3
NXG-220-G3	20 zone expander	2/3
NXG-504	4 relay output expander	2/3
NXG-510	10 relay output expander	2/3
NXG-001	Plastic housing /w tamper switch	2
NXG-005	Pry-off tamper switch incl metal U-bracket	2/3
NXG-003	Housing /w tamper sw - Metal EN Grade 2	2
NXG-003-DIN	DIN-rail mounting kit	2/3
NXG-868	Wireless expander 868 MHz Gen 2	2
NXG-433	Wireless expander 433 MHz	2
NXG-7002(-SIM)	4G/wifi communication expander (- SIM includes SIM card)	2

Mains Power Specifications

Mains input voltage	230 VAC +10%, −15%, 50 Hz ±10%
Current consumption at 230 VAC	240 mA max.
Transformer output:	
NXG-4	16.3 VAC 35 VA
NXG-8	16.3 VAC 40 VA
NXG-9	16.3 VAC 40 VA

Installation Instructions for Service Persons

An appropriate disconnect device, to control the mains power to this device, is to be provided as part of building installation according to the local wiring rules.

Power Supply Specifications

Power supply type	EN 50131-6 Type A for indoor use inside the supervised premises
Power supply voltage	13.8 VDC ± 0.4 V
Power supply current	2 A max. at 13.8 VDC ± 0.4 V
Main board consumption:	
xGenLite	130 mA at 13.8 VDC ± 0.4 V
Maximum system current available:	
xGenLite	2000 mA at 13.8 VDC ± 0.4 V
Auxiliary power output (AUX. POWER):	
xGenLite	13.8 VDC ± 0.4 V, 1 A max.

Battery power output (BAT):	
NXG-4	13.8 VDC ± 0.2 V, 350 mA max.
NXG-8	13.8 VDC ± 0.2 V, 350 mA max.
NXG-9	13.8 VDC ± 0.2 V, 570 mA max.
Battery type	Lead acid rechargeable BS127N: 7.2 Ah 12 V nominal BS130N: 12 Ah 12 V nominal BS131N: 18 Ah 12 V nominal (NXG-8 only) **Note:** Use of the second battery is not compliant for EN installations.
Minimum voltage	9.45 VDC
Over-voltage threshold	16.3 VDC ± 5%
Maximum voltage at power supply, auxiliary power output and battery power output	14.5 VDC
Battery low condition	11.3 to 11.8 VDC
Battery disconnect voltage	9.77 VDC
Maximum ripple voltage V, p-p	200 mV typical, 400 mV max.

General Features

Code combinations:	
xGenLite	From 10,000 (4 digits) to 100,000,000 (8 digits)
Maximum user number:	
NXG-4	40
NXG-8, NXG-9	100
User Permissions:	
NXG-4	32
NXG-8, NXG-9	64
Onboard zones:	
NXG-4	4 (default); 8 if zone doubling enabled.
NXG-8, NXG-9	8 (default); 16 if zone doubling enabled.
Maximum zone number:	
NXG-4	16
NXG-8, NXG-9	48
Additional inputs:	
NXG-4, NXG-8	1: box tamper
NXG-9	2: box tampers
End-of-line resistor	820 Ω (2-wire smoke) 3.3 kΩ, 4.1 kΩ, 4.7 kΩ (alarm) 3.74 kΩ, 6.98 kΩ (zone doubling)

Onboard outputs:	
NXG-4	4: bell, strobe, siren and power outputs
NXG-8, NXG-9	5: bell, strobe, siren and power outputs
Maximum output number	32
Maximum action number	32
Partitions:	
NXG-4	4
NXG-8, NXG-9	8
Maximum keypad:	
NXG-4	16
NXG-8, NXG-9	24
Maximum expander modules, incl keypads:	
NXG-4	24
NXG-8, NXG-9	32
Non-volatile Memory	
Event log capacity	1024
Data retention (log, program settings)	10 years

Ethernet Connection (IP only)

Supported standard	IEEE 802.3u
Speed	10BASE-T or 100BASE-TX
Duplex	Half-duplex and full-duplex
Cabling	FTP (foiled twisted pair) Cat 5e cable or better

xGenLite Bus

Type	4 wire RS485 bus High common mode tolerance (25V)
Capacity	Up to 32 devices
Range	800m
Recommended Cable	Belden 7201A, 3107A or 9842, 2 pair twisted shielded data cable or exact equivalent (see “Cable Requirements” on page 18)

Current Consumption

Product	Main description	Current Consumption (non-alarm)	Current Consumption (alarm)
NXG-8, NXG-9	8 zone panel	130 mA typical	130 mA typical
NXG-4	4 zone panel	130 mA typical	130 mA typical
NXG-1820	Touchscreen keypad	100 mA typical, 40 mA in idle mode	175 mA max with sounder and screen on max brightness

Product	Main description	Current Consumption (non-alarm)	Current Consumption (alarm)
NXG-208-G3	8 zone expander	25 mA	25 mA
NXG-220-G3	20 zone expander	30 mA	30 mA
NXG-504	4 relay output expander	20 mA idle 70 mA 4 relays on	20 mA idle 70 mA 4 relays on
NXG-510	10 relay output expander	20 mA idle 160 mA 10 relays on	20 mA idle 160 mA 10 relays on

Output Current Rating

Output	Total Max Output Current		
	35 VA Transformer	40 VA Transformer	55 VA Transformer
Combined J2 BELL+, J2 AUX+ (Smoke), and J7 AUX+ (Outputs) Combined J2 POS (XR Bus), and J3 POS (NX Bus)	1.0 A max at 13.8 VDC	1.2 A max at 13.8 VDC	1.4 A max at 13.8 VDC

Auxiliary Current and Battery Capacity

xGen Lite (EMEA)

Discharge Time	Charge Time	7.2 Ah Battery	12 Ah Battery	18 Ah Battery	Reference
12 h	72 h	470 mA	870 mA	1370 mA	EN 50131 Grade 1 and 2
12 h	24 h	170 mA	370 mA	620 mA	INCERT

Note: Main board quiescent current is not included in the table above.

Example for EN Grade 2

When using battery backup as specified for EN Grade 2 using a 7.2 Ah battery, the maximum available auxiliary current is 470 mA.

Environmental

Operating temperature	−10 to +55°C
Humidity	95% non-condensing
IP protection grade	IP30
NXG-4, NXG-8 metal enclosure	EN 50131 Grade 2, Class II
NXG-9 polycarbonate enclosure	EN 50131 Grade 2, Class II
Alarm transmission class EN50136-2/EN 50131-10:	
Onboard IP	SP4 & DP4
Cellular	SP4 & DP4

NXG-1820 ACE classification	Type A

Physical Dimensions and Weight

Product	Main description	Dimensions (HxWxD)	Weight (g)
NXG-4(-RF)(-Z)	xGenLite /w metal enclosure	214 x 232 x 94 mm (enclosure only) 359 x 232 x 94 mm (with antennas)	1435 g
NXG-8(-Z)	NXG-8 /w standard metal enclosure	292 x 291 x 91 mm	2075 g
NXG-8(-Z)-CB	NXG-8 /w large metal enclosure	394 x 256 x 118 mm	7150 g
NXG-9-RF(-Z)	NXG-9 /w standard poly housing	220 x 253 x 112 mm	1800 g
NXG-9(-RF)(-Z)-LB	NXG-9 /w large poly housing	394 x 256 x 118 mm	2800 g
NXG-8(-Z)-BO	NXG-8, board only	273 x 89 x 25 mm	210 g
NXG-4(-RF)(-Z)-BO	NXG-4, board only	192 x 89 x 25 mm	155 g
NXG-9(-RF)(-Z)-BO	NXG-9, board only		210 g
NXG-001	Plastic Enclosure	371 x 371 x 118 mm	1830 g
NXG-003(-G3)	Metal Enclosure	475 x 395 x 130 mm	7150 g
NXG-1820	Touchscreen keypad	18 x 82 x 125 mm	150 g
NXG-208	8 zone expander	135 x 80 x 55 mm	150 g
NXG-220	20 zone expander	135 x 80 x 64 mm	180 g
NXG-504	4 relay output expander	135 x 80 x 55 mm	150 g
NXG-510	10 relay output expander	135 x 80 x 64 mm	180 g

Fuses

Battery	4 A, resettable
12 V aux (combined for J2 BELL+, J2 AUX+, J7 AUX+)	
xGen Lite 4	3 A, resettable
System LAN (combined for J2 POS, J3 POS)	
xGen Lite 4	2 A, resettable
Mains, mains fuse	500 mA, fast 20x5
Note: Mains fuse is part of the mains terminal block.	

Maintenance

No regular maintenance needed. System will report servicing when necessary.

System Monitoring

The system provides monitoring for the following items.

Monitoring function	Message	Cause
AC Mains	Mains fail	Loss of external power supply
Battery	Battery low	Battery low voltage
	Battery test fail	Exhausted battery
		Battery charger fail
	Fuse/power output fail	Output overload
Power outputs	Fuse/power output fail	Exhausted fuse
		Fuse loss
		Short circuit
		Overload
Power supply	Power unit/power output fail	Power unit failure
		Overvoltage
Tampers	Device tamper	Device sabotage

SIA and CID Reporting Code Descriptions

#	SIA code	CID code	Function
0	FA	E110	Fire Alarm
1	FR	R110	Fire Alarm Restore
2	PA	E120	24 Hour Alarm
3	PR	R120	24 Hour Alarm Restore
4	BA	E130	Burg Alarm
5	BR	R130	Burg Alarm Restore
6	*B	E570	Bypass
7	*U	R570	Bypass Restore
8	TA	E383	Tamper
9	TR	R383	Tamper Restore
10	*T	E380	Trouble
11	*R	R380	Trouble Restore
12	XT	E384	Sensor Low Battery
13	XR	R384	Sensor Low Battery Restore
14	*S	E381	Wireless Supervision
15	*R	R381	Wireless Supervision Restore
16	SS	E200	Fire Supervision
17	SR	R200	Fire Supervision Restore
18	NA	E391	Zone Activity Supervision

#	SIA code	CID code	Function
19	NS	R391	Zone Activity Supervision Restore
20	BG	E378	Cross Zone initial trip
21	BR	R378	Cross Zone initial trip Restore
22	AS	E389	Fire Maintenance Alarm
23	AN	R389	Fire Maintenance Alarm Restore
24	DL	E426	Door Propped
25	DH	R426	Door Propped
26	DF	E423	Door Forced
27	DR	R423	Door Forced
28	TP	E611	Start Walk test zone
29	TE	E389	End Zone Test
30	TP	E611	Walk test zone passed
31	TE	E389	Walk Test zone failed
32	TA	E383	Tamper (Anti-mask)
33	TR	R383	Tamper Restore (Anti-mask)
34	BA	E139	Burglary Alarm (Unverified)
35	BV	E130	Burglary Alarm (Verified)
36	HA	E129	Hold-up Alarm (Unverified)
37	HV	E120	Hold-up Alarm (Verified)
38	PA	E129	Panic Alarm (Unverified)
39	HV	E120	Panic Alarm (Verified)
64	FA	E115	Manual Fire
65	MA	E100	Manual Auxiliary
66	PA	E123	Manual Audible Panic
67	HA	E122	Manual Silent Panic
68	HA	E124	Duress
69	JA	E461	Keypad Lockout
70	TA	E137	Box Tamper
71	TR	R137	Box Tamper Restore
72	AT	E301	Mains Fail Event
73	AR	R301	Mains Fail Event Restore
74	YT	E302	Battery Low Event
75	YR	R302	Battery Low Event Restore
76	YI	E312	Over Current
77	YJ	R312	Over Current Restore
78	YA	E320	Siren Tamper
79	YH	R320	Siren Tamper Restore
80	LT	E351	Telephone Fault

#	SIA code	CID code	Function
81	LR	R351	Telephone Fault Restore
82	YC	E354	Communication Failure
83	YK	R354	Communication Failure Restore
84	ET	E333	Device Failure
85	ER	R333	Device Failure Restore
86	OP	E401	Open
87	CL	R401	Close
88	OP	E401	First Open
89	CL	R401	Last Close
90	CG	E451	Partial Close
91	EE	E374	Exit Error
92	CR	E459	Recent Close
93	AB	E406	Abort
94	OC	E406	Cancel
95	RP	E602	Automatic Test
96	RX	E601	Manual Test
97	JT	E625	Clock Changed
98	LB	E627	Start Local Program
99	LX	E628	End Local Program
100	RB	E627	Start Remote Program
101	RS	E628	End Remote Program
102	TS	E607	Start Walk Test Mode
103	TE	R607	End Walk Test Mode
104		E466	Technician Arrival
105	YZ	R466	Technician Left
106	FT	E310	Ground Fault
107	FR	R310	Ground Fault Restore
108	LF	E606	Start Listen In
109	LE	R606	End Listen In
110	OK	E451	Early Opening (Disarmed before Opening window)
111	CJ	R452	Late Closing (Armed after the Opening Window)
112	OI	E453	Fail to Open
113	CI	E454	Fail To Close
114	XQ	E344	Wireless Jam
115	XH	R344	Wireless Jam Restore
116		E414	System Shut Down
117	RR	R414	System Turn On
118	RC	E323	Output Activated

#	SIA code	CID code	Function
119	RO	R323	Output Restored
120	SC	E531	Device Enrolled
121	DG	E422	User Activated Output
122	DG	E422	Door Access
123	DV	E421	Door Access Denied
124	YW	E305	Watchdog Reset
125	OP	R451	Partial Open
126	BC	E401	Abort Alarm
127	JK	E102	Guard Tour Fail
128	NA	E641	Activity Monitor Fail
129	DG	E422	Valid Code Entered
130	DP	E421	Valid Code Out Of Schedule
131	DV	E421	Valid Code Void
132	DV	E421	Valid Code Lost
133	DV	E421	Valid Code Expired
134	RU	E628	Remote Program End
135	CL	E102	Man Down
136	RR	E305	Power Up
137	RR	R305	Power Up Restore
138	RX	R601	Manual Test Restore
139	OJ	E452	Late Opening
140	CK	R451	Early Closing
141	UB	E532	Device Bypass
142	UU	E531	Device Unbypass
143	YF	E304	Checksum Failure Failure
144	YG	R304	Checksum Failure Restore
145	YT	E338	Expander Low Battery
146	YR	R338	Checksum Failure Restore
147	YT	E337	DC Fail
148	YR	R337	DC Fail Restore
149		E609	Video Event
150	LT	E351	IP Path Fault
151	LR	R351	IP Path Fault Restore
152		E458	Geofence1 Entered
153		R458	Geofence1 Exited
154		E458	Geofence2 Entered
155		R458	Geofence2 Exited
156	YP	R351	Power Supply Fault

#	SIA code	CID code	Function
157	YQ	R351	Power Supply Restore

EN 50131-3 and EN 50136-2 Compliancy

In order to be compliant with the technical specification EN 50131-3 (Alarm systems – Control and indicating equipment), the following guidelines must be taken into account:

- The tamper of the warning device should be connected to a 24-hour zone input.
- Overriding is not supported with xGenLite. In case a zone is faulted, one shall bypass the zone manually before arming or verify the zone and clear the fault. See user instructions.
- Hold-up zones are not allowed to be set for bypass.
- Zone isolation is not supported.
- EN 50136-2 (Alarm transmission systems and equipment – Part 2: Requirements for Supervised Premises Transceiver (SPT):

  - Upon configuring alarm transmission path and remote connection details, default user/installer keys shall be changed.

  - Minimum PIN length is 6 digits.

Options Affected by EN 50131 Regulations

EN 50131 Grade 2 Required settings

The following options and values are mandatory for EN 50131-1 Grade 2 regulations.

- Period, 24 h for every path to meet ATS Class 2, 4 h for the IP path to meet Class 4.
- View Areas and Control Areas settings are identical
- Buzzer silent, never
- Quick set, off
- Function keys, all set to None
- User group options, 25. No OP/CL reports option set to No
- Inhibit, set to No for all zones with type 5. Panic, 6. 24H
- Swinger shunt, set to Yes for all zones
- ACK on keypad, set to None for all zones with type 9. Keyswitch
- Entry time, 45 s maximum
- Entry alarms, Instant
- Active, set to No for all schedules.
- Activation, internal and external siren 90 to 900 s
- Delay time, external siren 600 s maximum
- Armed display, 30 s maximum

- Mains reporting delay, 3600 s maximum
- User code required, enabled
- Armed display, always
- Alarm list, disabled
- Inhibit includes, all allowed except engineer reset, which must be disabled
- Pending alarms, enabled
- Swinger shunt ≥ 3
- Report restore, on ACK
- Line fault, enabled per path used
- Line fault delay, 0 s

Refer to xGenLite Reference Manual for additional features, accessible at level 3.

For EN 50131-3 & T031, it is required to apply the following supervision settings for wireless expanders:

- Short supervision: 20 minutes
- Long supervision: 2 hours
- Smoke supervision: 4 hours

Caution: When any option, any additional function or any additional zone type in this section does not comply with the EN 50131 requirements, the EN 50131 compliance label must be removed from the system.

Optional Functions

- Detection of storage device – failure
- Detection of low output voltage

EN 50131 Compliance Precautions

Installation

In order to install an EN 50131 compliant system, please make sure that all system components are EN 50131 compliant.

Programming

Make sure that all system settings are in line with regulatory compliance guidelines.

Size of log / event history

For full EN 50131 Grade 2 compliance, the system must store at least 500 events.

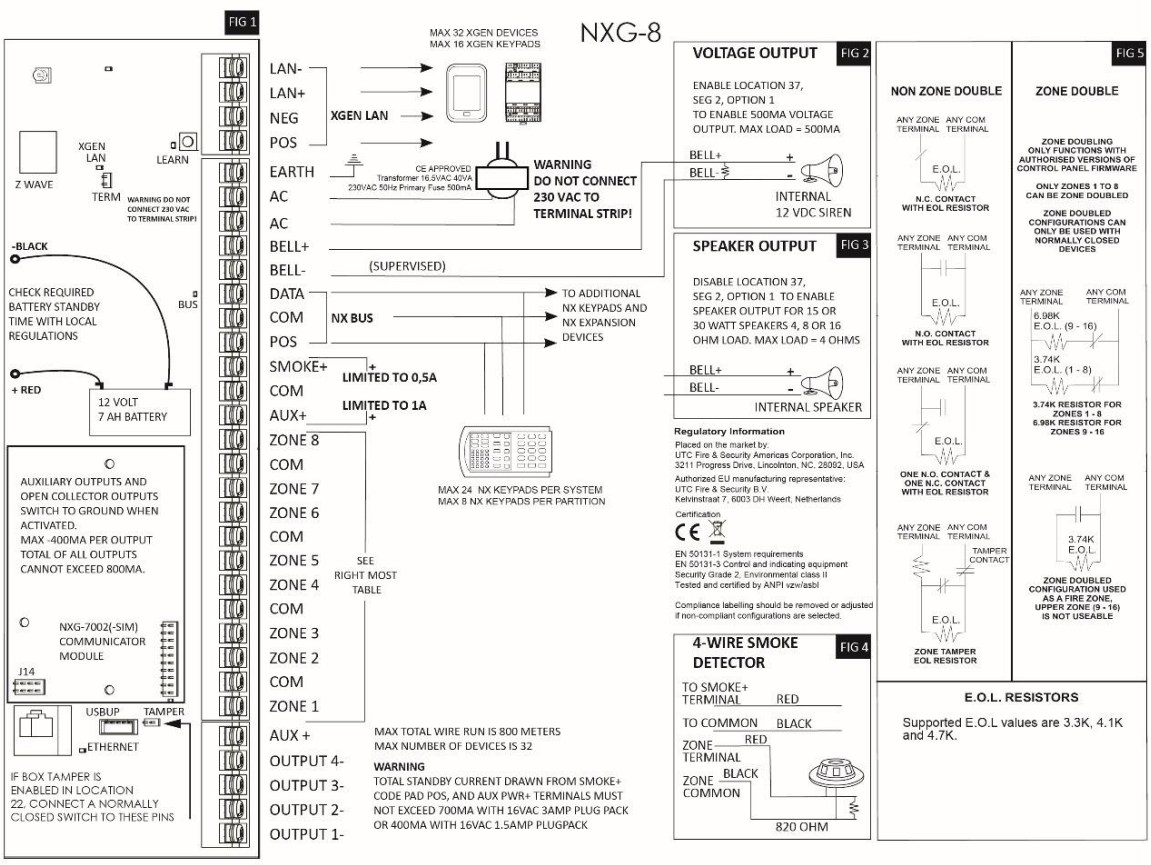
Marking

It is only allowed to mark the system with the EN 50131 compliance label, if the following requirements are met:

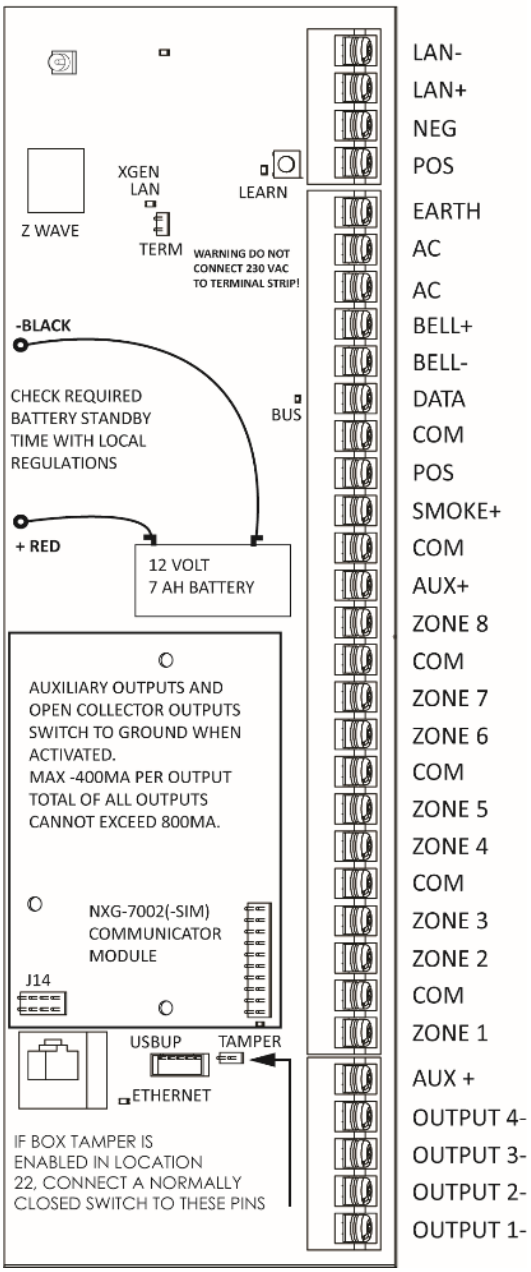
- All system components are EN 50131 compliant.
- All settings are done according to EN 50131.

If any of these two items is not valid, the EN 50131 compliance label must be removed from the system.

NXG-8 Wiring Diagram



NXG-8 Terminals



Top to bottom:

LAN-, LAN+, NEG, POS: Terminals for xGenLite RS485 bus.

LEARN: Enrollment button, hold down for 3 s to activate automatic device enrollment feature.

TERM: Term link for xGenLite RS485 bus. A TERM link should be installed on the two furthest devices.

EARTH, AC, AC: Connect transformer (16 VAC 1.5 A) to terminals for power.

−BLACK, +RED: Connect leads to 12V Sealed Lead Acid backup battery.

BELL+, BELL−: Connect to external 12V siren or internal piezo screamer.

DATA, COM, POS: NetworX 3-wire bus for legacy modules and keypads.

SMOKE-, AUX+: Two or four wire smoke detectors, NXG-8 supports two wire smoke detectors and will drop power to the SMOKE- terminal to perform smoke alarm verification.

COM, AUX+: Terminal for aux power to zones.

ZONE 1 to 8, COM – terminals to connect to zones. Supports single EOL, zone doubling, and dual EOL tamper monitoring.

J14: Ethernet WAN link header must be fitted if no communicator module is installed, and must be removed to accommodate communicator module.

J11: Terminal to connect communicator module to xGenLite.

Ethernet: Connect Ethernet cable to RJ45 socket to provide internet connectivity to xGenLite.

J13: 5-pin connector used to upgrade and program xGenLite with USBUP tool.

TAMPER: Connect to panel box tamper.

AUX+: Terminal for auxiliary power to outputs.

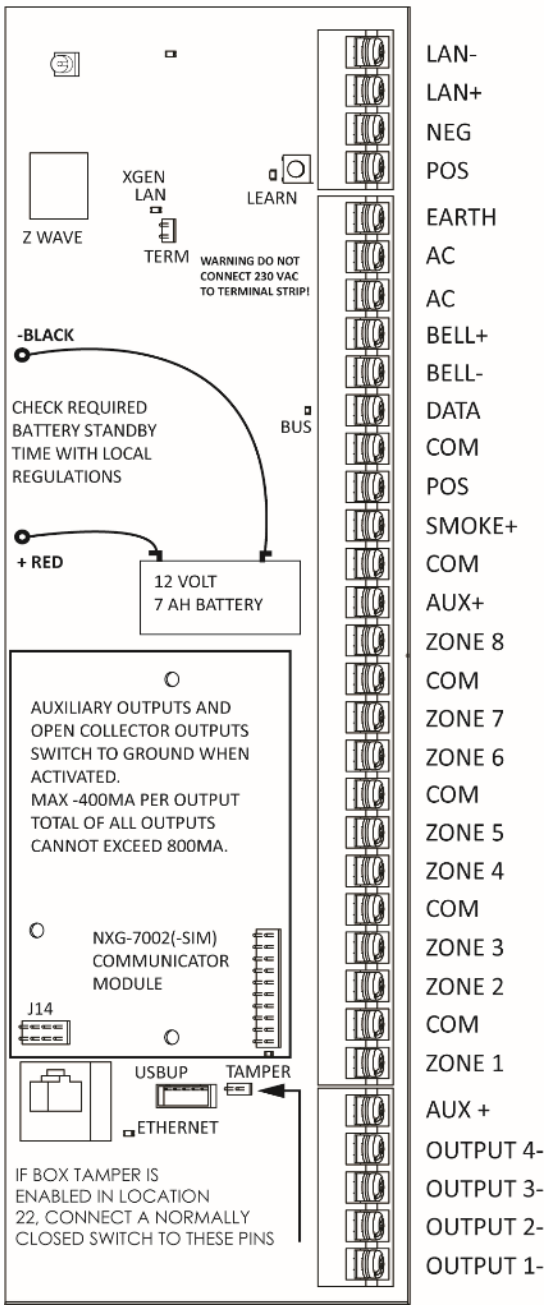
OUTPUT 4: Open collector output switches to ground, follows armed state at default.

OUTPUT 3: Open collector output switches to ground, follows ready state at default.

OUTPUT 2: Open collector output switches to ground, follows siren state at default.

OUTPUT 1: Open collector output switches to ground, follows strobe state at default.

NXG-8 LEDs



Top to bottom:

D7 LAN: Green LED is lit when connected to UltraSync, remains off when not connected to UltraSync.

D4 LEARN: Red LED blinks slowly during auto enrollment, blinks quickly during manual enrollment.

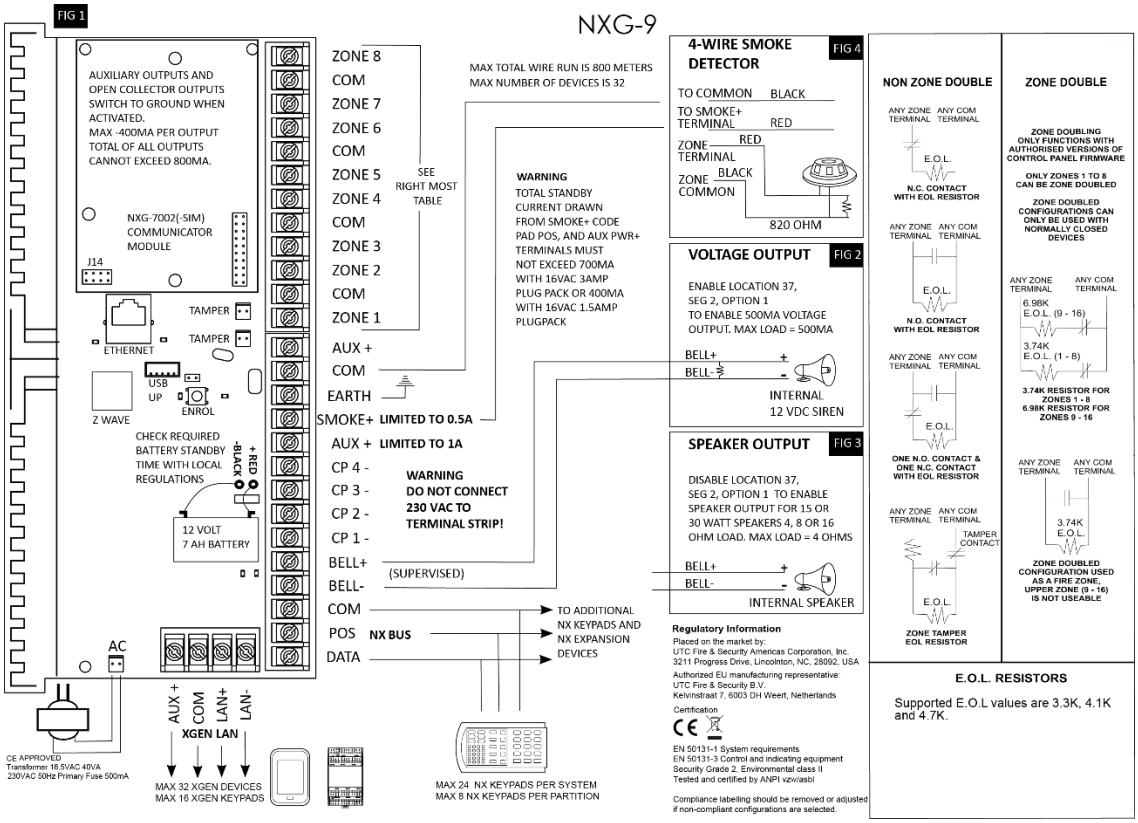
D3 BUS: Red LED blinks to indicate xGenLite bus is available.

D1 ETHERNET: Red LED is lit when Ethernet cable is connected to WAN port, blinks when data is sent or received, and is off when cable is disconnected or J14 connector is removed.

If 4G / WiFi router module is installed, LED is lit when panel has established connection to the module, and blinks when panel is communicating with the module.

Check “Connection Status” web page to verify connection to UltraSync.

NXG-9 Wiring Diagram



Refer to “NXG-8 Wiring Diagram” on page 14. The NXG-9 unit functionality is the same the NXG-8 except that the connections are spatially orientated differently.

NXG-9 Terminals

Refer to “NXG-8 Terminals” on page 15. The NXG-9 unit functionality is the same the NXG-8 except that the connections are spatially orientated differently.

NXG-9 LEDs

Refer to “NXG-8 LEDs” on page 16. The NXG-9 unit functionality is the same the NXG-8 except that the LEDs are spatially orientated differently.

Detector EOL Wiring

Other than the 3K3 end-of-line resistor support, the xGenLite Grade 2 panels support the following end-of-line resistor value combinations in ohm (*):

Combination	A	B	C
Tamper (short)	0	0	0
Normal	3.3 kΩ	4.7 kΩ	4.1 kΩ
Alarm	6.6 kΩ	9.4 kΩ	8.2 kΩ
Tamper (open)	∞	∞	∞

(*) Refer to the detector installation manual for EOL values and wiring instructions.

Power Requirements

The xGenLite intrusion panel family is designed to be used with a 16 VAC 1.5 A, 35 or 40 VA transformer which is included with xGenLite panel kits. This transformer includes a 500 mA 250 VAC fast blow replaceable fuse on the terminal block. If more current is required, add NXG-320 Smart Bus Power Supplies.

Cable Requirements

The system RS-485 communication bus is used to connect keypads and in- and output expanders to the xGenLite intrusion panel.

- Belden 7201A, 3107A or 9842 cable is recommended.

  Cable must provide:
  >= 13 twists per metre or >= 4 twists per foot,
  <= 52 pF per metre or <= 16 pF per foot,
  and characteristic impedance 100 to 120 Ω.
- 800 m total cable run on system.
- Max. 800 m from remote device to xGenLite control panel.
- Max. 32 devices plus panel.
- Max. 16 keypads, as part of the 32 device limit.

Grounding

All devices designed for the system have earth connections via metal studs to the metal housing. Make sure that these metal studs make good connection to the housing (beware of paint). The earth connections of every piece of equipment in the system can be used for connecting the screen of shielded cables.
If a device is placed in a plastic housing the earth lug of the device does not have to be connected.

In one building several cabinets or devices are earthed to a safety ground. The safety ground for the building must be checked by a licensed contractor.

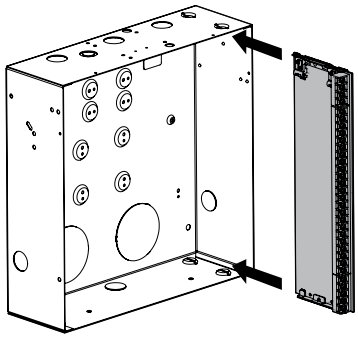
Shielding

The shielding of all shielded cables used in the system should only be connected at one side to one common earthing point in a building. If a shielded LAN cable is routed via more than one plastic device the shielding from incoming and outgoing cable must be connected.

Termination Links

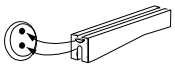
Put a jumper across TERM on the panel and the furthest device to ensure correct RS-485 termination and avoid communication issues with signal reflection, etc.

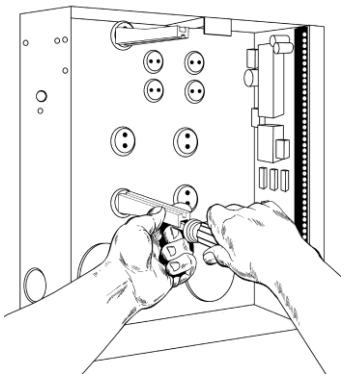
Installing Panel

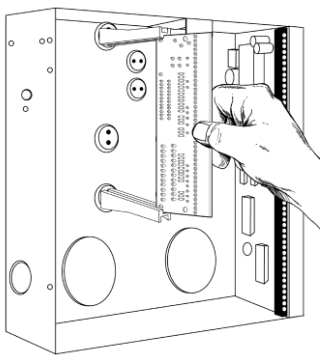


1. The xGenLite should be located away from damp areas (e.g. bathrooms, kitchens), away from sources of heat, dust or interference (e.g. air conditioners, washing machines, dryers, refrigerators) and away from external walls.
2. The metal enclosure should be installed with the door opening from the top to bottom.
3. Guides are cut into the enclosure to hold the panel, two on the top and two on the bottom. Two plastic brackets are pre-installed on the xGenLite. Slide the panel into the guides as shown in the diagram. The terminal strip should face towards you once installed.
4. A plastic strap is provided to allow the door to form a temporary surface to hold light parts.

Installing Legacy NX Modules







Inside the enclosure there are several 2-holed insertion points. These allows for either vertical or horizontal placement of legacy NX modules. Each insertion point has a larger hole and a smaller hole.

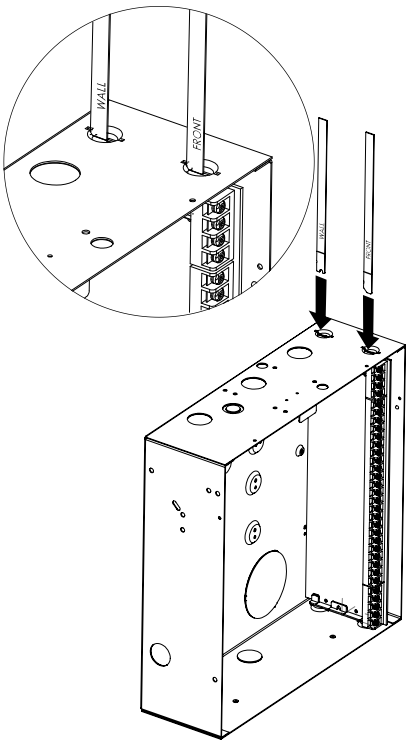
1. The black plastic PCB guides feature a groove to hold an expansion module. The end with the half-moon protrusion fits into the larger hole. The smaller hole is for the screw.
2. Place the first black plastic PCB guide in the top insertion point, groove facing downward. The half-moon protrusion will be in the large hole. It does not require force to insert. Insert one of the provided screws into the smaller hole (from inside the enclosure) to secure it in place. A screwdriver should reach through the groove that runs the length of the guide to tighten the screw. The second PCB guide should be positioned opposite the first (groove facing up) and placed in the lower insertion point, using the same procedures described above. Once mounted, screw it in securely.
3. The NX module should slide freely in the grooves of both guides.

Installing Antennas

A number of antennas may be provided depending on the model purchased. These include:

- Multi-antennas for legacy 433 63-bit, LoNa 80plus and Z-Wave
- 3G/4G antennas for WiFi/cellular module
- WiFi antennas for WiFi/cellular module

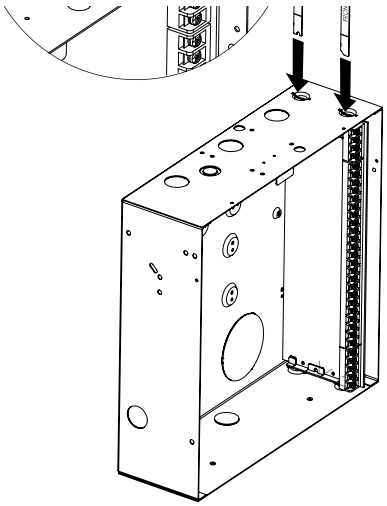
Wireless Sensor and Z-Wave Antennas



If two black antennas have been provided:

1. Install panel into metal enclosure first.
2. Antenna must be installed vertically for best performance.
3. Each antenna is keyed (shaped differently) and labelled. Antennas are reasonably flexible, do not apply excessive force. Match the antenna to the shape molded on the plastic bracket and push to insert.
4. The line printed on each antenna will disappear when fully inserted.
5. Remove antennas before attempting to remove panel.

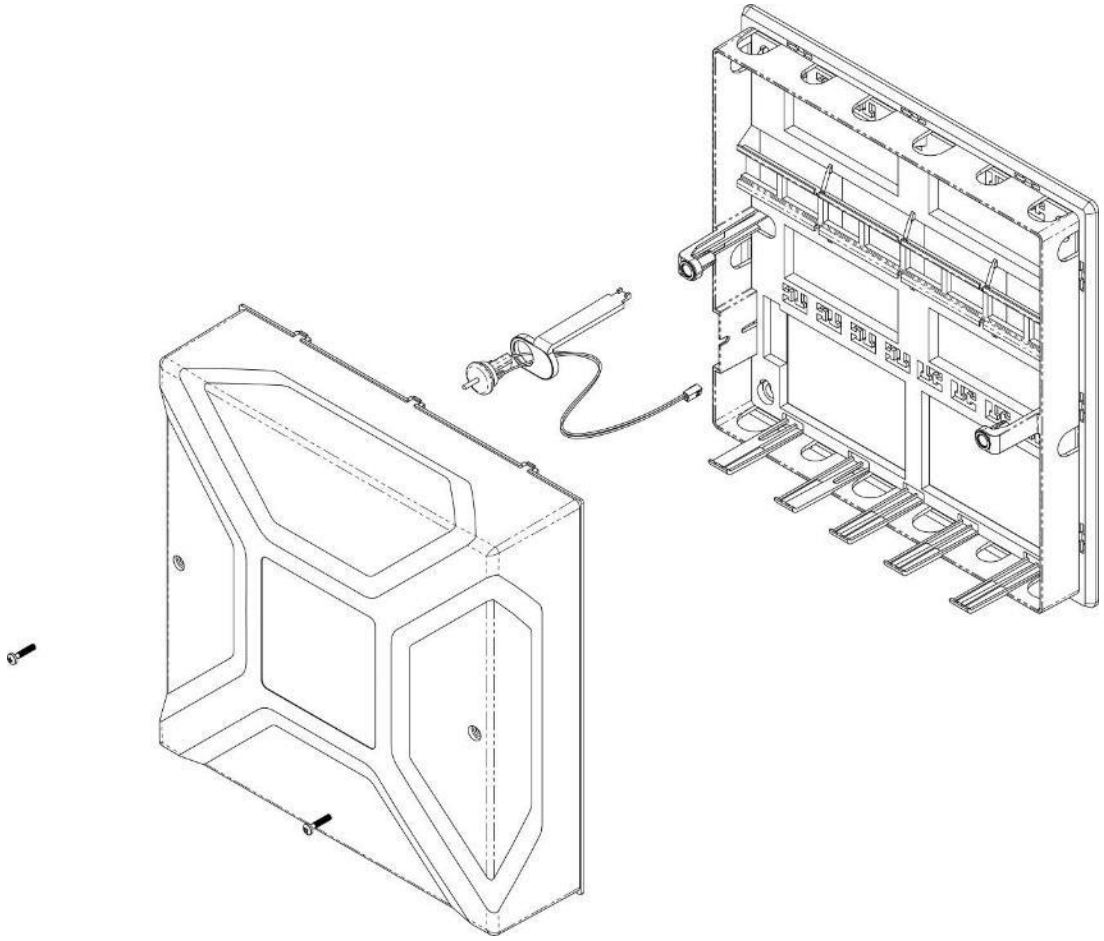
4G Cellular and WiFi Router Module Antennas



If the optional 4G Cellular and WiFi Router has been installed, a single set of antennas should be connected to “MAIN” on the module. The antennas should be installed vertically, and as high up as possible.

The module includes MIMO wireless technology to improve reception of 3G/4G and WiFi wireless signals. This requires the installation of a second set of antennas to “DIV” on the 4G/WiFi Router Module. The second set of antennas will perform best when separated from the MAIN antennas by at least 20 cm.

NXG-001 Plastic Enclosure



The NXG-001 features a DIN rail for mounting xGenLite modules, a tamper switch, and integrated cable management.

The enclosure should be installed in accordance with EN 50131-1 Environmental Class II to provide operating conditions within:

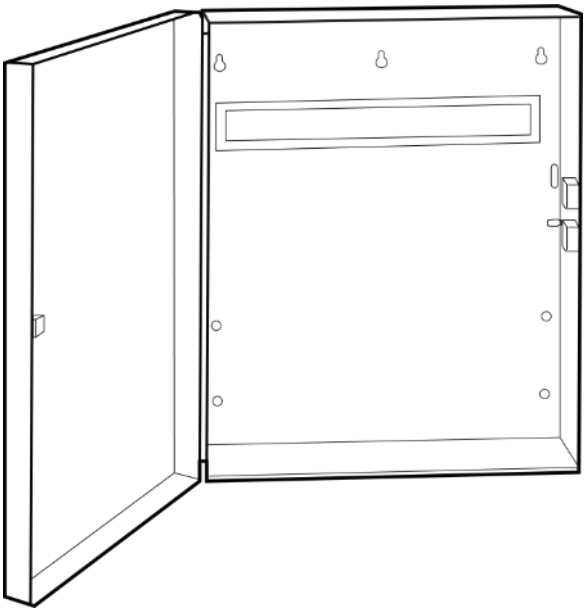
- Temperature range: −10 to +55°C.
- Humidity range: Average 93% relative humidity, noncondensing

The lid can be removed by releasing the two screws using the supplied Allen key.

Refer to drilling template provided with enclosure for mounting instructions.

To install a module, release the locking tab(s) and place on the DIN rail then push the locking tab(s) to secure the module. To remove a module, use a small flat-blade screwdriver to release the locking tab(s) on the xGenLite module then remove from the DIN rail. Refer to module installation manual for further details.

NXG-003 xGen Metal Enclosure



A spare metal enclosure is available for those installations where additional xGen zone and/or output expanders are required or in case a larger backup battery is required. The xGen NXG-003 metal enclosure includes a tamper switch and one metal DIN rail. A second metal DIN rail (NXG-003-DIN) can be added if required but in that case a backup battery of max 12 VDC / 7 Ah will fit the enclosure.

The enclosure should be installed in accordance with EN 50131-1 Environmental Class II to provide operating conditions within:

- Temperature range: −10 to +55°C.
- Humidity range: Average 93% relative humidity, non-condensing

To install a module, release the locking tab(s) and place on the DIN rail then push the locking tab(s) to secure the module. To remove a module, use a small flat-blade screwdriver to release the locking tab(s) on the xGen module then remove from the DIN rail. Refer to module installation manual for further details.

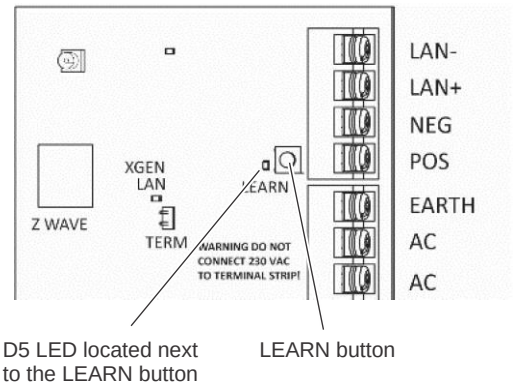
Enrolling Modules

New devices such as zone expanders, wireless zone expanders, output expanders, smart power supplies, and keypads need to be enrolled so they can be programmed and supervised.

