



xGenConnect Installation and Programming Guide

Copyright © 2023 Carrier. All rights reserved. Specifications subject to change without prior notice.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Carrier, except where specifically permitted under US and international copyright law.

Trademarks and patents

Caddx, xGenConnect name and logo are trademarks of Carrier.

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:

Carrier Fire & Security Americas Corporation Inc.
13995 Pasteur Blvd
Palm Beach Gardens, FL 33418, USA

AUTHORIZED EU REPRESENTATIVE:

Carrier 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. CARRIER 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.

EU compliance



Certification

EN 50131-1:2006+A1:2009+A2:2017 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)

This product was tested and certified to EN 50136-2:2013 for Alarm transmission system performance SP3 and SP4 for reporting over IP(LAN) to the UltraSync and OH NetRec.

This product was tested and certified to EN 50136-2:2013 for Alarm transmission system performance SP3 and SP4 for reporting over GPRS to the UltraSync and OH NetRec.

This product was tested and certified to EN 50136-2:2013 for Alarm transmission system performance DP2 and DP3 for reporting over IP(LAN) and GPRS to the UltraSync and OH NetRec.

Tested and certified by Kiwa Nederland 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

Carrier 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: firesecurityproducts.com

REACH

Product may contain substances that are also Candidate List substances in a concentration above 0.1% w/w, per the most recently published Candidate List found at ECHA Web site.

Safe use information can be found at <https://firesecurityproducts.com/en/content/intrusion-intro>



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: 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: recyclethis.info.

Contact information

www.firesecurityproducts.com/en/page/caddx

Content

Important information	iv
Limitation of liability	iv
Product Warnings	iv
Warranty Disclaimers	v
Disclaimer	vi
Intended Use	vi
Advisory messages	vii
Introduction	1
System Capacity	1
xGenConnect Specifications	2
Product Codes	2
Mains Power Specifications	3
Installation Instructions for Service Persons	3
Power Supply Specifications	3
General Features	4
Current Consumption	5
Output Current Rating	6
Auxiliary Current and Battery Capacity	6
Environmental	7
Physical Dimensions and Weight	7
Fuses	8
Maintenance	8
System Monitoring	8
SIA and CID Reporting Code Descriptions	9
EN 50131-3 and EN 50136-2 Compliancy	12
Options Affected by EN 50131 Regulations	13
Optional Functions	14
EN 50131 Compliance Precautions	14
Alarm Transmission Path and Alarm Transmission System	
Faults	15
EN 50131 and INCERT certified components	15
Other regulations	16
Installation	17
NXG-8(E) Wiring Diagram	17
NXG-8(E) Terminals	19
NXG-8(E) LEDs	20
NXG-9 Wiring Diagram	21
NXG-9 Terminals	21
NXG-9 LEDs	21
NXG-4 Wiring Diagram	22
NXG-4 Terminals	22

NXG-4 LEDs	22
Detector EOL Wiring	23
Hardwired Shock Sensor	23
Power Requirements	24
Cable Requirements	24
Grounding	24
Shielding	25
Termination Links	25
Installing NXG-8 panel / NX-003 housing	25
Installing Legacy NX Modules	26
Installing Antennas	26
Installing NXG-8(E)-CB panel / NX-003-CB housing	28
NXG-320 Plastic Enclosure	29
NXG-003-G3 xGen Metal Enclosure	30
Enrolling Modules	30
Deleting Modules	32

Arming and Disarming Your System 33

Keypress Tamper	33
Lock Out on 3 Invalid PIN Attempts	33
Lock Out on 10 Invalid Card Attempts	33
Arm Your System with NXG-1820-EUR keypad	33
Arm Your System with NXG-183x-EUR keypad	34
Disarm Partitions with NXG-1820-EUR keypad	35
Disarm Partitions with NXG-183x-EUR keypad	35
Arm/Disarm Your System with Simplified Arm-Disarm mode enabled	36
Arm/Disarm Your System with NXG-1832 / NXG-1833-EUR keypad and user card	36
Activate SOS Feature (NXG-1820-EUR only)	37

Programming Methods 39

Account Access	39
Method 1: DLX900 Management Software	40
Method 2: Web Server	42
Method 3: UltraSync+ App	45
Method 4: NXG-1820 Keypad	51

Programming with Web Pages 52

Recommended Items to Change	52
Learning Wireless Zones	53
Adding a User	57
Adding Cards to Users	59
Adding a Keyfob	61
Advanced Keyfob Programming	62
AB Alarm Confirmation	64
Country	64
Programming Doors	64
Programming Card Security	67

Programming Cameras 68
Configuring Email Reports 80
Configuring OH Reports 81
Enabling Push Notifications on Smartphone 84
Enable SMS Notification 89

Programming Scenes 91

Programming Instructions 94

Programming Instructions for System Options 94
Programming Instructions for Permissions 98
Programming Instructions for Menus 100
Programming Instructions for Holidays 102
Programming Instructions for Users 105
Programming Instructions for Zones 108
Programming Instructions for Custom Zones 111
Programming Instructions for Partitions 115
Programming Instructions for Schedules 118
Programming Instructions for Arm-Disarm 122
Programming Instructions for Communicator 127
Programming Instructions for UltraSync 131
Programming Instructions for Event Lists 133
Programming Instructions for Channels 135
Programming Instructions for Zone Reporting 139
Programming Instructions for System Event Reporting 141
Programming Instructions for Actions 143
Programming Instructions for Action Groups 145
Programming Instructions for Scenes 147
Programming Instructions for Outputs 148
Combining Actions with Schedules 149
Walk Test 150
User Reporting 150

Appendix 1: System Status Messages 151

Appendix 2: App and Web Error Messages 153

Appendix 3: NetworX Modules Compatibility 154

Appendix 4: Advanced Menu Tree 156

Appendix 5: NXG-183x Keypad Features 157

Glossary 161

Index 167

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Carrier Fire & Security 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 Carrier Fire & Security 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 Carrier Fire & Security 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, Carrier Fire & Security 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 CARRIER FIRE & SECURITY PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH CARRIER FIRE & SECURITY HAS NO CONTROL AND FOR WHICH CARRIER FIRE & SECURITY SHALL NOT BE RESPONSIBLE INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND OPERATING SYSTEM COMPATIBILITY; MONITORING SERVICES; ELECTROMAGNETIC OR OTHER INTERFERENCE, AND PROPER INSTALLATION AND MAINTENANCE OF AUTHORIZED PRODUCTS (INCLUDING ALARM OR OTHER CONTROL PANEL AND SENSORS).

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

PRODUCTS), SOFTWARE, SERVICES OR OTHER OFFERINGS WILL NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

CARRIER FIRE & SECURITY 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

CARRIER FIRE & SECURITY 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.

CARRIER FIRE & SECURITY 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.

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

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

CARRIER FIRE & SECURITY 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

CARRIER FIRE & SECURITY 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 CARRIER FIRE & SECURITY 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 CARRIER FIRE & SECURITY.

Disclaimer

THE INFORMATION IN THIS DOCUMENT IS SUBJECT TO CHANGE WITHOUT NOTICE. CARRIER FIRE & SECURITY 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 FIRESECURITYPRODUCTS.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 xGenConnect 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 firesecurityproducts.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 xGenConnect is an advanced intrusion panel for protecting your home, business, and assets.