The enrollment procedure discovers the serial number of the new device and adds it to the device database in the panel.

To enroll a module:

1. Press and hold the LEARN button until the LED next to the button blinks, then release button.



2. The panel is now in automatic enrollment mode and will search for new devices.
3. The D5 LED will stop blinking to indicate enrollment mode is finished.
4. Proceed to programming the system and the additional devices.

Enrollment can also be initiated:

- Using the NXG-1820 keypad: press Menu, Installer PIN, ENTER, go to Program > Devices > System Devices > Control > Enroll Function – 0 = Inactive – Automatic Enroll.
- Using the xGenLite Web Server: click the Advanced Menu, go to Devices > System > Control > Enroll Function > Automatic Enroll, click Save.
- Using DLX900: click Devices > Device Info > Auto Enroll.

Deleting Modules

Devices such as zone expanders, output expanders, and keypads can be removed from the system by deleting the serial number from the device database.

To delete a module:

1. On the keypad press Menu, Installer PIN, ENTER, go to Program > Devices.

   This menu will be displayed:

   1. System Devices
      1. Control
      2. Keypad
      3. Zone Exp
      4. Output Exp
      5. Power Supply

2. Interlogix Transmitters
    1. Transmitter Number
    2. Serial Number
    3. User
    4. Options
    5. Scene
3. Tablet Keypads
    1. Name
    2. Serial Number
    3. Area Group
    4. Keypad Options

2. Select the category and type. For example, to remove a keypad, touch System Devices > Keypad.
3. Touch Device UID (Serial).
4. Touch the serial number displayed.
5. Touch Clear.
6. Touch OK.

The device has now been removed.

Deleting devices can also be done:

- Using the xGenLite Web Server: click the Advanced Menu, click Devices, find the device to be removed, delete the serial number, click Save.
- Using DLX900: click Devices > Device Info, select the device, then click “Remove Device”.

Arming and Disarming Your System

You may arm and disarm partitions from a NXG-1820 keypad.

Only users with an authorized user code (Level 2 user) will be allowed to use the xGen alarm system. Users with no valid user code (Level 1 user) do not have access as defined by EN 50131-3.

Keypress Tamper

The NXG-1820 keypad will be locked in screensaver mode when unused for a preset time. This stops unauthorized users from interacting with the system or viewing detailed status.

A valid PIN is required to unlock the screen and access the system. Users can set PIN codes between 4 and 8 digits in length.

Note: EN 50131 Grade 2 required settings – There are no disallowed account codes. 5 digits minimum to provide 10,000 possible combinations.

Lock Out on 3 Invalid Attempts

If an invalid PIN code is entered three times, the keypad will deny all login attempts for 90 seconds. Attempts are counted from any method (e.g. keypad, app, or web page). You must wait the full 90 seconds before trying again with the correct PIN. This is to prevent brute-force attacks on guessing PIN codes.

Arm Your System in Away Mode

Enter a valid PIN code to unlock the screen.

Touch the Away or Away + button to arm your system in Away mode:

The icon will change to red when the alarm system is set in away mode.

If your system has multi-Partition control enabled, the Away + button will be displayed.

A valid PIN code will need to be entered to determine what permissions they have, this includes which Partitions and at what time/day that user has access.

Arm Your System in Stay Mode

Enter a valid PIN code with Stay permissions to unlock the screen.

Touch the Stay or Stay + button to arm your system in Stay mode:

The icon will change to yellow when alarm system is set in Stay mode.

If your system has multi-Partition control enabled, the Stay + button will be displayed.

A valid PIN code will need to be entered to determine what permissions they have, this includes which Partitions and at what time/day that user has access.

Arm Your System in Instant Stay Mode

Enter a valid PIN code with Stay permissions to unlock the screen.

To arm in Instant Stay mode touch the Stay button two times until the icon is red and displays “Instant”:

This indicates the alarm system is set in Instant Stay Mode.

Arm Your System in Night Mode

Enter a valid PIN code with Stay permissions to unlock the screen.

To arm in Night Mode touch the Stay or Stay + button a total of three times until the icon is red and displays “Night Mode”:

Touching the Night Mode button again will cycle the system back to Stay Mode.

Disarm One or More Partitions

Touch the Off or Off + button to disarm your system:

If your system has multi-Partition control enabled, the Off + button will be displayed.

A valid PIN code will need to be entered to determine what permissions they have, this includes which Partitions and at what time/day that user has access.

Activate SOS Feature

Touch the SOS button to display the SOS feature:

On this screen touch and hold the appropriate button for 2 seconds to activate Manual Fire Alarm, Manual Medical Alarm, or Manual Panic Alarm.

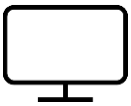
Depending on how your system is programmed, the control room may receive the corresponding event. Check with your control room to determine what action will be taken.

If silent alarm is enabled, then the keypad will not display any signs that the panic button was pressed.

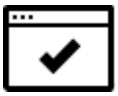
To cancel a SOS alarm – return to the home screen, touch the Status button and turn the Partition off.

Programming Methods

Once your devices have been cabled and installed, there are four (4) ways to access and program your xGenLite system:



Method 1: Via DLX900 Management Software – All features can be programmed using a PC with Microsoft Windows 7, 8 and 10. DLX900 allows easier programming of complex sites as the graphical interface can show all options from multiple menus simultaneously.



Method 2: Via a built-in Web Server – All features can be accessed from a web browser via drop-down and click-through menus. No software installation is required. This allows access to most commonly accessed features for basic programming or minor changes.

Method 3: Via UltraSync+ app – this provides access to the built-in Web Server via a smartphone app. A camera setup “wizard” is also included. Camera footage is only viewable by using the app.

Method 4: Via on-site keypad – The NXG-1820 touchscreen offers a programming menu allowing full system configuration. Refer to the NXG-1820 Installation Manual. The xGenLite Reference Guide will also assist you in navigating the menus.

Account Access

Note: Installer Account Disabled When Armed

If a non-engineer account arms the system at any time, engineer accounts will not be able to log in, any current program mode will end, and this will be recorded in the event log. Ask the end-user to disarm the panel and leave it disarmed so you can log in to program it.

Note: Remote Access May Require Level 2 User Authorization

Two remote access features “Enable Web Program” and “Always Allow DLX900” require an authorized master (Level 2) user to enter their PIN code on a NXG-1820 keypad before remote programming can be performed.

If either “Enable Web Program” or “Always Allow DLX900” have been disabled, ask a Master User to press Menu, enter their PIN code on a keypad, then Settings. The panel will now be in Program Mode and you can use an engineer (Level 3) user such as “installer” to perform programming via the web page, app, or DLX900.

Method 1: DLX900 Management Software

DLX900 is an ideal tool for programming xGenLite systems. This software is installed on a PC with Microsoft Windows 7, 8, or 10. It features a graphical interface, allowing installers and Central Monitoring Stations to program and manage complex sites. Customer details and all panel programming are stored in a local database.

DLX900 supports a variety of connection methods:

- Direct connection over LAN
- Remote connection over UltraSync (includes LAN or cellular)
- Remote connection over dial-up PSTN

Connect to xGenLite using DLX900 on LAN

1. Turn on power to your system
2. Connect an Ethernet cable to the J13 Ethernet port on the xGenLite and wait 10 seconds for the local router to assign the xGenLite an IP address if DHCP is available.
3. On the keypad press Menu, PIN, ENTER, go to Installer > Communicator > IP Configuration > IP Address and note the IP address displayed.
4. Install DLX900 on a suitable computer.
5. Start DLX900.
6. Create a new customer.
7. Enter the IP address of your system.
8. Click Save.
9. Click Connect via TCP/IP.
10. Click Read All.
11. Refer to “Programming with DLX900” on page 94.

Connect to xGenLite using DLX900 on UltraSync

In order for DLX900 to connect to an xGenLite system you will need the Download Access Passcode (under Communicator\Remote Access menu) and the xGenLite unit must be enabled to allow remote connections (under Communicator\IP Config).

1. Install DLX900 on a suitable computer, refer to DLX900 installation instructions.
2. Start DLX900.
3. Create a new customer.
4. Enter the serial number, Download Access Passcode and Web Access Passcode of the system.
5. Click Save.
6. Click Connect via TCP/IP.
7. Click Read All.
8. Refer to “Programming with DLX900” on page 94.

Connect to xGenLite using DLX900 on Dial-up

1. Install DLX900 on a suitable computer, refer to DLX900 installation instructions.
2. Start DLX900.
3. Create a new customer.
4. Enter the Download Access Passcode of the system.
5. Click Save.
6. Click Connect via Dial-up.
7. Click Read All.
8. Refer to “Programming with DLX900” on page 94.

Method 2: Web Server

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

- Simple forms to set up most commonly used features
- View system and zone status
- Arm and disarm partitions
- Bypass/Un-bypass zones
- Turn chime mode on and off
- Add, remove and edit users
- Access to the advanced programming menu

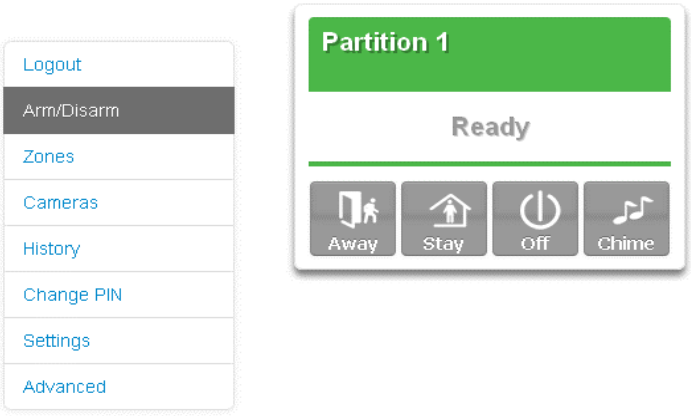
Connect to xGenLite Web Server over LAN

1. Turn on power to your system
2. Connect an Ethernet cable to the J13 Ethernet port on the xGenLite and wait 10 seconds for the local router to assign the xGenLite an IP address if DHCP is available.
3. On the keypad press Menu, PIN, ENTER, go to Installer > Communicator > IP Configuration > IP Address and note the IP address displayed.
4. Open your web browser
5. Enter the IP address from step 3 and the xGenLite login screen should appear. Some browsers may require you to enter **http://**

6. Enter your username and password, by default this is **installer** and **9713**.

   Note: On EN Grade 2 panels all PIN codes are 6 digits, use installer 971300.

You should now see a screen similar to:



Troubleshooting

If you are unable to get an IP address in step 3, then your (wireless) router may not be configured for automatic DHCP or certain security settings may be enabled.

- Check your router settings and try again.
- On a NXG-820 touchscreen keypad press Menu, PIN, ENTER, go to Installer > Communicator > IP Configuration > IP Options. “Enable DHCP” should be ticked, “Disable Web Pages on LAN” should be unticked.

Check LAN Connection to UltraSync

UltraSync is a cloud-based service that allows remote management and remote access to a xGenLite system if enabled. This includes secure connections between the UltraSync+ app, xGenLite, and cameras. No programming, email addresses, user names, or PIN codes are stored on these servers for greater security.

It features full redundancy to route encrypted alarm messages from your panel to a Central Monitoring Station.

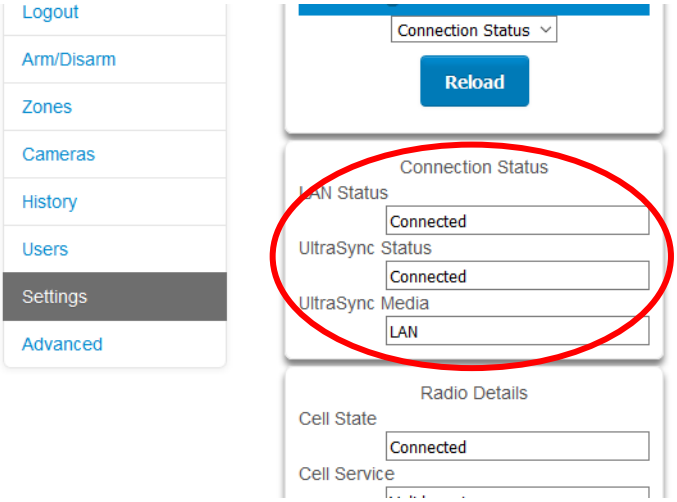
1. Log in to the Web Server as shown above
2. Click Settings
3. Select Connection Status in the drop-down menu
4. Check:

   - LAN Status should display “Connected”

   - UltraSync Status should display “Connected”

   - UltraSync Media should display “LAN” for Ethernet and “dual-path” for dual path

   - UltraSync Media should display “Cellular” for single-path cellular



If it does not:

1. Check cable connection.
2. Check router settings.
3. On the NXG-1820 touchscreen keypad press Menu, PIN, ENTER, go to Installer > Communicator > IP Configuration > IP Options. “Enable UltraSync” should be ticked.

Connect to xGenLite via 4G Cellular and WiFi Router Module

Note: Dual path is only available if the panel Ethernet reporting and the cellular module reporting are used.

An optional 4G Cellular and WiFi Router Module provides dual-path reporting over WiFi/Ethernet and 4G. If the primary path (WiFi/Ethernet) is not working, the module will switch to 4G back-up reporting path to the central monitoring station. Multiple 4G networks are supported using dual-SIM cards for further redundancy.

Alternatively, the module can be set by the central monitoring station to use 4G single path reporting. This is useful for sites with no broadband internet.

The module is pre-configured. Once installed on the xGenLite panel, it will automatically register on available mobile network(s). Refer to the 4G Cellular and WiFi Router Module manual for further details.

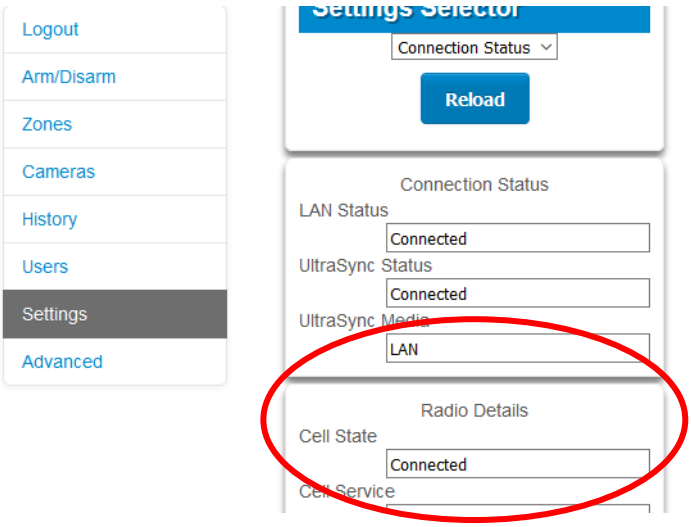
Check 4G connection to UltraSync

1. Log in to the Web Server as shown above.
2. Click Settings.
3. Select Connection Status in the drop-down menu.
4. Check:

   - UltraSync Status should display “Connected”.

   - Cell Service should display “Valid service”.

- Signal Strength should display a value. Check your cellular radio manual for acceptable values.



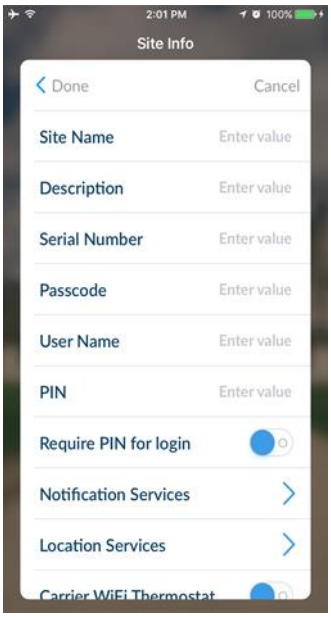
If it does not, check the 4G connection:

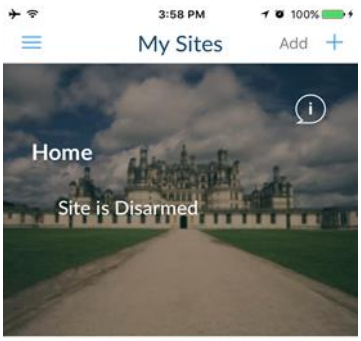
1. Check Settings > Network > Enable UltraSync is checked.
2. Alternatively from a keypad press MENU, go to Program > Communicator > IP Configuration > IP Options > Enable UltraSync: Y.
3. Look at Cell State, it should display “Connected”. Please wait until Cell State displays “Connected”, click Reload to refresh the status.

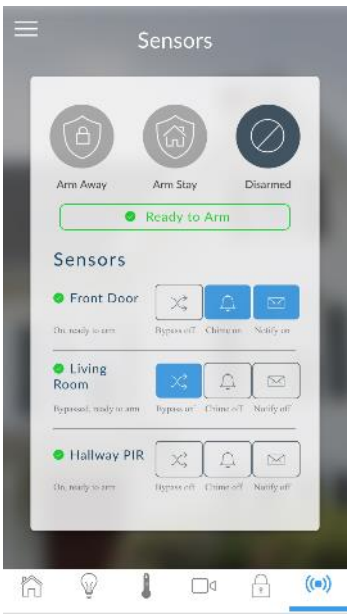
   Signal level should be between −89 to −51.
4. Check module is correctly installed.
5. Check antennas are correctly installed, move antennas to a higher location, install additional antennas to activate MIMO feature, or install high gain antenna(s).
6. Contact your service provider to check the SIM card is active and that cellular reporting is enabled for your unit on the UltraSync Portal.

Congratulations, your xGenLite system is connected to your network and UltraSync. It is now ready to be programmed. Refer to “Programming with Web Pages” on page 42.

Method 3: UltraSync+ App







UltraSync+ is a smartphone app that allows you to:

- Check the status of your system
- Arm and Disarm partitions
- Bypass zones
- Manage users
- Perform system programming

Access from the app is disabled by default for security. To allow access these settings must be enabled on your xGenLite system:

- Web Access Code

  It permits remote access from the UltraSync+ app. Set it to 00000000 to prevent the app from connecting.

- User Name and PIN code

  The UltraSync+ app requires any user name and PIN code to log in to the system and display features available to that user.

Set Web Access Code and change installer PIN code

To enable the UltraSync+ app:

1. On the NXG-1820 keypad press Menu, PIN, ENTER, go to Program, scroll down to UltraSync > Web Access Passcode.
2. Enter a new 8-digit Web Access Passcode.

Change installer PIN code:

1. On the NXG-1820 keypad press Menu, PIN, ENTER, go to Users > Add/Modify

2. Enter a new PIN code.

Connect to xGenLite via UltraSync+ app

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

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

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

   Locate the 12-digit serial number barcode on the xGenLite circuit board. Alternatively log in to xGenLite Web Server and go to Settings > Details to view it.

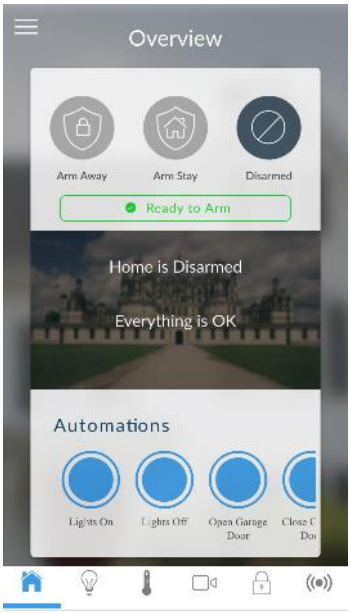
   The default Web Access Passcode of 00000000 disables remote access. To change it, log in to xGenLite Web Server and go to Settings > Network.

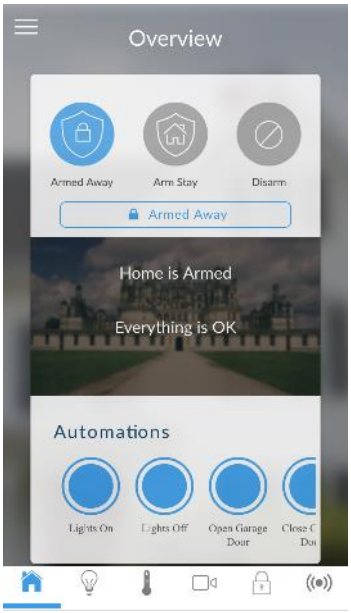
   The default username and PIN code is “installer” 9713 (for an installer) and “User 1” 1234 (for a user). Please note that there is a space between “User” and “1”. You may also use any other valid user account. Only menus a user has access to will be displayed.

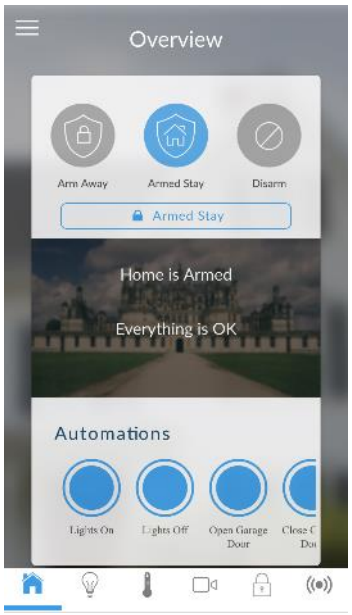
   Note: EN 50131 Grade 2 default codes are 971300, 123400.
7. Click the Done button to save the details, then Sites to go back.
8. Click the name of the Site, the app will now connect you to xGenLite.

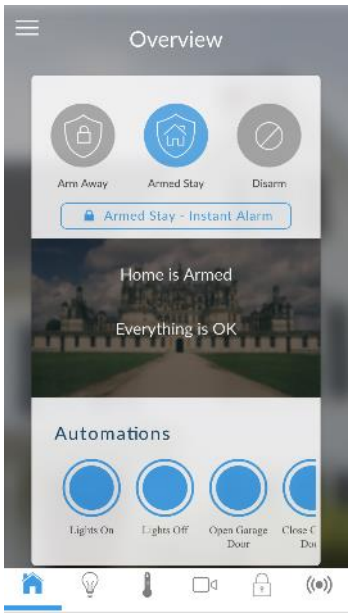
Using the App

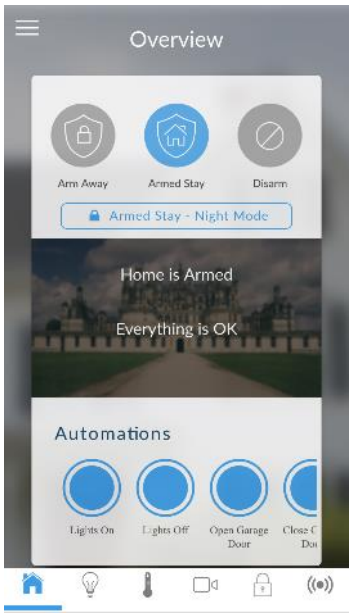
The first screen that will appear once you connect is the Overview screen. This will display the status of your system and allows you to arm or disarm partitions by touching Arm Away, Arm Stay, or Disarm. It also allows you to activate programmed automation scenes.

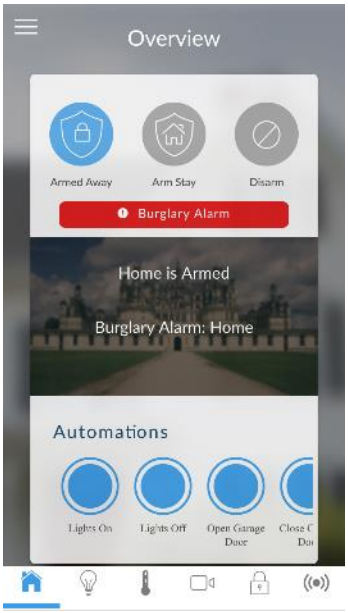

Overview
Arm Away
Arm Stay
Disarmed
Ready to Arm
Home is Disarmed
Everything is OK
Automations
Lights On
Lights Off
Open Garage Door


Overview
Armed Away
Arm Stay
Disarm
Armed Away
Home is Armed
Everything is OK
Automations
Lights On
Lights Off
Open Garage Door


Overview
Arm Away
Armed Stay
Disarm
Armed Stay
Home is Armed
Everything is OK
Automations
Lights On
Lights Off
Open Garage Door

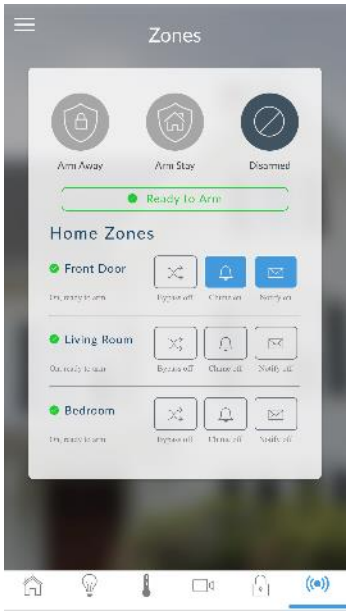

Overview
Arm Away
Armed Stay
Disarm
Armed Stay - Instant Alarm
Home is Armed
Everything is OK
Automations
Lights On
Lights Off
Open Garage Door


Overview
Arm Away
Armed Stay
Disarm
Armed Stay - Night Mode
Home is Armed
Everything is OK
Automations
Lights On
Lights Off
Open Garage Door


Overview
Armed Away
Arm Stay
Disarm
Burglary Alarm
Home is Armed
Burglary Alarm: Home
Automations
Lights On
Lights Off
Open Garage Door

The menu bar is located along the bottom of the app. Touch the Zones icon (last icon with a dot and wireless signals) to view zone status.

- Touch Bypass to ignore a zone or touch it again to restore it to normal operation.
- Touch Chime to add or remove a zone from the Chime feature.
- Touch Notify to receive push notifications when there is activity from that zone.

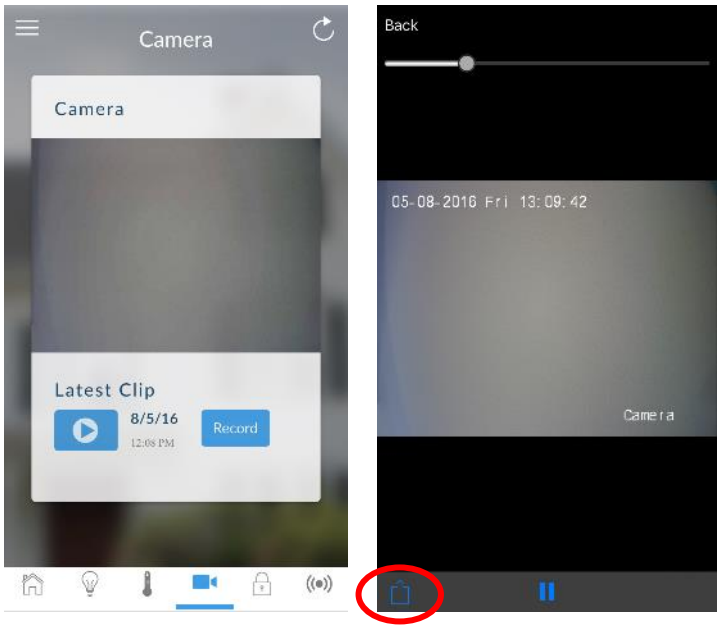


Touch the Camera icon to view cameras connected to your system.

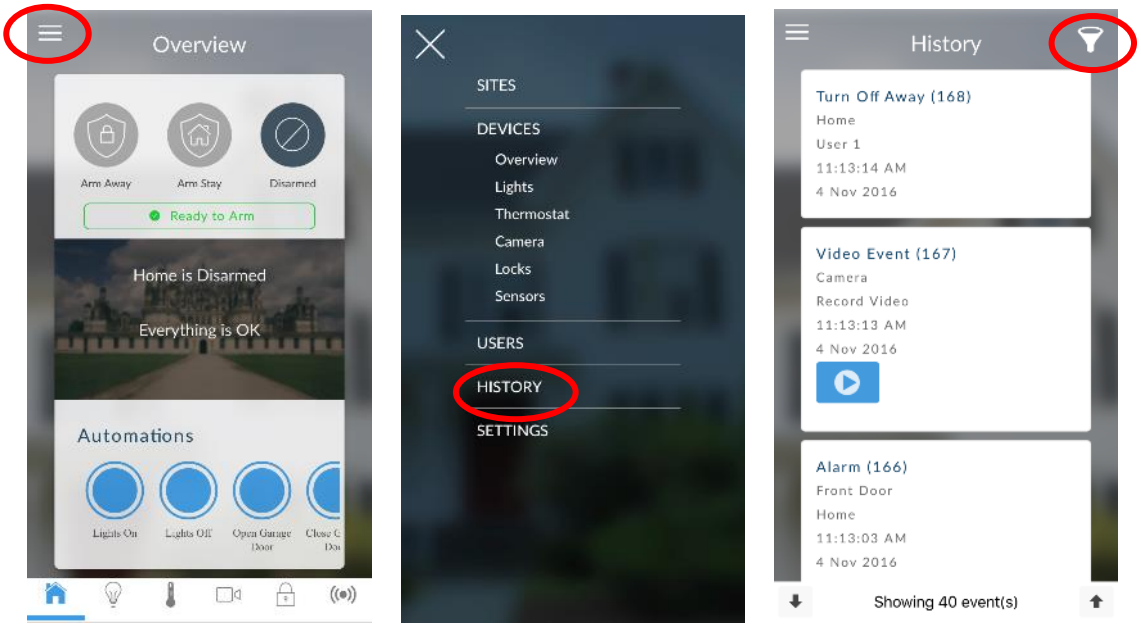
Live snapshots from each camera will be shown.

- Touch the snapshot to open the live stream in full screen. Rotate your device to make the image bigger. Touch the screen then Back to return to the Camera screen.
- Touch the Play button under each camera to view the last recorded clip by that camera. Touch the Share button to save or forward the clip.

- Touch the Record button to request that camera record a short clip which can be retrieved at a later date.



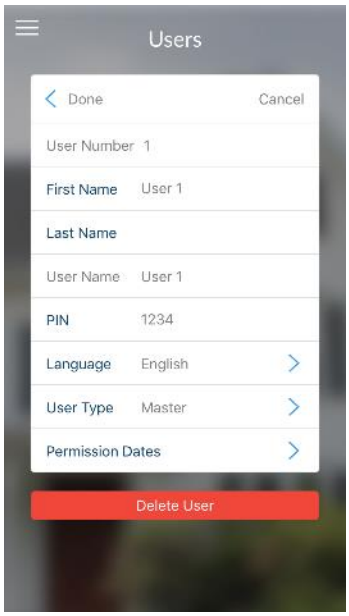
Video clips can also be accessed from the History screen. Touch Menu , HISTORY, then change Selected Events to Video. Touch “Press to Play Video” to retrieve the clip from the camera. Once downloaded, you can save or forward the clip.



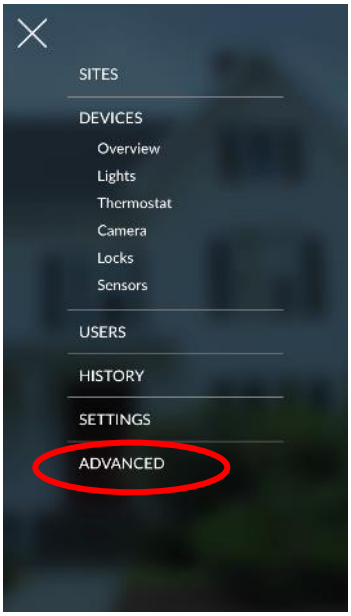
This History screen displays the event log of the xGenLite, recording important events and allowing authorized users the ability to audit the system. Changing the Selected Events to Alarms will display the filtered Mandatory Event Log.

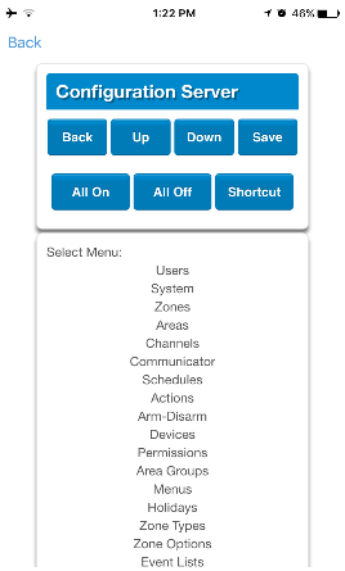
Events followed with an * have not yet been reported to a control room or have failed to report. Events followed with ** are for events not intending to be reported to a control room.

Master users will have access to the full Users menu for creating and managing users. Touch Menu , USERS. Change User Type to Custom to show additional options.



When you log in with the installer account you will have access to the ADVANCED menus for setting up and programming the xGenLite. Refer to the xGenLite Reference Guide for additional help on the Advanced screen.





Troubleshooting

If you have trouble connecting to your system using the app, here is a checklist:

- Check the serial number, web access passcode, user name and PIN codes match those in the xGenLite.
- Web Access Passcode must not be 00000000.
- Web Access Passcode must be from 4 to 8 digits.

- User Name must be entered with a space between the first and last name and with correct capitalization.
- If connected by Wired LAN, check the cable is plugged in and that the connection is working.
- Check Settings > Network > Enable UltraSync is ticked.
- Check that your mobile device has access to the internet (e.g. open a web browser).
- Check the UltraSync servers are correct under Advanced > UltraSync:

  - Ethernet Server 1 – xg1.ultraconnect.com:443

  - Ethernet Server 2 – xg1.zerowire.com:443

  - Wireless Server 1 – xg1w.ultraconnect.com:8081

  - Wireless Server 2 – xg1w.zerowire.com:8081
- Power cycle connected equipment including xGenLite and customer supplied router(s).

Method 4: NXG-1820 Keypad

The NXG-1820 is able to access all panel programming features with a valid installer code.

1. Press Menu, Installer PIN, ENTER, go to Program.
2. Scroll through the menus using the up and down buttons. Refer to Appendix 3: Advanced Menu Tree on page 155.
3. Press an item to go down a level or to select an option. Press the back arrow to go up a level or to cancel without saving.
4. Repeatedly press the back arrow to return to the main menu.

Note: NetworX keypads (including NX-1820) have limited access to xGenLite programming menus. xGenLite keypads (NXG-180 and touchscreen) are able to program legacy NetworX devices via the Advanced > Devices menu.

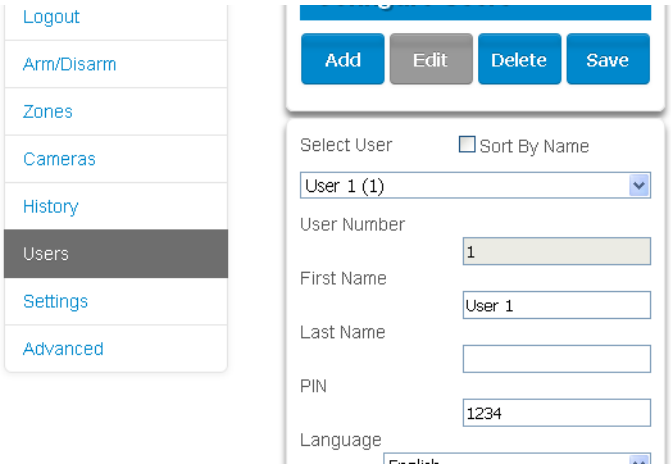
Programming with Web Pages

Most commonly used features can be programmed from the xGenLite Web Server > Settings menu. The same menus are displayed from the UltraSync+ app by clicking Menu > Settings.

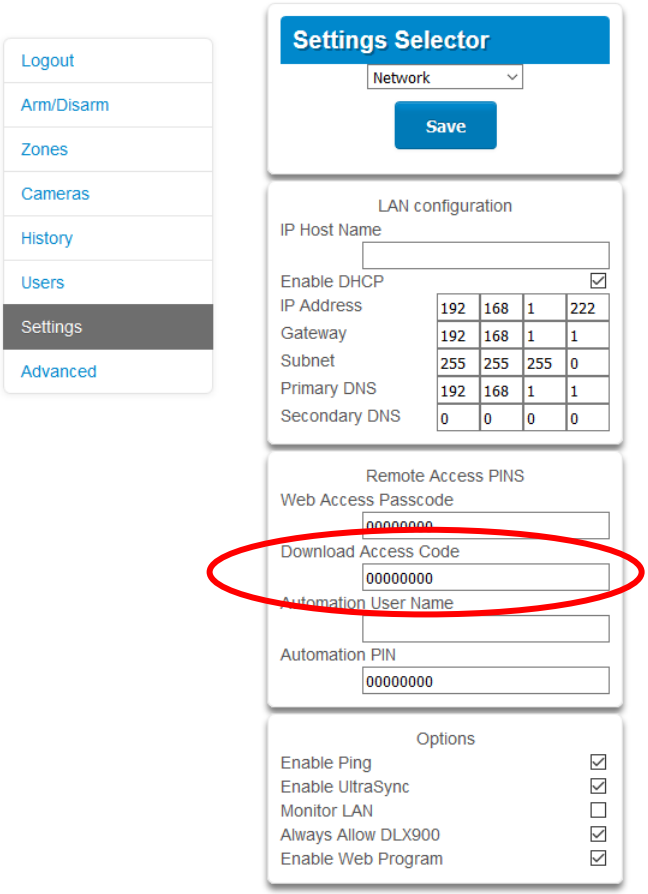
Recommended Items to Change

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

  Note: EN 50131 Grade 2 default codes are 971300, 123400.
- User 1 username is “User 1” at default, there is a space between “User” and “1”. Usernames are required to provide access to the xGenLite Web Server and UltraSync+ app.

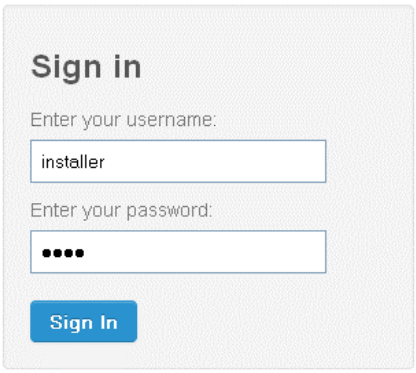


- Web Access Passcode. This provides access to the xGenLite Web Server, UltraSync, and UltraSync+ app.
- DLX900 access for upload/download is allowed if the panel is at factory default with the installer account set to PIN 9713. This is a convenience feature to allow the installer to connect to the panel for the first time and perform a Send All to program the panel. Once the installer PIN is changed, the Download Access Passcode of 00000000 disallows DLX900 access. Log in to the Web Server and go to Settings > Network to change the code:



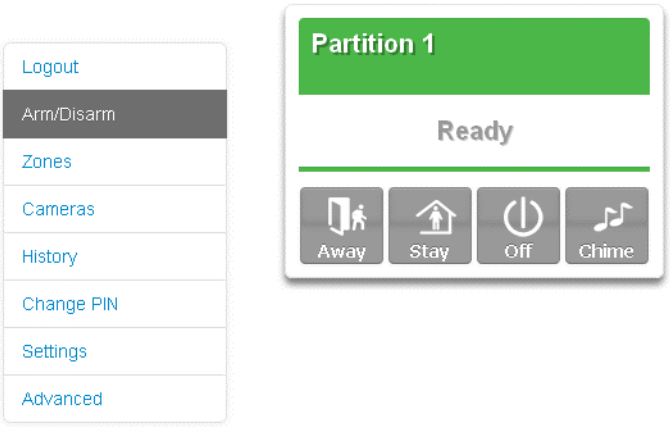
Learning Wireless Zones

1. Log in to the Web Server.

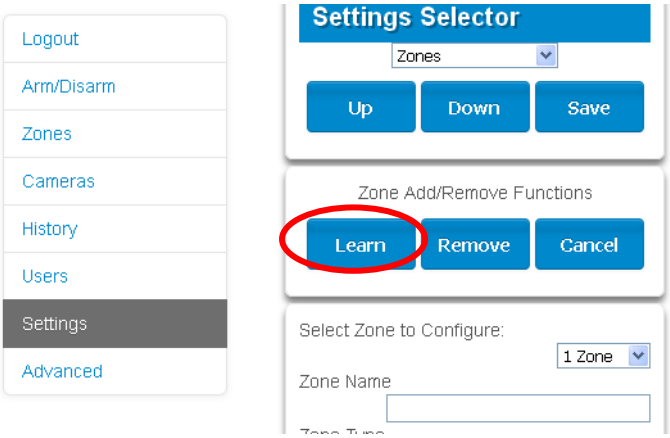


2. Enter your username and password, by default this is “installer” and “9713”, then click Sign In.

3. You should now see a screen similar to the one shown below.



4. Click Settings.
5. Click Zones.
6. Click Learn:



7. Activate the zone. Consult the detector manual for instructions, generally this is performed by opening the detector's case. This will send a tamper signal to xGenLite.
8. The screen will indicate the device has been learnt and a serial number will appear.
9. Customize zone settings if required by referring to the Zone Guide, Zone Profile Type Guide, and Zone Options Guide on the following pages.

Zone Types Table

Default Number	Default Name	Zone Attribute	Siren Attribute	Keypad Sounder	Report Delay	No Keypad Display	Momentary Switch	Zone Inhibit	Swinger Shutdown
		Armed							
1	Day Zone	Instant	Yelping	Y	Y	N	N	N	Y
2	24 Hour Audible	Instant	Yelping	Y	Y	N	N	N	Y
3	Entry Exit Delay 1	Entry 1	Yelping	Y	Y	N	N	N	Y
4	Entry Exit Delay 2	Entry 2	Yelping	Y	Y	N	N	N	Y
5	Follower	Handover	Yelping	Y	Y	N	N	N	Y
6	Instant	Instant	Yelping	Y	Y	N	N	N	Y
7	24 Hour Silent	Instant	Silent	N	Y	N	N	N	Y
8	Fire Alarm	Fire	Fire	Y	N	N	N	N	N
9	Entry Exit Delay 1 Auto-Bypass	Entry 1	Yelping	Y	Y	N	N	Y	Y
10	Entry Exit Delay 2 Auto-Bypass	Entry 2	Yelping	Y	Y	N	N	Y	Y
11	Instant Auto-Bypass	Instant	Yelping	Y	Y	N	N	Y	Y
12	Event Only	Event Only	Silent	N	N	Y	N	N	N
13	Momentary Key Switch	Keyswitch	Silent	N	N	N	Y	N	N
14	Latching Key Switch	Keyswitch	Silent	N	N	N	N	N	N
15	CO Detector	Instant	Four Pulse	Y	N	N	N	N	N
16	Exit Terminate	Exit Terminate	Silent	N	N	N	N	N	N
17	Holdup	Holdup Delay	Silent	N	N	N	N	N	N
18	24 Hour Local Sounder	Instant	Silent	Y	N	N	N	N	N
		Disarmed							
1	Day Zone	Local	Silent	Y	N	N	N	N	N
2	24 Hour Audible	Instant	Yelping	Y	Y	N	N	N	Y
3	Entry Exit Delay 1	Event Only	Silent	N	N	N	N	N	N
4	Entry Exit Delay 2	Event Only	Silent	N	N	N	N	N	N
5	Follower	Event Only	Silent	N	N	N	N	N	N
6	Instant	Event Only	Silent	N	N	N	N	N	N
7	24 Hour Silent	Instant	Silent	N	Y	N	N	N	Y
8	Fire Alarm	Fire	Fire	Y	N	N	N	N	N
9	Entry Exit Delay 1 Auto-Bypass	Event Only	Silent	N	N	N	N	N	N
10	Entry Exit Delay 2 Auto-Bypass	Event Only	Silent	N	N	N	N	N	N
11	Instant Auto-Bypass	Event Only	Silent	N	N	N	N	N	N

Default Number	Default Name	Zone Attribute	Siren Attribute	Keypad Sounder	Report Delay	No Keypad Display	Momentary Switch	Zone Inhibit	Swinger Shutdown
12	Event Only	Event Only	Silent	N	N	Y	N	N	N
13	Momentary Key Switch	Keyswitch	Silent	N	N	N	Y	N	N
14	Latching Key Switch	Keyswitch	Silent	N	N	N	N	N	N
15	CO Detector	Instant	Four Pulse	Y	N	N	N	N	N
16	Exit Terminate	Event Only	Silent	N	N	N	N	N	N
17	Holdup	Holdup Delay	Silent	N	N	N	N	N	N
18	24 Hour Local Sounder	Instant	Silent	Y	N	N	N	N	N

Zone Options Table

		Zone Options										Zone Reporting					Zone Contact Options		
Default Number	Default Name	Bypassed Stay Mode	Forced Arm Enabled	Bypass	Cross Zone	EOL	Automatic Zone Test	Night Mode	Zone Inactivity Test	Follow Any Armed Area	Final Set Door	Single EOL	Delayed in Stay	Alarms	Alarm Restores	Bypass-Unbypass	Zone Lost-Low Battery	Zone Trouble and Restore	Normally Open	Fast Loop	Zone Report Event
1	Bypass			Y		Y								Y	Y	Y	Y	Y			130:BA
2	Bypass Stay	Y	Y	Y		Y								Y	Y	Y	Y	Y			132:BA
3	Bypass – Forced Arm		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
4	Bypass – Cross Zone			Y	Y	Y								Y	Y	Y	Y	Y			130:BA
5	Fire		Y			Y								Y	Y	Y	Y	Y			110:FA
6	Panic		Y			Y								Y	Y	Y	Y	Y			120:PA
7	Silent Panic					Y								Y	Y	Y	Y	Y			122:HA
8	Normally Open no EOL			Y										Y	Y	Y	Y	Y	Y		130:BA
9	Normally Closed no EOL			Y										Y	Y	Y	Y	Y			130:BA
10	Gas Detected					Y								Y	Y	Y	Y	Y			151:GA
11	High Temp					Y								Y	Y	Y	Y	Y			158:KA

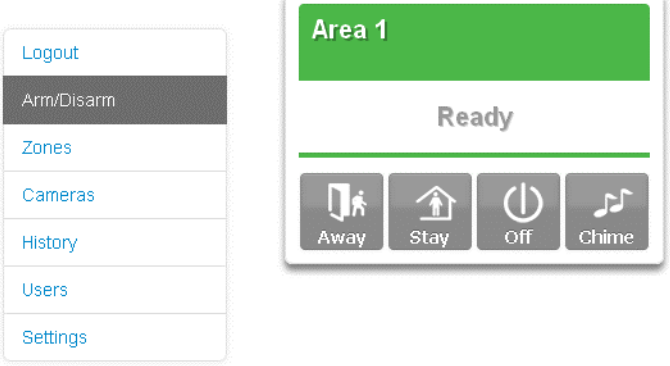
		Zone Options												Zone Reporting					Zone Contact Options		
Default Number	Default Name	Bypassed Stay Mode	Forced Arm Enabled	Bypass	Cross Zone	EOL	Automatic Zone Test	Night Mode	Zone Inactivity Test	Follow Any Armed Area	Final Set Door	Single EOL	Delayed in Stay	Alarms	Alarm Restores	Bypass-Unbypass	Zone Lost-Low Battery	Zone Trouble and Restore	Normally Open	Fast Loop	Zone Report Event
12	Water Leakage					Y								Y	Y	Y	Y	Y			154:WA
13	Low Temp					Y								Y	Y	Y	Y	Y			159:ZA
14	High Temp					Y								Y	Y	Y	Y	Y			158:KH
15	Fire Alarm Pull Station					Y								Y	Y	Y	Y	Y			115:FA
16	Night Mode	Y		Y		Y		Y						Y	Y	Y	Y	Y			135:BA
17	Final Set Door			Y		Y					Y			Y	Y	Y	Y	Y			130:BA
18	Medical		Y			Y								Y	Y	Y	Y	Y			100:MA
19	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
20	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
21	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
22	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
23	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
24	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
25	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
26	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
27	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
28	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
29	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
30	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
31	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA
32	Blank		Y	Y		Y								Y	Y	Y	Y	Y			130:BA

Adding a User

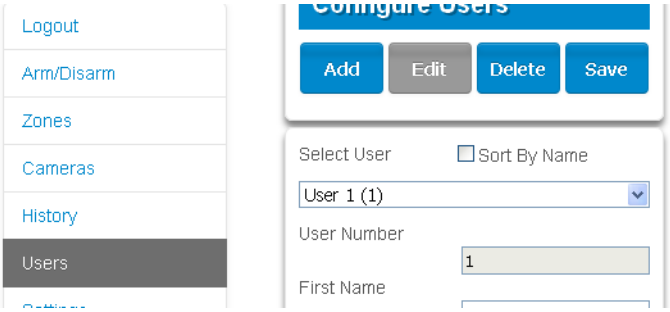
The xGenLite system supports up to 100 users. Each user is assigned a PIN code and a user number. This allows them to interact with the system.