With large expansion capabilities, multi-partition mode, wireless expansion, door control features, advanced user permissions, advanced schedules, and home automation features, the xGenConnect 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, doors, 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 xGenConnect intrusion panel is designed to be operated from the NXG-1820 touchscreen keypad with 3.5-inch screen, or from the NXG-183x keypad with graphic display. These keypads allow access to all programming features.

System Capacity

Feature	NXG-4	NXG-8	NXG-8E	NXG-9
On-board zones	4	8	8	8
Max Zones	4 hardwired 16 wireless	48	192	48
Partitions	4	8	8	8
Users	40	100	256	100
Max Keyfobs	8	16	64	16
Max Tablets	4	4	4	4
Max keypads	16	24	24	24
Max Expander Modules incl. Keypads and Tablets	24	32	32	32
Max doors	4	16	16	16
On-board outputs	3 OC, BELL	4 OC, BELL, Smoke	4 OC, BELL, Smoke	4 OC, BELL, Smoke
Main event log capacity	1024	1024	1024	1024
Access event log capacity	5000	5000	5000	5000

xGenConnect Specifications

Product Codes

Product	Description	EN grade
NXG-4	xGenConnect panel, 4 zones, 4 partitions, max. 16 zones, with IP on-board	2
NXG-4-RF	xGenConnect panel, 4 zones, 4 partitions, max. 16 zones, with IP and LoNa Receiver on-board	2
NXG-8	xGenConnect panel, 8 zones, 8 partitions, max. 48 zones, with IP on-board	2
NXG-8-CB	xGenConnect panel, 8 zones, 8 partitions, max. 48 zones, with IP on-board, large metal housing	2
NXG-8E	xGenConnect panel, 8 zones, 8 partitions, max. 192 zones, with IP on-board	2
NXG-8E-CB	xGenConnect panel, 8 zones, 8 partitions, max. 192 zones, with IP on-board, large metal housing	2
NXG-9-LB	xGenConnect panel, 8 zones, 8 partitions, max. 48 zones, with IP on-board, large poly housing	2
NXG-9-RF-LB	xGenConnect panel, 8 zones, 8 partitions, max. 48 zones, with IP and LoNa Receiver on-board, large poly housing	2
NXG-4-BO	xGenConnect board, 4 zones, 4 partitions, max. 16 zones, with IP on-board	2
NXG-4-RF-BO	xGenConnect board, 4 zones, 4 partitions, max. 16 zones, with IP and LoNa Receiver on-board	2
NXG-8-BO	xGenConnect board, 8 zones, 8 partitions, max. 48 zones, with IP on-board	2
NXG-8E-BO	xGenConnect board, 8 zones, 8 partitions, max. 192 zones, with IP on-board	2
NXG-9-BO	xGenConnect board, 8 zones, 8 partitions, max. 48 zones, with IP on-board, for poly housing	2
NXG-9-RF-BO	xGenConnect board, 8 zones, 8 partitions, max. 48 zones, with IP and LoNa Receiver on-board, for poly housing	2
NXG-1820-EUR	3.5 inch Touchscreen keypad, multilingual	2/3
NXG-183x-EUR	LCD keypad, multilingual	2
NXG-208-G3	8 zone expander	2/3
NXG-208N	xGenConnect 8 zone expander board	2
NXG-216N	xGenConnect 16 zone expander board	2
NXG-220-G3	20 zone expander	2/3
NXG-504	4 relay output expander	2/3
NXG-508N	xGenConnect 8 relay expander board	2
NXG-510	10 relay output expander	2/3
NXG-005	Pry-off tamper switch incl. metal U-bracket	2/3
NX-002	Small metal enclosure for NXG-4, no cam lock, no tamper	2

Product	Description	EN grade
NX-003	Standard metal enclosure for NXG-8/8E, with cam lock, no tamper	2
NX-003-CB	Large metal enclosure for NXG-8/8E, with cam lock, tamper, including stand-offs	2
NX-005-C	Housing tamper switch	2
NXG-003-DIN	DIN-rail mounting kit	2/3
NXG-868	Wireless expander 868 MHz Gen 2	None
NXG-433	Wireless expander 433 MHz	2
NXG-7002(-SIM)	4G/Wi-Fi communication expander (-SIM includes SIM card)	2
NXG-7102(-SIM)	4G communication expander (-SIM includes SIM card)	2

Mains Power Specifications

Mains input voltage	230 VAC +10%, -15%, 50/60 Hz ±10%
Current consumption at 230 VAC	240 mA max.
Transformer output:	
NXG-4, NXG-8(E)	16.3 VAC 40 VA
NXG-9	20 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:	
NXG-4	140 mA at 13.8 VDC ± 0.4 V
NXG-8(E)	125 mA at 13.8 VDC ± 0.4 V
NXG-9	150 mA at 13.8 VDC ± 0.4 V
Maximum system current available:	2000 mA at 13.8 VDC ± 0.4 V
Auxiliary power output (AUX. POWER):	13.8 VDC ± 0.4 V, 600 mA max.
Auxiliary power output (bus):	13.8 VDC ± 0.4 V, 600 mA max.
Battery power output (BAT):	
NXG-4	13.8 VDC ± 0.2 V, 350 mA max.
NXG-8(E)	13.8 VDC ± 0.2 V, 350 mA max.
NXG-9	13.8 VDC ± 0.2 V, 570 mA max.

Battery type	Certified sealed lead acid rechargeable. 7.2 Ah 12 V nominal 12 Ah 12 V nominal (NXG-8 and NXG-9 only) 18 Ah 12 V nominal (NXG-8 only) Minimum energy level of the battery in its charged state is 100%
Minimum voltage	9.45 VDC
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, 550 mV max.

General Features

Code combinations:

xGenConnect	From 10,000 (4 digits) to 100,000,000 (8 digits)
-------------	--

Maximum user number:

NXG-4	40
NXG-8, NXG-9	100
NXG-8E	256

User Permissions:

NXG-4	32
NXG-8, NXG-9	64
NXG-8E	128

Onboard zones:

NXG-4	4 (default); 8 if zone doubling enabled.
NXG-8(E), NXG-9	8 (default); 16 if zone doubling enabled.

Maximum zone number:

NXG-4	16
NXG-8, NXG-9	48
NXG-8E	192

Additional inputs:

NXG-4, NXG-8(E)	1: box tamper
NXG-9	2: box tampers

End-of-line resistor

Standard	4.7 k Ω / 9.4 k Ω (Aritech), 4.1 k Ω / 8.2 k Ω (Guardall), 1 k Ω / 2 k Ω (Galaxy), 3.3 k Ω / 6.6 k Ω (NX)
Aritech	4.7 k Ω / 9.4 k Ω / 14.7 k Ω / 19.4 k Ω
Guardall	4.1 k Ω / 8.2 k Ω / 12.3 k Ω / 16.4 k Ω
Galaxy	1 k Ω / 2 k Ω
Vanderbilt	4.7 k Ω / 9.4 k Ω / 6.9 k Ω / 11.6 k Ω
2-wire smoke	820 Ω

Zone Doubling	3.74 k Ω / 6.98 k Ω See "Detector EOL Wiring" on page 23 for more information.
Onboard outputs:	
NXG-4	4: bell, strobe, siren and power outputs
NXG-8(E), NXG-9	5: bell, strobe, siren and power outputs
Maximum output number	32
Maximum action number	32
Partitions:	
NXG-4	4
NXG-8(E), NXG-9	8
Maximum keypad:	
NXG-4	16
NXG-8(E), NXG-9	24
Maximum expander modules, incl. keypads:	
NXG-4	24
NXG-8(E), NXG-9	32
Non-volatile Memory	
Main event log capacity	1024
Access event log capacity	5000
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

xGenConnect Bus

Type	4 wire RS485 bus High common mode tolerance (25V)
Capacity	Up to 32 devices
Range	800 m
Cable flammability rating	VW-1

Current Consumption

Product	Main description	Current Consumption (non-alarm)	Current Consumption (alarm)
NXG-8(E)	8 zone panel	125 mA typical	125 mA typical
NXG-9	8 zone panel	150 mA typical	150 mA typical
NXG-4	4 zone panel	140 mA typical	140 mA typical

Product	Main description	Current Consumption (non-alarm)	Current Consumption (alarm)
NXG-1820	Touchscreen keypad	100 mA typical, 40 mA in idle mode	175 mA max with sounder and screen on max brightness
NXG-1830-EUR, NXG-1831-EUR	LCD keypad	90 mA typical, 35 mA minimum	160 mA max.
NXG-1832-EUR, NXG-1833-EUR	LCD keypad with integrated Mifare card reader	130 mA typical, 40 mA minimum	200 mA max.
NXG-208-G3	8 zone expander	25 mA	25 mA
NXG-208N	xGenConnect 8 zone expander board	30 mA	30 mA
NXG-216N	xGenConnect 16 zone expander board	30 mA	30 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-508N	xGenConnect 8 relay expander board	20 mA idle 130 mA 8 relays on	20 mA idle 130 mA 8 relays on
NXG-510	10 relay output expander	20 mA idle 160 mA 10 relays on	20 mA idle 160 mA 10 relays on
NXG-7002	4G Cellular and Wi-Fi Router Module	118 mA minimum, 138 mA average	200 mA

Output Current Rating

Output	35 VA Transformer	40 VA Transformer	55 VA Transformer
Combined J2 BELL+, J2 AUX+ (Smoke), and J7 AUX+ (Outputs)	500 mA max at 13.8 VDC	600 mA max at 13.8 VDC	600 mA max at 13.8 VDC
Combined J2 POS (XR Bus), and J3 POS (NX Bus)	500 mA max at 13.8 VDC	600 mA max at 13.8 VDC	600 mA max at 13.8 VDC

Auxiliary Current and Battery Capacity

xGenConnect (EMEA)

Discharge Time	Charge Time	7.2 Ah Battery	12 Ah Battery	18 Ah Battery	Reference
NXG-4					
12 h	72 h	460 mA	N/A	N/A	EN 50131 Grade 1 and 2
24 h	48 h	160 mA	N/A	N/A	INCERT Grade 2
NXG-8(E)					
12 h	72 h	475 mA	875 mA	1200 mA	EN 50131 Grade 1 and 2

Discharge Time	Charge Time	7.2 Ah Battery	12 Ah Battery	18 Ah Battery	Reference
24 h	48 h	175 mA	375 mA	625 mA	INCERT Grade 2
NXG-9					
12 h	72 h	450 mA	850 mA	N/A	EN 50131 Grade 1 and 2
24 h	48 h	150 mA	350 mA	N/A	INCERT Grade 2

Note: Main board quiescent current is included in the table above.

Example for NXG-8 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 475 mA.

Environmental

Operating temperature	-10 to +55°C
Humidity	95% non-condensing
IP protection grade	IP30
NXG-4, NXG-8(E) 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 & DP3
Cellular	SP4 & DP3
NXG-1820 ACE classification	Type A
NXG-183x ACE classification	Type A

Physical Dimensions and Weight

Product	Main description	Dimensions (HxWxD)	Weight (g)
NXG-4(-RF)	xGenConnect /w metal enclosure	214 x 232 x 94 mm (enclosure only) 359 x 232 x 94 mm (with antennas)	1435 g
NXG-8(E)	NXG-8(E) /w standard metal enclosure	292 x 291 x 91 mm	2075 g
NXG-8(E)-CB	NXG-8(E) /w large metal enclosure	394 x 256 x 118 mm	7150 g
NXG-9-RF	NXG-9 /w standard poly housing	220 x 253 x 112 mm	1800 g
NXG-9(-RF)-LB	NXG-9 /w large poly housing	394 x 256 x 118 mm	2800 g
NXG-8-BO	NXG-8, board only	273 x 89 x 25 mm	210 g
NXG-4(-RF)-BO	NXG-4, board only	192 x 89 x 25 mm	155 g
NXG-9(-RF)-BO	NXG-9, board only		210 g
NXG-003-G3	Metal Enclosure	475 x 395 x 130 mm	7150 g

Product	Main description	Dimensions (HxWxD)	Weight (g)
NXG-1820-EUR	Touchscreen keypad	18 x 82 x 125 mm	150 g
NXG-183x-EUR	LCD keypad	133 x 130 x 25 mm	300 g
NXG-208	8 zone expander	135 x 80 x 55 mm	150 g
NXG-208N	xGenConnect 8 zone expander board	153 x 57 mm	60 g
NXG-216N	xGenConnect 16 zone expander board	153 x 57 mm	60 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-508N	xGenConnect 8 relay expander board	153 x 57 mm	70 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+)	
NXG-8(E)	1.1 A, resettable
NXG-9	2 A, resettable
System LAN (combined for J2 POS, J3 POS)	
NXG-8(E)	1.1 A, resettable
NXG-9	2 A, resettable
Mains, mains fuse	500 mA, fast 20x5
Note: Mains fuse is a 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

Monitoring function	Message	Cause
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
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

#	SIA code	CID code	Function
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
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

#	SIA code	CID code	Function
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
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

#	SIA code	CID code	Function
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
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 xGenConnect. 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.

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 Partitions and Control Partitions settings are identical
- Buzzer silent, never
- Quick set, off
- Function keys, all set to None
- User group options, No OP/CL reports option set to No
- Inhibit, set to No for all zones with type Panic, 24H
- Swinger shunt, set to Yes for all zones
- ACK on keypad, set to None for all zones with type Keypad
- 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 10 to 70 s
- 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
- Partition option to override EN50131-1 Arming Cancellation set to No
- User option not to report open/close events – only with at least one CIE (Control and Indicating Equipment) in the system

Refer to *xGen Reference Guide* 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.

Events are read-only, they cannot be deleted or altered by users of any level. At least 500 mandatory events are stored in a separate memory location. Mandatory events will be preserved and will not be overwritten by non-mandatory events according to the EN 50131 standard. To view only mandatory events, select Event History Filter > Alarm.

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.