1. Log in to the Web Server.

2. Enter your username and password. A master code is required to add users, by default this is “User 1” (with a space between “User” and “1”) and “1234”. Then click Sign In.
3. The Arm/Disarm screen will appear:



4. Click Users.



5. Click Add.
6. Enter a unique PIN code between 4 and 8 digits.
7. Enter a First and/or Last Name.
8. Select a User Type:

   - Master users can arm and disarm partitions. They can create, delete, or modify user codes. They can also change system settings.

   - Standard users can arm and disarm partitions. But 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.

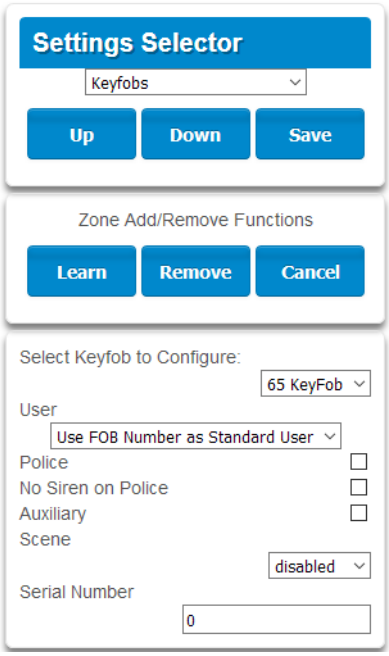
   - Duress users will send a duress event when they are used to arm or disarm the system.

- Custom users can have additional permissions and settings configured.

9. Click Save.

Adding a Keyfob

1. Log in to the Web Server.
2. Click Settings.
3. Click Keyfobs.
4. Use the drop-down menu to select the keyfob number you want to add to the system.



5. Click Learn.
6. Trigger the keyfob learning function for 2 seconds (on 63-bit keyfobs hold down the arm and disarm buttons, on 80plus keyfobs hold down the Arm + 2 buttons). The screen will show the keyfob has been found and the Serial Number will appear.

   The keyfob will have access to Area 1 and the panel will report the **keyfob number** to the Central Monitoring Station when it is used.

7. Click Save.

Advanced Keyfob Programming

Three levels of access are possible:

1. Area 1 only: This is the default behaviour after learning a keyfob. The User is set to “Use FOB Number as Standard User”.
2. All partitions: Click the drop-down User menu to assign the keyfob a User number. The keyfob will inherit partitions and permissions of that user. New users and the default Master and Standard user accounts have access to ALL

partitions. This **user number** is reported to the Central Monitoring Station when the keyfob is used.

3. Custom permissions > Keyfobs can be restricted to selected partitions.

   Simple Method: navigate to the User menu and select a suitable Area Group. The arm and disarm buttons on the keyfob will arm/disarm all partitions in the Area Group.

   Advanced Method:

   a. Create a new User.

   b. Change the User Type to Custom.

   c. Assign an unused Permission to the User.

   d. Create one or more Area Groups. Each one has a set of selected partitions.

   e. Modify the Permission and assign the appropriate Area Group to the Control Groups displayed. For example, the Permission can Away Arm both Area 1 and 2, but Disarm only Area 1.

   f. Return to the Settings > Keyfob menu.

   g. Select the User that has been created.

   The keyfob is now linked to the custom user, and the custom permissions will be applied. When the arm button is pressed, all partitions in the Away Arm Control Group will be away armed. When the disarm button is pressed, all partitions in the Disarm Control Group will be disarmed.

Keyfob Options:

- Tick the Police option to allow Panic Alarms to be sent to the Central Monitoring Station when Arm + Disarm Buttons are pressed at the same time. In addition, the panel will display the status and sound audible alerts. Please consult with your Central Monitoring Station what action will be taken.
- Tick “No Siren on Police” for Silent Panic, when activated the xGenLite will have no indication the panic has been triggered, the Silent Panic event will be sent to the Central Monitoring Station. Please consult with your Central Monitoring Station what action will be taken.
- Tick Auxiliary to allow the keyfob to send an Auxiliary Alarm. On the 63-bit keyfob this is performed when the LIGHT and STAR buttons are pressed at the same time, on the 80plus keyfob this is performed when 1 and 2 buttons are pressed. Please consult with your Central Monitoring Station what action will be taken.
- Select a pre-programmed Scene from the drop-down menu. When the Scene button is pressed on that specific keyfob, the xGenLite will “run” this scene. On the 63-bit keyfob this is the LIGHT button, on the 80plus keyfob this is the 2 button.

Note: When programming the Scene under the Settings > Scenes menu, the “Scene Trigger” is optional. Select the actions you want to be performed when the scene is “run” by the keyfob.

Programming Cameras

Adding Cameras Using the New Device Setup

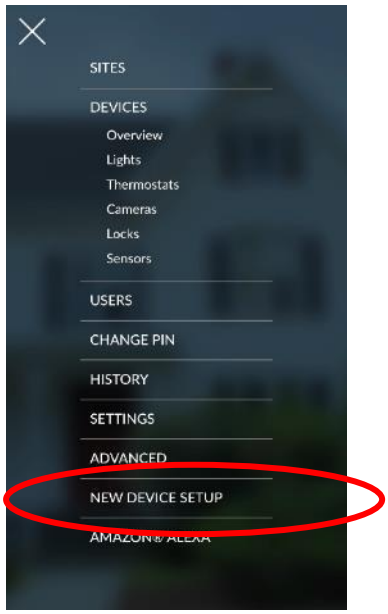
The UltraSync+ app has a built-in guide to help you add cameras. This feature is supported on the Bullet Camera, Desktop Camera, and Doorbell Camera. Cameras must be connected to the same network as the xGenLite.

Before adding cameras:

- The xGenLite must be programmed
- The UltraSync+ app must be able to connect to the site

To add a camera:

1. Connect power to the camera using the included plug pack. It will take 3 to 4 min to initialize. A new camera out of the box will automatically start WiFi Discovery Mode if no Ethernet cable is connected.
2. Launch UltraSync+ app on a smartphone.
3. Click the site name to connect to the panel.
4. Click Menu – New Device Setup



5. Follow the on-screen instructions.

Adding Cameras using the Settings Screen

Cameras contain advanced options and features which can be programmed directly in the camera. These may include:

- Image adjustment
- Noise reduction

- Day/Night settings
- IR mode
- Recording format / quality / codec
- Storage allocation and formatting the micro SD card (if included)
- Advanced network configuration
- Time zone and daylight savings
- Camera naming and text overlay
- Privacy mask

Only perform these steps if you are familiar with the operation of the camera. Incorrect settings may cause the camera to perform poorly. Default the camera to factory settings if this occurs.

1. Connect the camera with an Ethernet cable to the same router / local area network as the panel.
2. Program the camera by following the camera's manual. Take care when changing quality settings - exceeding the customer's upload bandwidth will cause the camera to appear slow or unresponsive.
3. If a WiFi connection is preferred:

   a. Enter the WiFi router's details on the Network - WiFi tab

   b. Click Save

   c. Check "Connected" appears

   d. Disconnect the Ethernet cable

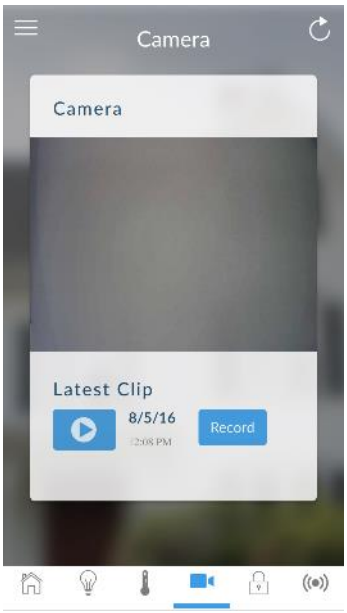
   e. Reboot the camera
4. From your iOS or Android device, open the UltraSync+ app.
5. Add the panel details with the installer account / PIN.
6. Log in to the site as the installer.
7. Touch Menu then Settings.
8. Select Cameras under the Settings Selector.

9. Click Scan for New Cameras. “Scanning…” will appear on the button, please wait for the message to disappear. The MAC Address will automatically be filled in.
10. Enter a Camera Name.
11. For Doorbell Camera, enable options for button press if desired.
12. Click Save.

    Note: The camera may take up to 3 minutes to finalize the link with ZeroWire and display on the Cameras screen of the app.
13. Close and relaunch the app.
14. Check video streaming and video clip playback can be performed. Lower the quality settings or recording duration if video appears slow or unresponsive.

Viewing Live Stream and Latest Clip

1. Click Camera icon on bottom of the screen.
2. All available cameras will be shown.



3. Click Live Stream to view the live video of a specific camera.
4. Click Latest Clip to view the last recorded clip from a specific camera. Please wait while the ZeroWire servers retrieve the last recorded video clip from the selected camera.
5. Click the Share button to download or forward the clip.

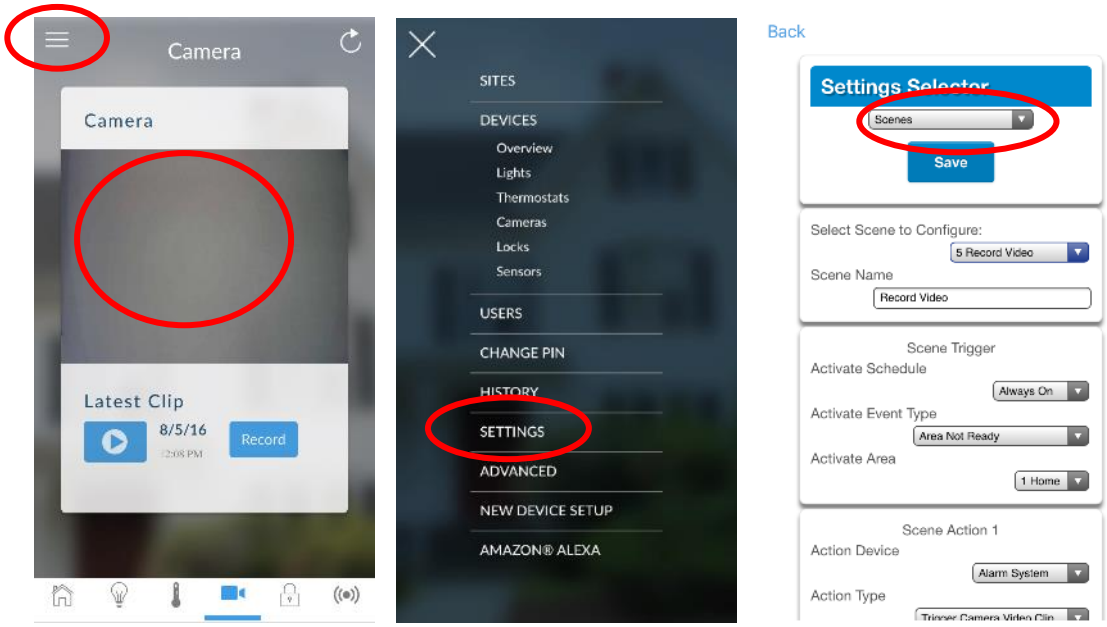
Programming event triggered camera clips

The panel can be programmed to capture a short video clip when selected events occur on the system. These clips can later be viewed from the UltraSync+ app.

The installer or master user must program which events should trigger video recording.

This is achieved using the Scenes feature.

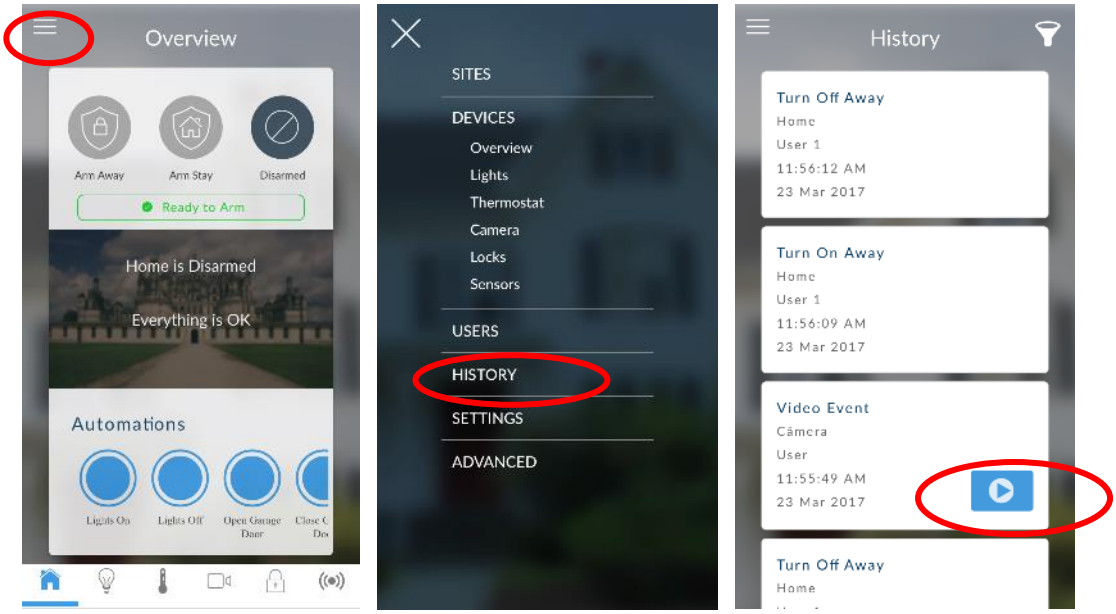
Note: Ensure you can view the Live Stream from the camera before continuing.



1. Log in to the UltraSync+ app.
2. Touch Menu then Settings.
3. Select Scenes under the Settings Selector.
4. Select the Scene to Configure and type a Scene Name.
5. Leave the “Enable App Button” ticked to show a shortcut button on the home screen of the UltraSync+ app. Untick this option to hide it.
6. Select the Activate Schedule - Always On to allow recording at all times.
7. Select the event that will trigger recording a video clip using the Activate Event Type drop-down box.
8. Select the Activate Zone/Area/User/Action if applicable.
9. Select Action Device (1) Alarm System, Action Type “Trigger Camera Video Clip”, then the cameras you wish to record a video clip when the event is triggered.
10. Click Save, Back.
11. Activate the event and wait for the programmed recording time (typically 15 seconds). Camera will record to the camera’s microSD card.
12. Click the camera icon and check the video clip plays back.

Viewing event triggered clips in History

1. Touch Menu then HISTORY.
2. Find the video event by using the navigation buttons and scrolling down.



Note: For faster searching you can show only Video events by selecting Video in Select Events.

3. Tap the event to play the video.
4. Click the Share button to download or forward the clip.

Troubleshooting Cameras

The panel and camera must be on the same subnet. Check IP address of panel and camera. For example, 192.168.33.xxx, first three sets of numbers must match on both devices.

Check device is communicating on network. Use a command prompt (cmd) in Windows to ping the panel and the camera. If both reply successfully then your device is connected correctly on the network. Alternatively, 3rd party network scanning apps and tools may be of assistance during installation.

Check the Settings > Connection Status web page. UltraSync Status must show connected. If not, contact your service provider for help. The panel may require to be “provisioned” and added to the web portal in order to authenticate to the cloud servers which the cameras will connect to.

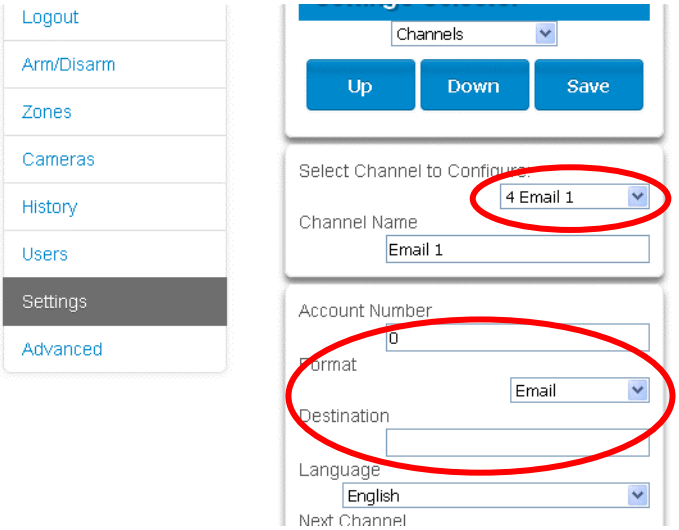
Only cameras specified for use with your panel will work. These cameras have additional encryption and security to protect against unauthorised 3rd party access.

Live video streams can only be viewed from the app. Try switching your smartphone between mobile data and WiFi to try a different connection.

Configuring Email Reports

1. Log in to xGenLite. Use an installer or master user account.
2. Click Settings.
3. Click Channels in the drop-down menu.

4. Click “Select Channel to Configure” where the Format is already set to Email.



5. Enter an email address in the Destination field.
6. Select an Event List.
7. Enter a Channel Name for future reference.
8. Click Save.

Installer and Engineer user types can customize Event List for selective reporting.

Configuring OH Reports

In certain applications, the xGenLite can be configured to support non-provisioned Osborne-Hoffman Reporting. This is done by entering specially formatted text in Channel > Destination.

Setting Up OH Reporting

1. The panel must not be provisioned in the UltraConnect Servers.
2. This configuration must be in reporting Channel 1. Click Settings > Channels to view Channel 1.
3. Select one the OH options in the channels report format field. Between CID and SIA; and between Cellular, IP, and Dual path.
4. In the Destination field, enter the OH Configuration using the format ip_address:ip_port:R:L:Reporting_period:Supervision_port LAN_Fault_Delay:Cell_fault_Delay. See below for details.

OH Configuration

Only ip_address:ip_port are mandatory to switch this feature on. Consult your central station for the correct values.

ip_address : ip_port : R : L : Polling interval_period : Supervision_port

Field description:

- ip_address: Public IP address of the OH Net Receiver.

- ip_port: IP port of OH Net Receiver.
- R: Receiver number in the OH message (optional), may be one or two hexadecimal characters (0–9, A–F), default is one (1) if left blank.
- L: Line number in the OH message (optional), must be single hexadecimal character (0–9, A–F), default is one (1) if left blank.
- Polling interval period: The number of seconds between OH heartbeat messages (optional). This will be initiated on the server on behalf of the panel. If specified it must be set at 1800 or above.
- Supervision_port: IP port of the OH Net Receiver Supervision port (optional). OH heartbeat messages will be sent to this port at the specified reporting period.
- LAN_Fault_Delay: The number of seconds for the LAN failure delay reporting to OH. If set, it must be a number between 90 and 255. The minimum delay is 90 seconds. If the path is restored within this time window, no fault event will be reported to OH.
- Cell_Fault_Delay: The number of seconds for the Cellular failure delay reporting to OH. If set, it must be a number between 90 and 255. The minimum delay is 90 seconds. If the path is restored within this time window, no fault event will be reported to OH.

Each field is separated by a colon ":" and no spaces.

Examples

All fields specified 11.22.33.44:9999:20:1:1800:8799:90:180

If you configure the Destination as "11.22.33.44:4099", the OH receiver will receive the alarm events and the "R&L" will be 1:1.

Similarly, if the Destination is set to "11.22.33.44:4099:2", the "R&L" will be 2:1.

The heartbeat interval is set to 1800 seconds (30 min) and is sent to OH, port 8799.

The LAN fault delay is set to 90 seconds. In case a LAN failure occurs and is restored within 90 seconds, the LAN fault message will not be reported to OH. If the fault remains present for a longer period, the LAN fault message will be reported after 90 seconds.

The Cellular fault delay is set to 180 seconds. In case a cellular failure occurs and is restored within 180 seconds, the cellular fault message will not be reported to OH. If the fault remains present for a longer period, the LAN fault message will be reported after 180 seconds.

Enabling Push Notifications on Smartphone

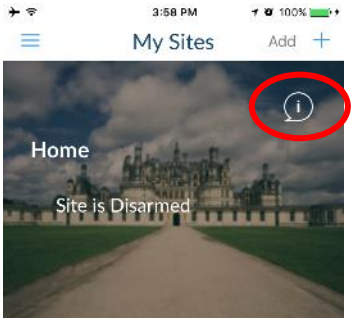
Smartphones with the UltraSync+ app can receive push notifications from the panel when system events occur.

You will need to have a:

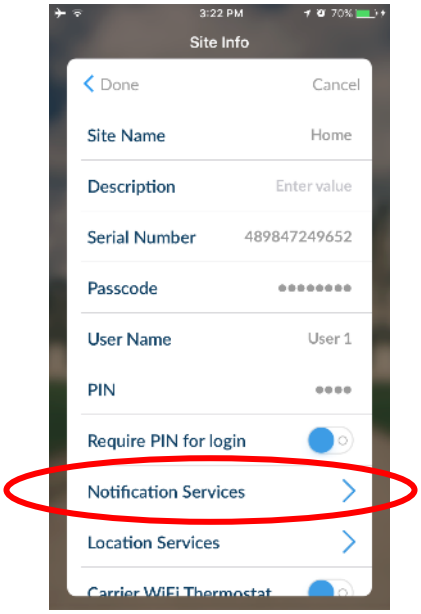
Fully configured and online xGenLite system.

Fully configured smartphone with internet access and Apple/Google account details. This must be signed in to the relevant Apple ID / Google account so their servers can deliver the message to the device.

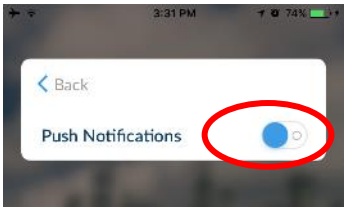
1. Open the UltraSync+ app.
2. Click the edit button next to the site you wish to receive notifications from.



3. Click Notification Services.



4. Enable Push Notifications.

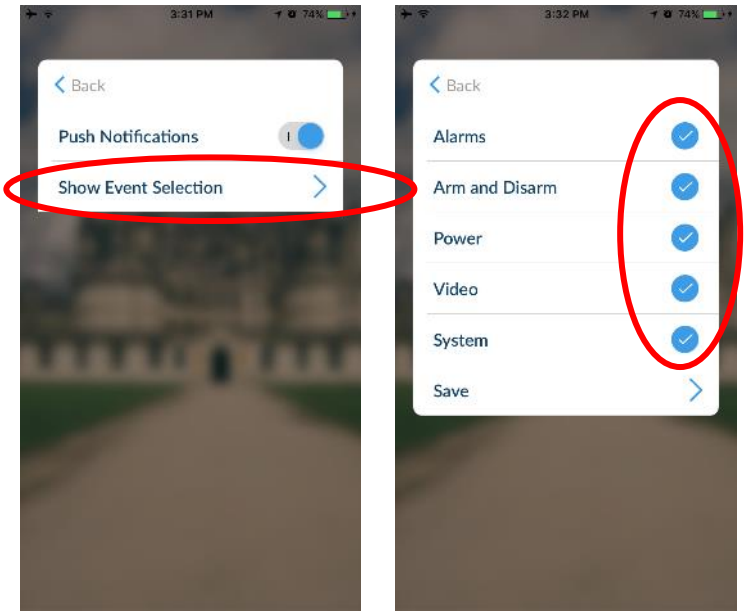


5. Wait for the registration process to complete.

   Note: A maximum of 13 devices can receive push notifications. Each device will occupy a Channel slot. Each channel will automatically be assigned the corresponding event list number.

6. Optional – select the events to be notified for:

   a. Click Show event selection.



   b. Select the events you want a notification for.

   c. Click Save >.

   d. Click Back.

7. Click Back.

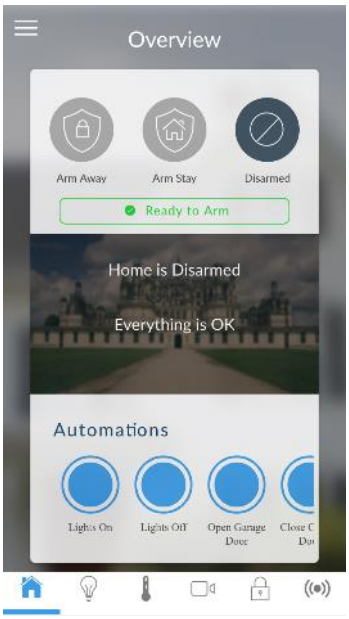
8. Click Done.

Note: If the device will no longer be used, repeat these steps and disable Push Notifications to free up the channel position for future use.

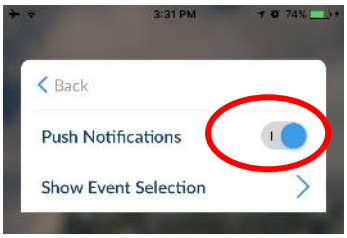
Troubleshooting Notifications

If notifications are not working:

- Check you can see the Arm/Disarm screen of the device you wish to receive notifications from, this ensures you have authority to access the xGenLite.



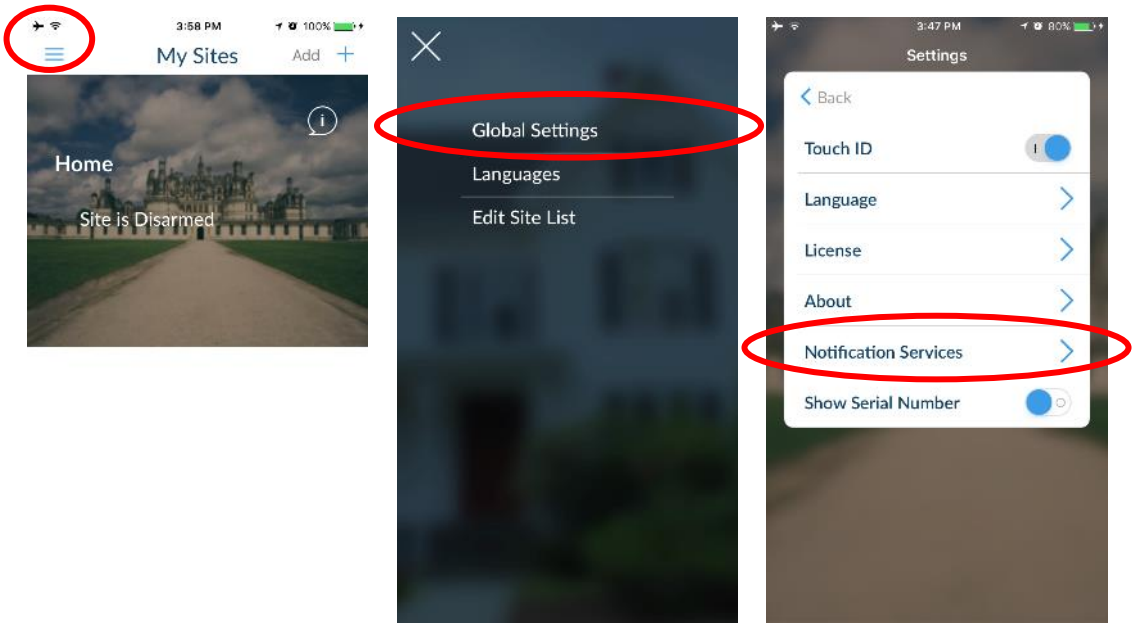
- Check the xGenLite has at least one unused channel: Log in to the Web Server and access the Settings > Channels screen.
- Check your site is registered for notifications in the app (follow instructions above).



- Check your smartphone has notifications enabled (on Apple iOS click Settings, Notifications, scroll down and click UltraSync, check “Allow Notifications” and “Show in Notification Centre” are enabled, optionally select the Alert Style as Banners or Alerts).
- If you are on iOS, ensure your phone is logged into your Apple account under iTunes or iCloud.

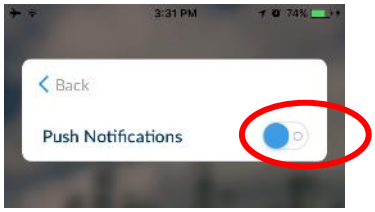
  If you are on Android, ensure your phone is logged into your Google account under Google Play or Settings. This is required as UltraSync sends the push notification to Apple and Google servers for delivery to your device. “Rooted” or “Jailbroken” phones may not have the required software to receive push notifications.
- Update your device to the latest version.

- If you have multiple devices registered to receive notifications, each device must have a unique name. This is set in the UltraSync+ app:
  1. Touch Menu from the Sites screen.
  2. Touch Global Settings.
  3. Touch Notification Services.
  4. The device name is displayed and can be changed.



Removing Notifications

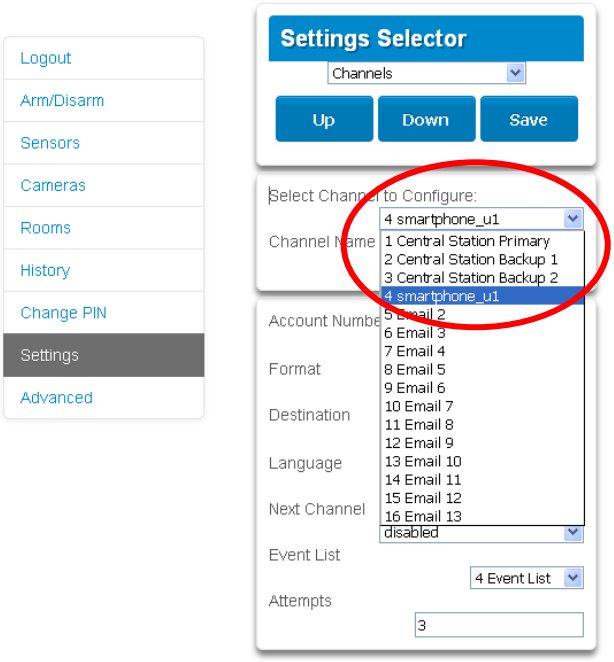
Follow the steps above and disable the “Push Notifications” option. This will automatically delete your device from the server and xGenLite.



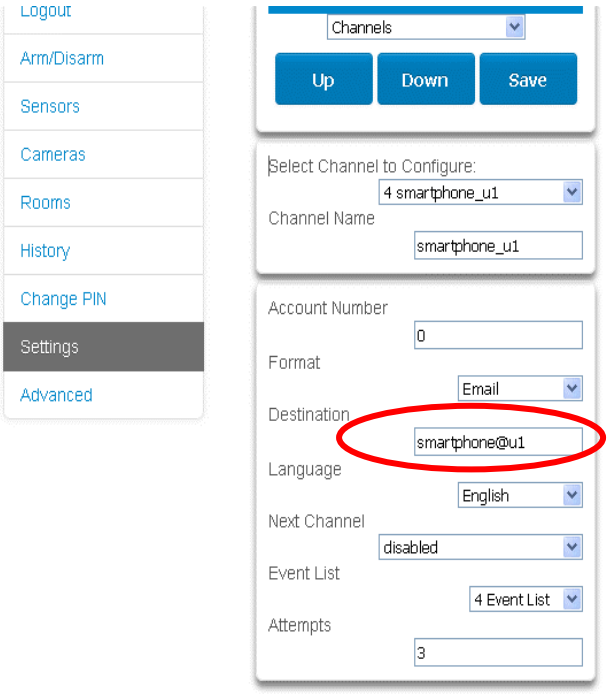
If you do not have access to the device, the xGenLite can be modified to stop sending the notifications:

1. Log in to the Web Server.
2. Click Settings.
3. Click Channels from the drop-down list.

4. Click the Channel Number in the drop-down list, your device name will appear.



5. Delete the content of the Destination field.



6. Click Save.
7. Your device will no longer receive notifications from this xGenLite and the Channel is available to be reused.

Z-Wave Home Automation Hub

If the xGenLite has been purchased with Z-Wave capabilities (either built-in to the main board, or as an optional expansion module), the xGenLite system is a security enabled Z-Wave controller supporting selected Z-Wave compliant devices including light switches, dimmers, thermostats, and secure/encrypted door locks.

A secure Z-Wave controller is required to fully utilize the product. xGenLite can act as a secure Z-Wave controller.

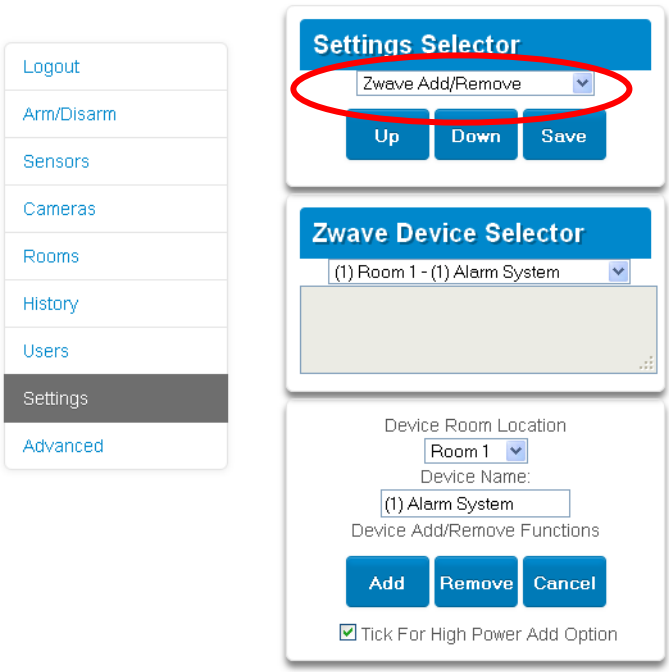
Z-Wave compliant devices regardless of manufacturer can be used in the same network and always-on devices can function as repeaters to extend the range of Z-Wave devices.

Door locks which support secure encryption can be used, unencrypted locks cannot be added to xGenLite.

xGenLite may natively support setting and retrieving on/off states, setting and retrieving dimming levels, and locking/unlocking.

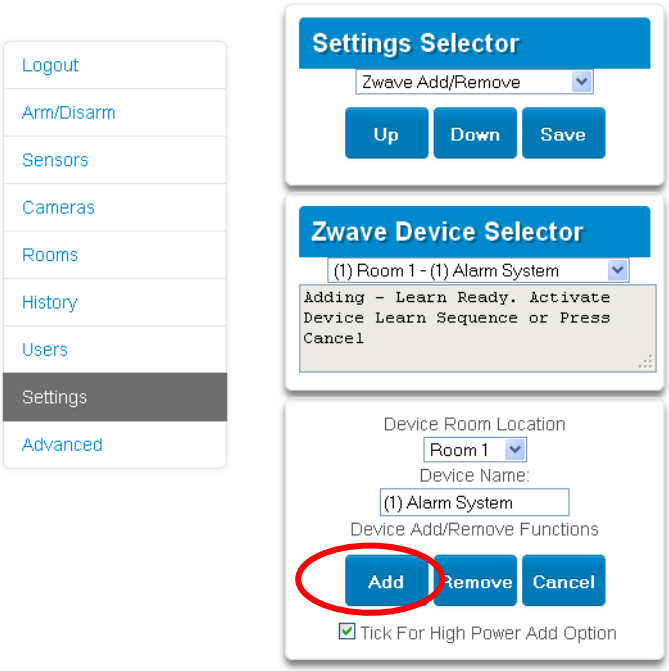
Adding Z-Wave Devices

1. Log in to the Web Server.
2. Click Settings > Rooms and edit Room Names.
3. Click Settings > Z-Wave Add/Remove. Appropriate access level is required for programming the Z-Wave devices into xGenLite.



4. If a Z-Wave device has been added before or to another system, you must first remove it before adding it to this system. To do this, click Remove, then activate LINK or REMOVE mode on the device.

5. Click Add.



6. Initiate LINK or ADD mode on Z-Wave device. See your Z-Wave device's manual for instructions.
7. Click Rooms.
8. Check you can see the device you just added. Click a button such as ON or OFF to verify you can control the device.

Programming Z-Wave Siren

Some Z-Wave sirens identify themselves to xGenLite as a true siren, while others identify themselves as binary on\off switches. There are slightly different programming steps for each.

If you have added a Z-Wave siren that identifies as a binary on/off type, you can program it to activate when the xGenLite siren activates:

1. Log in to the panel.
2. Click Advanced > Devices > Zwave Devices.
3. Select the Z-Wave siren in the drop-down list.
4. Click Zwave Options.
5. Enable Siren Mode.
6. Click Save.
7. Arm your system and trip a sensor to cause the built-in xGenLite siren to activate. Verify your Z-Wave siren also activates.
8. Disarm your system.

Some Z-wave sirens can follow each keypad beep during Exit Delay and Entry Delay. This is enabled under:

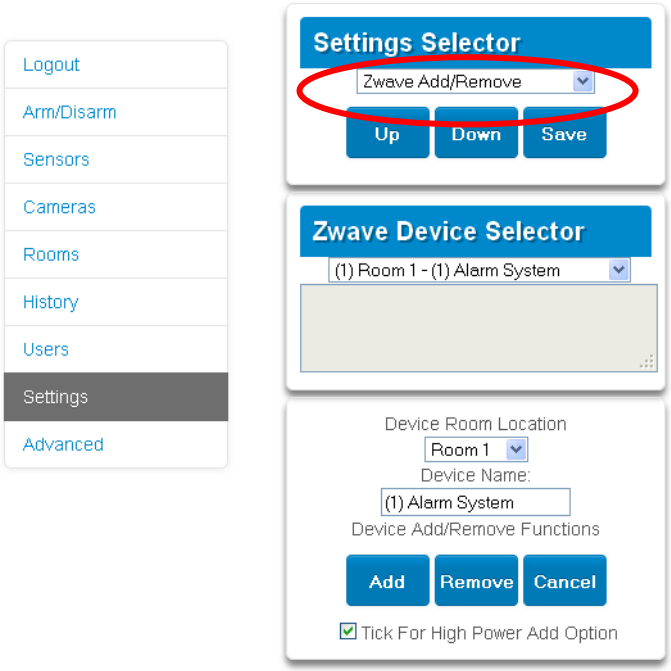
1. Log in to the panel.
2. Click Advanced > System > Siren Options.
3. Enable Z-Wave Siren Chirps Entry and Exit.
4. Click Save.

When this option is disabled, only the built-in xGenLite siren should sound during Entry and Exit Delay.

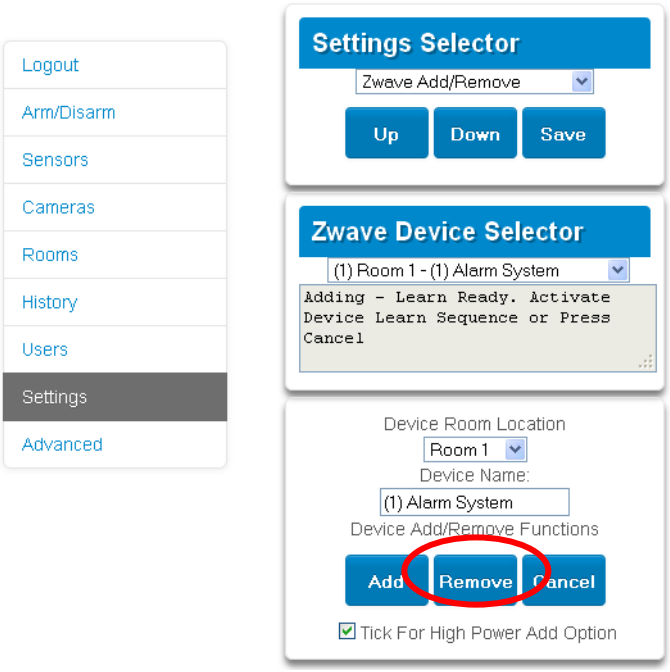
Note: Some Z-wave sirens have a built-in 30 second timer and ignore advanced features.

Removing Z-Wave Devices

1. Log in to the panel.
2. Click Settings > Z-Wave Add/Remove.



3. Click Remove.

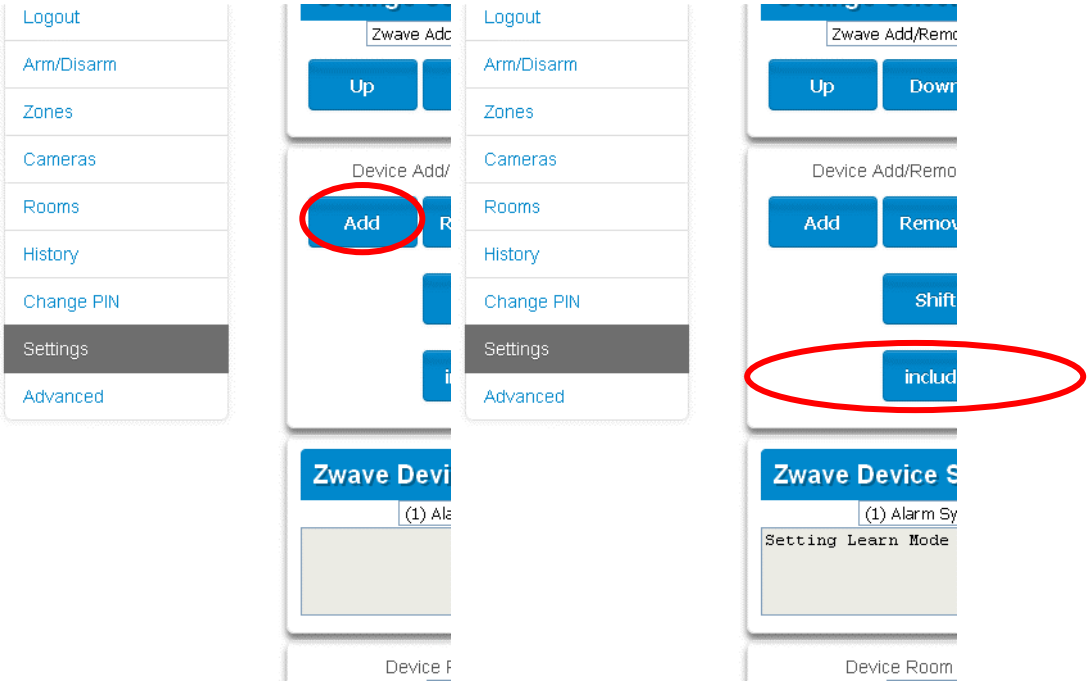


4. Press the include button on the Z-Wave device you want to remove. See your Z-Wave device's manual for instructions.
5. Device will no longer appear in xGenLite menus.