Alarm Transmission Path and Alarm Transmission System Faults

The alarm panel is able to continually monitor single (IP or cellular) and dual (IP and cellular) paths for communication issues when provisioned with an appropriate service grade. If one or both paths become unavailable, the issue will be logged in the event history, communicated by the UltraSync server to the control room, and displayed on a local keypad. Most communication issues are temporary and resolve automatically without user intervention.

- IP PATH Failure 999: The alarm panel is unable to communicate with the central station. Alarm reporting is not possible as no paths are available. Check if the communication path is functioning. For cellular, check reception, antenna connection, and SIM card. For IP, check the cable, router, and internet connection.
- IP PATH Restore 999: The communication paths to the central station have been restored.
- IP PATH Failure 998: The alarm panel is unable to communicate with the central station via cellular. Alarm reporting may be possible via IP path where provisioned. Check reception, antenna connection, and SIM card.
- IP PATH Restore 998: The cellular communication path to the central station has been restored.
- Channel1 – Fail to Communicate: The alarm panel is unable to communicate with the central station. Check the internet connection or cellular reception.
- Channel1 – Communication Restore: The communication path to the central station has been restored.
- Cell Link Fault: The GSM modem is removed or failed.

EN 50131 and INCERT certified components

The xGenConnect system is EN and INCERT certified with the following components.

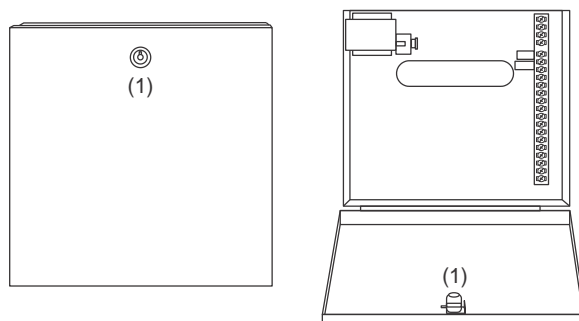
- Power supplies: NXG-320, NXG-320-CPU
- Keypads: NXG-1820-EUR (Grade 2 only), NXG-183x-EUR (Grade 2 only), NX-1048-EN
- Readers: NX-1701E
- Expanders: NXG-504, NXG-508N, NXG-510, NXG-208, NXG-208N, NXG-216N, NXG-220, NXG-208-G3, NXG-220-G3, NX-216E-EN, NX-216Z8, NX-507E, NX-508E
- Wireless expanders: NXG-433
- GSM Module: NXG-7002(-SIM), NXG-7102(-SIM)
- Housings: NX-003 and NX-003-CB with NX-005-C tamper mounted

Other regulations

INCERT

The following options and values are mandatory for INCERT T031ed2 regulations.

- Engineer tamper reset: On.
- The cabinet must be equipped with a cam lock (item 1 in figure below). In case of retrofit from NX-4 to NXG-4, the cam lock must be ordered separately, part number 600-CL.

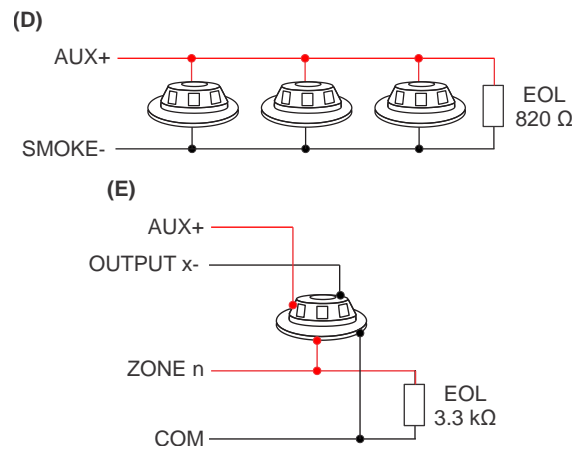
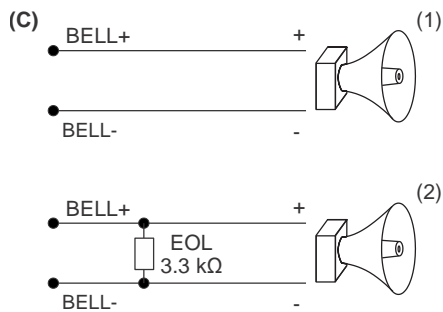
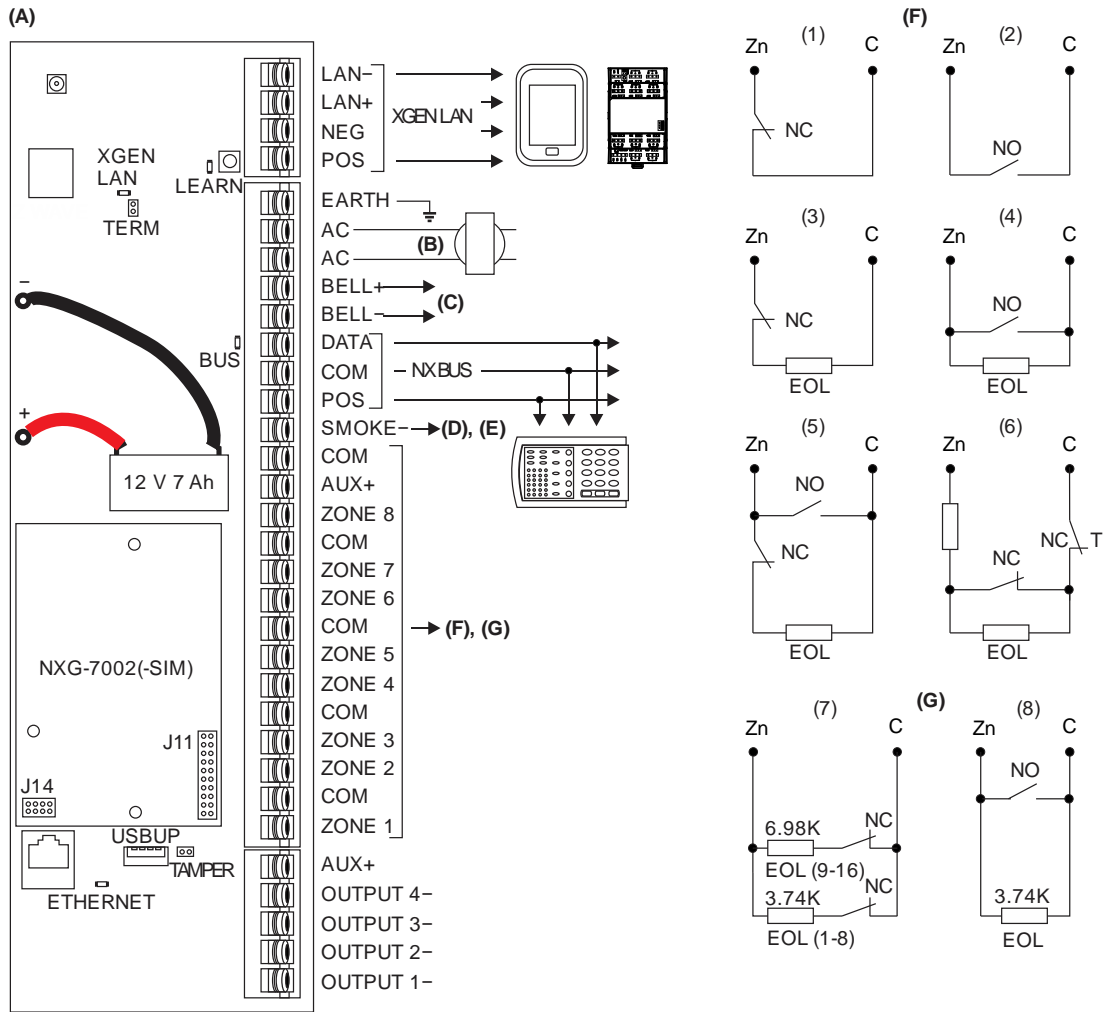


Caution: NXG-8(E)-CB panels and NX-003-CB large metal housings are delivered with optional housing stand-offs.