Adding xGenLite to existing Z-Wave network as Secondary Controller

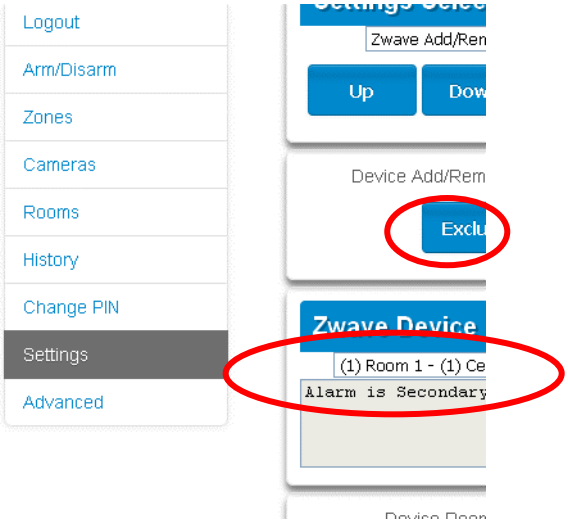
1. Log in to the panel.
2. Click Settings > Z-Wave Add/Remove.
3. Start the Add process on the primary controller of the existing network.

4. Press the **Include** button on the xGenLite (the secondary device):



Primary Controller will add xGenLite to it.

xGenLite Include button and status will update to indicate it has been added as Secondary Controller.



5. Save settings on Primary Controller.

Removing xGenLite from existing Z-Wave network as Secondary Controller

1. Log in to the panel.
2. Click Settings > Z-Wave Add/Remove.
3. Start the Remove process on the primary controller of the existing network.

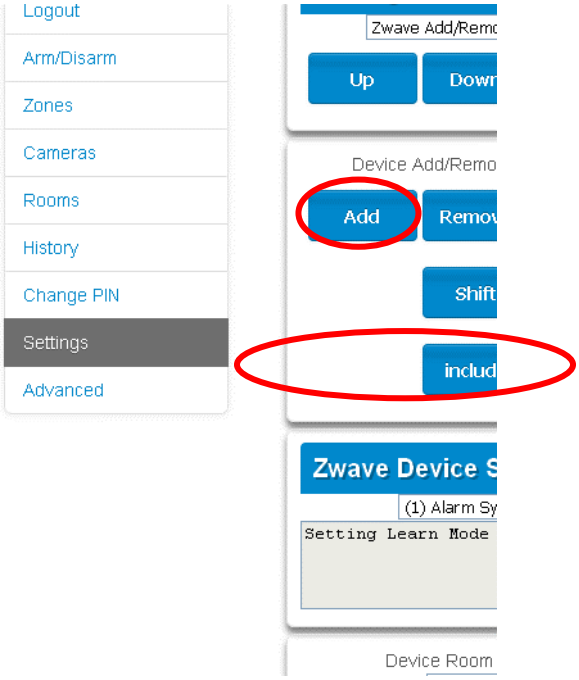
4. Press the **Exclude** button on the xGenLite (the secondary device):

5. Primary Controller will remove xGenLite from it.
6. xGenLite status will update to indicate it has been added as Secondary Controller.
7. Save settings on Primary Controller.

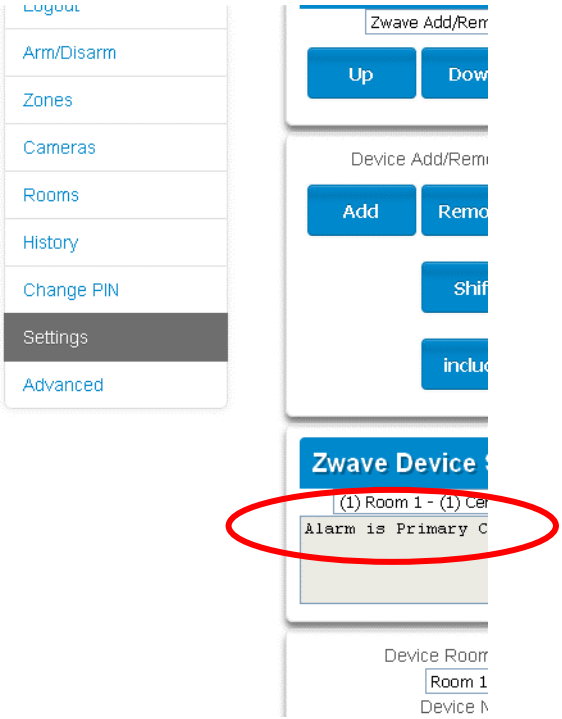
Adding xGenLite to existing Z-Wave network as Primary Controller

1. Log in to the panel.
2. Click Settings > Z-Wave Add/Remove.
3. Start the Control Shift function on the primary controller of the existing network. This will typically involve pressing a “Shift” button.

4. Press the **Include** button on the xGenLite (the primary device):



5. xGenLite now displays “Alarm is Primary Controller” to indicate successful shift:

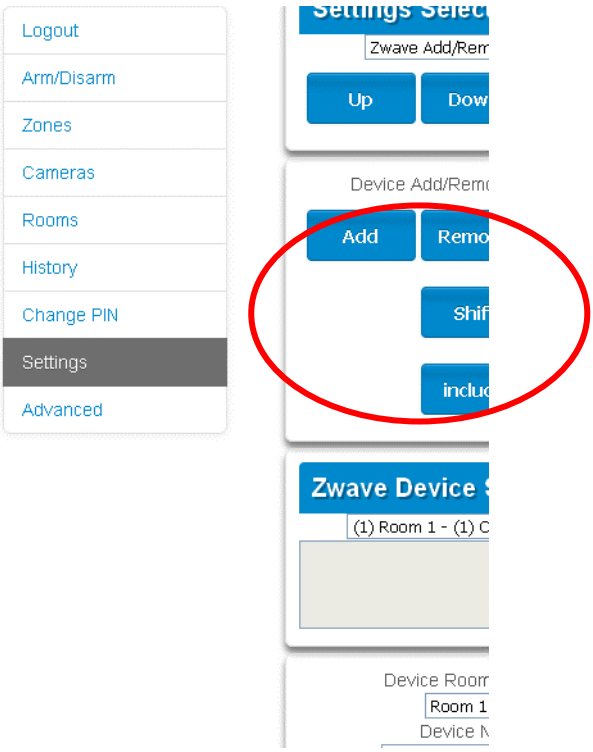


6. xGenLite will now be the Primary Z-Wave Controller, and the other network is the Secondary Z-Wave Controller.

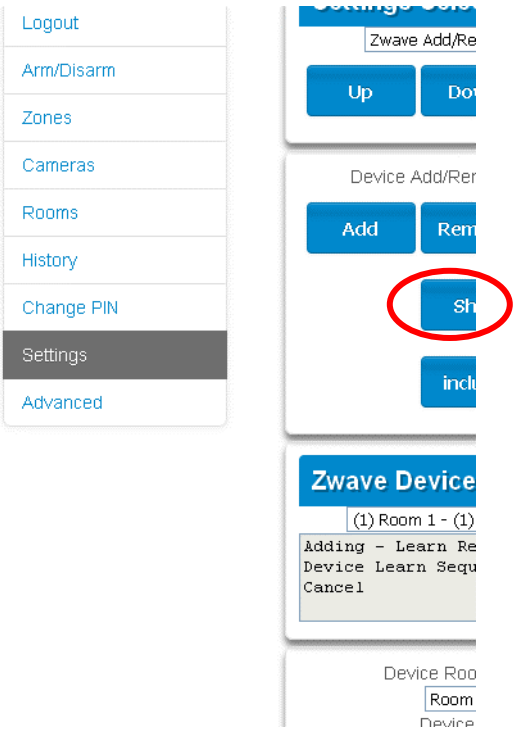
Relinquish Primary Control of xGenLite to another Controller

1. Log in to the panel.
2. Click Settings > Z-Wave Add/Remove.

3. Check xGenLite is the primary controller and a secondary controller is already learnt in to xGenLite. xGenLite in Primary Controller mode has Add, Remove, Cancel, Shift, and Include buttons.

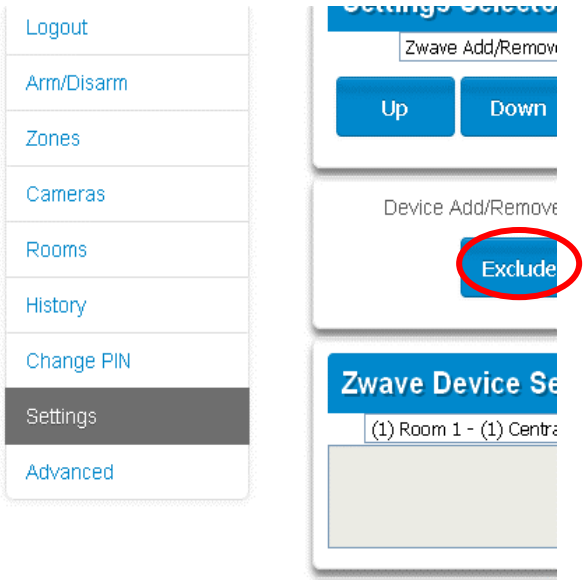


4. Press the Shift button on xGenLite (the Primary Controller).



5. Press the **Exclude** button on the Secondary Controller.

6. xGenLite Primary Controller relinquishes control and becomes Secondary Controller. Only the Exclude button is visible indicating the xGenLite is Secondary Controller.



Secondary Controller shifts into Primary Controller.

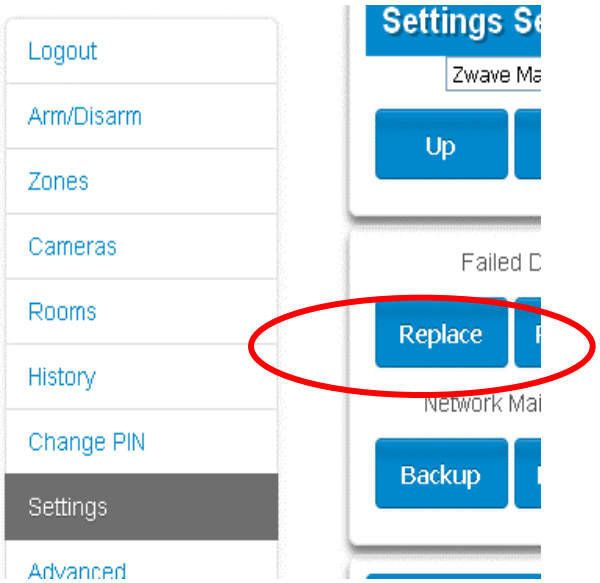
Creating a Device Association

Z-Wave supports a feature called “association”. This allows you to control multiple Z-Wave devices such as lights or even a scene from a single Z-Wave on/off switch.

1. Click Settings > Zwave Device Association
2. Select the Z-Wave device from the drop-down menu.
3. Select an Association Group. Check the Z-Wave device’s manual for supported groups.
4. Select one or more devices to associate. These are the devices that will change state when the device in step 2 is triggered.
5. Click Add.
6. Trigger the device in step 2.
7. Check that the devices in step 4 respond and turn on or off.

Replacing a Failed Node

1. Click Settings > Zwave Maintenance
2. On the Failed Device Selector, click the node to be replaced.



3. Click the Replace button.

   Status will show “Device Not found in failed list” if the device is working.
4. Press the include button on the new node. The old device has now been replaced with the new device.

Creating a Device Association

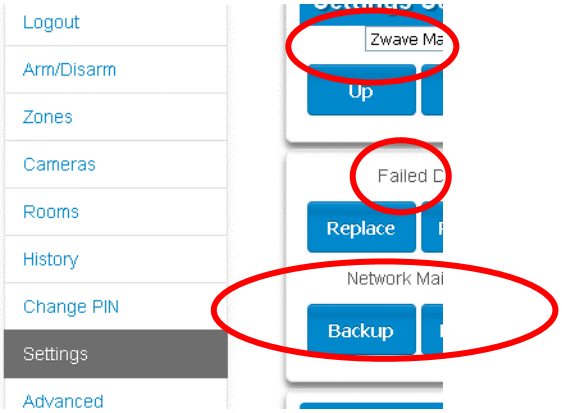
1. Z-Wave supports a feature called “association”. This allows you to control multiple Z-Wave devices such as lights or a scene from a single Z-Wave on/off switch.
2. Click Settings > Zwave Device Association
3. Select the Z-Wave device from the drop-down menu.
4. Select an Association Group. Check the Z-Wave device’s manual for supported groups.
5. Select one or more devices to associate. These are the devices that will change state when the device in step 2 is triggered.
6. Click Add.
7. Trigger the device in step 2.
8. Check that the devices in step 4 respond and turn on or off.

Removing a Failed Node

1. Click Settings > Zwave Maintenance
2. On the Failed Device Selector, click the node to be removed.

3. Click the Remove button.
4. Status will show “Device Removed” when a failed device is removed.

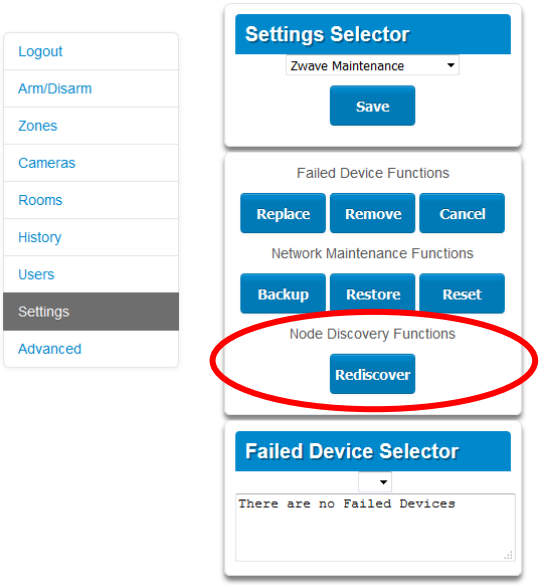
   Or “Device Not found in failed list” if the device is working.



Rediscover Z-Wave Nodes

Z-Wave is a mesh network technology meaning each device can communicate with all nearby devices, and adding more devices generally provides better performance and range. After all Z-Wave devices have been added and installed in their final physical locations, follow these steps to “heal” the Z-Wave network and create the communication paths between each device:

1. Click Settings > Zwave Maintenance.
2. Click the Rediscover button.



Status will show “Rediscovering”.

Status will show “Rediscovery Complete” when successful.

Backup Z-Wave Network

The panel contains a database of all Z-Wave devices and the network configuration. This is separate from the panel programming, and wireless transmitter devices. The Z-Wave Network can be backed up to the internal memory of the panel or downloaded to a computer using DLX900.

To perform a backup of the Z-Wave Network:

1. Click Settings > Zwave Maintenance.
2. Click the Backup button.

Status will show “Backing Up Network”.

Status will show “Network Backed Up” when successful.

Reset Z-Wave Network

The panel contains a database of all Z-Wave devices and the network configuration. The Z-Wave Network can be cleared without affecting panel programming.

To reset the Z-Wave Network back to factory defaults:

1. Click Settings > Zwave Maintenance.
2. Click the Reset button.
3. Click OK to warning message.

Status will show “Resetting Network”.

Status will show “Network Reset” when successful.

Restore Z-Wave Network

The panel contains a database of all Z-Wave devices and the network configuration. If a backup has been previously made, the Z-Wave Network can be restored.

To perform a Z-Wave Network restore:

1. Click Settings > Zwave Maintenance.
2. Click the Restore button.

Status will show “Restoring Network”.

Status will show “Restore Complete” when successful.

Allow a few minutes for the network to refresh itself before programming devices.

Send User PINs to Z-Wave Door Lock

xGenLite can send user PIN codes to a Z-Wave Door Lock. This allows the same PIN codes on the alarm system to operate the door lock.

This feature is available to User Types > Engineer, Master, and Custom users with Z-Wave menu access.

Communication is one way from the xGenLite to the lock, instructing the lock to add or remove PIN codes. Each lock is individually controlled.

When “Send PIN(s) to Lock” is selected, xGenLite queries the lock for the number of standard users it supports. Some locks support up to 250 PINs, others are limited to 40. Check your lock documentation.

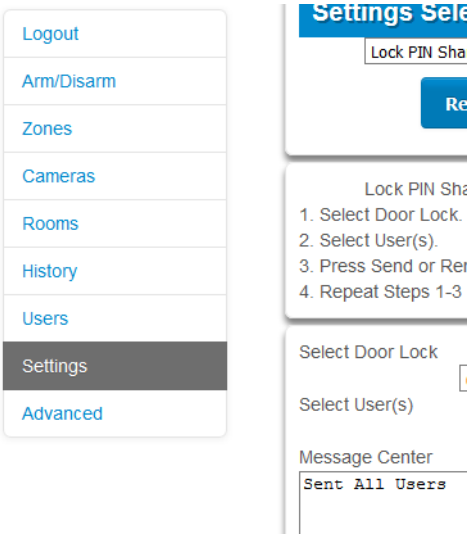
Each xGenLite user number is sent to the same numbered slot in the lock, up to the maximum slots available in the lock. For example, xGenLite user number 1 will be sent to the Z-Wave Door Lock slot 1. Users exceeding the capacity of the lock will not be sent.

Existing PIN codes in the door lock will be over-written. If the lock detects a duplicate PIN then the send command will fail.

Selecting “Remove PIN(s) from Lock” will clear all PIN codes from the lock, whether or not they were added by the xGenLite.

Some door locks have special master/installer PIN codes, these will not be changed. However, if they are default standard user PIN codes then xGenLite will have access to change or remove them. Each lock is different and you should test this feature on your specific lock to ensure only the appropriate codes are present.

As PIN codes can also be changed directly on the door lock, over time there may be a mismatch in PINs on the door lock compared to the panel. To avoid this confusion, only make PIN code changes on the panel and sync them to the door lock.



1. Log in to the panel.
2. Click Settings > Lock PIN Share.

3. Select the Z-Wave Door Lock in the drop-down list. If the lock does not appear, follow instructions on Adding Z-Wave Devices.
4. Wait for the “Building User List – Please Wait” message to be replaced with “Ready”.
5. The default will have “All Users” pre-selected. You may select an individual user instead.
6. Optional and recommended, click “Remove PIN(s) from Lock”. This ensures any extra PIN codes are removed from the lock and only the PIN codes from the panel can operate the lock. Once completed it will show “Removed All Users”.
7. Click “Send PIN(s) to Lock”.

   PIN codes will be sent to Z-Wave door lock one at a time. Once completed it will show “Sent All Users”.
8. Test PIN codes on door lock and verify only the codes you **want can** operate the lock.
9. Refer to door lock manual to remove or change installer / master codes from door lock.

Programming Scenes

xGenLite can perform automation features such as recording video clips when a door is opened, turning on a Z-Wave light when motion is detected, and much more.

This is achieved by creating a “Scene”. Each scene can perform up to 16 actions when a certain condition is met.

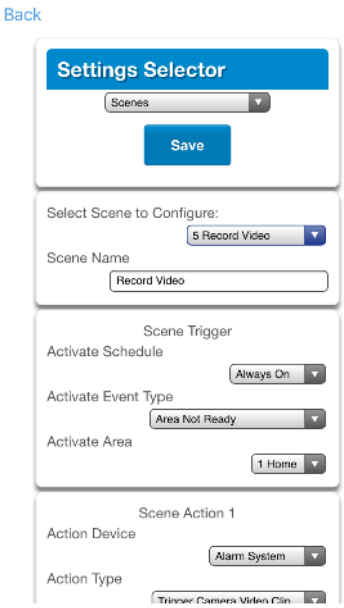
For a full list of functions that can be used to create a scene, refer to the Reference Guide.

To create a scene:

1. Log in to the panel.
2. Select Settings > Scenes.
3. Select the Scene to Configure.
4. Enter a Scene Name. Tip: a name based on the result will help you remember what the scene is. For example, “Downstairs Light On” or “Open Garage Door”.
5. Tick the “Enable App Button” option to show a shortcut button on the home screen of the UltraSync+ app. Untick this option to hide the shortcut.
6. Select Schedule to “Always On”.

   Note: To **restrict** the day and time when the scene will check the trigger, select a schedule from the drop-down. Schedules can be created under Settings > Schedules.
7. Select the Activate Event Type. For example, “Area Not Ready” and “Area 1”.
8. Under Scene Action 1, select Alarm System or the Z-Wave device to control.
9. Select Action Type.
10. Select any additional options as desired.
11. Repeat step 8 to 10 to add additional Scene Actions.
12. Click Save.

13. Test the scene to check if the behavior is desired.



Special Scene Triggers: Geosphere / Geolocation Entered Exited

UltraSync+ app can send the panel a message when a user's mobile phone has entered (within 200 meters) or left (outside 300 meters of) a physical area. This can then be used as a scene trigger. For example, turn on an external security light when the user arrives home.

To enable this scene trigger:

1. Open UltraSync+ app.
2. Click (i) Site Info button.
3. Click Location Services.
4. Click Edit Map.
5. Zoom and move the map to the desired location.
6. Click Save Map.
7. Enable "Geo Actions", this will send the message to the panel.
8. Enable "Check Status on Leaving" if you want a reminder notification from the app when it detects you have left the home location. This feature is independent of the "Notification Services" feature.
9. Click Back.
10. Click Sites.

Special Scene Triggers: Sunrise Sunset

The panel can trigger scenes based on the sunrise/sunset schedule specific to a geographical location. For example, turn on an external security light automatically at sunset.

To enable this scene trigger:

1. Open UltraSync+ app.
2. Click (i) Site Info button.
3. Click Location Services.
4. Click Edit Map.
5. Zoom and move the map to the desired location.
6. Click Save Map.
7. Click “Set Sunrise-Sunset Location”, this will load the sunrise and sunset times specific to the selected location into your panel.
8. Click Back.
9. Click Sites.

Special Scene Triggers: Camera Motion Detection

Selected camera models support motion detection that can be used as a scene trigger.

To enable this scene trigger:

1. Open UltraSync+ app.
2. Log in to the site.
3. Click Cameras.
4. Click the settings icon for the desired camera.
5. Turn on “Enable Motion Detection”.
6. Selected camera models also allow a detection area to be drawn.
7. Click Done.

Special Scene Triggers: Z-Wave Devices

For panels with Z-Wave capabilities, Z-Wave on/off devices can trigger scenes. For example, run a Welcome Home scene when a Z-Wave on/off switch is pressed.

To enable this scene trigger:

1. Add the Z-Wave device.
2. Add a Z-Wave Device Association between the Z-Wave Device and alarm system.
3. Create a new scene and select “Z-Wave Devices” as the scene trigger.
4. Select turn on or turn off for the Z-Wave on/off switch.
5. Select up to 16 actions to perform.
6. Click Save.
7. Test the behaviour by turning the Z-Wave device on or off.

User Reporting

If a scene performs arm/disarm control of an area, User 99 will be reported to the Central Monitoring Station.

xGenLite with Amazon Alexa

xGenLite is Alexa-enabled. Users can use their voice to turn on a Z-Wave device or run an automation scene.

Here are some things you can do:

- Use Alexa to voice control your lights on the xGenLite

  “Alexa, turn off bedroom lights”
- Use Alexa to voice control your fan on the xGenLite

  “Alexa, turn on fan”
- Use Alexa to voice control your xGenLite scenes

  “Alexa, turn on Welcome Home”

To enable Alexa on your xGenLite:

1. Install and configure the UltraSync+ app on your smartphone. Refer to page “Method 3: UltraSync+ App” on page 35 for instructions.
2. Install the Amazon Alexa device using the end-user’s Amazon account. Refer to the instructions with the Amazon Alexa.
3. Open UltraSync+ app on your smartphone.
4. Click the site name to login.
5. Click Menu.
6. Click Amazon® Alexa.
7. Click “Enable Alexa”.
8. A new user will be created on the xGenLite system. Note the details shown on the app.
9. On a computer, login to the Amazon Alexa website: https://alexa.amazon.com/spa/index.html
10. Search for the UltraSync skill and enable it.
11. Click Settings – Account Linking.
12. Enter the details shown on the UltraSync+ app in the UltraSync skill. Amazon Alexa will use this xGenLite user to login and interact with xGenLite.
13. Click Manage Smart Home Devices.
14. Click Devices to check what devices and scenes can be Alexa controlled.
15. Click Discover to update the list.

Notes

- Z-Wave devices must be pre-programmed in the xGenLite. Check that your panel has Z-Wave capabilities.
- Scenes must be pre-programmed in xGenLite.

- Amazon Alexa must be purchased separately and a valid Amazon account is required to operate it.
- Amazon Alexa integration is not supported in all regions.
- Not all Alexa features may be available on this device, learn more at www.interlogix.com.
- Amazon Alexa Terms and Conditions do not allow control of garage doors, door locks, or cameras. Arming and disarming is also not allowed. Actions that control these items inside scenes will be skipped, the remainder of the scene will run correctly.

DLX900 Software

DLX900 is a tool for programming xGenLite systems. This software is installed on a PC with Microsoft Windows 7, 8, or 10. It features a graphical interface, allowing installers and Central Monitoring Stations to program and manage complex sites.

Customer details and all panel programming are stored in a local database on the computer. This allows companies to create standard templates for quicker programming of customer panels.

Installing DLX900

Download the latest version from https://www.interlogix.com/library.

You will need administrator privileges to install DLX900.

Double click the installation file and select the correct region. This will affect the panels the software will support.

Upgrading from DL900

DLX900 in Australia supports NetworX panels as in DL900.

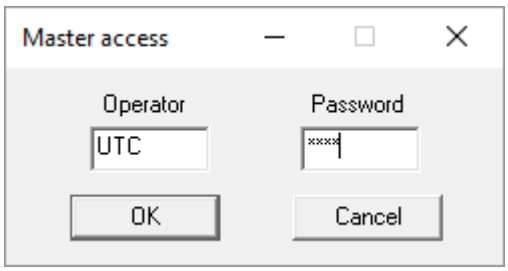
If DL900 has been installed previously, DLX900 can automatically import and upgrade the database. It is recommended you save a backup of your database and ensure you have a copy of DL900 in case you need to revert back.

Once DLX900 is installed, right click the icon, click “More”, and select “Run as Administrator”

Login to DLX

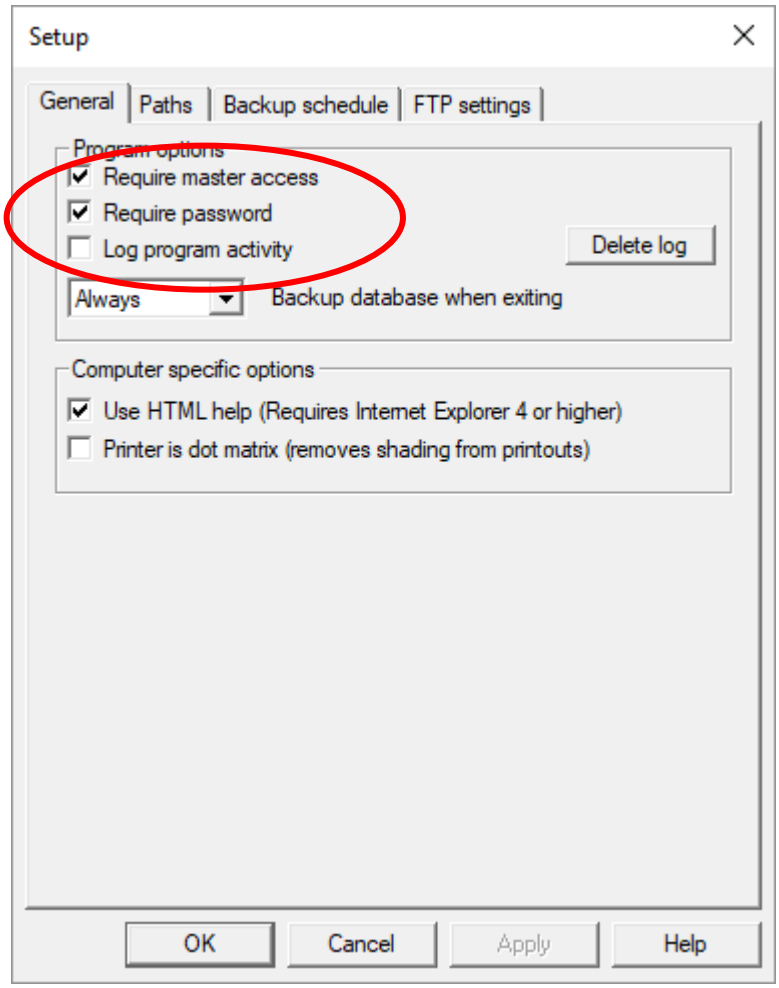
Default user name and password for DLX900 is UTC 1234.

Enter this twice (once for master access, once for operator access) to login.

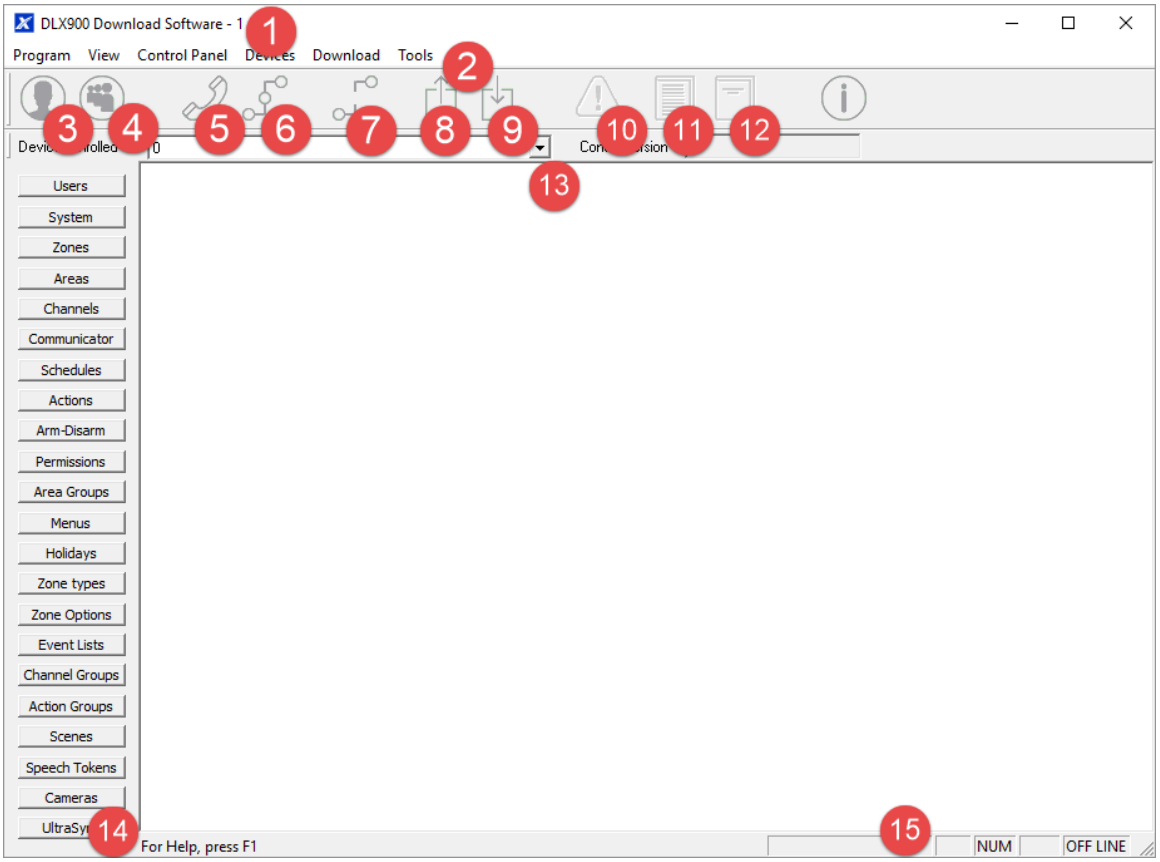


You must change the password. To change the default accounts and passwords: click Program – Setup – Add/change Operators. Click the user then “Set Password”.

To enable or disable password prompt(s): click Program > Setup > Program Setup.



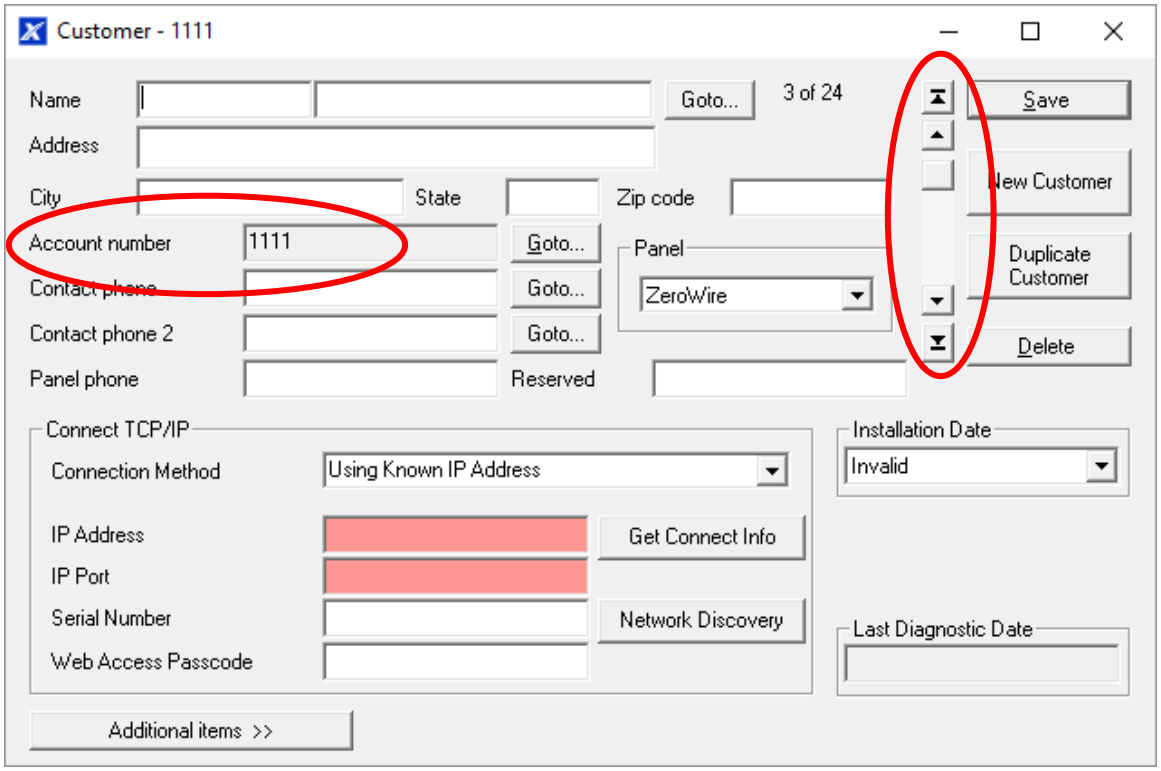
Navigating the Main Window



1. Window Title: Displays currently selected customer's account number.
2. Menu Bar: Program contains settings for DLX900, View turns on/off Toolbar and Status Bar, View also has shortcut to the customer list, Control Panel displays all top-level programming menus for the currently selected customer's control panel, Devices displays all programmed expansion devices, Download displays connection commands, Tools displays DLX900 database management tools and Diagnostics.
3. View Customer: Add/edit/delete customers, select customer to view.
4. View Customer List: Show all customers in current DLX900 database.
5. Call control panel: Use PSTN modem to connect to control panel.
6. Connect TCP/IP: Connect to control panel using TCP/IP.
7. Disconnect: End current session and disconnect from control panel.
8. Send all data: Send all programming menus from DLX900 to control Panel.
9. Read all data: Read all programming data from control panel into DLX900.
10. View Status: View control panel system status (armed state, alarms, and troubles).
11. Read All Event Log: Retrieve all event history.
12. Read 10 Events: Retrieve last 10 items from event history.

13. Devices Enrolled: Drop-down menu with shortcuts to enrolled expander devices.
14. Control Panel Menu: Shortcuts to control panel settings, available on selected panels.
15. DLX900 Status: Shows a progress bar of read and send commands, Caps Lock, Scroll Lock, Num Lock, and Online/Offline connection state to control panel.

Customer Window



Each customer must have a unique Account Number.

Selecting a Customer

DLX900 will load programming for the currently displayed customer in any menus displayed. Select a customer by:

- Using the Up and down arrow buttons to navigate through your customers;
- Entering the customer's detail in the name or contact phone field, then click Goto;
- Clicking the Account number Goto, then enter the account number; or
- Clicking View Customer List, then click the customer displayed.

Duplicating a Customer

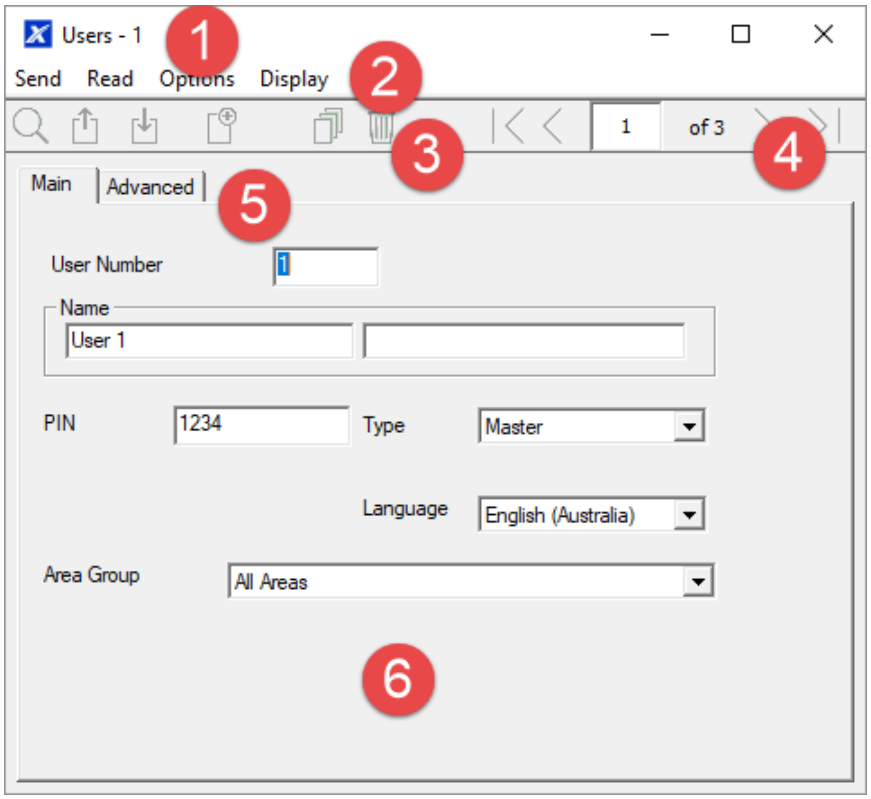
DLX900 allows easy duplication of customer programming for similar sites.

1. Select a customer with the programming to duplicate.

2. Click Duplicate Customer.
3. Enter a new Account Number.
4. Tick “Copy customer information” if you want the contact details and serial number of the panel to also be copied. This is useful if you are testing new programming for the same customer.
5. Click OK.

Navigating the Menus

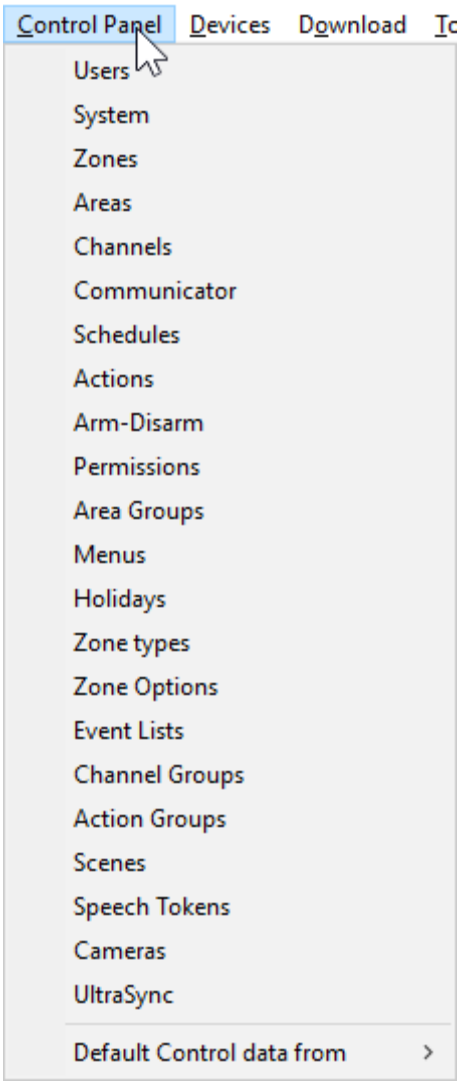
Each menu has a set of common elements:



1. Menu Name: Displays the menu name and current customer’s account number.
2. Menu Bar: Commands to Send data to the panel, Read data from the panel, and Options to restore factory defaults for this menu.
3. Tool Bar: Search for customers, Send only this menu’s data to the panel, Read only this menu’s data from the panel, Add a new record, Copy the current record, and Delete the current record.
4. Navigation Buttons: Jump to the first record, go back one record, enter a record number, see the number of records for the current menu, go forward one record, jump to the last record.
5. Sub-menu Tabs: These reflect the sub-menus in the Reference Guide.
6. Programming options: Changes to these settings are saved immediately to the database, to make them “active” perform a Send command.

Control Panel Menu

This menu features all programming locations for the main panel. For supported models, these menus also appear on the left side of the Main Menu.



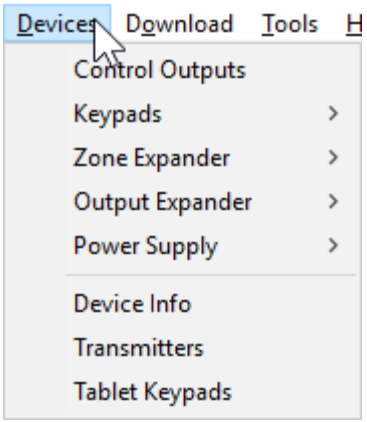
Loading Control Panel Defaults

DLX900 can load factory default data for the currently selected customer panel:

1. Click Control Panel.
2. Click Default Control data from > Factory defaults.

Devices Menu

The Devices Menu displays all expansion devices including keypads, input expanders, output expanders, power supplies, touchscreen tablets, wireless devices, and keyfobs.

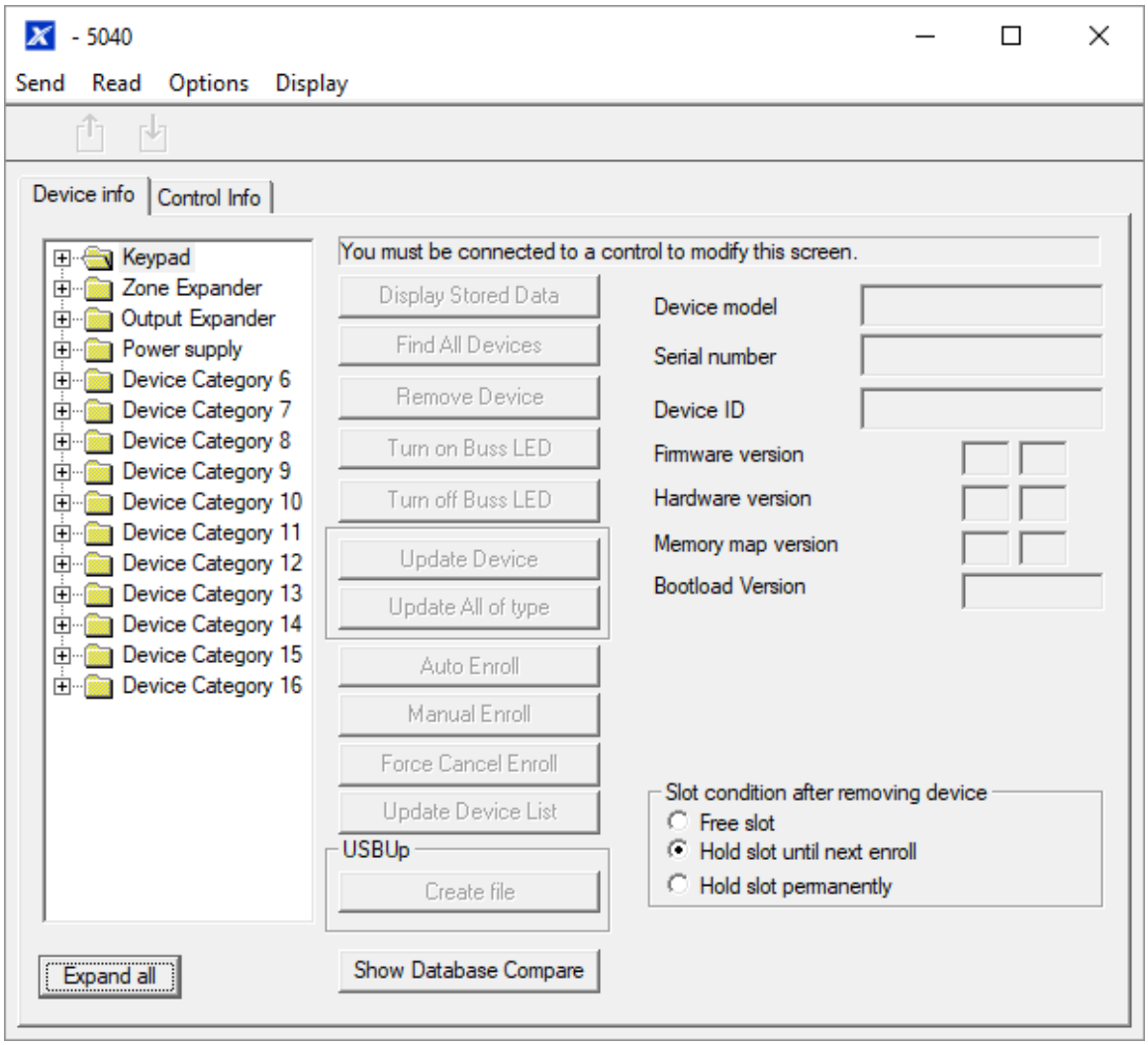


Each of these devices may have separate programming stored inside that device. This menu allows you access to those programming locations.

Programming is retrieved from all enrolled devices when you perform a Read All.

Device Info

Click Devices > Device Info to show all expansion devices:

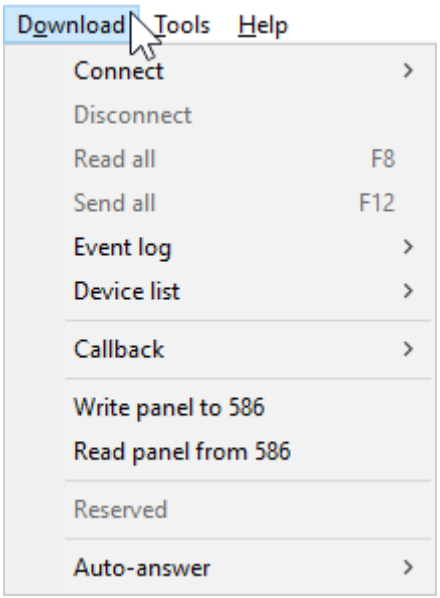


The Device Info menu allows:

- Adding and removing of devices: Click Remove Device, Auto Enroll, Manual Enroll, or Add Device under the device category.
- Identification of devices: Click Turn on / off Buss LED to flash an LED of the specific device.
- Re-ordering of devices: Drag and drop the device to re-number it, use the “Slot condition after removing device” to determine if DLX900 should refresh all device numbering or to reserve the device number for future use.
- Display of device information including firmware and serial number.
- Access programmed data: Select the device and click Display Stored Data, this is the same as accessing the device via the Devices Menu.
- Export of programming information for a specific device: Select the device and click Create file. DLX900 will create a special file. This file can be copied to a USBUp and then inserted into a suitable device to program it without a computer.

- Export control panel information for use with USBNav – on the Control Info tab click Create file to save current panel programming to a special file. This file can be copied to a USBUp and then inserted into a xGenLite system to program it without a computer.

Download Menu



This menu allows you to:

- Initiate a connection to the panel.
- Disconnect from a panel.
- Read all programming, including all connected expansion devices and backup copies where available.
- Send all programming to the panel.
- Read the event log.
- Initiate a callback session before download, where this feature is enabled on the panel.
- Write programming to a NX-586 / NX-588. This allows on-site programming of selected panels without the need for a computer.
- Read programming from a NX-586 / NX-588. This allows retrieval of panel programming from selected panels on-site without the need for a computer.
- Enable auto-answer for callback.

Reading Data

All programming located inside a customer panel can be retrieved and stored in the DLX900 database for further editing or backup purposes.

Reading All Data

To retrieve the contents of all control panel menus and store it in DLX900:

1. Select the customer you want to connect to.
2. Connect to the panel.
3. Click the Read All button on the toolbar. Alternatively, from any menu click Read > Read Control to only retrieve panel programming without data stored inside expansion devices.
4. Wait for the progress bar on the bottom right to complete. DLX900 will retrieve data from multiple menus, each will have its own progress bar.
5. Disconnect from the panel.

All data is now stored in your local database. Any changes made in DLX900 will not be reflected in the customer panel. To make changes “live”, follow the instructions on Sending All Data.

Note: Z-wave and Transmitter programming is NOT copied during this process.

Reading Data from a Selected Menu

Programming from a single menu can be retrieved from the control panel into DLX900:

1. Select a customer to connect to.
2. Connect to the panel.
3. Open the menu you wish to read.
4. Click Read > Read Menu.

   Data from all tabs in the current menu will be read into DLX900. Wait for the progress bar on the bottom right to complete.
5. Disconnect from the panel.

Sending Data

Once programming has been created in DLX900, it must be sent to the panel using a “Send” command.

Sending All Data

To send the contents of all DLX900 menus to the control panel:

1. Select the customer you want to connect to.
2. Make all changes required to customer programming.
3. Connect to the panel.

4. Click the Send All button on the toolbar. Alternatively, from any menu click Send > Send Control.
5. Wait for the progress bar on the bottom right to complete. DLX900 will send data to multiple locations in the panel, each will have its own progress bar.
6. Disconnect from the panel.

All panel programming has been copied to the panel.

Sending Data from a Selected Menu

Programming from a single menu can be sent from DLX900 to the control panel:

1. Select the customer you want to connect to.
2. Connect to the panel.
3. Open the menu you wish to send.
4. Click the Send > Send Menu.

   Data from all tabs in the current menu will be sent to the panel. Wait for the progress bar on the bottom right to complete.
5. Disconnect from the panel.

Tools Menu

This menu provides database management features to maintain DLX900. This includes:

- Compact Database: The database may grow in size over time with adding and removing of customers. Click this option to clean the database and make it smaller.
- Repair Database: DLX900 will check the database for any errors and repair them where possible.
- Backup Database: The database should be regularly backed up and copied off the computer to a secure location. DLX900 will regularly request to perform a backup of the database when you exit the program. To change the frequency of the backup request, click Program > Setup > Program Setup > Backup Schedule.
- Restore Database: The database can be restored to a new computer if required.
- Import Customers: Specific customers can be recovered from an existing database backup file. This will read all customers or a specific customer (account number) into the current database.
- Export Customers: Specific customers can be saved to a new database.
- Diagnostics: Display real-time communication data between the panel and DLX900.

Programming with DLX900

This section of the manual will describe the steps needed to program each feature using the DLX900 software.

Selected screen shots of the xGenLite Web Server are also included for your reference. Similar screens appear on the UltraSync+ app.

Programming Instructions for System Options

Goal

Program System Options including time and date, tamper, siren, timers, and service settings.

Pre-conditions

Time and date are automatically updated using an Internet time server by default, this setting is enabled under Communicator > IP Config.

If you want to allow xGenLite to send diagnostic emails then check email is set up correctly under Communicator > Email and xGenLite is connected to a network.

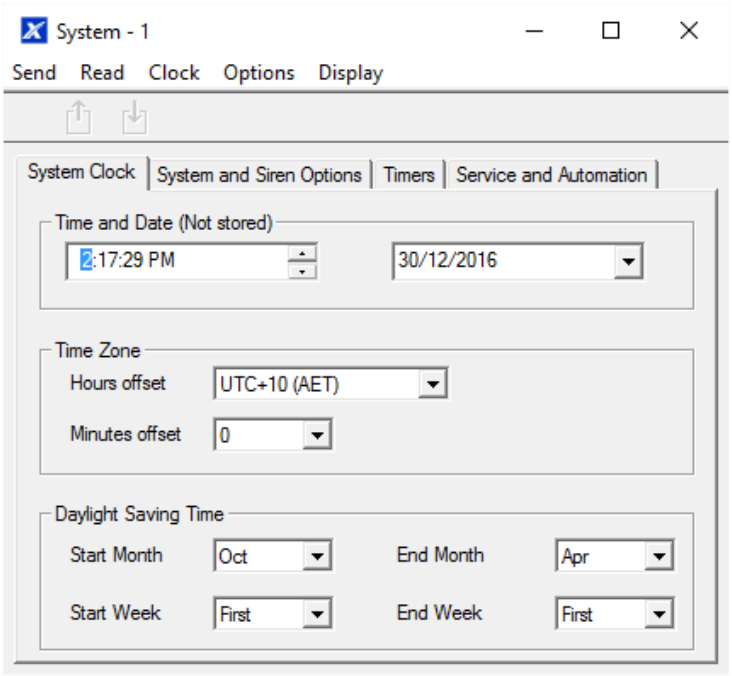
Note: Ensure you set the correct time zone here.

Programming Sequence

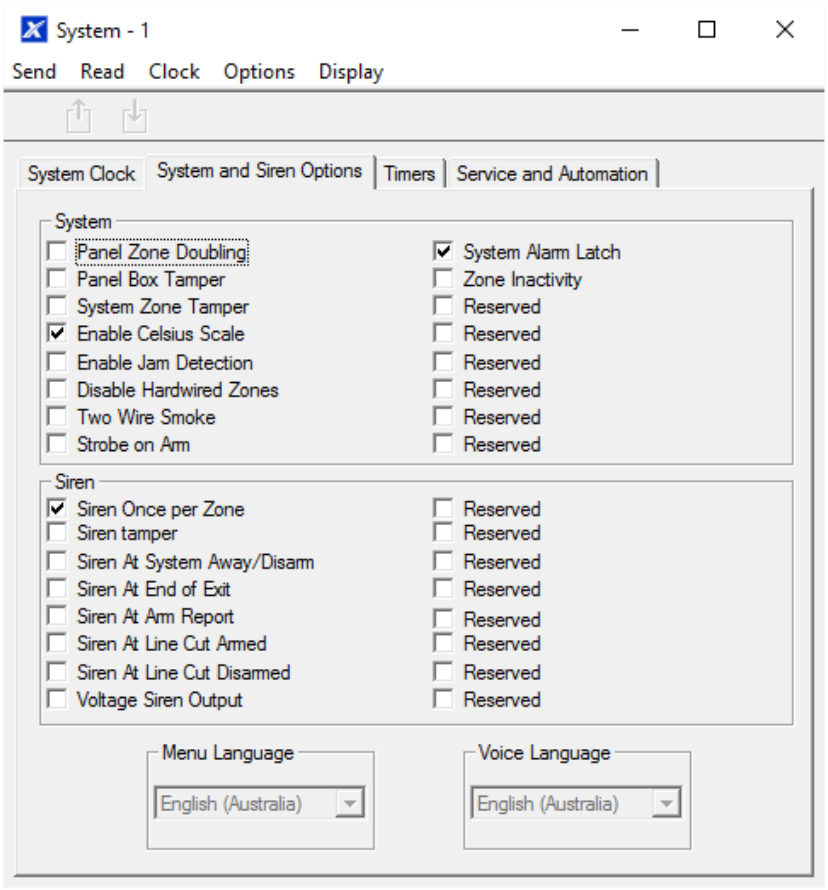
```
2. System
   a) System Clock
   b) System and Siren
   c) Timers
   d) Maintenance and Test
```

Instructions

1. Open System

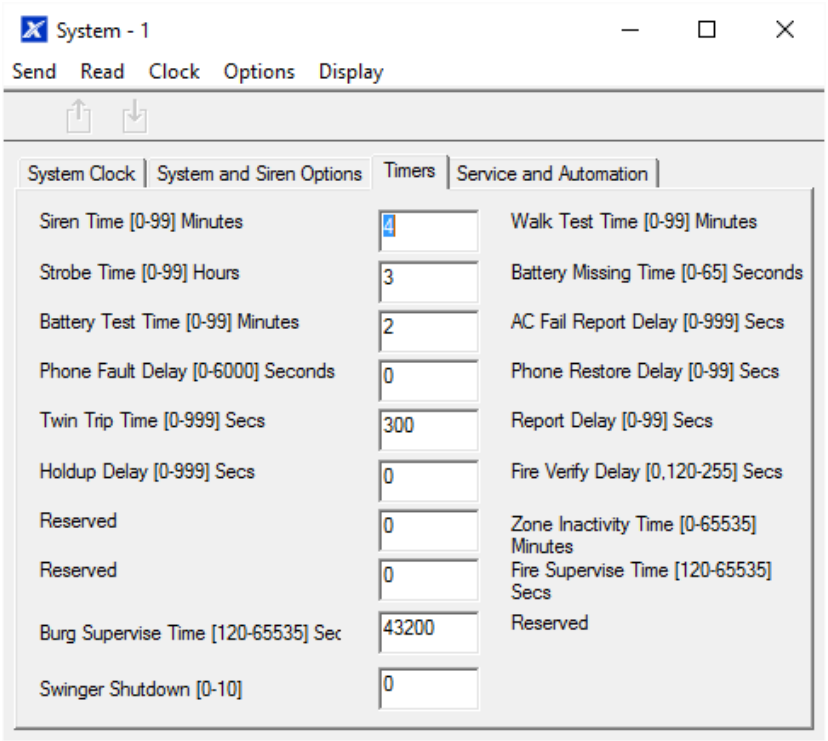


2. Select the right Time Zone using the Hours and minutes offset
3. If you wish to update the time and date
4. Go to System and Siren Options

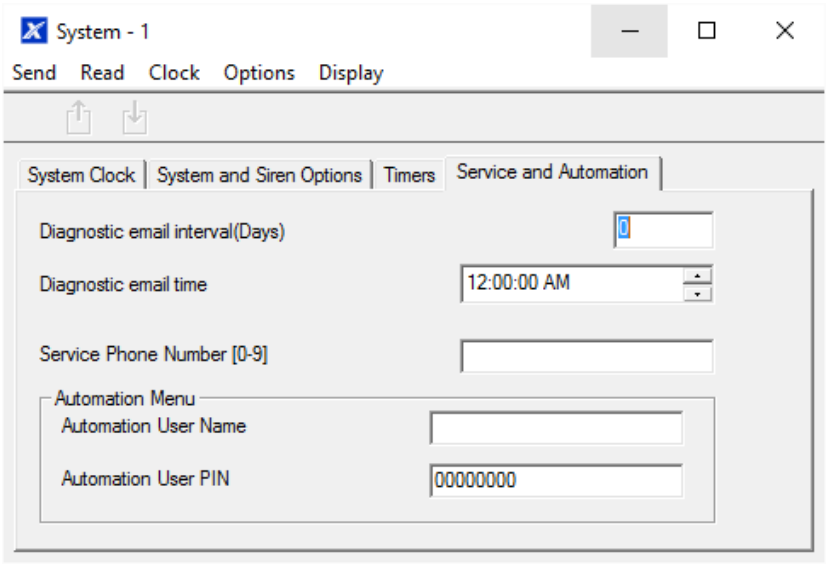


5. Select the settings you want to enable

6. Go to Timers

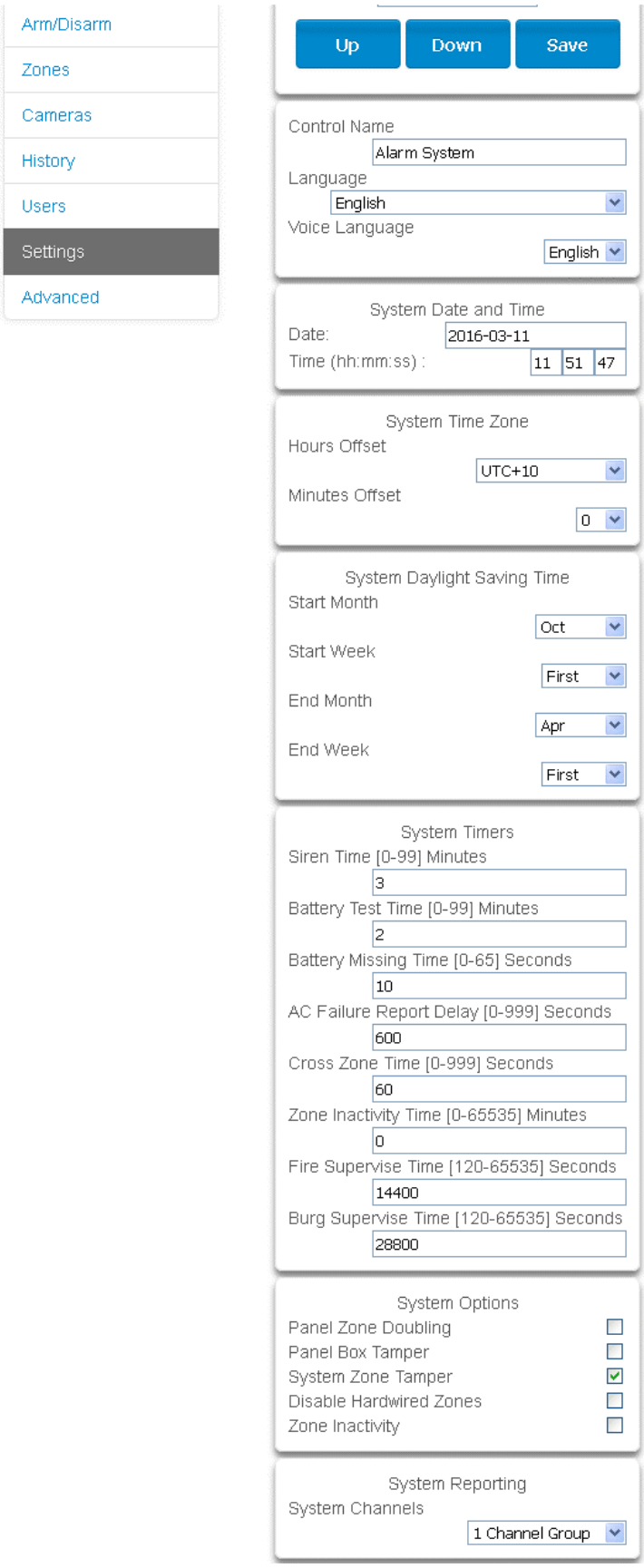


7. Enter the settings for global timers. Note Entry/Exit times are not here, go to Areas > Area Timers.
8. Go to Maintenance and Test



9. Enter a Diagnostic email interval. This is the number of days to wait before sending an email at the specified time. This verifies email communication is working.

Web Page


Arm/Disarm
Zones
Cameras
History
Users
Settings
Advanced
Up
Down
Save
Control Name
Alarm System
Language
English
Voice Language
English
System Date and Time
Date:
2016-03-11
Time (hh:mm:ss) :
11
51
47
System Time Zone
Hours Offset
UTC+10
Minutes Offset
0
System Daylight Saving Time
Start Month
Oct
Start Week
First
End Month
Apr
End Week
First
System Timers
Siren Time [0-99] Minutes
3
Battery Test Time [0-99] Minutes
2
Battery Missing Time [0-65] Seconds
10
AC Failure Report Delay [0-999] Seconds
600
Cross Zone Time [0-999] Seconds
60
Zone Inactivity Time [0-65535] Minutes
0
Fire Supervise Time [120-65535] Seconds
14400
Burg Supervise Time [120-65535] Seconds
28800
System Options
Panel Zone Doubling
Panel Box Tamper
System Zone Tamper
Disable Hardwired Zones
Zone Inactivity
System Reporting
System Channels
1 Channel Group

Programming Instructions for Permissions

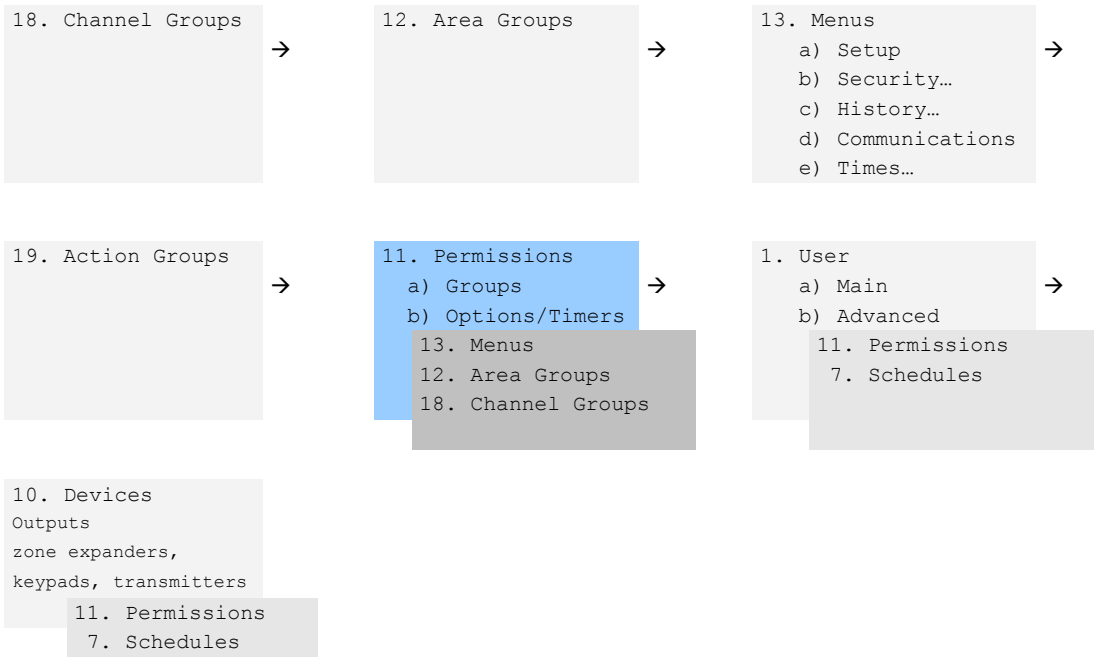
Goal

Create a list of permissions that will restrict users, keypads, and devices to specific parts of the system.

Pre-conditions

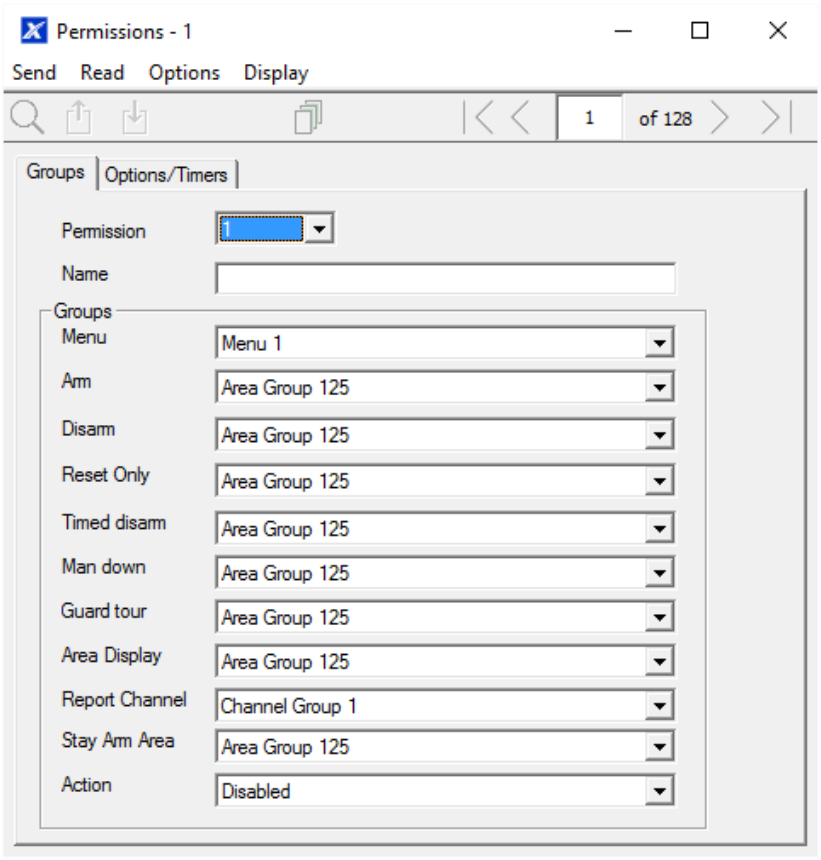
Have programmed or customized Channel Groups, Area Groups, Menus, and Action Groups. Alternatively you can use the preset groups.

Programming Sequence



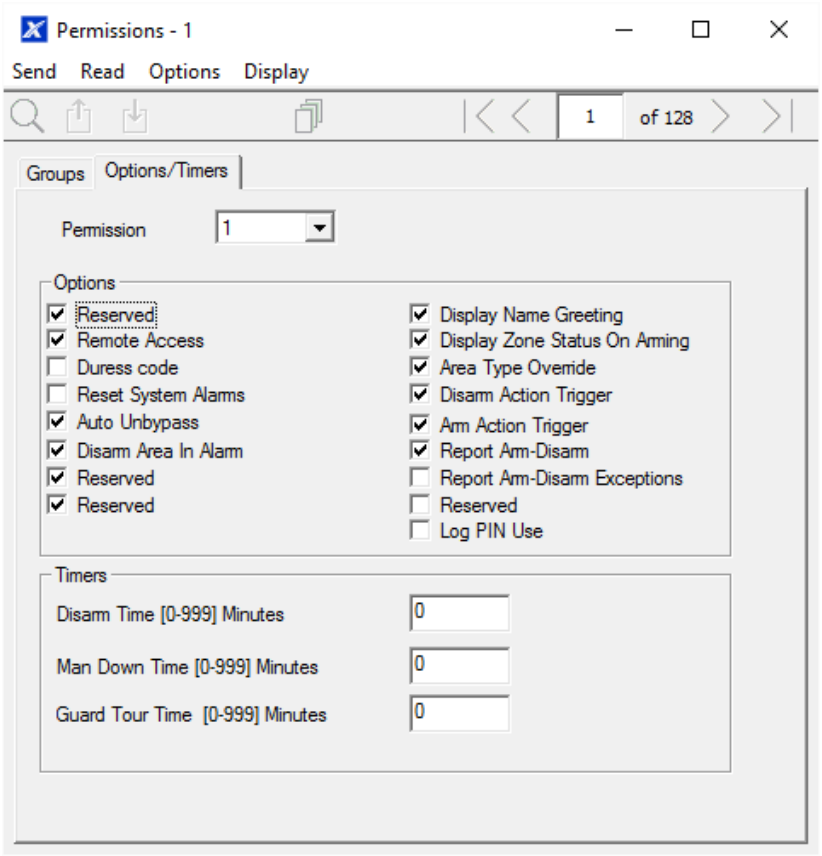
Instructions

1. Open Permissions



2. Select the permission number you want to modify
3. Enter a functional name for the permission
4. Select the Groups for each item which will give access to the items selected inside the group. For example, if this permission is assigned to a user, then that user will have access to Arm each of the Areas that are selected inside the Area Group and no others.

5. Click the Options/Timers tab



6. Select the user options that you want to apply to this permission. Descriptions of each item are available in the xGenLite Reference Guide.

Next

- Program Users or Devices

Programming Instructions for Menus

Goal

Create a list of menus that a user or device has access to on the xGenLite system.

Pre-conditions

None.

Notes

The menus that will be available are the ones that the device has permission to display AND the ones that a user has access to, at the specified time and date which is controlled by Schedules.

Users have up to 4 levels of access and devices have up to 2. This allows very sophisticated and fine grained control of access.

64 custom menus can be created. The preset ones will help you create a system quickly without needing to modify these.

Programming Sequence

13. Menus
    a) Setup
    b) Security…
    c) History…
    d) Communications
    e) Times…

→

11. Permissions
    a) Groups
    b) Options/Timers
    13. Menus
    12. Area Groups
    18. Channel Groups
    19. Action Groups

→

1. User
    a) Main
    b) Advanced
    11. Permissions
    7. Schedules

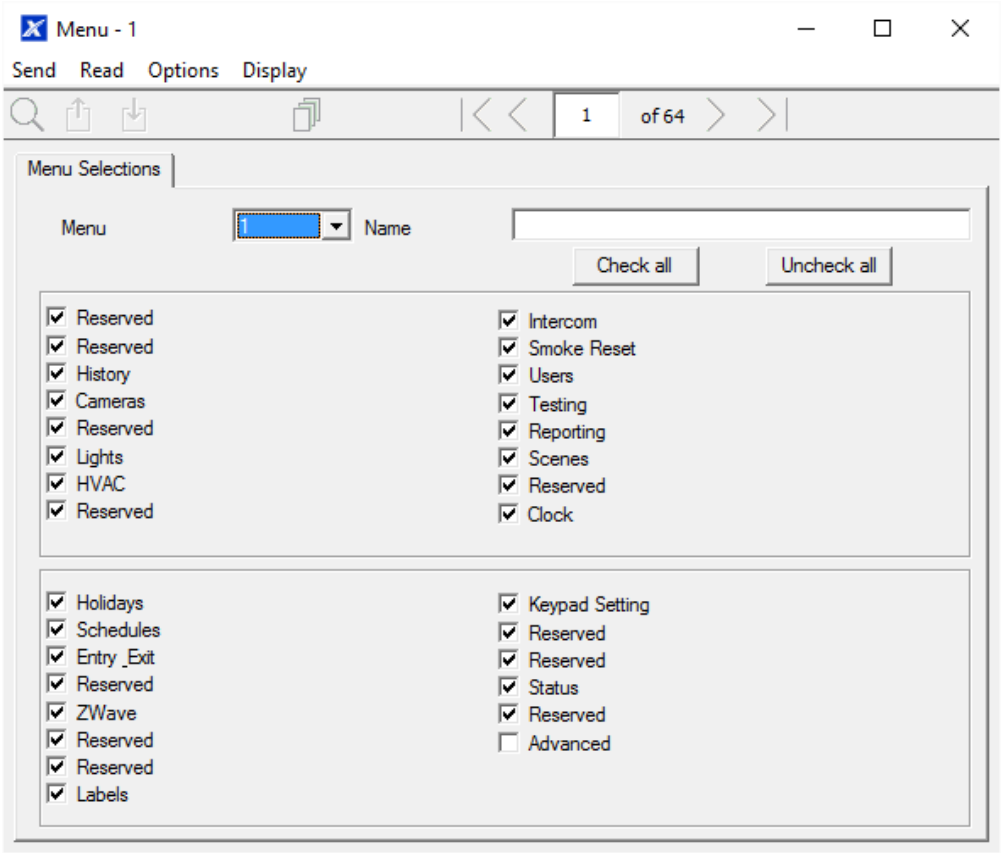
→

10. Devices
Outputs
zone expanders,
keypads, transmitters

11. Permissions
7. Schedules

Instructions

1. Open Menus



2. Select the Menu number
3. Enter a descriptive name
4. Tick each item that you want a user / device to have access to.

Next

- Program Permissions
- Assign the Permission to a User or a Device

Programming Instructions for Holidays

Goal

Create a list of holidays to provide or prevent access to the xGenLite system on the specific dates.

Pre-conditions

None.

Notes

Ticking Holidays in a Schedule for a permission PREVENTS access.

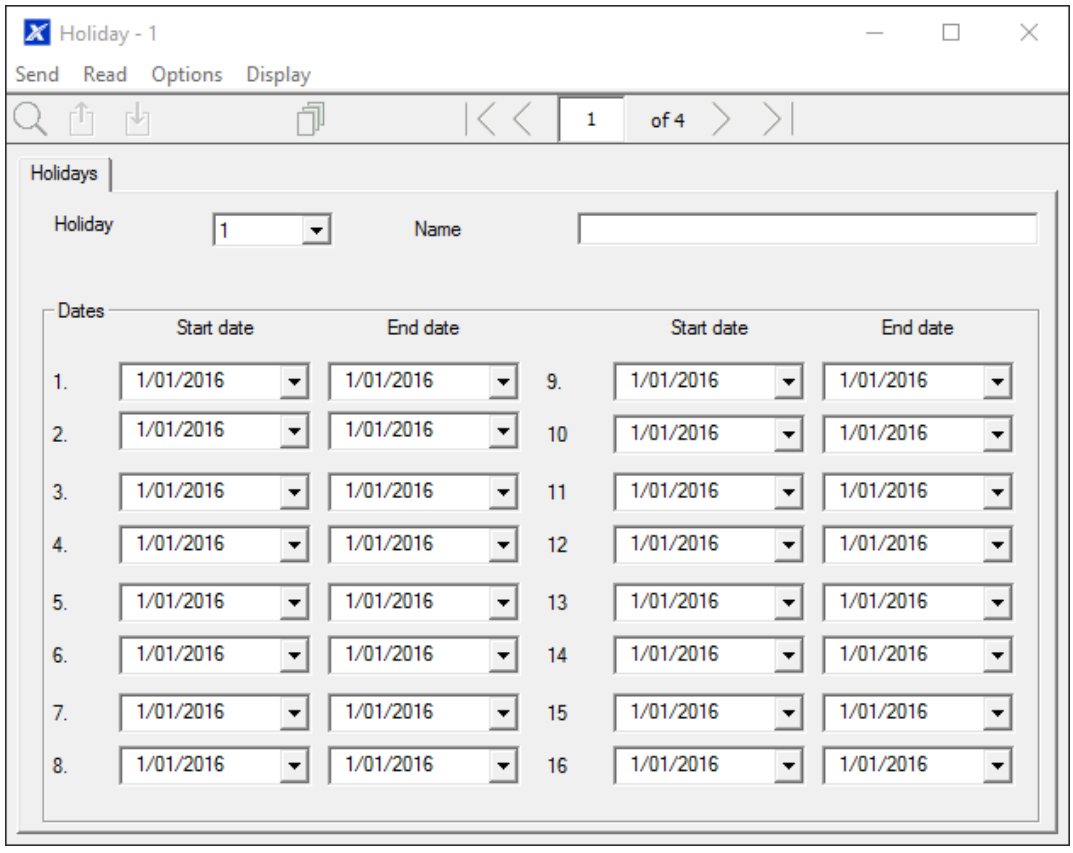
Holiday schedules may impact automation features such as Actions if they are in use. For example, you may not want an Action to play on a holiday, so take care in programming the associated Schedule and permissions.

Programming Sequence

14. Holidays → 7. Schedules → 14. Holidays

Instructions

1. Open Holidays



2. Select one of the 4 Holidays available
3. Enter a name for the Holidays
4. Enter the start and end date for each holiday you have

Next

- Program Schedules

Example

Office Worker

User Permission 1 – All Areas

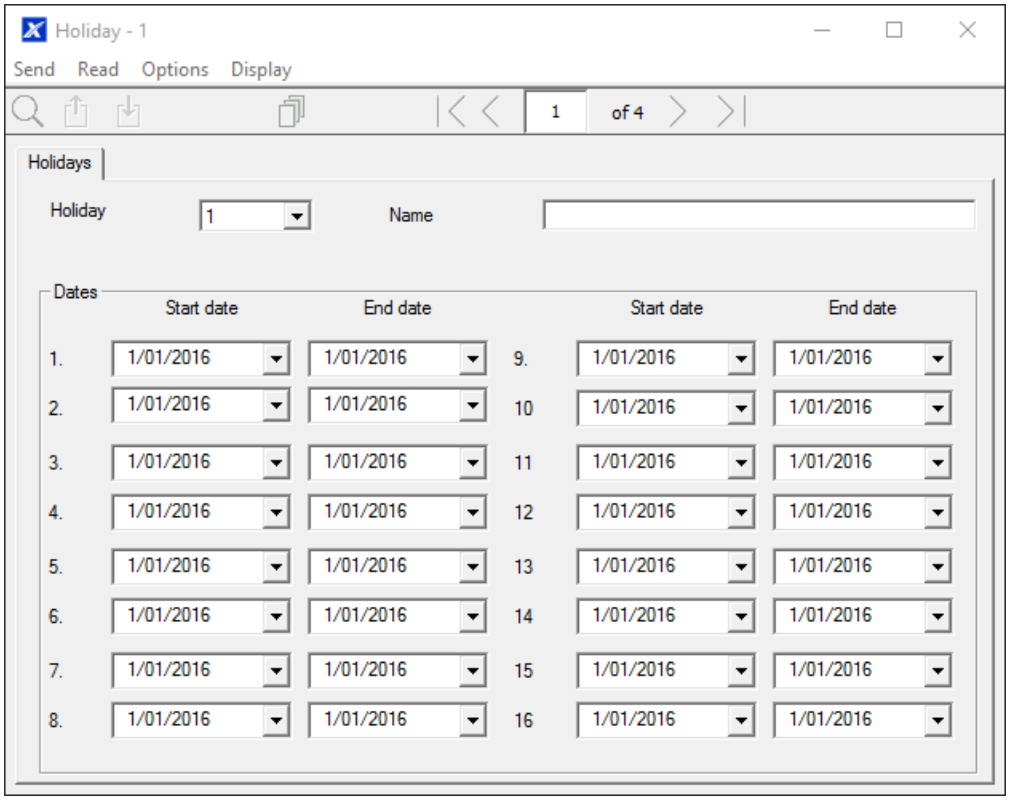
Office Schedule 1 – 8am-8pm M-F, Holidays 1 (ticked)

An office is not staffed during a public holiday and you want to prevent access to the building to staff on this date.

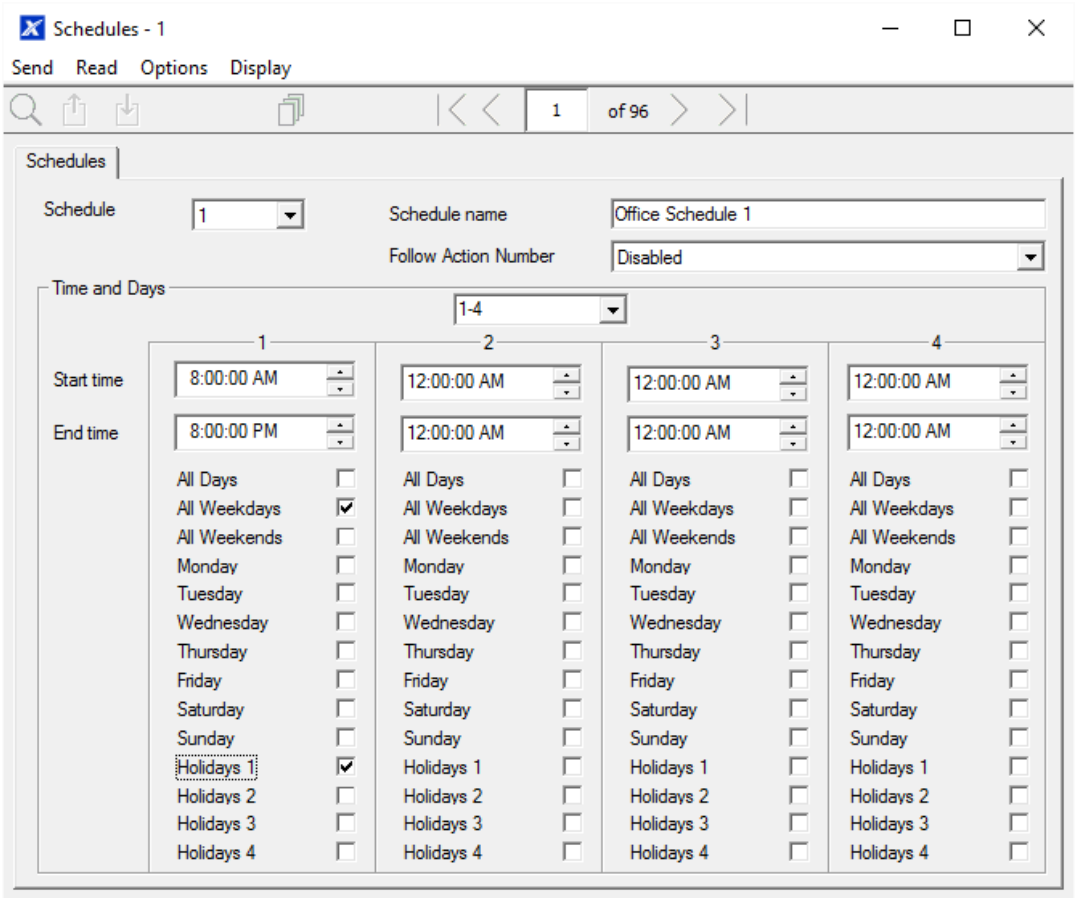
The public holidays in NSW, Australia for 2019 are:

- New Year's Day: 1 January
- Australia Day: 26 January
- #Additional Day: 28 January
- Good Friday: 19 April
- Day following Good Friday: 20 April
- Easter Sunday: 21 April
- Easter Monday: 22 April
- Anzac Day: 25 April
- Queen's Birthday: 10 June
- Labour Day: 7 October
- Christmas Day: 25 December
- Boxing Day: 26 December

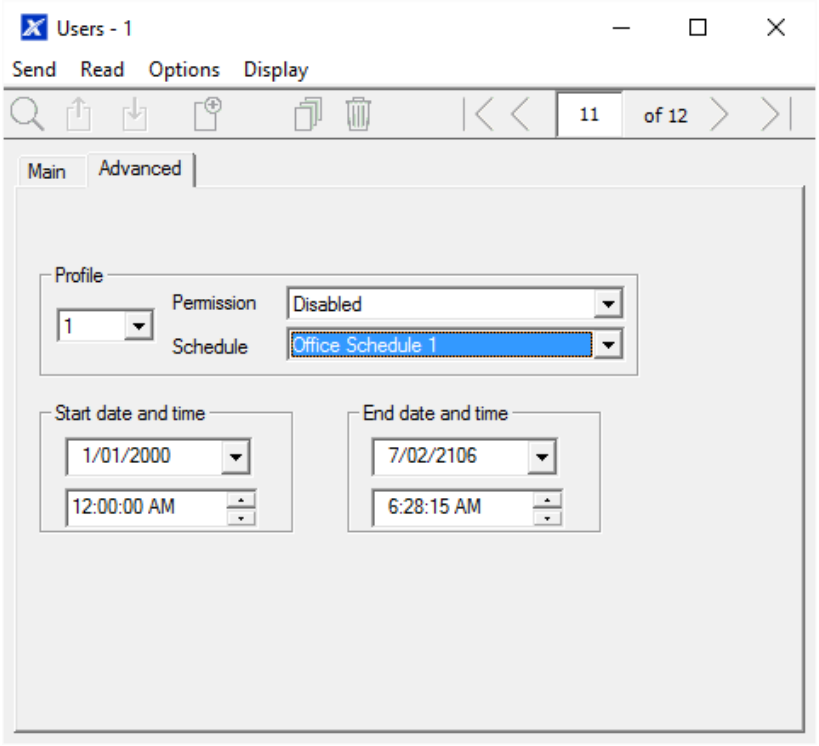
Open Holidays and program the date ranges.



Next, go to Schedules and tick “Holidays 1”:



Then assign that schedule to the User:



Programming Instructions for Users

Goal

Add/Edit/Remove users from your xGenLite system.

Pre-conditions

- Have programmed or customized Permissions. Alternatively you can use the defaults.
- Have programmed or customized Schedules. Alternatively you can use the defaults.

Notes

PIN codes must be unique across the system, no two users can share the same PIN code.

PIN codes must be 4 to 8 digits in length.

EN 50131 Grade 2 required settings are 6 digits minimum.

User name must be assigned to give that user access to UltraSync+ app or xGenLite Web Server. A user with no first name will be unable to gain remote access.

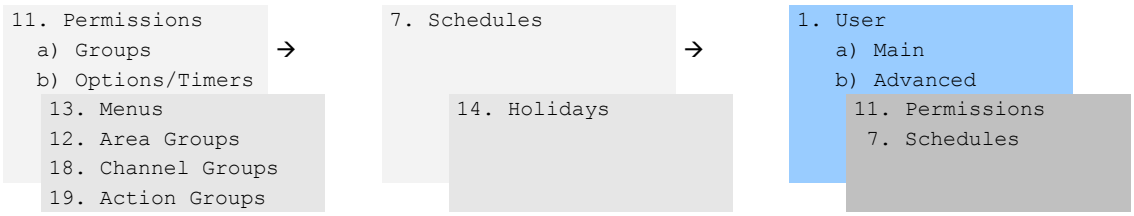
The default installer account is User 256 with user name installer and PIN 9713, with Master Engineer user type. These details are used to Log in to the Web Server web pages and UltraSync+ app.

The default master account is “User 1” and PIN 1234.

The default standard account is “User 2” and PIN 5678.

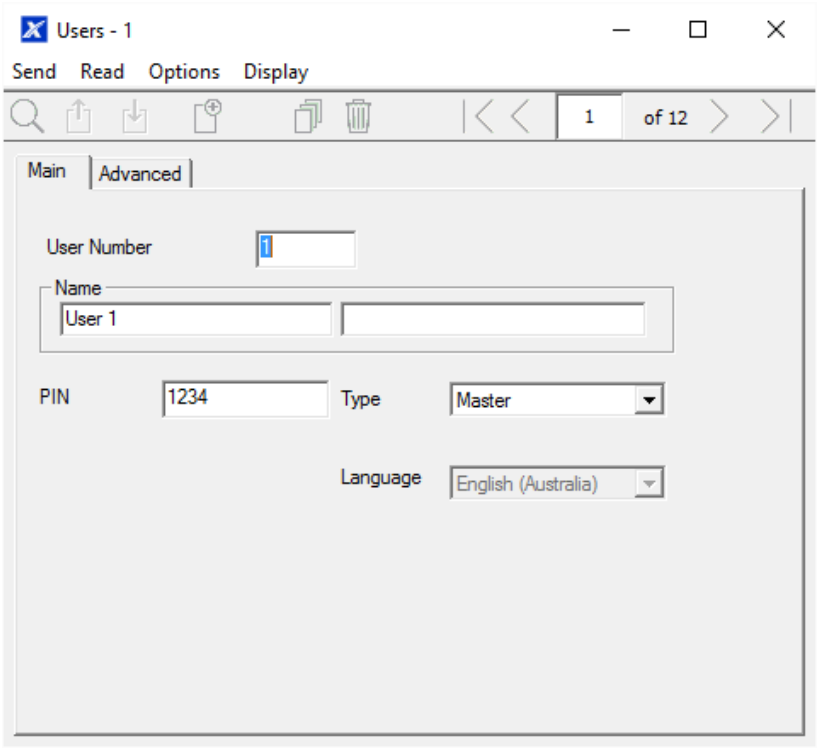
Note: EN 50131 Grade 2 default codes are 971300, 123400, 567800.