Using stand-offs is not compliant with EN 50131-1 and INCERT.

Installation

NXG-8(E) Wiring Diagram



(A) NXG-8(E)

(B) Transformer

16 VAC, 1.5 A, 40 VA transformer. Fuse 500 mA, 250 VAC. See also "xGenConnect Specifications" on page 2.

(C) Voltage output / Speaker output

- (1) Indoor Siren/Speaker
Siren Options > Voltage Siren Output is OFF. By default, speaker output for 15 or 20 W speaker with 4, 8 or 16 Ω load.
- (2) Voltage Output for 12 VDC indoor siren
Siren Options > Voltage Siren Output is ON.
Max. load = 500 mA
Requires 3.3 k Ω EOL.

(D) 2-wire smoke detector

Enable Two Wire Smoke feature
Program zone 8 as Zone type "Fire" and Zone options "Fire"
820 Ω resistor

(E) 4-wire smoke detector

Program Zone type "Fire" and Zone options "Fire"
3.3 k Ω resistor

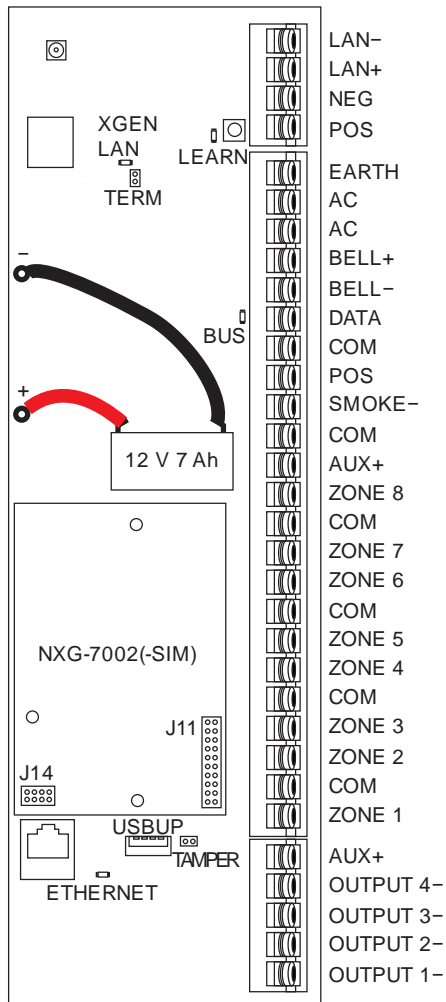
(F) Single zone

- (1) NC contact
 - (2) NO contact
 - (3) NC contact with EOL resistor
 - (4) NO contact with EOL resistor
 - (5) One NO contact and one NC contact with EOL resistor
 - (6) Zone tamper EOL resistor
- See "Detector EOL Wiring" on page 23 for supported resistor values.

(G) Doubled zone

- (7) 3.74K resistors for zones 1 to 8.
6.98K resistors for zones 9 to 16.
- (8) Doubled zone configuration used as a fire zone.
Upper zone (9 to 16) is not usable.

NXG-8(E) Terminals



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

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

TERM: Term link for xGenConnect 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 indoor 12 VDC siren or speaker.

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 xGenConnect.

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

J13: 5-pin connector used to upgrade and program xGenConnect with USBUP-EUR-V2 tool.

TAMPER: Connect to panel box tamper.

AUX+: Terminal for auxiliary power to outputs.

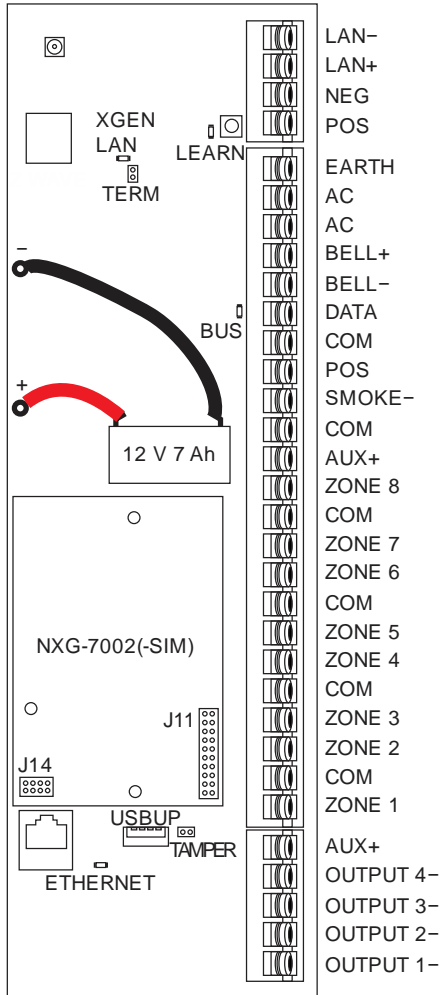
OUTPUT 4: Open collector output switches to ground, power output, by default inverted, can be assigned to an Action.

OUTPUT 3: Open collector output switches to ground, power output, by default inverted, can be assigned to an Action.

OUTPUT 2: Open collector output switches to ground, hold-off for outdoor siren, by default inverted, can be assigned to an Action.

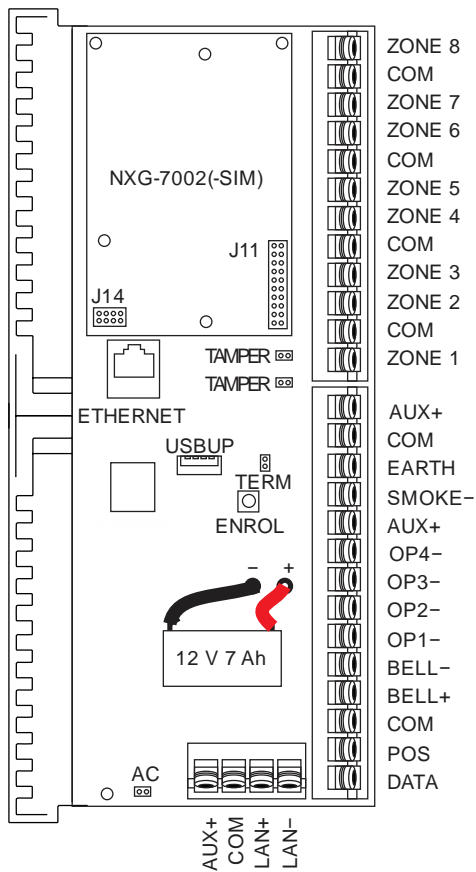
OUTPUT 1: Open collector output switches to ground, hold-off for outdoor flash, by default inverted, can be assigned to an Action.