Programming Sequence



Instructions

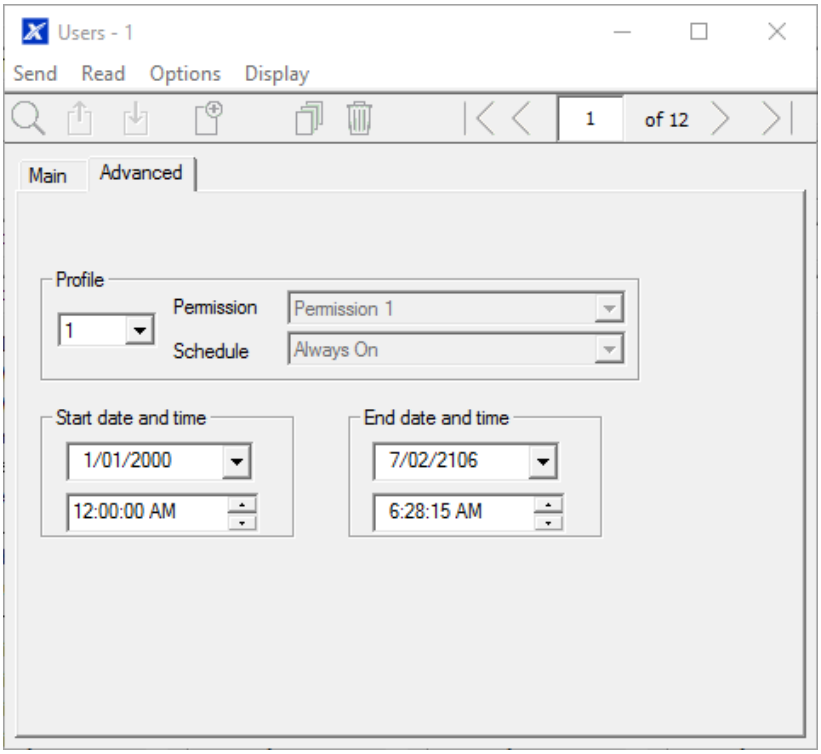
1. Open Users



2. Select the User number you want to modify with the Left and Right arrow keys on the top right. You can also Search, Add, Copy, and Delete a user by clicking the corresponding button on the toolbar.

3. Enter a first name and/or last name for the user. It is case sensitive and provides the user name to log in from the UltraSync+ app.
4. Enter a new PIN code for the user. It must be unique and 4 to 8 digits long.
5. Select the user type that you want to apply to this user. Descriptions of each type are available in the xGenLite Reference Guide.

6. The Status option determines if that user can interact with the system, or if their access has expired.
7. Click the Advanced tab.

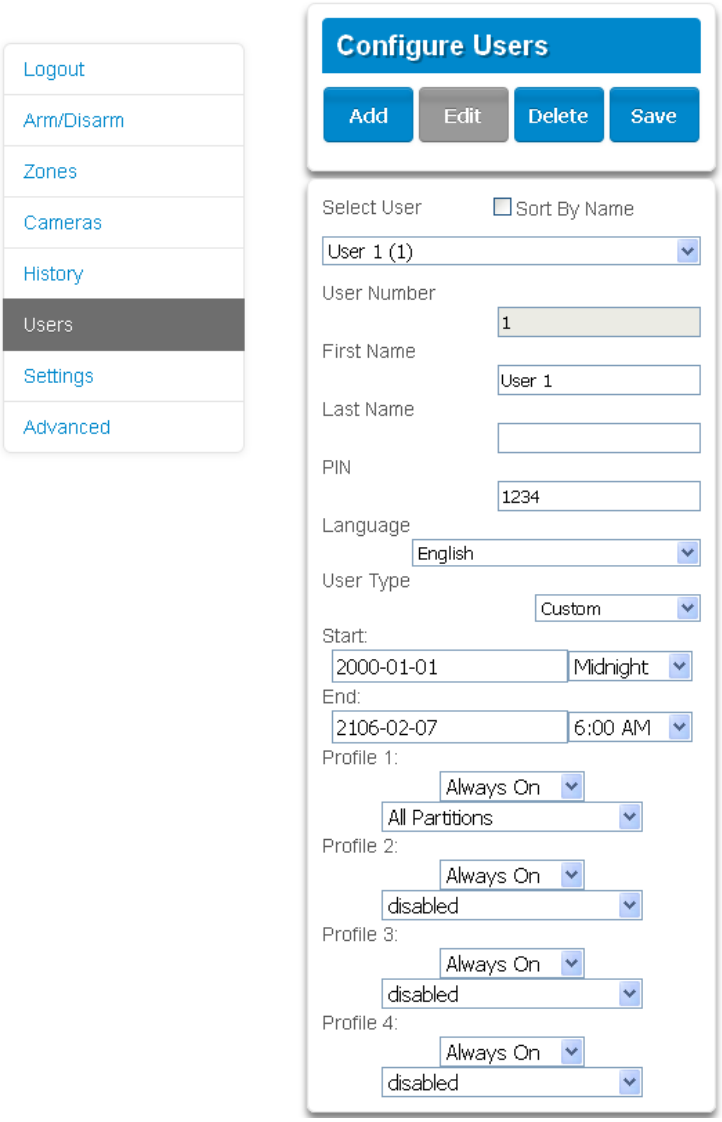


8. You can set the start/end date and time for when this user will have access to the system. This can be used to provide temporary user access. If Active is selected on the previous tab then the end date and time on this screen will be set to maximum.
9. You can program up to 4 levels of access for each user. Permission 1 is applied when Schedule 1 is true.

The combination of one Permission and one Schedule is called a “Permission Profile” (left drop-down menu). Permission Profile 1 is the highest level and will override Permission Profile 2 when Schedule 1 is active. Refer to xGenLite Reference Guide for more details.

To enable Permission Profiles the user type must be first set to Custom on the Main tab.

Web Page



Programming Instructions for Zones

Goal

Program zones and add them to Areas.

Pre-conditions

None.

Notes

Use defaults for Zone Types and Zone Options to quickly set up your system.

Zones can have one or two profiles. The first profile will be active during the selected schedule, it takes priority over the second profile/schedule. The second profile will be active during the selected schedule if the first profile is not active.

If no schedule is set (or is currently active) in either the first or second zone profile then the zone will be disabled.

See the next section for programming custom zones.

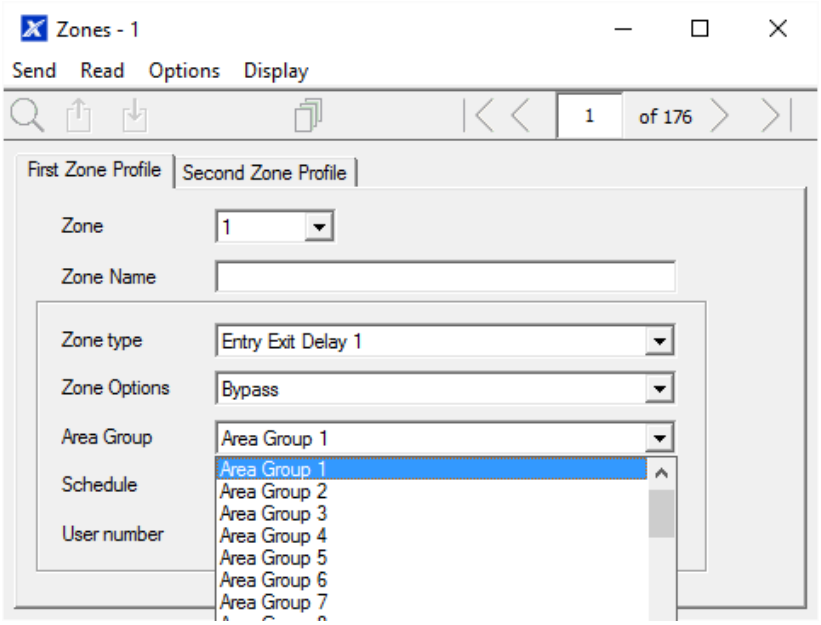
Programming Sequence

```
7. Schedules                    →   15. Zone Types              →   16. Zone options
                                    - Area Armed
                                    - Area disarmed
    14. Holidays

3. Zones                        →   4. Areas                    →   12. Area Groups
   a) Profile 1                     a) Area Options
   b) Profile 2                     b) Area Timers
                                    c) Area Reporting
    15. Zone Type                    7. Schedule
    16. Zone Options                18. Channel Groups
    12. Area Group
     7. Schedule
     1. User
```

Instructions

1. Go to Zones.



2. Select a zone number you want to program.
3. Enter a name for the zone.
4. Select a zone type preset.
5. Select a zone options preset.
6. Select an Area group for the zone. If you want a zone to be in its own Area then select an Area group with only one Area. To create a zone in a common

Area, select an Area group with multiple Areas. Alternatively come back to this step later.

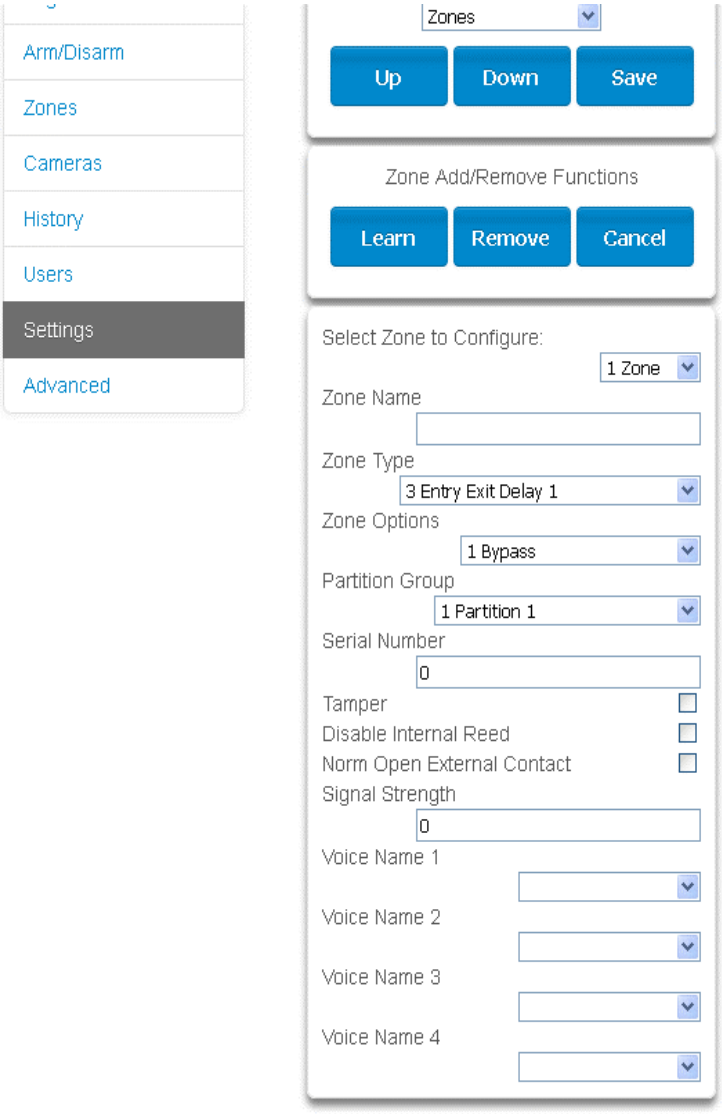
7. For a standard installation set the schedule to a preset which is 24 hours every day, holidays should NOT be ticked in this schedule. This will enable the first zone profile.

   If you want the zone settings to change based on a schedule, then select the first schedule here.

8. If you are setting up a keyswitch zone then the user number field controls which user profile will be used to arm/disarm. The keyswitch zone will report as default User 99.

9. If you are programming a second zone profile, then go to that now and repeat steps 4 to 7.

Web Page



Next

- Zones are assigned to one or more Areas using Area Groups. If necessary, program Areas and Area Groups, then assign an Area Group to each zone (step 6).

Programming Instructions for Custom Zones

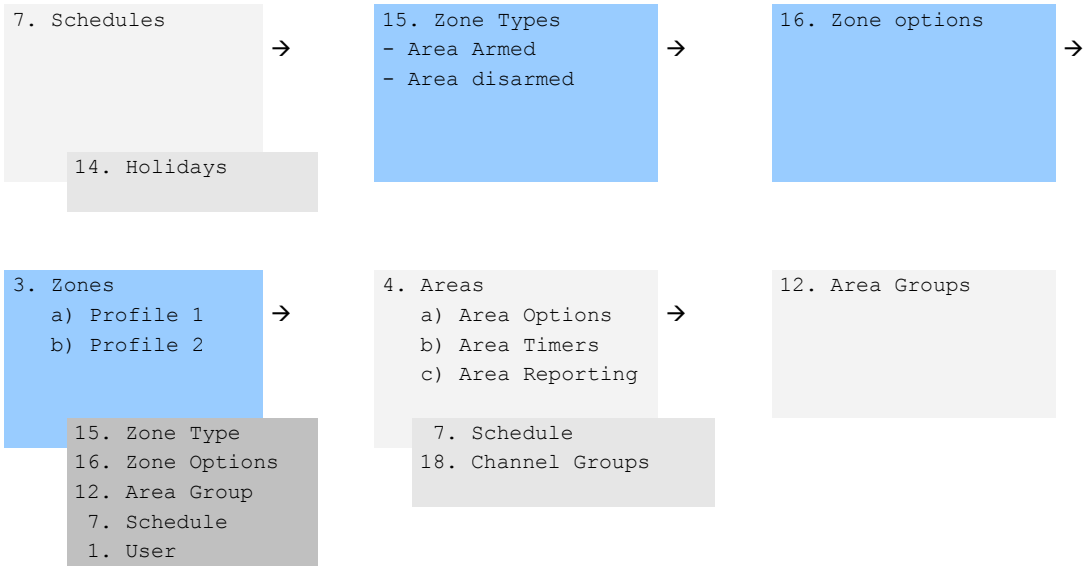
Goal

Program zones with advanced customization, including setting zone behavior to follow a schedule or armed/disarmed state.

Pre-conditions

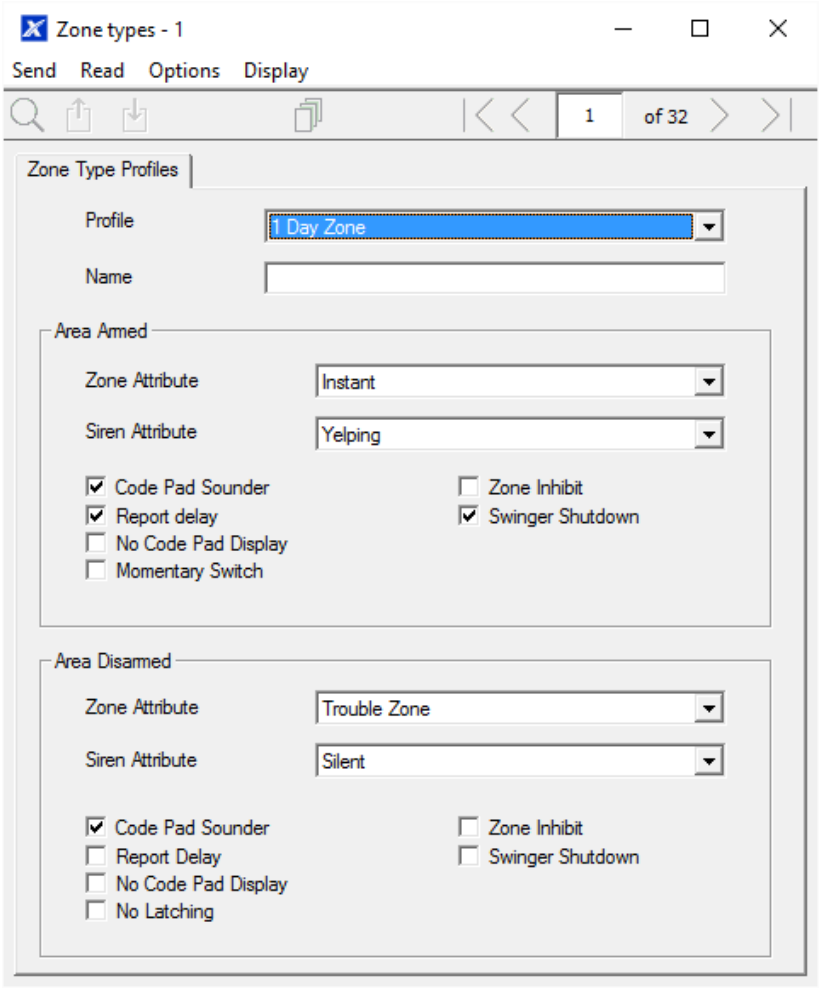
Program the schedule you want the zone to follow if needed. Alternatively use the defaults.

Programming Sequence

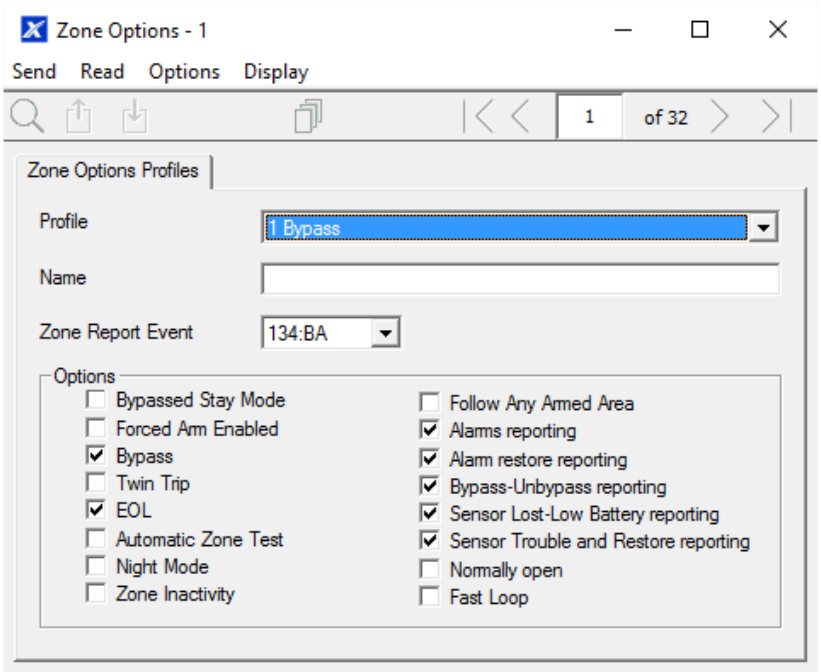


Instructions

1. Go to Zone Type.

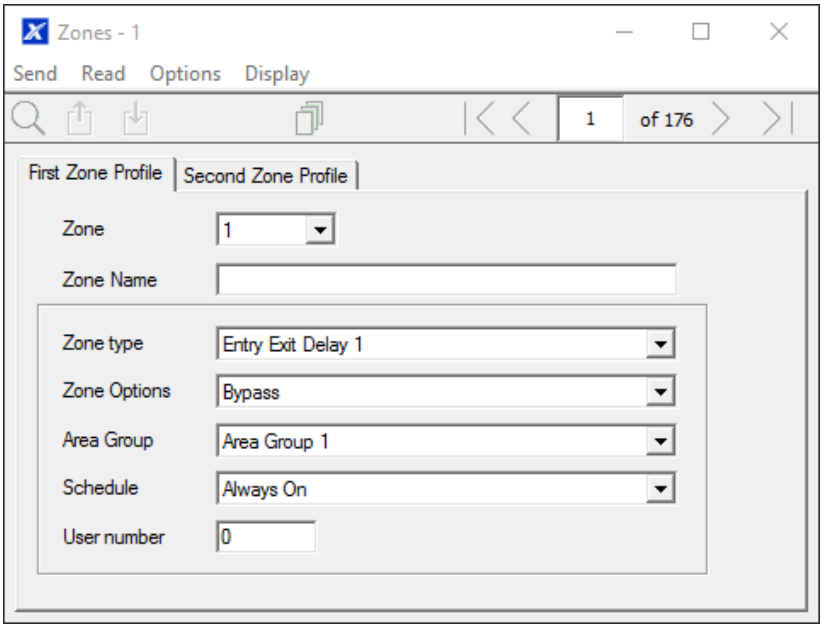


2. Go to Zone Options.



3. Select the options you want, the SIA/CID event code can be customized. See the xGenLite Reference Guide for a table of codes.

4. Go to Zones.

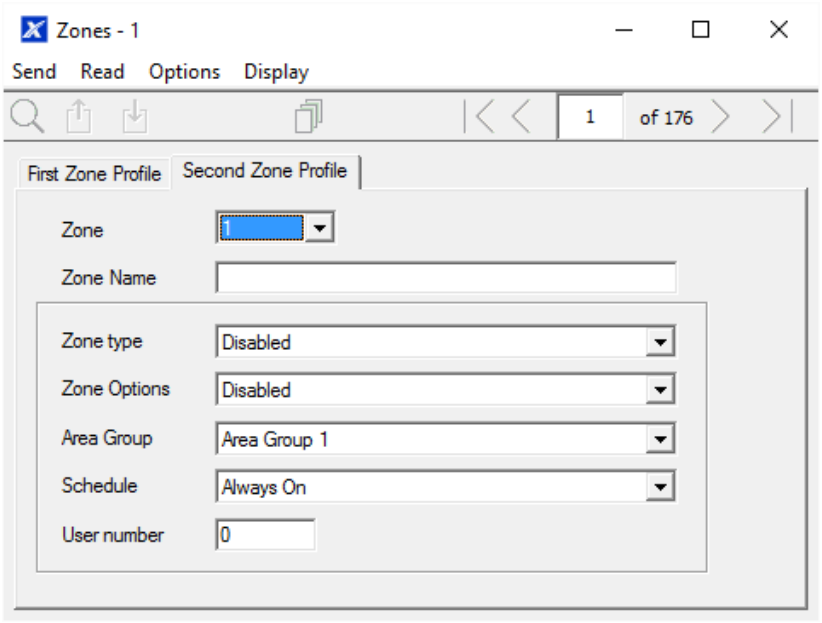


5. Select a zone number you want to program.
6. Enter a name for the zone.
7. Select the zone type profile you just created.
8. Select the zone options profile you just created.
9. Select an Area Group for the zone. If you want a zone to be in its own Area then select an Area Group with only one Area. To create a zone in a common Area, select an Area Group with multiple Areas. Alternatively come back to this step later.
10. For a standard installation set the schedule to a preset which is 24 hours every day, holidays should NOT be ticked. For example, “Always On”. This will enable the first zone profile.

    If you want the zone settings to change based on a schedule, then select the first schedule here.

    If no schedule is set in either the first or second zone profile then the zone will be disabled.
11. If you are setting up a keyswitch zone then the user number field controls which user profile will be used to arm/disarm. The keyswitch zone will report as default User 99.

12. If you are programming a second zone profile, then go to that now and repeat steps 4 to 7.



Next

- Zones are assigned to one or more Areas using Area Groups. If necessary program Areas and Area Groups, then assign an Area Group to each zone (step 8).

Programming Instructions for Areas

Goal

Program Areas, Entry/Exit Times, Reporting Options, and Area Groups.

Pre-conditions

Programmed Communicator, Channels, and Channel Groups.

Programming Sequence

6. Communicator
   a) Options
   b) IP Config
   c) Ethernet
   d) Radio
   e) Dial IP
   f) Email
   g) Remote Access
   h) System Event Reporting
   18. Channel Groups

→ 5. Channels
   6. Communicator
   17. Event Lists

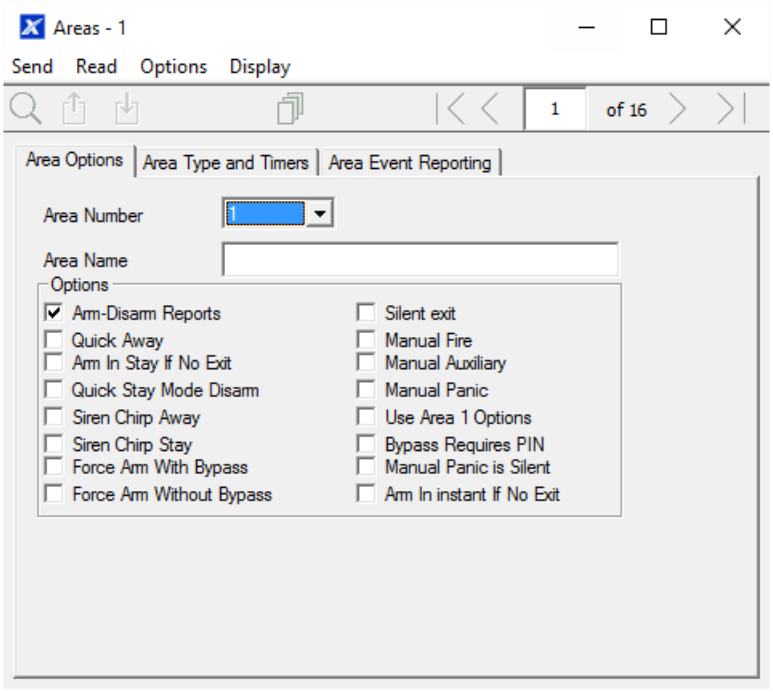
→ 18. Channel Groups →

4. Areas
   a) Area Options
   b) Area Timers
   c) Area Reporting
   7. Schedule
   18. Channel Groups

→ 12. Area Groups

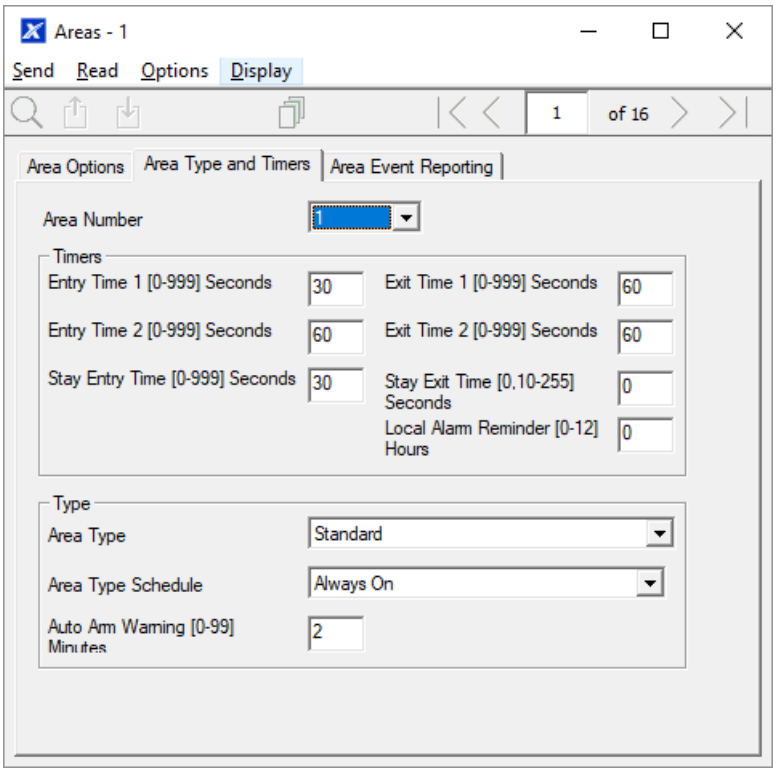
Instructions

1. Go to Areas.

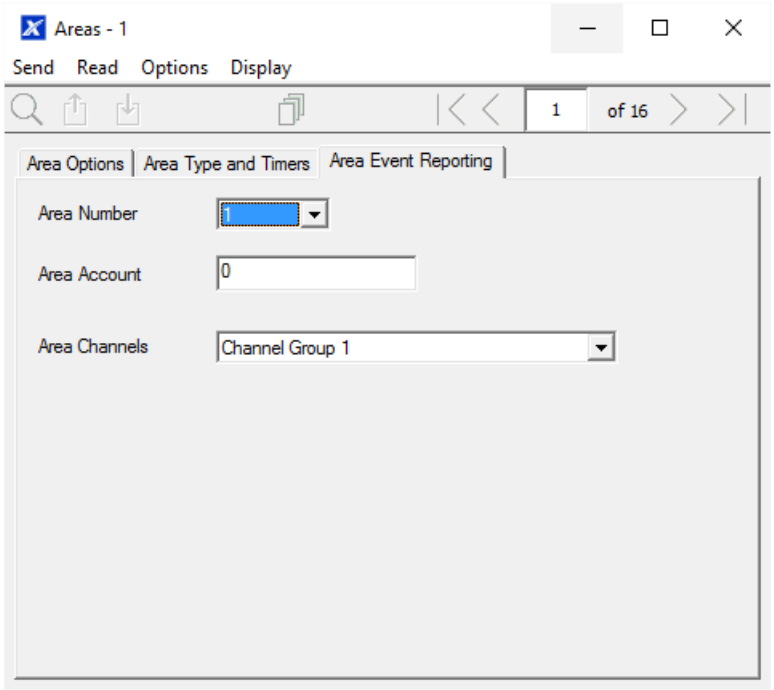


2. Select an Area Number.
3. Enter a descriptive name.
4. Select the Options you want to enable for this Area. Area 2 and above have “Use Area 1 Options” ticked to allow faster programming of your system. Untick this box if you want to customize options for Area 2 and above.

5. For advanced programming you can assign a Schedule and an Area Time Disarm function to occur according to the schedule. Refer to the xGenLite Reference Guide for more details.
6. Go to Area Timers.



7. Enter the timers that apply to this Area.
8. Go to Area Reporting.

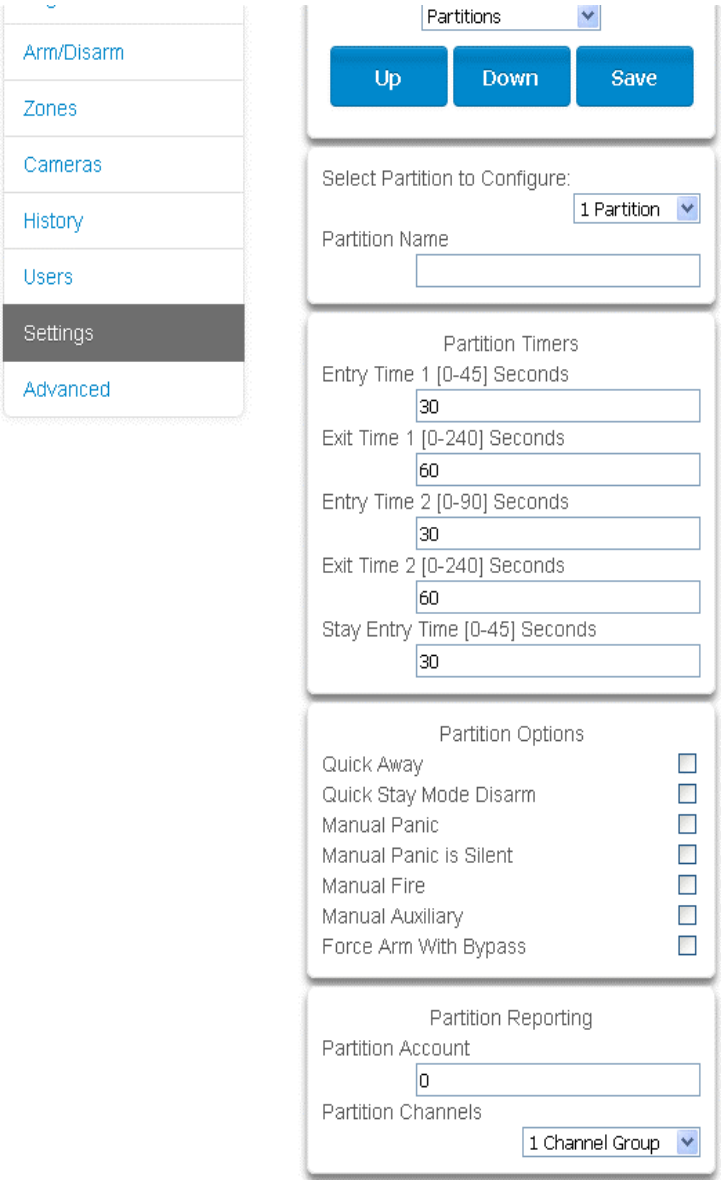


9. Assign the Area an account number and the Channel Group you want this Area to report to. See Programming Instructions for Zone Reporting for more details on how this works.

Next

- Customize Area Groups if needed.

Webpage



Programming Instructions for Schedules

Goal

Create a schedule to provide or prevent access to the xGenLite system on the specific dates and times.

Pre-conditions

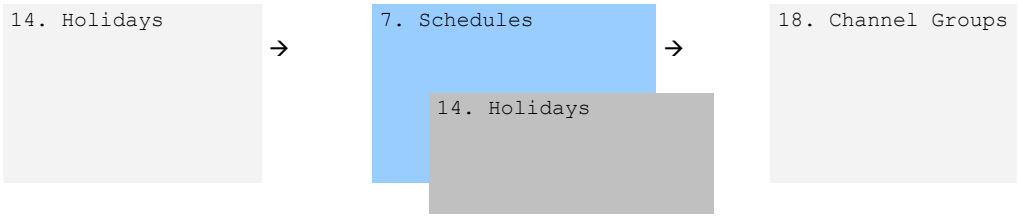
Holidays have been programmed if needed.

Notes

Ticking Holidays in a Schedule PREVENTS access on the holiday dates.

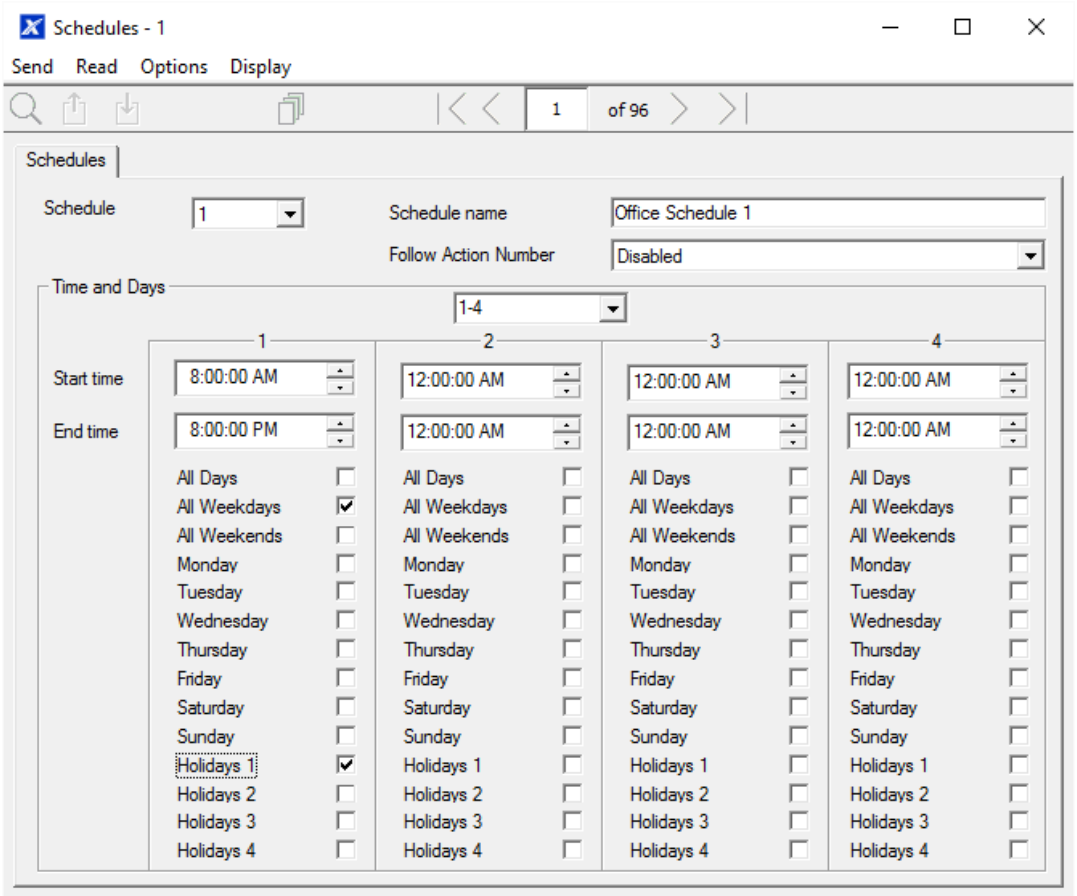
xGenLite automatically handles schedules that span midnight (e.g. bakers hours), do not tick the following day of the AM hours. (See Reference Guide for more details.)

Programming Sequence



Instructions

1. Go to Menu 7. Schedules.

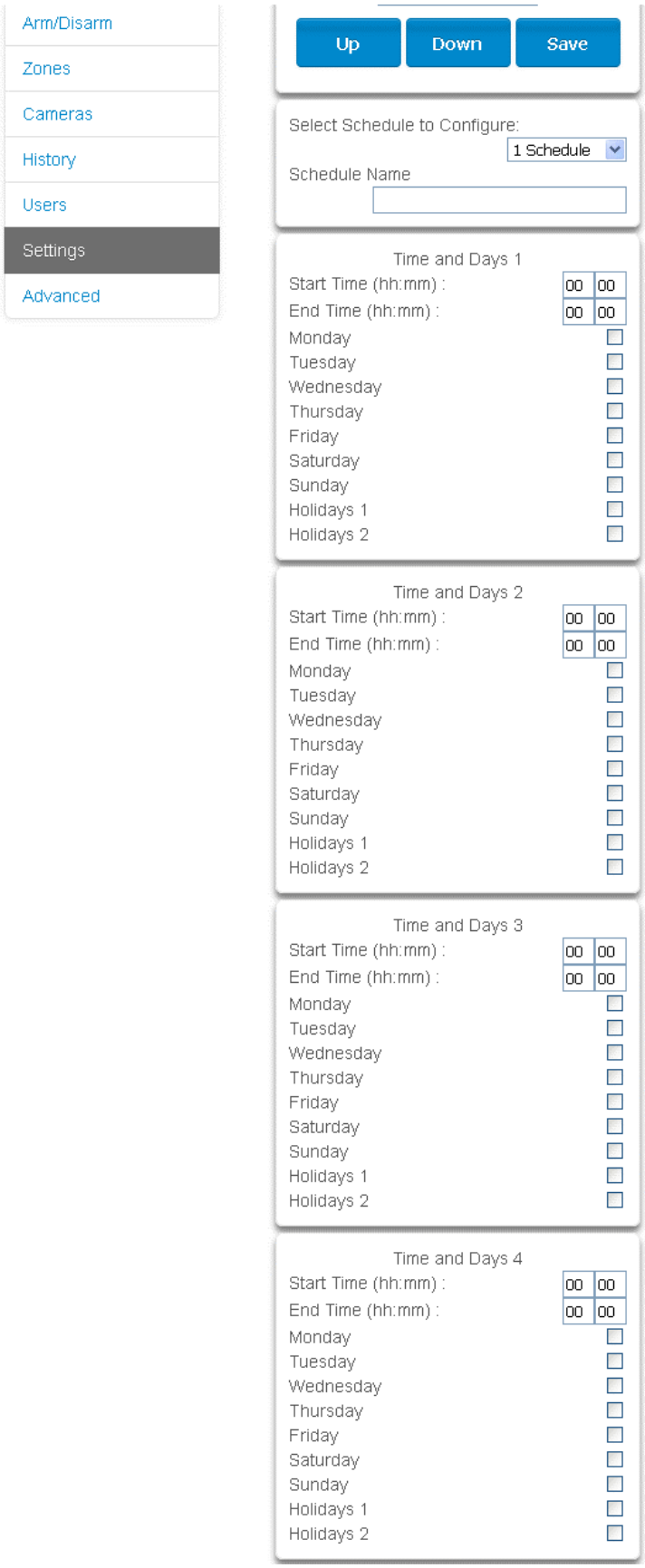


2. Enter a name for the Schedule.
3. Select the first Start and End time.
4. Select the days you want this start and end time to apply to.
5. If you are using the DLX900 software you will be able to see 4 sets of times and days, click the drop-down in the middle to access more. Each schedule can have up to 16 sets of times and days.

   If you are using a NXG-1820, press the Up and Down buttons to access the 16 sets of times and days.

6. To allow an Action to control when this Schedule is active/inactive, select the Follow Action Number.
7. Now the schedule is ready to be assigned to a User or used by another part of the system.

Webpage


Arm/Disarm
Zones
Cameras
History
Users
Settings
Advanced
Up
Down
Save
Select Schedule to Configure:
1 Schedule
Schedule Name
Time and Days 1
Start Time (hh:mm) :
End Time (hh:mm) :
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Holidays 1
Holidays 2
Time and Days 2
Start Time (hh:mm) :
End Time (hh:mm) :
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Holidays 1
Holidays 2
Time and Days 3
Start Time (hh:mm) :
End Time (hh:mm) :
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Holidays 1
Holidays 2
Time and Days 4
Start Time (hh:mm) :
End Time (hh:mm) :
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Holidays 1
Holidays 2

Example

For example, you could create a 24/7 schedule and then have this schedule follow an action. Next assign a keypad permission this schedule. Now based on what the action does, we can conditionally enable or disable a keypad. This provides a high level of flexibility and multiple sets of rules using actions can be set up like this.

Programming Instructions for Arm-Disarm

Goal

Automatically Arm and Disarm your xGenLite system.

Pre-conditions

Areas have been programmed.

Notes

The Arm-Disarm will function as if it is the user you select. You will need to program valid user permissions including Area Groups, User Schedule, Profile levels, and active date and time.

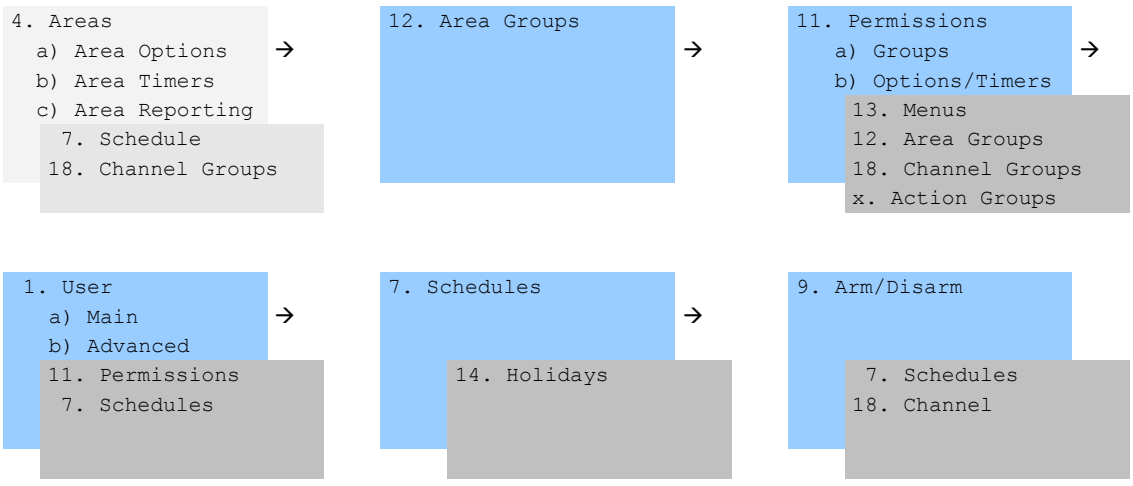
Creating a new user only for the purpose of Arm-Disarm will make it easier to maintain.

Use defaults for Schedules, Area Groups and Permissions for faster programming.

xGenLite will sound a warning prior to the Arm-Disarm from arming an Area. This is set in Areas > Area Timers > Area Type Delay.

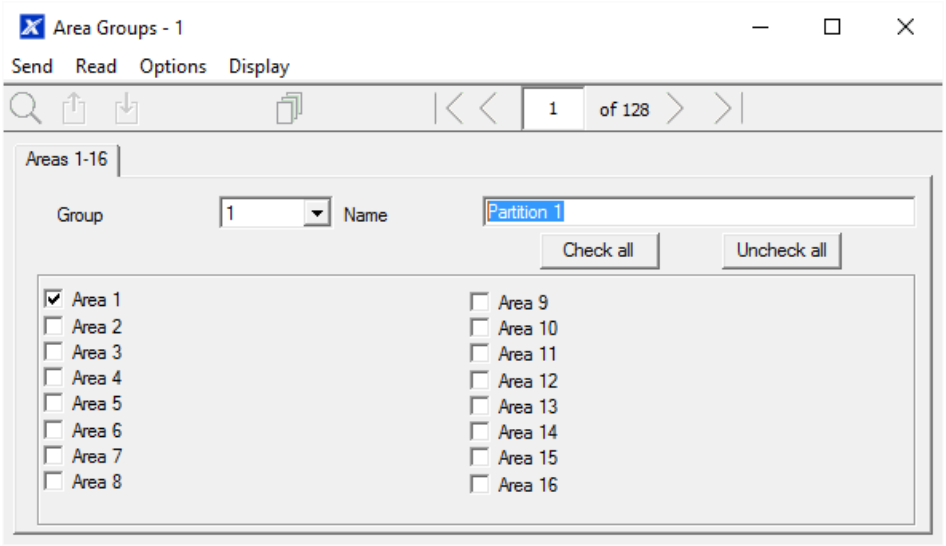
If a user with Area Type Override option disarms an Area with Arm-Disarm, then the Arm-Disarm will no longer function on that Area. To re-enable Arm-Disam that Area must be manually armed.

Programming Sequence

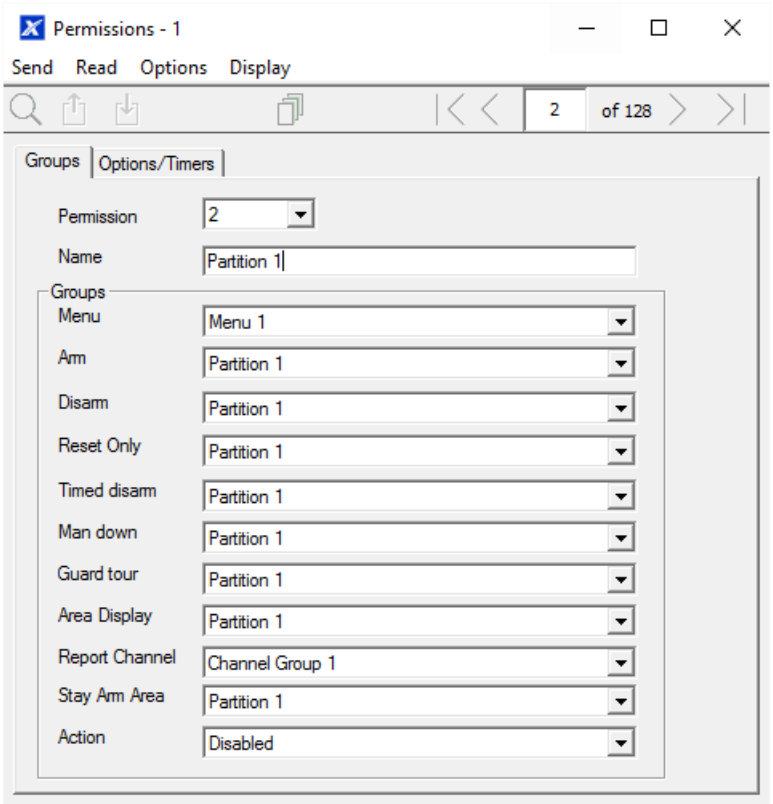


Instructions

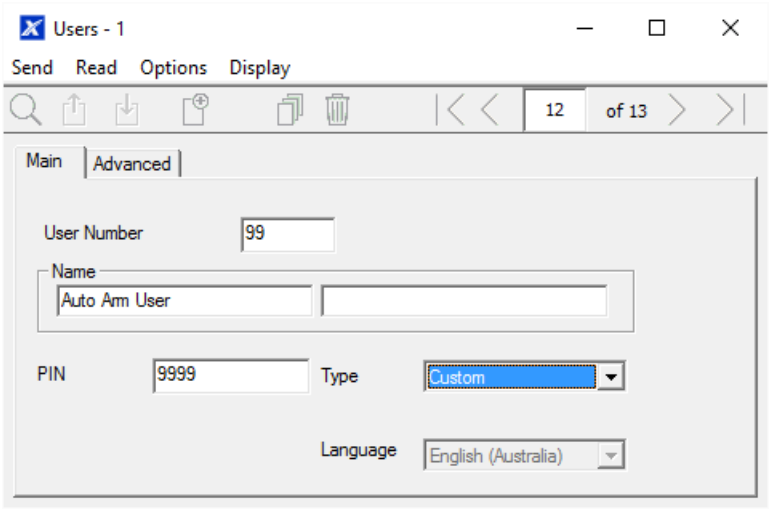
1. Create an Area Group and select the Areas you want to be Armed according to the schedule you will create later.



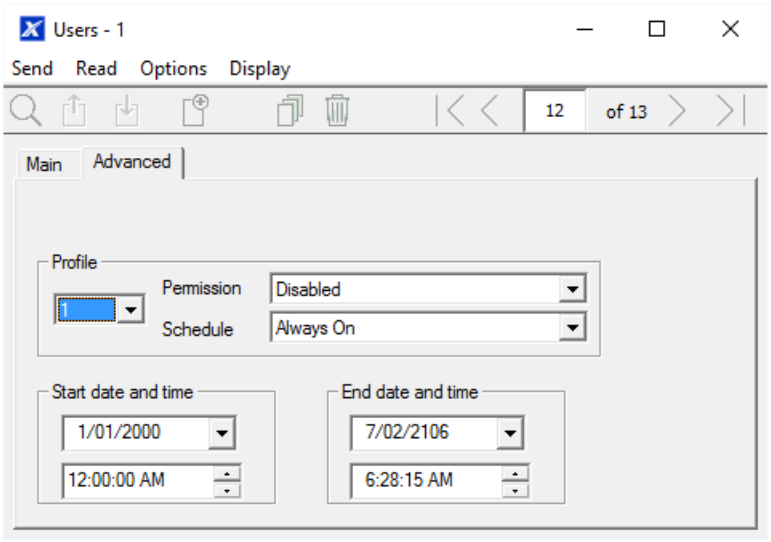
2. Create an Area Group and select the Areas you want to be Disarmed according schedule. This can be the same or different as the Area Group you selected above.
3. Create a Permission and select the corresponding Area Group for Arm and Disarm.



4. Open Users and create a new user. Suggested you provide a descriptive name such as “Auto Arm User” to make troubleshooting in the future easy.

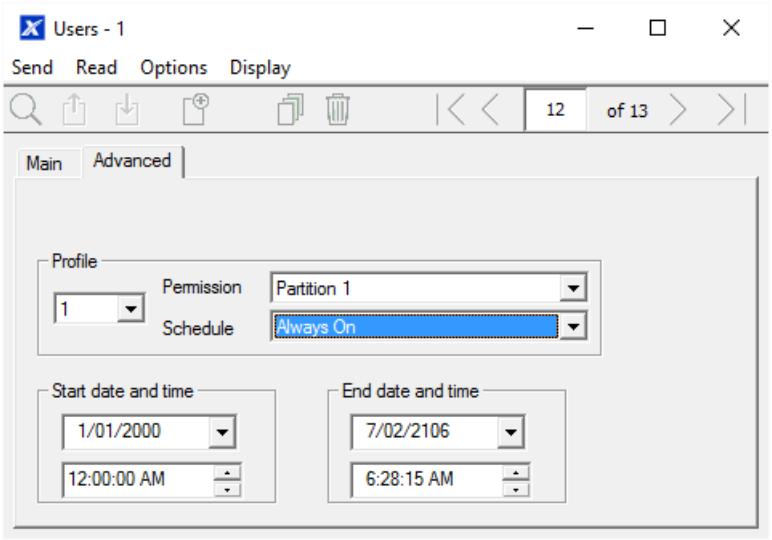


5. Go to the Advanced tab.

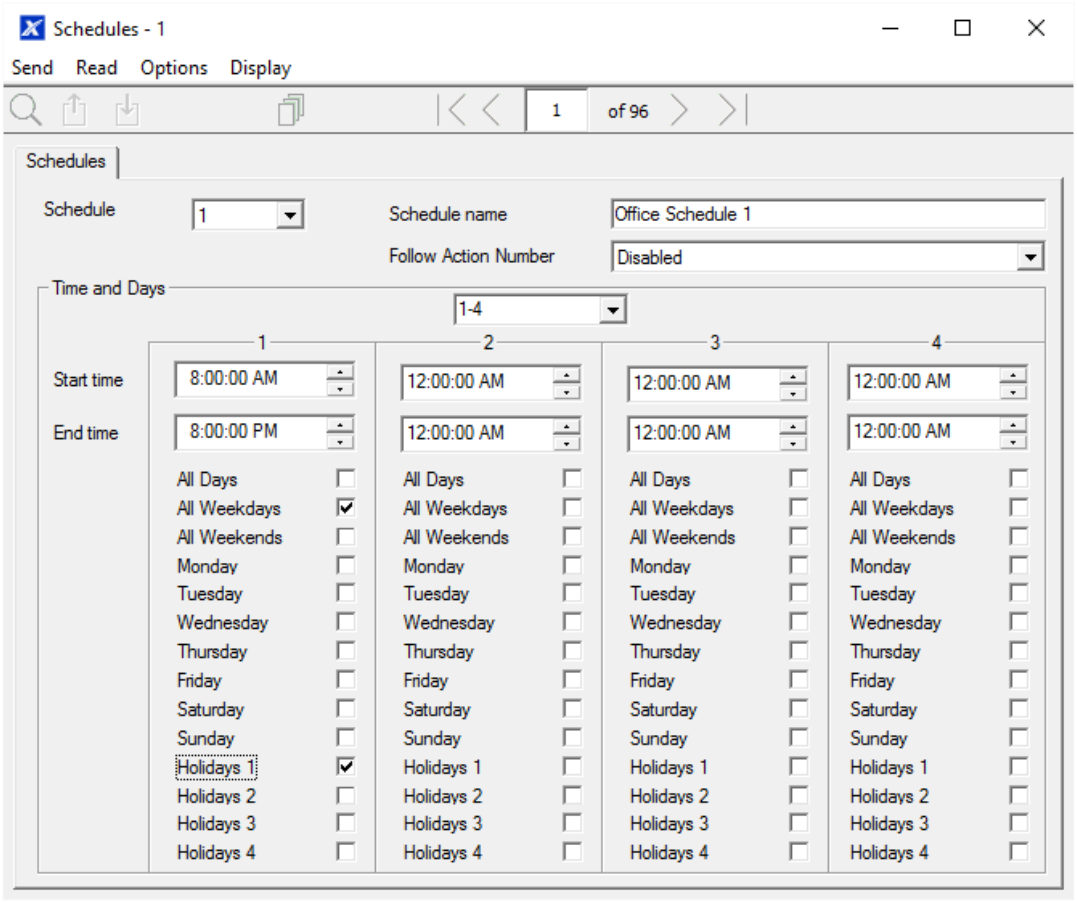


6. Select the Permission you created above. If you want a simple Arm-Disarm then leave the Schedule here as Always On. The Schedule selected here is

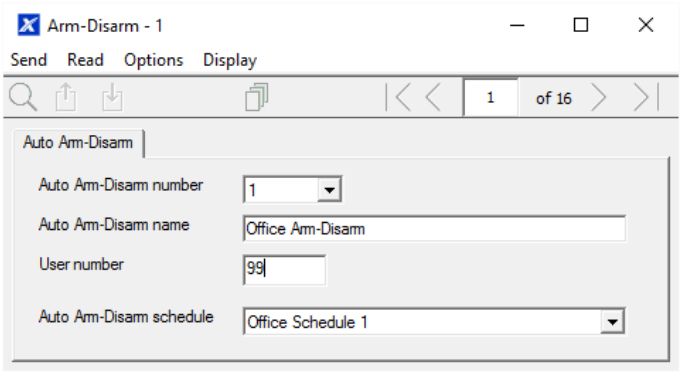
only for the **User.** It determines when the User is allowed to perform an Arm-Disarm, not when the Arm-Disarm will occur.



7. Create a Schedule for when you want the Arm-Disarm to occur.



8. Open Arm-Disarm.



9. Select the Arm-Disarm number.
10. Enter a descriptive name for this Arm-Disarm.
11. Enter the User number you created above.
12. Select the Schedule for when you want to automatically Arm-Disarm the system.
13. Test the Arm-Disarm to ensure it is working as you want.

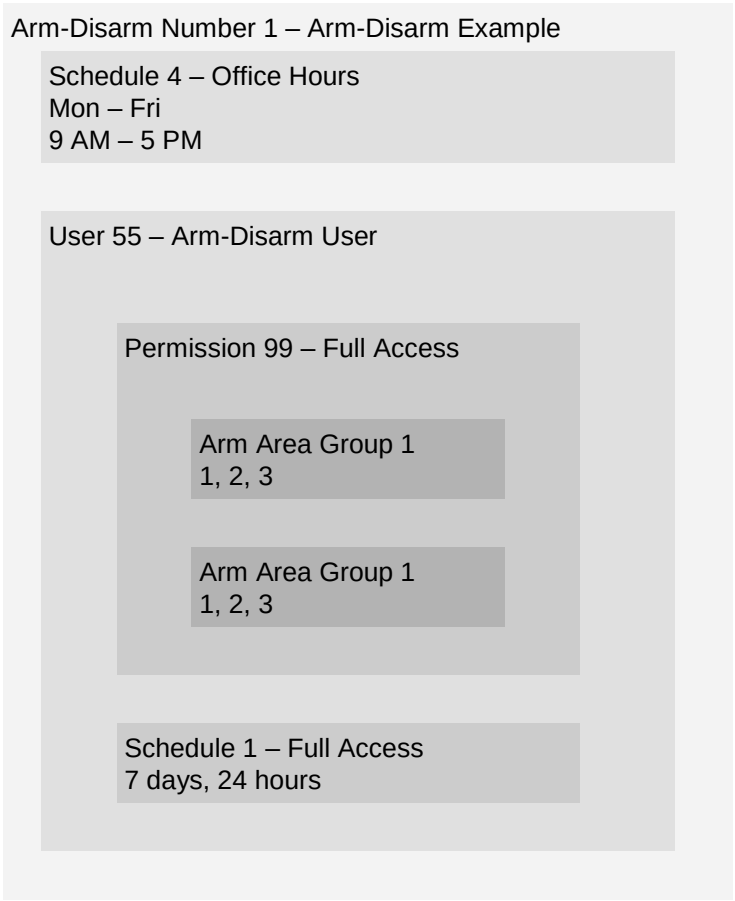
Example

An office with 3 Areas wants to automatically be disarmed during office hours, and armed out of office hours.

We create Schedule 4 Mon-Fri 9am-5pm. Then User 55 with permission to arm and disarm Area 1, 2, and 3 at any time or day.

Then each weekday at 9am the system will disarm Areas 1, 2, and 3 as if it were user 55 and report those disarm events (openings) to the communication channels specified.

At 5pm each weekday the system would arm Areas 1, 2, and 3 as if it were user 55 and report those arm events (closings) to the communication channels specified.



→ See “Programming Instructions for Schedules” on page 117 to program

→ See “Programming Instructions for Users” on page 105 to program

→ See “Programming Instructions for Permissions” on page 98 to program

→ See “Programming Instructions for Schedules” on page 117 to program

Programming Instructions for Communicator

Goal

Configure each communication path for delivering event messages.

Pre-conditions

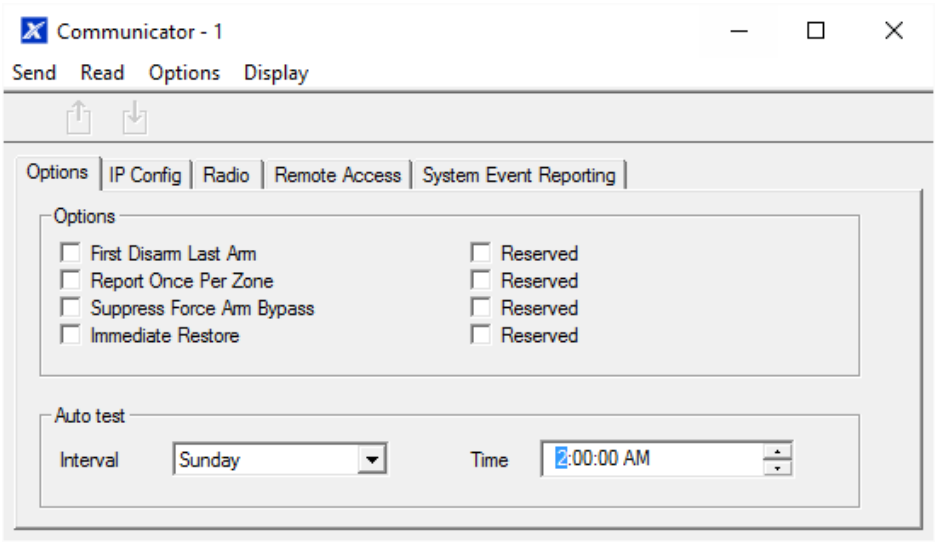
None.

Programming Sequence

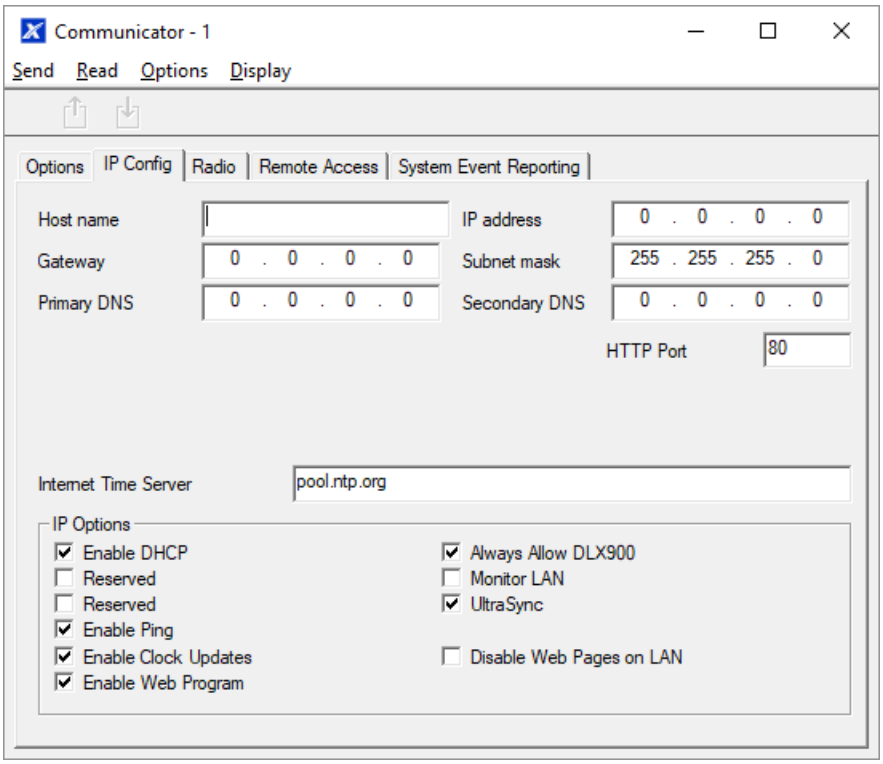
```
6. Communicator
  a) Options
  b) IP Config
  c) Ethernet
  d) Radio
  e) Dial IP
  f) Email
  g) Remote Access
  h) System Event Reporting
     18. Channel Groups
```

Instructions

1. Open Communicator.



2. Select reporting options.
3. Select when you want xGenLite to perform an automatic communication test.
4. Click IP Config.

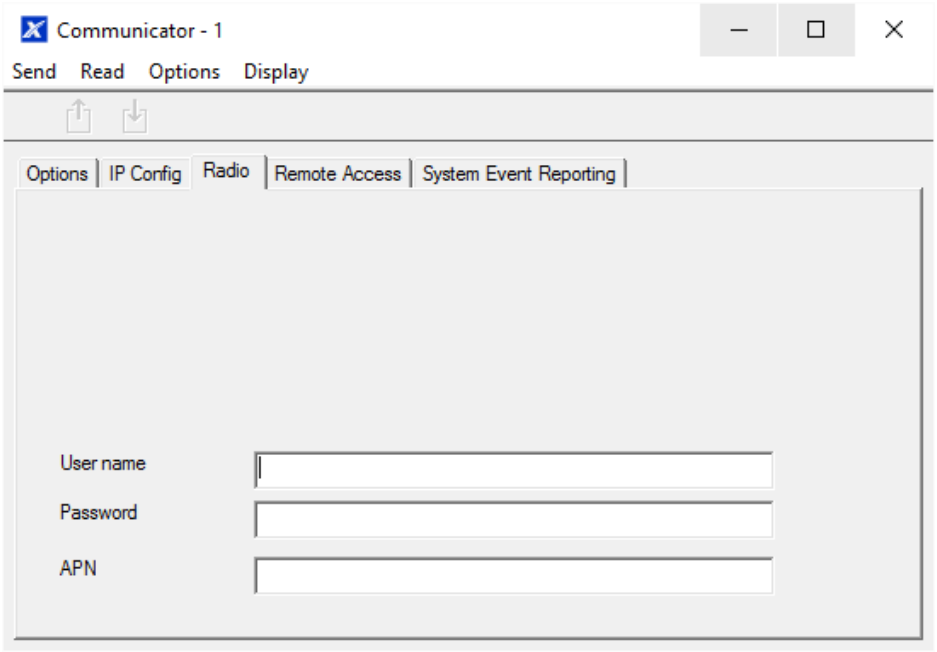


5. Edit IP settings for the xGenLite system, if DHCP is enabled on the xGenLite and a DHCP server is available, then this screen will automatically be filled in.

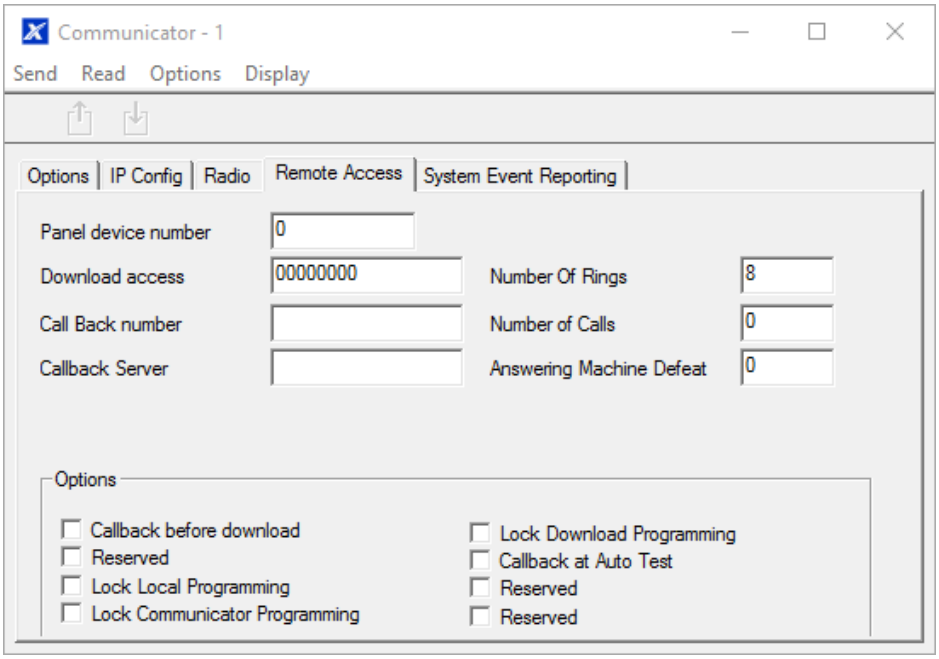
   - Enable Clock Updates: Will keep the time and date correct using the provided Internet Time Server, no manual adjustment will be needed when daylight savings occurs provided the time zone is set correctly in System.

   - Monitor LAN: This will monitor the physical LAN connection and report communication fail if the cable is disrupted.

6. Click Radio and enter settings if required, this will depend on the SIM card and operator you are using.



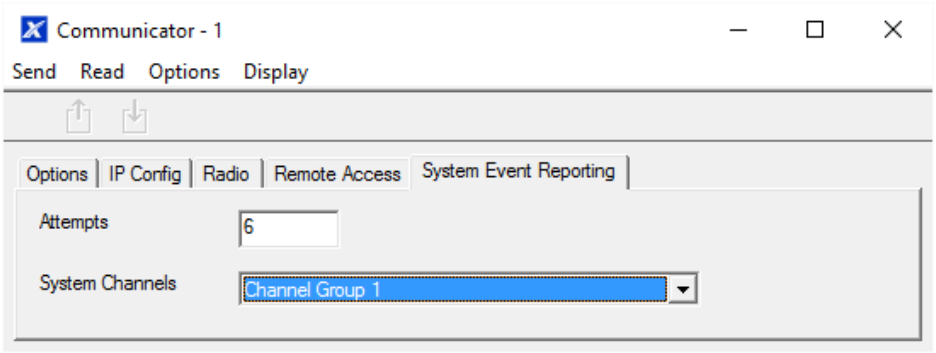
7. Click Remote Access



8. Edit Remote Access settings for the xGenLite system.

   - Download Access Code: Gives access to DLX900 to access the xGenLite panel programming.

9. Click System Event Reporting.



10. Select the channel group to send system events (e.g. low battery).

Next

- Perform tests on each of the communication paths to verify they are functioning correctly.
- Program Channels.
- Program Channel Groups.
- Verify Number of Attempts, next channels (back-up channels), and multi-path reporting function correctly.

Programming Instructions for UltraSync

Pre-conditions

At least one user has been given a username and PIN code (see “Programming Instructions for Users” on page 105).

xGenLite is connected to internet and has been allocated an IP address (see “Programming Instructions for Communicator” on page 126, IP Config).

Notes:

UltraSync provides a secure VPN connection to your xGenLite system over the internet. You will need to provide your xGenLite serial number, Web Access Passcode, and a valid Username and PIN code that exists in your xGenLite system. These codes provide multiple levels of security for the connection.

The Web Access Passcode is needed for:

- Web console over the internet via a secure VPN
- UltraSync+ app
- DLX900 software connecting over IP, in addition to Download Access Code

The Web Access Passcode is NOT needed for:

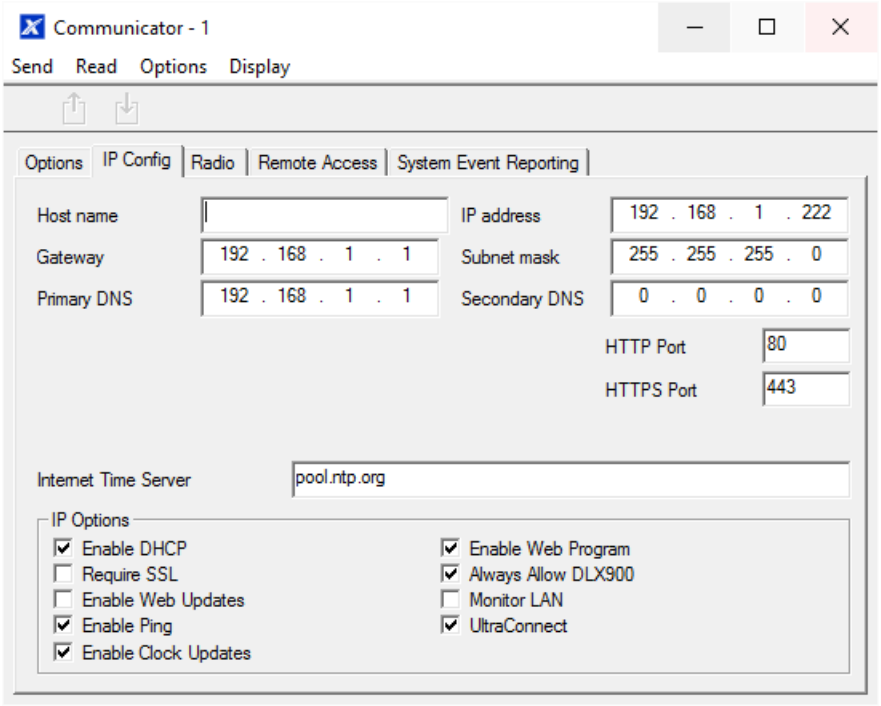
- Email services
- Web console over a local LAN connection

Once UltraSync is set up, you may connect to your xGenLite system using the UltraSync+ app on your smartphone or tablet. This may require a separate

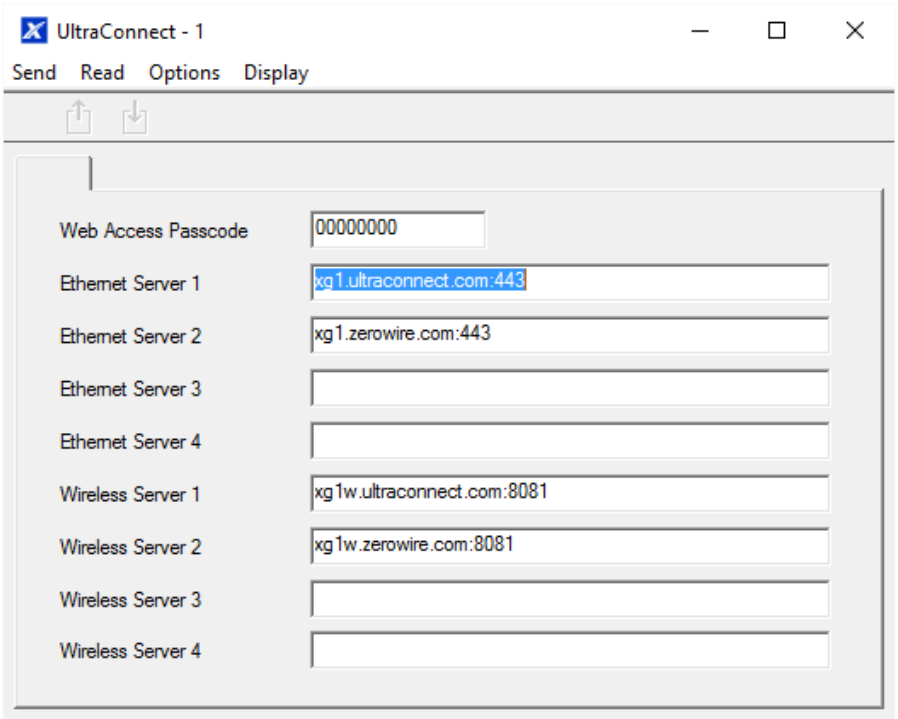
account and downloading additional software. See further instructions in the User Manual.

Instructions

1. Go to Menu 6. Communicator > 3. IP Config.



2. Under sub-menu 12. IP Options, tick the box “Enable UltraSync”.
3. Go to Menu 22. UltraSync.



4. Enter a new 8 digit Web Access Passcode. All zeros disables UltraSync remote access.

5. Enter the required details into your device/software. This will usual be your xGenLite serial number, Web Access Passcode, and a valid Username and PIN code. The xGenLite serial number can be found in the Device Info menu.
6. Verify the UltraSync service is working by using your device/software to connect your xGenLite system.

Troubleshooting

- Check the Web Access Passcode is correct. It cannot be 00000000.
- Check there is a valid user and they have a First name, this will be the login name.
- Check the serial number is correct. It is printed on the xGenLite module.
- Check that the user permissions are currently valid.

See also “Appendix 2: App and Web Error Messages” on page 154.

Programming Instructions for Event Lists

Goal

Create segmented lists of events so Channels can selectively deliver event messages.

Pre-conditions

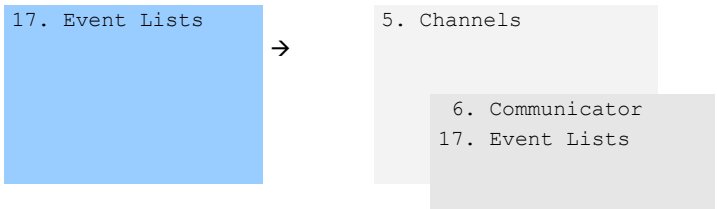
None.

Notes

If an event message is enabled in an Event List, then the Channel will attempt to deliver it. If an event message is not enabled on the Event List, the Channel will not attempt delivery even if the message has been sent to it.

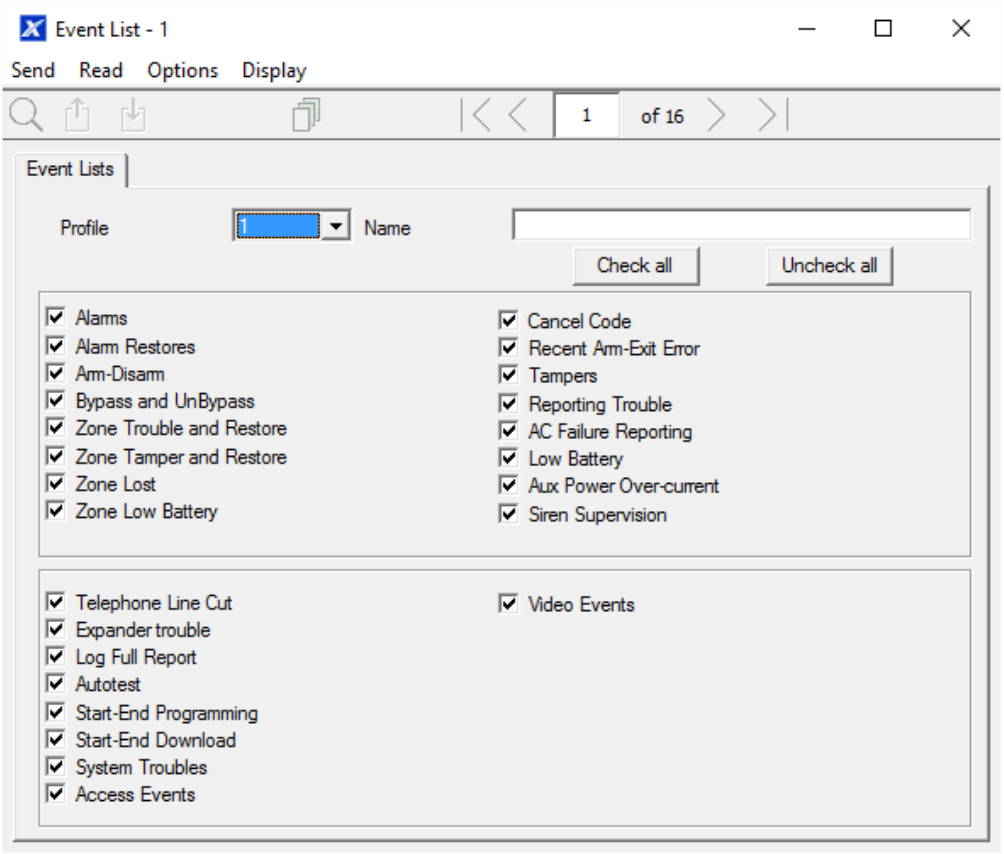
Event List set up for push notifications is automatically performed by the UltraSync+ app when required. The panel will assign the next available channel and matching event list number. No configuration via the web pages or DLX900 is required.

Programming Sequence



Instructions

1. Open Event Lists.



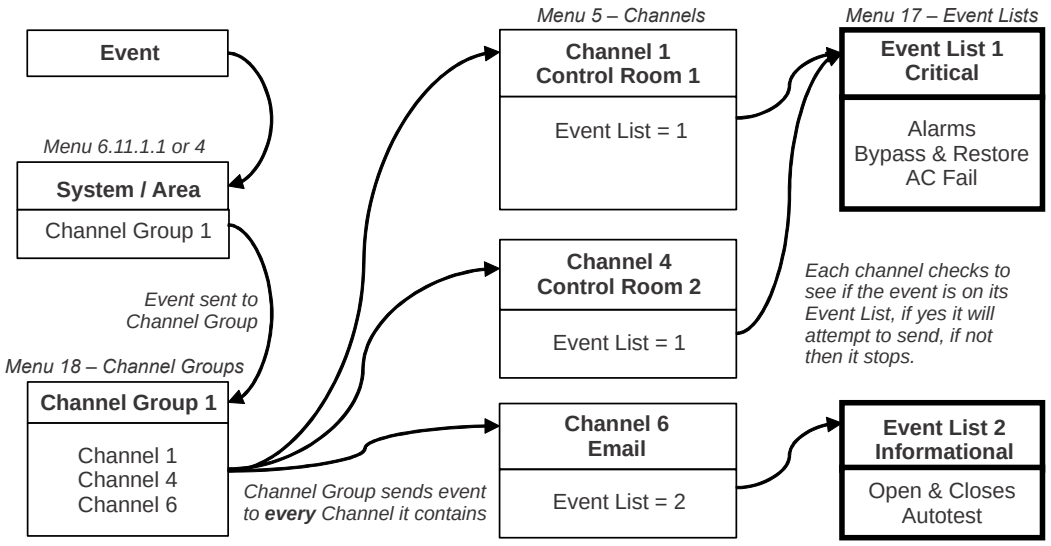
2. Enter a name for the list.
3. Check the events you want to include in the list.

Example

In this example we have created two lists: Critical and Informational. This allows us to selectively deliver event messages to different destinations.

We open up Event Lists and enter the name “Critical”. We tick Alarms, Alarm Restores, Bypass and Bypass Restore, and AC Fail Reporting.

Then we click to Event List 2 and enter the name “Informational”. Tick Opening and Closing, and Autotest Report.



Programming Instructions for Channels

Goal

Set up communication paths and destinations for delivering event messages.

Pre-conditions

Communicator must be programmed (see “Programming Instructions for Communicator” on page 126).

Event Lists must be programmed (see “Programming Instructions for Event Lists” on page 131).

Notes

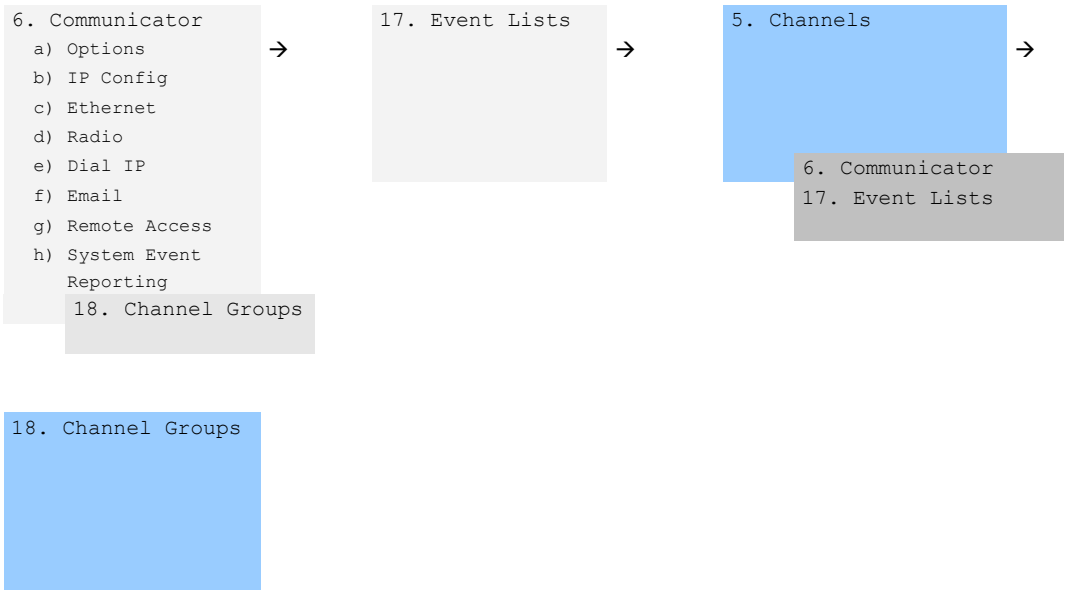
Area Account Number will take priority over Account Number entered here for Zone events. If no Area Account Number is entered then this number will be used instead.

Next Channel must be a higher value than the current Channel Number. Circular loops are not permitted.

Take note of the Sequence Attempts under Communicator > System Event Reporting (6.11.2). This is the number of times xGenLite will attempt the sequence of Channels you set up in this section.

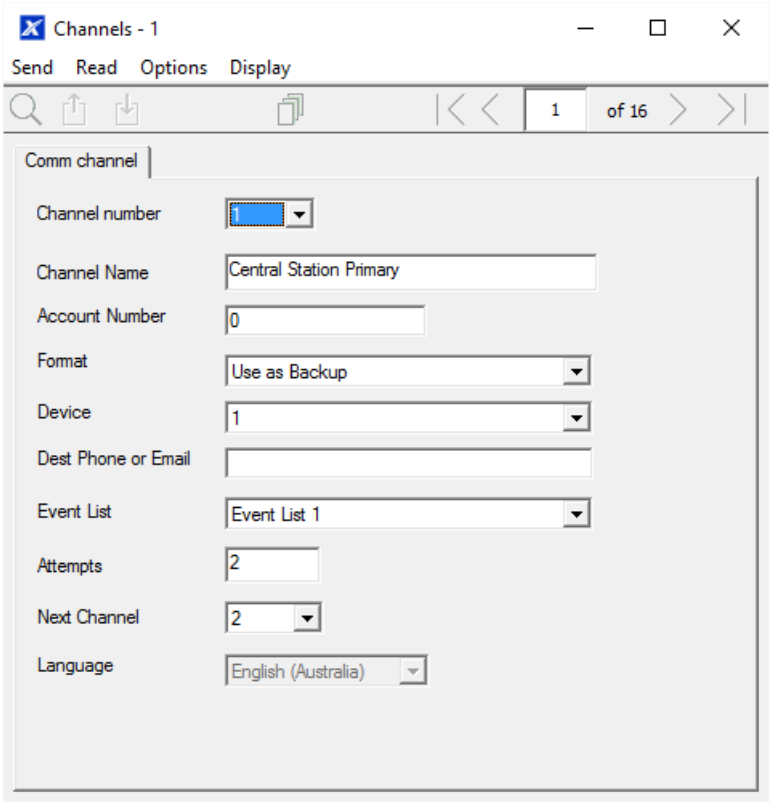
Channel set up for push notifications is automatically performed by the UltraSync+ app when required. The panel will assign the next available channel and matching event list number. No configuration via the web pages or DLX900 is required.

Programming Sequence



Instructions

1. Go to Channels.



2. Enter an Account Number up to 8 digits, hex values are accepted.
3. Select the Format of the communication channel, this will automatically use the settings programmed for that Format in the Communicator menu.
4. Select the reporting device, by default Device 1 is the xGenLite panel.
5. Enter the destination phone number, email address or IP address depending on which Format you selected.

6. Select what events you want to be sent via this Channel by selecting the appropriate Event List. Events that arrive at this channel will be checked that they on this Event List, if they are, then will be routed through this Channel. Events that arrive at this Channel which are not on this list will be blocked.

   If the Channel is used for push notifications to UltraSync+ app, the Event List number will be the same as the Channel number.

7. Enter the number of Attempts that you want xGenLite to try sending the event message on this Channel before switching to the Next Channel.

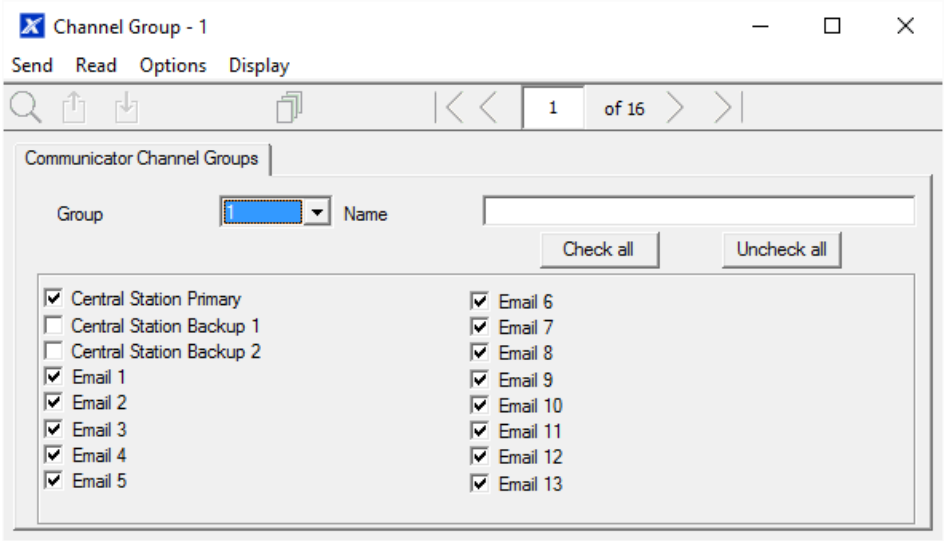
8. Select the Next Channel Number to use if the event message fails to be sent on this Channel.

   Each Channel can have one Next Channel as a backup. This allows you to chain up to 15 backup paths should the primary one fail. Enter Next Channel as 0 to end the chain of channels.

9. You have now finished programming one channel. If you entered a Next Channel, then go to that Channel number and program that now.

10. Once you have programmed each channel and backup channels you have completed this section. Check or edit Sequence Attempts under Communicator > System Event Reporting (6.11.2).

11. Go to Channel Groups. Here you will group channels together so selected event messages will be sent to multiple destinations at the same time. Another way to think of Channel Groups is “multi-path reporting”.



12. Select each channel you want to be part of a group.

    Messages sent to a Channel Group will be checked against each Channel’s Event List. If it is on the list then xGenLite will attempt to send it. If not, then xGenLite will not send it, even if the Channel is in the same group.

Done. Your Channels are now set up and ready for use. When an event is generated by the system or a zone it can now be sent to a Channel for reporting.