NXG-8(E) LEDs



- 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 xGenConnect 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 / Wi-Fi 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(E) Wiring Diagram” on page 17. The NXG-9 unit functionality is the same the NXG-8 except that the connections are spatially orientated differently.

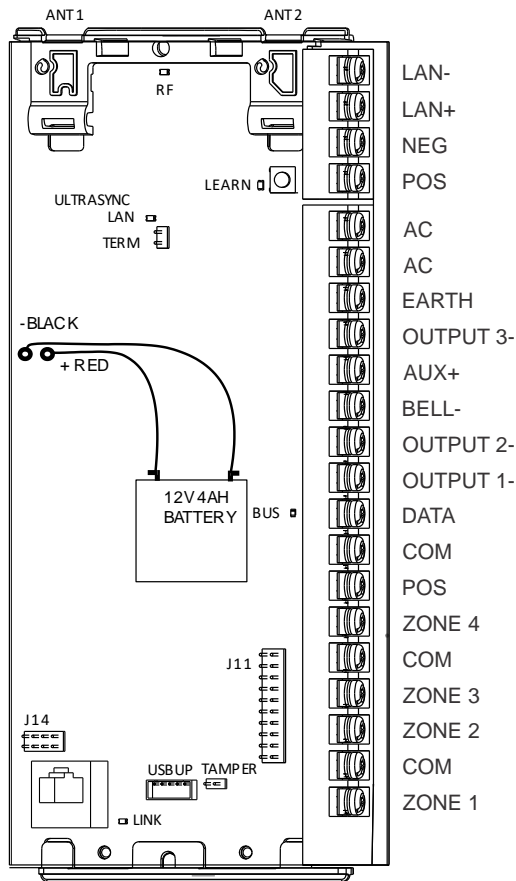
NXG-9 Terminals

Refer to “NXG-8(E) Terminals” on page 19. The NXG-9 unit functionality is the same as the NXG-8 except that the connections are spatially orientated differently.

NXG-9 LEDs

Refer to “NXG-8(E) LEDs” on page 20. The NXG-9 unit functionality is the same the NXG-8 except that the LEDs are spatially orientated differently.

NXG-4 Wiring Diagram



Refer to “NXG-8(E) Wiring Diagram” on page 17. The NXG-4 unit functionality is the same as NXG-8 except that the connections are spatially orientated differently.

NXG-4 Terminals

Refer to “NXG-8(E) Terminals” on page 19.

The NXG-4 unit functionality is the same as NXG-8 except it provides two additional connections:

- Antenna 1: After the board is installed in the metal enclosure, insert the antenna with the corresponding icon.
- Antenna 2: After the board is installed in the metal enclosure, insert the antenna with the corresponding icon.

Caution: Removing one or both antennas will cause the panel to report a panel housing tamper.

NXG-4 LEDs

Refer to “NXG-8(E) LEDs” on page 20.

The NXG-4 unit functionality is the same as NXG-8 except it has the following additional LED:

- D5 RF: Red LED blinks when message is sent or received from a 63bit / 80plus transmitter.

Detector EOL Wiring

When the System > EOL Resistor Value > Normal Range option is set to Standard, the inputs on the xGenConnect panels and zone expanders support the following end-of-line resistor value combinations:

Standard	Caddx	Aritech	Guardall
Tamper (short)	0	0	0
Normal	3.3 k Ω	4.7 k Ω	4.1 k Ω
Alarm	6.6 k Ω	9.4 k Ω	8.2 k Ω
Tamper (open)	∞	∞	∞

Note: The value Standard does not report fault/anti-mask on the panel on-board zones.

The option System > EOL Resistor Value > Normal Range is a system wide parameter. Other system wide EOL resistor value options are Guardall, Aritech, Galaxy and Vanderbilt. The system EOL setting can be overwritten per individual zone with another EOL value if needed.

Go to the zone number settings and set the appropriate EOL resistor value, different from the one set under System > EOL Resistor Value > Normal Range according to the following table.

	Aritech	Guardall	Vanderbilt	Galaxy
Tamper (short)	0	0	0	0
Normal	4.7 k Ω	4.1 k Ω	4.7 k Ω	1.0 k Ω
Alarm	9.4 k Ω	8.2 k Ω	9.4 k Ω	2.0 k Ω
Fault	14.7 k Ω	12.3 k Ω	6.9 k Ω	—
Anti-mask	19.4 k Ω	16.4 k Ω	11.6 k Ω	—
Tamper (open)	∞	∞	∞	∞

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

Hardwired Shock Sensor

Hardwired shock sensors can be wired to the xGenConnect system. For each zone, a gross attack and pulse count level can be set under Zones > Shock Sensor Options.

Gross Attack Count

A gross attack measures big blows to the sensor. It records shocks on a scale of 1 to 9 (0 = disabled) where 1 is the most sensitive. An alarm is generated after a specified point on the scale. This prevents natural blows activating the alarm.

Pulse Count

A pulse attack measures vibrations to the sensor. It records the number of vibrations (1 to 32, 0 = disabled) over a 30 second period with 1 second intervals.

An alarm is generated when the vibrations add up to more than the specified number within any 30 second period. The 30 second period is a rolling time window. For example, if Pulse Count is set to 6, when the sixth vibration occurs, the timer rolls back 30 seconds and counts how many vibrations occurred during this time. If all 6 vibrations occurred during the 30 second window, an alarm is generated. Shock pulse counting prevents small repetitive attacks such as the window frame being attacked with a glasscutter.

Gross Attack and Pulse Count events will be logged in the panel event log. The Shock Gross Alarm will include the peak value which caused the alarm. This allows to adjust the Gross Attack Count value in case it is set to sensitive.

Hardwired shock sensors are supported with xGenConnect panels firmware version 11.xx and higher, and NXG-2xxN firmware version 0.11 or higher. Note that only the first 8 inputs of the NXG-216N zone expander support wired shock sensors. The last 8 inputs can be used as normal intrusion zones; however, no shock analyzation is available on these inputs.

Power Requirements

The xGenConnect intrusion panel family is designed to be used with a 16 VAC 1.5 A (NXG-4, NXG-8, NXG-8E), 20 VAC 1.5 A (NXG-9), 35 or 40 VA transformer which is included with xGenConnect 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 xGenConnect intrusion panel.

- For cable specifications, see “xGenConnect Specifications > xGenConnect Bus” on page 5.
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 xGenConnect 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.