Example

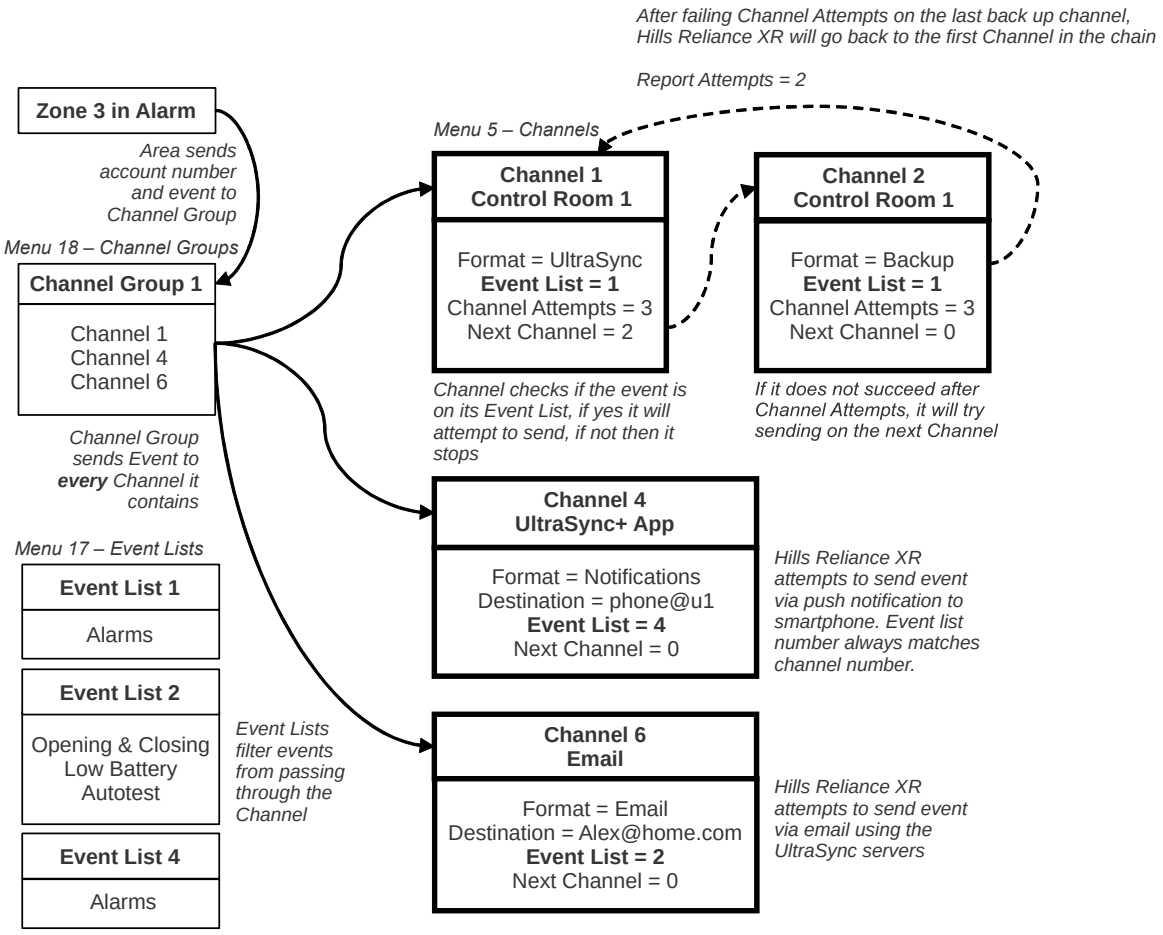
In this example we have multi-path, prioritised/selective event reporting via three reporting paths – one control room with backup, push notification to a smartphone, and an email address. These are grouped into “Channel Group 1”.

All alarms are reported to Control Room 1 and push notification goes to UltraSync+ app installed on User 1’s smartphone. Control room 1 has a backup receiver.

When a channel receives an alarm message, xGenLite checks that the channel’s Event List includes alarm messages and then attempts to deliver the message via that channel.

When Channel 1/2/4 receives a low battery report, it is ignored because Event List 1 does not include the “low battery” event.

Low priority alerts such as opening and closings, low batteries, and autotest reports, are sent via Channel 6 as an email to a building manager. When Channel 6 receives the alarm event it takes no further action because Event List 2 does not include the “alarm” event.



Notice that Channel 2 is not selected in the Channel Group. The xGenLite will still deliver to this destination if Channel 1 cannot be reached. If Channel 2 were included in the Channel Group then the control room will receive duplicate messages.

Next

- Program your Areas and Zones.

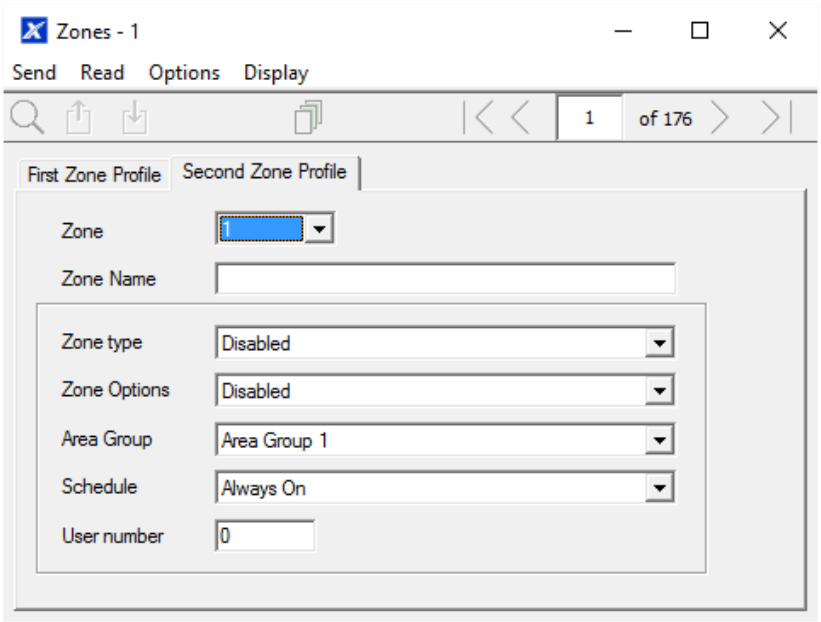
Programming Instructions for Zone Reporting

Goal

Direct event messages (e.g. alarm, bypass, tamper) from zones to specific destinations.

Pre-conditions

- The zone must have valid zone options programmed (see “Programming Instructions for Zones” on page 108), by default you should not need to modify these.
- The zone must be allocated a valid Area Group (see “Programming Instructions for Zones” on page 108).



- Channels and Channel Groups must be programmed (see “Programming Instructions for Channels” on page 133).

Notes

Each zone may be allocated to multiple Areas through an Area Group.

Events will be sent to the lowest numbered Area in the Area Group.

A zone may have a Second Zone Profile, when this becomes active all events will be sent to the Area Group programmed in the second profile.

Programming Sequence

3. Zones

12. Area Groups

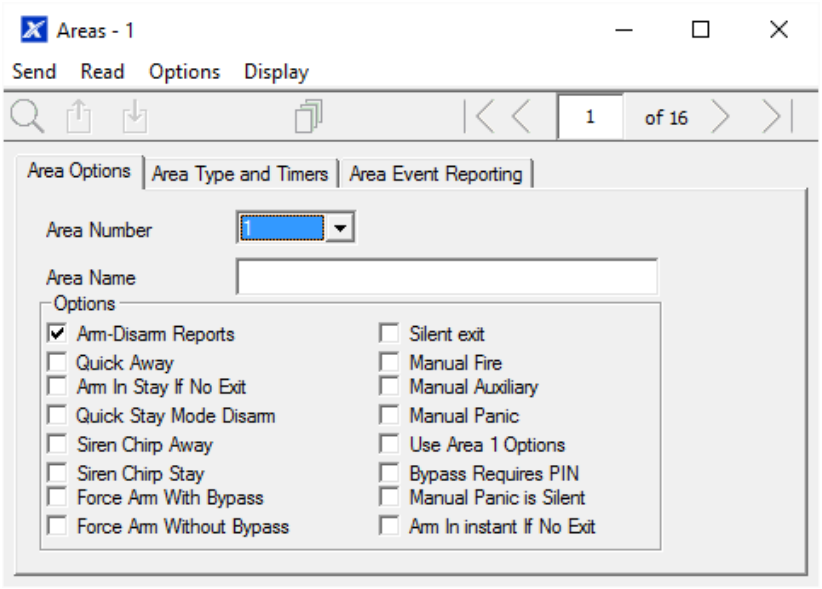
→

4. Areas
   a) Area Options
   b) Area Timers
   c) Area Reporting

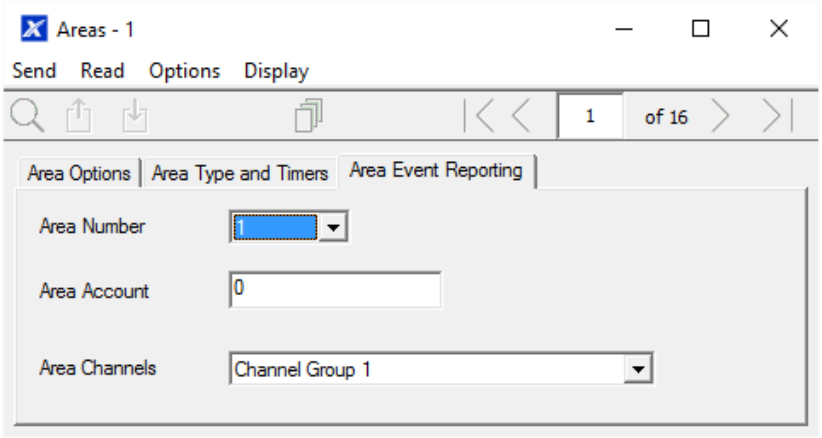
7. Schedule
18. Channel Groups

Instructions

1. Open the lowest Area number for the Zone.



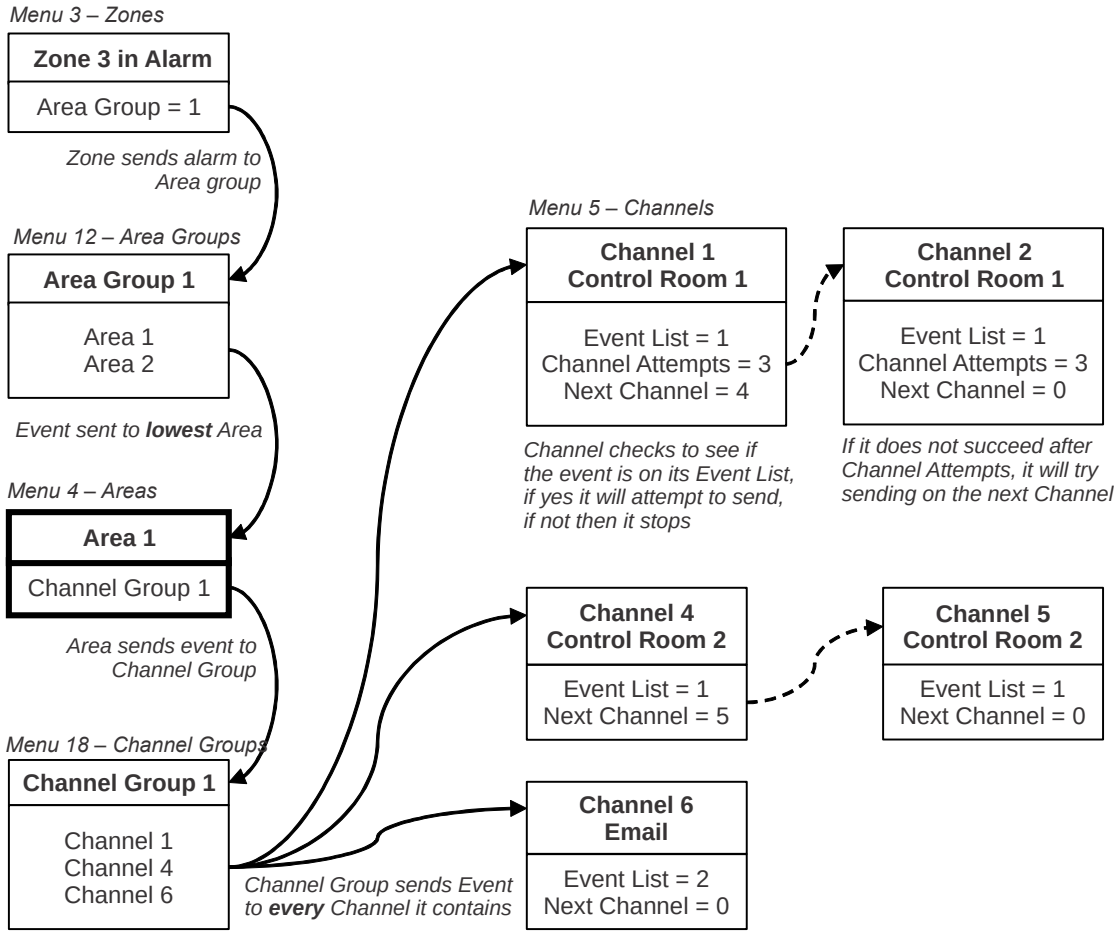
2. Go to Area Reporting.



3. Enter an account number.
4. Select a valid Channel Group.

Done. All zones that are a part of that Area will now report to the selected Channels within the Channel Group.

Example



Next

- Program Users.
- Program advanced Schedules and Alternate Zone Profiles.

Programming Instructions for System Event Reporting

Pre-conditions

Communicator must be programmed (see “Programming Instructions for Communicator” on page 126).

Event Lists must be programmed (see “Programming Instructions for Event Lists” on page 131).

Channels and Channel Groups must be programmed (see “Programming Instructions for Channels” on page 133).

Notes

The system event will only be reported by a channel, if that Channel includes that event in the associated Event List(s).

Take note of the Sequence Attempts under Communicator > System Event Reporting (6.11.2). This is the number of times xGenLite will attempt the sequence of Channels you set up in this section.

Programming Sequence

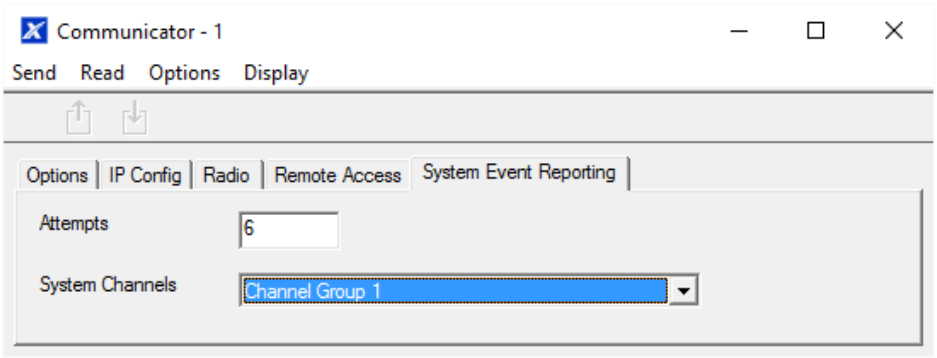
17. Event Lists → 5. Channels → 18. Channel Groups →

6. Communicator
17. Event Lists

6. Communicator
a) Options
b) IP Config
c) Ethernet
d) Radio
e) Dial IP
f) Email
g) Remote Access
h) System Event Reporting
→ 18. Channel Groups

Instructions

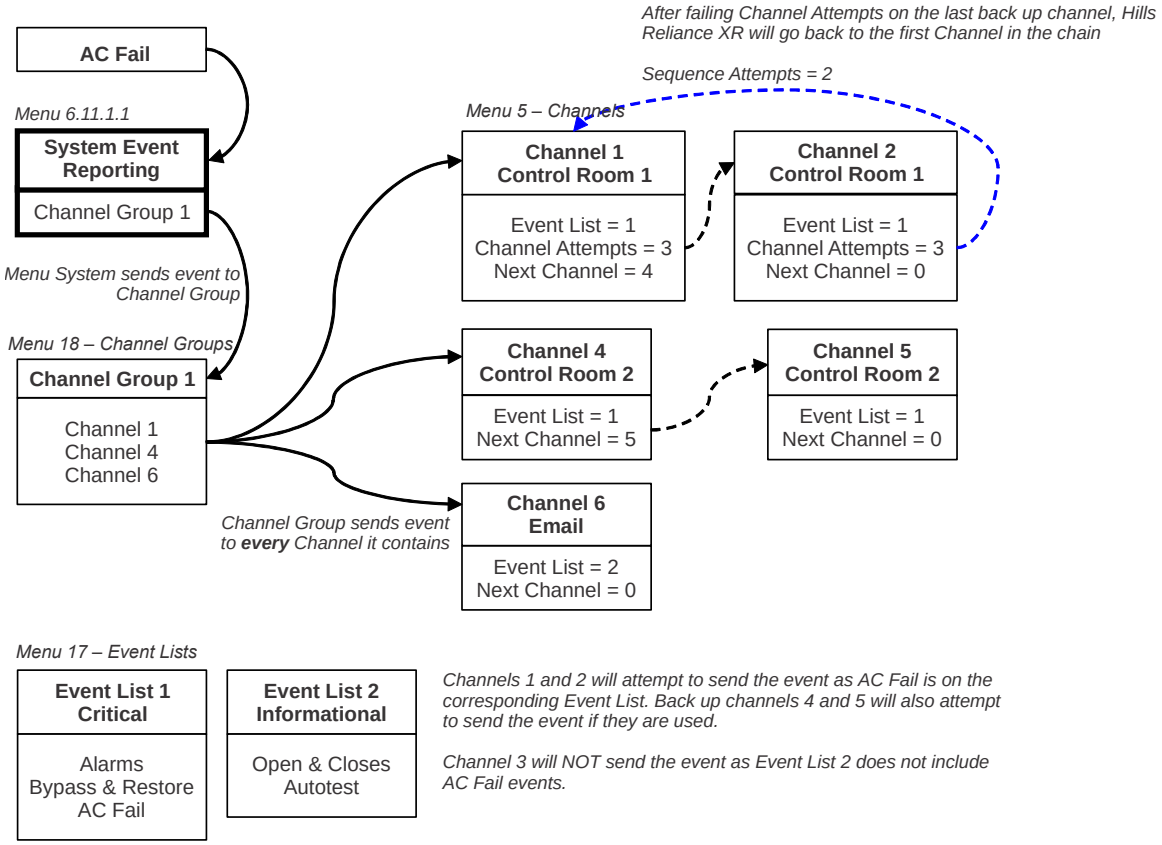
1. Go to Communicator, System Event Reporting.



2. Select a Channel Group.

Done. The xGenLite will now report system events to the Channels selected in the Channel Group you just selected.

Example



Programming Instructions for Actions

Goal

Create an action to monitor up to four input events and drive one output event (action result).

Event 1	and or	Event 2	and or	Event 3	and or	Event 4	=	Action State	+	Action Result

Pre-conditions

Program the input and output events you want the Action to monitor or control.

Notes

See xGenLite Reference Guide for more details on Actions.

Write/Plan out on paper what you want to create to make it easier to set up Actions and associated settings.

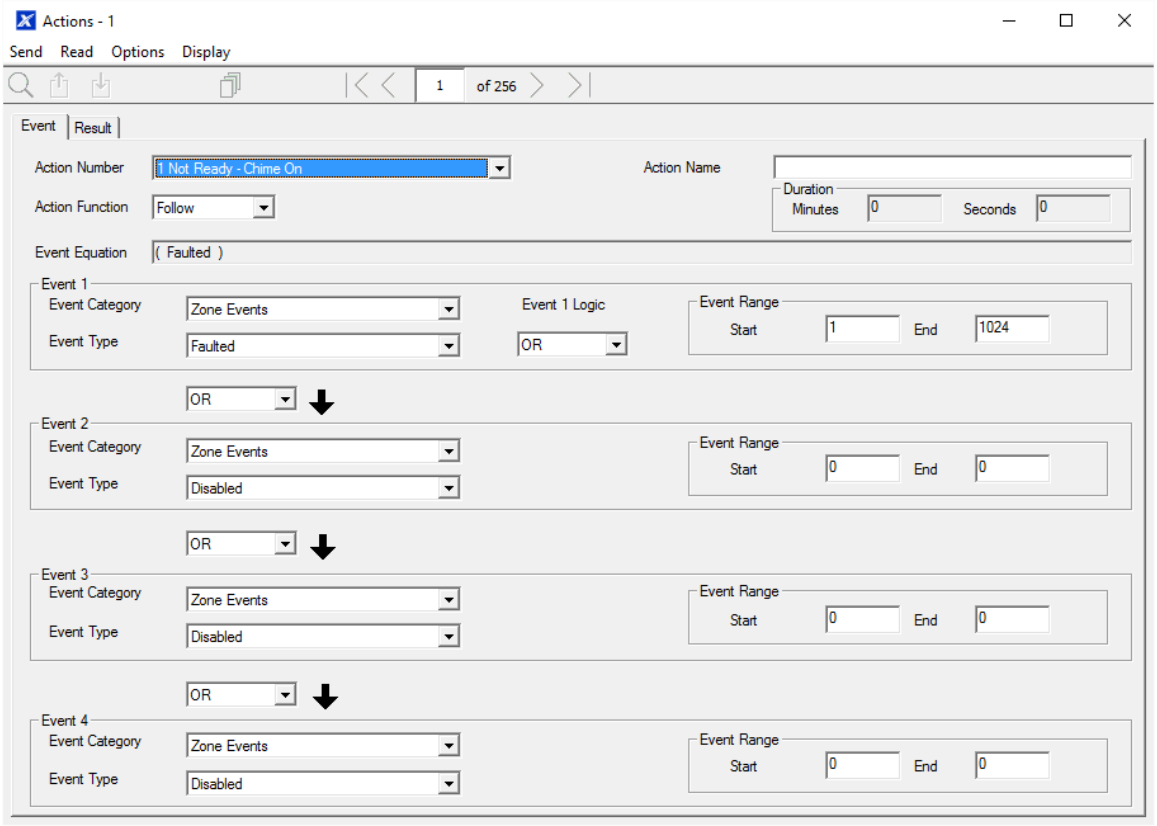
Actions can be used without programming an Action Result. For example, outputs are controlled by setting them to monitor an action, when the Action State is true the output state will follow.

Programming Sequence

Events to be monitored → 8. Actions → 19. Action Groups

Instructions

1. Open Actions.



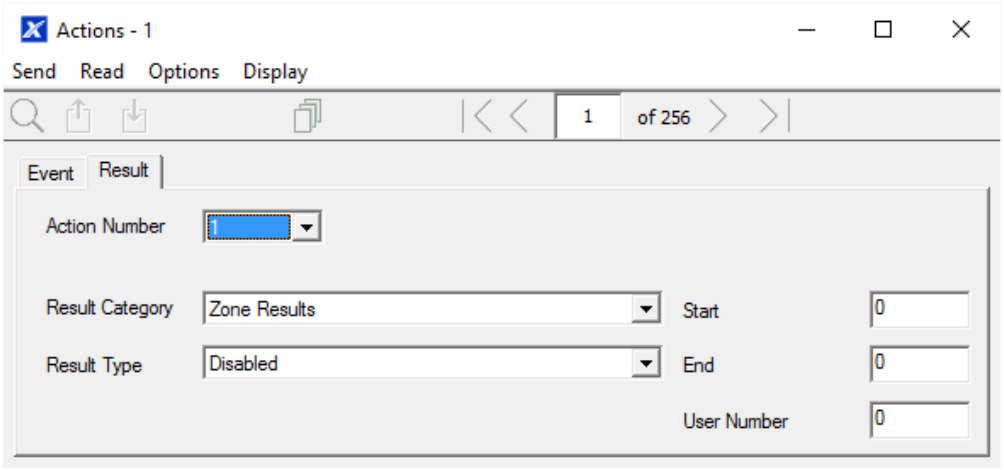
2. Select the Action Number you want to create.
3. Enter a descriptive name for this action.
4. Select the Action Function and the duration (optional) for the **Action State**.

   For example, Timed 5 seconds would cause the Action State to activate for 5 seconds when all the conditions in the Event Equation are satisfied.
5. Select the Event 1 logic, this will be applied before Event 1.

   For example, “Inverted OR” results in “NOT Event 1”.
6. Program the first event by using the Category and Type menus.
7. Enter the Event Range for the selected Category.

   For example, if you want to select Areas 1-4 then set the Event range Start=1 and End=4.
8. Select Event 2 logic and repeat for the remaining events.

9. If you want to program an action result, click the Result tab.



10. Select the Category, Type, Start and End Range.
11. Test the Action by satisfying the Event Logic and checking the desired response.

Next

- Program the device you want to monitor the Action if needed.
- If you want to control an Output, go to that Output and program it to follow the Action.
- If you want a user or device to have access to the action, then program Action Groups and Permissions.

Programming Instructions for Action Groups

Goal

Create a list of actions a user or device has access to.

Pre-conditions

Program the actions you want to use.

Notes

See xGenLite Reference Guide for more details on Actions.

Action Groups can allow you to create a convenient menu for a user to trigger specific Actions from a NXG-1820.

Permissions control what actions a User or Device has access to.

Both the User AND Device need to have access to the desired Action for it to be displayed on a NXG-1820 screen.

Programming Sequence

8. Actions → 19. Action Groups → 11. Permissions
   a) Groups
   b) Options/Timers
   → 13. Menus, 12. Area Groups, 18. Channel Groups, x. Action Groups

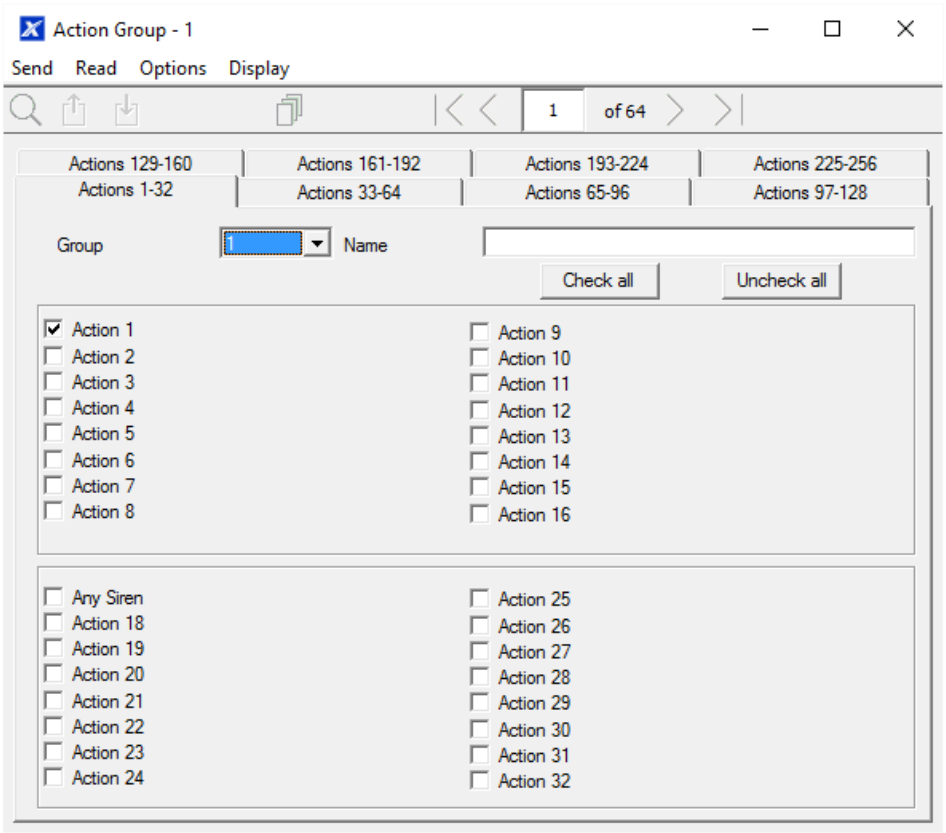
10. Devices
Outputs
zone expanders,
keypads, transmitters
→ 1. User
   a) Main
   b) Advanced

11. Permissions
7. Schedules

11. Permissions
7. Schedules

Instructions

1. Open Action Groups.



2. Select an Action Group Number.
3. Enter a descriptive Name.
4. Select the Actions you want to include.

Next

- Assign Action Group to a Permission.
- Assign Permission to a User or Device.

Programming Instructions for Scenes

Goal

Create a scene that performs multiple functions when a certain condition is met.

Pre-conditions

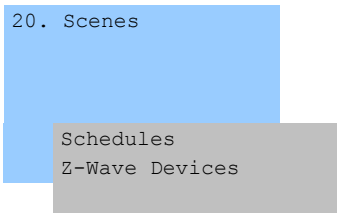
The schedule you want the Scene to follow needs to be programmed.

If you wish to perform Z-Wave Device Actions the Z-Wave device(s) must be learnt in.

Notes

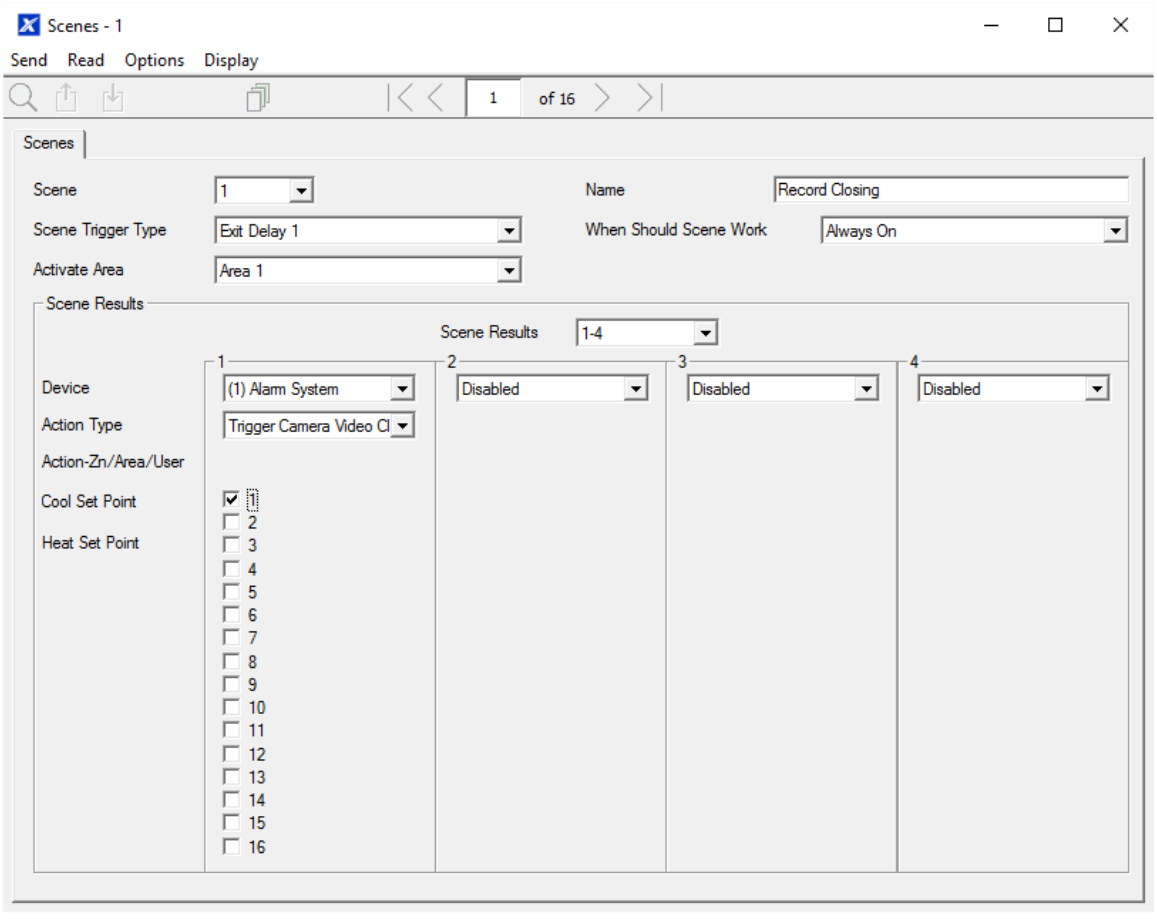
User 99 will be reported for alarm system control events.

Programming Sequence



Instructions

1. Open Scenes.



2. Select Event Type and the Area.
3. Select the Schedule that will determine when this Scene is active.
4. Now program the sequence of actions that you want to happen.

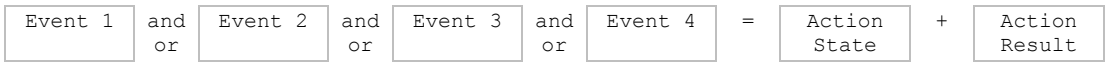
Example

When Exit Delay 1 is running in the Office Area, set Camera 1 to start recording.

Programming Instructions for Outputs

Goal

Turn an output on or off according to an Action.



Pre-conditions

Program the Action and any associated components.

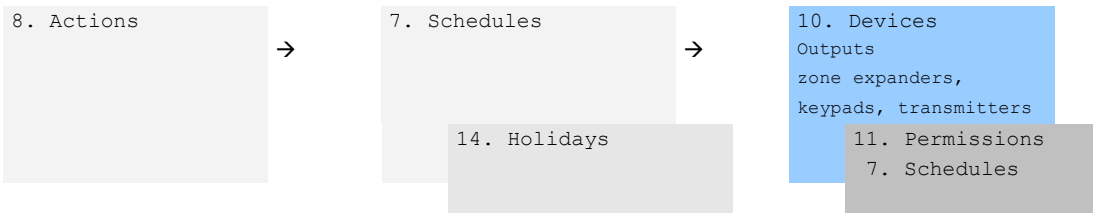
Notes

See xGenLite Reference Guide for more details on Actions.

Write/Plan out on paper what you want to create. This makes it easier to set up Actions and associated settings.

Actions can be used without programming an Action Result. For example, outputs on xGenLite are controlled by monitoring an Action State, no Action Result needs to be programmed.

Programming Sequence

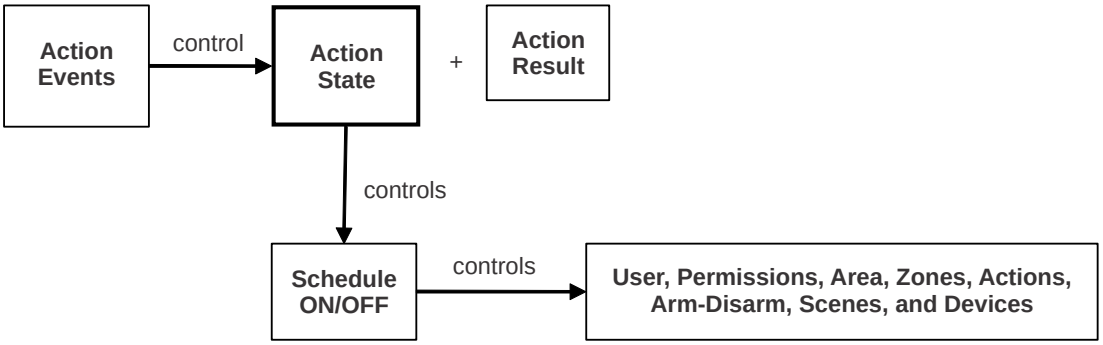


Instructions

1. Select the Device that has the physical outputs you want to control.
2. Select Outputs.
3. Select Action.
4. Select the Schedule.

Combining Actions with Schedules

Schedules can control when a user has access, when an automatic Arm-Disarm occurs, when devices can be used, and more. Actions can turn Schedules on and off, making Schedules conditional based on when certain events occur.



The outcome is that we can control Users, Permissions, Areas, Zones, Actions, Arm-Disarm, Scenes, and Devices, based on various system conditions. This provides automation features that allows the system to respond in real-time to changing conditions.

This functionality is achieved by going to that Schedule, and selecting Follow Action Number.

Take care when combining multiple schedules and actions as troubleshooting can get confusing. Always check and test functionality a single step at a time. Users and Zones can have multiple levels of permissions, be sure to check that each permission level is appropriate at all times.

Example

When a certain user is in the building we can prevent an automatic Arm-Disarm from occurring.

First program an Action with the conditions you want and the Duration of the Action if necessary.

Next program Arm-Disarm with a User and Schedule.

Then set the Schedule to Follow Action Number.

When the action events are met, then the Schedule will become active and will be able to perform an Arm-Disarm at the appropriate time. If the conditions are not met then the Arm-Disarm will never occur.

Arming and Disarming Your System

You may arm and disarm partitions from a NXG-1820 keypad.

Only users with an authorized user code (Level 2 user) will be allowed to use the xGenLite alarm system. Users with no valid user code (Level 1 user) do not have access as defined by EN 50131-3.

Keypress Tamper

The NXG-1820 keypad will be locked in screensaver mode when unused for a preset time. This stops unauthorized users from interacting with the system or viewing detailed status.

A valid PIN is required to unlock the screen and access the system. Users can set PIN codes between 4 and 8 digits in length.

Note: EN 50131 Grade 2 required settings - There are no disallowed account codes. 5 digits minimum to provide 10,000 possible combinations.

Lock Out On 3 Invalid Attempts

If an invalid PIN code is entered three times, the keypad will deny all log in attempts for 90 seconds. Attempts are counted from any method (e.g. keypad, app, or web page). You must wait the full 90 seconds before trying again with the correct PIN. This is to prevent brute-force attacks on guessing PIN codes.

Arm Your System in Away Mode

Enter a valid PIN code to unlock the screen.

Touch the Away or Away + button to arm your system in Away mode:

The icon will change to red when the alarm system is set in away mode.

If your system has multi-Area control enabled, the Away + button will be displayed.

A valid PIN code will need to be entered to determine what permissions they have, this includes which Areas and at what time/day that user has access.

Arm Your System in Stay Mode

Enter a valid PIN code with Stay permissions to unlock the screen.

Touch the Stay or Stay + button to arm your system in Stay mode:

The icon will change to yellow when alarm system is set in Stay mode.

If your system has multi-Area control enabled, the Stay + button will be displayed.

A valid PIN code will need to be entered to determine what permissions they have, this includes which Areas and at what time/day that user has access.

Arm Your System in Instant Stay Mode

Enter a valid PIN code with Stay permissions to unlock the screen.

To arm in Instant Stay mode touch the Stay button two times until the icon is red and displays “Instant”:

This indicates the alarm system is set in Instant Stay Mode.

Arm Your System in Night Mode

Enter a valid PIN code with Stay permissions to unlock the screen.

To arm in Night Mode touch the Stay or Stay + button a total of three times until the icon is red and displays “Night Mode”:

Touching the Night Mode button again will cycle the system back to Stay Mode.

Disarm One or More Areas

Touch the Off or Off + button to disarm your system:

If your system has multi-Area control enabled, the Off + button will be displayed.

A valid PIN code will need to be entered to determine what permissions they have, this includes which Areas and at what time/day that user has access.

Activate SOS Feature

Touch the SOS button to display the SOS feature:

On this screen touch and hold the appropriate button for 2 seconds to activate Manual Fire Alarm, Manual Auxiliary Alarm, or Manual Panic Alarm. These buttons can be enabled and disabled in the Area Options menu.

Depending on how your system is programmed, the control room may receive the corresponding event. Check with your control room to determine what action will be taken.

If silent alarm is enabled, then the keypad will not display any signs that the panic button was pressed.

To cancel a SOS alarm – return to the home screen, touch the Status button and turn the Area off.

Walk Test

1. Log in to panel web page.
2. Click Settings.
3. Click Walk Test.
4. Click Start.
5. Trigger each sensor by walking past PIRs, opening and closing reed switches, pressing tamper buttons, etc. Siren will chirp multiple times for each zone triggered.
6. Click Stop.
7. Click History.

User Reporting

When enabled, quick arming/disarming from the keypad without a PIN code will report user 98 to the Central Monitoring Station. SOS functions also report as user 98.

If the installer PIN is used to arm/disarm, user 256 is reported to the Central Monitoring Station. On legacy NX keypads user 255 will appear in event history.

Appendix 1: System Status Messages

Various messages may appear on the Status screen of xGenLite Web Server and UltraSync+ app.

System

- AC power fail: The security system has lost its electricity power. May take up to 5 min to clear once power restored.
- Low battery: The security system's back up battery requires charging. May take up to 5 min to clear once battery charged.
- Battery test fail: The security system's back up battery requires changing. If after 48 hours this message does not clear, replace with a new battery. If the power fails, the system will not be operational.
- Box tamper: The security system's cabinet tamper input has activated.
- Siren trouble: The security system's external siren has a problem. Check the panel is securely installed on the wall.
- Over current: The security system is drawing too much current. Disconnect some hardwired inputs.
- 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. Check the internet connection, Ethernet cable, or cellular reception is sufficient.
- Fire alarm: A fire alarm has been activated from the panel.
- Panic: A panic alarm has been activated from the panel.
- Auxiliary: An auxiliary alarm has been activated from the panel.

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 zone 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.

Zone Number. Zone Name

- In alarm: This zone has triggered a system alarm condition.
- Is bypassed: This zone is bypassed (inhibited) and will not activate an alarm.
- Chime is set: This zone is part of the chime group.
- Is not secure: This zone is not closed.
- Fire alarm: This zone has triggered a fire alarm.
- Tamper: This zone has triggered a tamper alarm.
- Trouble fault: This zone has an open circuit.
- Loss of wireless supervision: This zone is a wireless device and has lost its communication link with the control panel. Check the zone is within range of the panel and has sufficient battery.
- Low battery: This zone is a wireless device and needs a battery replacement.

Appendix 2: App and Web Error Messages

Various error messages may appear in the xGenLite 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”: Changes cannot be saved, check you have permission or contact your installer.
- “Nothing displayed can be Saved”: No changes are possible on this screen.
- “Program Success!” Changes have been saved.
- “Name Saved”: Changes have been saved.

Zones Page

- “No Zones Configured for Your Access”: Displayed on Zones page when there are no zones available to view

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 []“

Appendix 3: Advanced Menu Tree

1. Users

2. System
- 1. System Clock
- 2. General Options
- 3. System Timers
- 4. Siren Options
- 5. Service and Test Options
- 6. Status
- 7. System Counts
- 8. Language
  - 1. Language
  - 2. Voice Language
- 9. Automation Menu

3. Zones
- 1. Zone Number
- 2. Zone Name
- 3. First Zone Profile
  - 1. Zone Type
  - 2. Zone Options
  - 3. Area Group
  - 4. Schedule Number
  - 5. User Number
- 4. Second Zone Profile

4. Areas
- 1. Area Number
- 2. Area Name
- 3. Area Entry-Exit Times
- 4. Area Options
- 5. Area Timers
- 6. Area Type Settings
- 7. Area Event Reporting

5. Channels
- 1. Channel Number
- 2. Channel Name
- 3. Account Number
- 4. Format
- 5. Device Number
- 6. Destination
- 7. Next Channel
- 8. Event List
- 9. Attempts
- 10. Language

6. Communicator
- 1. General Options
- 2. Auto Test
- 3. IP Configuration
  - 1. IP Host Name
  - 2. IP Address
  - 3. Gateway
  - 4. Subnet
  - 5. Primary DNS
  - 6. Secondary DNS
  - 7. Ports
  - 8. Time Server
  - 9. IP Options
- 4. Radio Configuration
  - 1. GPRS Username
  - 2. GPRS Password
  - 3. APN
- 5. Remote Access
  - 1. Panel Device Number
  - 2. Download Access Code
  - 3. Call Back Number
  - 4. Callback Server
  - 5. Number Of Rings
  - 6. Number of Calls
  - 7. Answering Machine Defeat
  - 8. 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. Keypad
  - 3. Zone Exp
  - 4. Output Exp
  - 5. Power Supply
- 2. Interlogix Transmitters
  - 1. Transmitter Number
  - 2. Serial Number
  - 3. User
  - 4. Options
  - 5. Scene
  - 6. Signal Strength
- 3. Z-Wave Devices
  - 1. Name
  - 2. Basic Type
  - 3. Generic Type
  - 4. Specific Type
- 4. Tablet Keypads
  - 1. Name
  - 2. Serial Number
  - 3. Area Group
  - 4. Keypad Options

11. Permissions
- 1. Permission Number
- 2. Permission Name
- 3. Control Groups
- 4. Permission Options
- 5. User Timer Options

12. Area Groups
- 1. Area Group Number
- 2. Area Group Name
- 3. Area List

13. Menus
- 1. Menu Number
- 2. Menu Name
- 3. Menu Selections

14. Holidays
- 1. Holiday Number
- 2. Holiday Name
- 3. Date Range

15. Zone Types
- 1. Zone Type Number
- 2. Zone Type Name
- 3. Zone Type Armed
- 4. Zone Type Disarmed

16. Zone Options
- 1. Zone Options Number
- 2. Zone Options Name
- 3. Zone Options
- 4. Zone Reporting
- 5. Zone Contact Options
- 6. Zone Report Event

17. Event Lists
- 1. Event List Number
- 2. Event List Name
- 3. Event List

18. Channel Groups
- 1. Channel Group Number
- 2. Channel Group Name
- 3. Channel List

19. Action Groups
- 1. Action Group Number
- 2. Action Group Name
- 3. Action Group List

20. Scenes
- 1. Scene Number
- 2. Scene Name
- 3. Activate Schedule
- 4. Activate Event Type
- 5. Activate Zone
- 6. Scene Actions

22. Cameras
- 7. Camera Number
- 8. Camera Name
- 9. LAN IP Address
- 10. MAC Address
- 11. Panel to Camera Connection

23. UltraSync
- 12. Web Access PIN
- 13. Ethernet Server 1
- 14. Ethernet Server 2
- 15. Ethernet Server 3
- 16. Ethernet Server 4
- 17. Wireless Server 1
- 18. Wireless Server 2
- 19. Wireless Server 3
- 20. Wireless Server 4

Index

Z