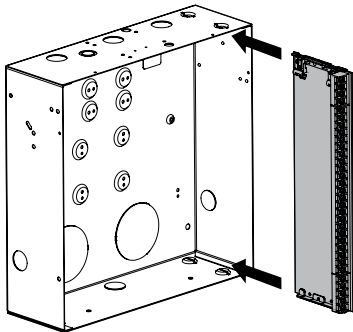
Shielding

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 NXG-8 panel / NX-003 housing

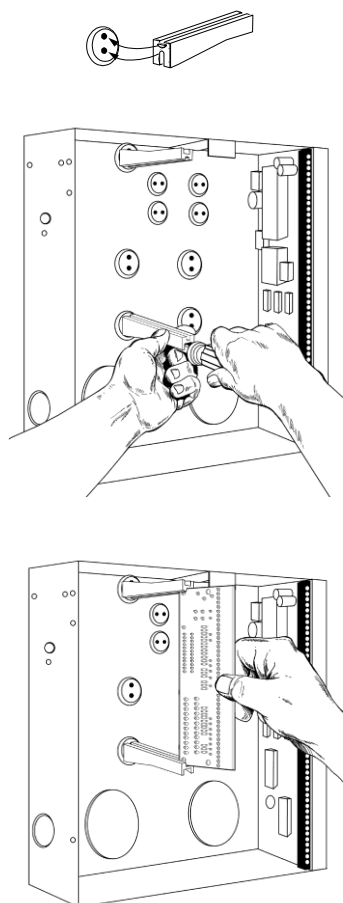


1. The xGenConnect should be located away from damp areas (e.g. bathrooms, kitchens), away from sources of heat, dust, or interference (e.g. air conditioners, washing machines, dryers, refrigerators) and away from external walls.

Due to safety reasons it is not allowed to wall-mount the device higher than 2 meters from the floor.

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 xGenConnect. 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.
5. When installing permanent, fixed wiring, insert an easily accessible, dedicated all-pole circuit breaker in the power distribution network.

Installing Legacy NX Modules



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

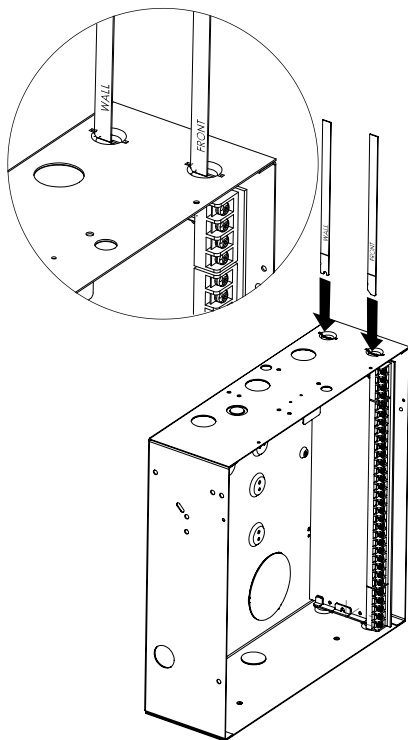
1. The black plastic PCB guides feature a groove to hold an expansion module. The end with the half-moon protrusion fits into the larger hole. The smaller hole is for the screw.
2. Place the first black plastic PCB guide in the top insertion point, groove facing downward. The half-moon protrusion will 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 (NXG-4 only)
- 4G antennas for Wi-Fi/cellular module
- Wi-Fi antennas for Wi-Fi/cellular module

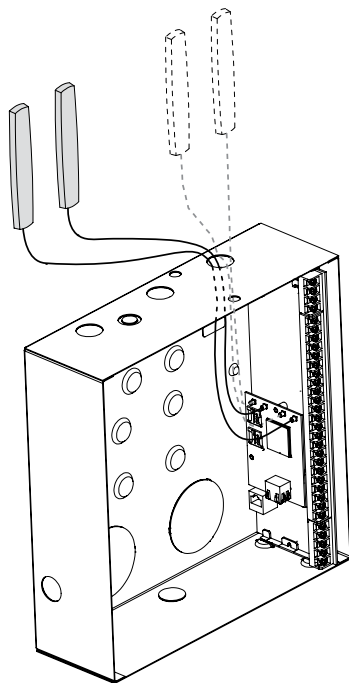
Wireless Sensor (NXG-4 only)



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.

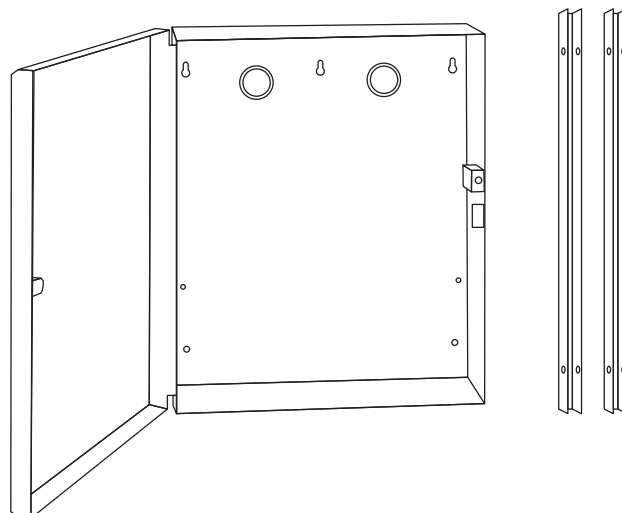
4G Cellular and Wi-Fi Router Module Antennas



If the optional 4G Cellular and Wi-Fi 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 4G and Wi-Fi wireless signals. This requires the installation of a second set of antennas to “DIV” on the 4G/Wi-Fi Router Module. The second set of antennas will perform best when separated from the MAIN antennas by at least 20 cm.

Installing NXG-8(E)-CB panel / NX-003-CB housing



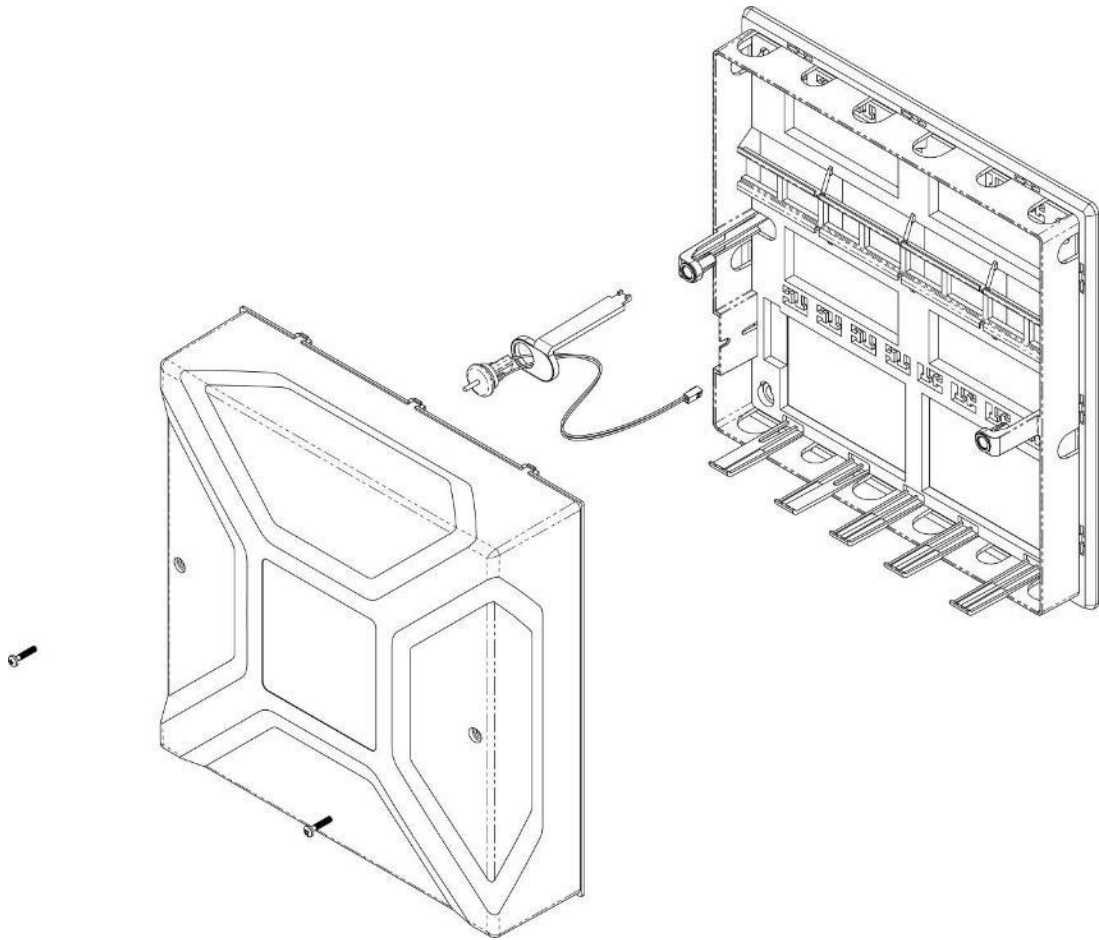
The large metal housing includes a tamper switch and a set of stand-offs and can be used for those installations where additional xGenConnect zone and/or output expanders are required or in case a larger backup battery is required.

Note: Using stand-offs is not compliant with EN 50131-1 and INCERT.

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

- Temperature range: -10 to $+55^{\circ}\text{C}$.
- Humidity range: Average 93% relative humidity, non-condensing

NXG-320 Plastic Enclosure



The NXG-320 plastic enclosure features a DIN rail for mounting xGen 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 $+55^{\circ}\text{C}$.
- Humidity range: Average 93% relative humidity, noncondensing

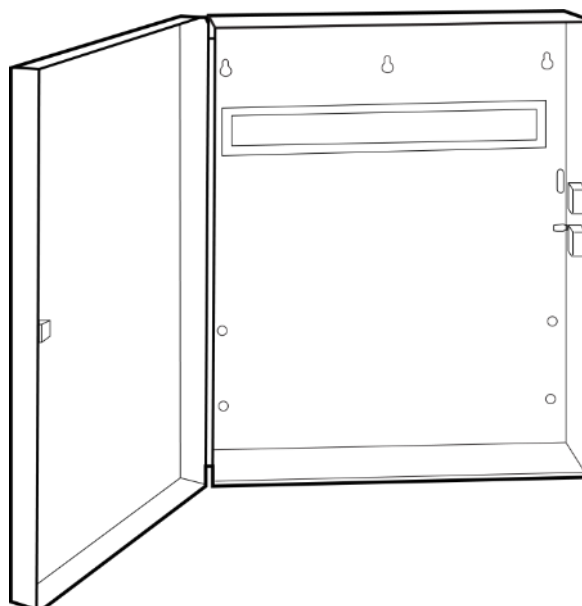
The lid can be removed by releasing the two screws using the supplied Allen key.

Note: The housing cover must be installed with the clips on top.

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 xGen module then remove from the DIN rail. Refer to module installation manual for further details.

NXG-003-G3 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-G3 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 $+55^{\circ}\text{C}$.
- 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.

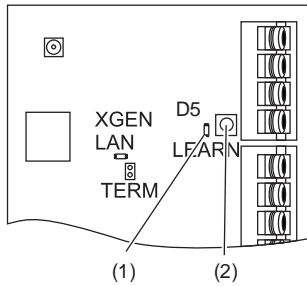
Enrolling Modules

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.



- (1) D5 LED located next to the LEARN button
 - (2) LEARN 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.

When installing multiple xGen devices/modules, it is recommended to use manual enroll to allow installer to control device numbering.

If auto-enroll does not complete for all connected devices:

1. Power cycle the panel/bus.
2. Connect batches of 4 devices at a time.
3. Push the LEARN button.
4. Confirm 4 additional devices enrolled.
5. Repeat for additional devices with batches of 4.

Enrollment can also be initiated:

- Using the NXG-18xx keypad: press Menu, Installer PIN, ENTER, go to Program > Devices > System Devices > Control > Enroll Function – 0 = Inactive – Automatic Enroll.
- Using the xGenConnect 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
 4. Tablet Keypads
 1. Name
 2. Serial Number
 3. Partition 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 xGenConnect 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 an NXG-18xx keypad.

Only users with an authorized user code (Level 2 user) will be allowed to use the xGenConnect 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-18xx 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 PIN 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.

Lock Out on 10 Invalid Card Attempts

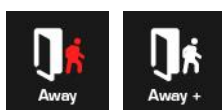
If an invalid card or tag is presented to the NXG-1832 / NXG-1833-EUR keypad 10 times, the keypad will ignore further attempts to read the card for the next 90 seconds. The card or tag may not be compatible with the system, not have been secured or added to a user, or the user card or tag may have been disabled.

Arm Your System with NXG-1820-EUR keypad

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.

Arm Your System with NXG-183x-EUR keypad

Arm Your System in Away Mode

Enter a valid PIN code to unlock the screen. Press the Arm Away button to arm your system in Away mode.

Enter your PIN and press Enter.

Note: In case the Quick Arm function is enabled, a PIN is not required to arm the system.

If your system has multi-partition control enabled, and the user has the Display Partition List option enabled, the Partition selection screen will be displayed.

Arm Your System in Stay Mode

Enter a valid PIN code to unlock the screen. Press the Arm Stay button to arm the system in Stay mode.

Using Up (2) and Down (8) buttons, select one of the following Stay Arming modes:

- Stay
- Stay Instant
- Stay Instant Night

Next, press Enter, enter your PIN, and then press Enter again.

Note: In case the Quick Arm function is enabled, a PIN is not required to arm the system in Stay mode.

If your system has multi-partition control enabled, and the user has the Display Partition List option enabled, the Partition selection screen will be displayed.

Disarm Partitions with NXG-1820-EUR keypad

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.

Disarm Partitions with NXG-183x-EUR keypad

Enter a valid PIN code to unlock the screen.

Typically, the buzzer will sound (continuous tone) announcing the entry delay.

Press the Disarm button followed by a valid PIN code to disarm your system.

If your system has multi-partition control enabled, and the user has the Display Partition List option enabled, the Partition selection screen 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/Disarm Your System with Simplified Arm-Disarm mode enabled

The NXG-183x-EUR keypad can be configured to arm and disarm the system in a simplified way. If the Simplified arm-disarm mode is enabled, pressing any of the numeric keys automatically starts entering user PIN.

Note: This mode is available for 4- or 6-digit PINs only.

You can enter your PIN (4 or 6 digits, depending on the system settings) without pressing the Enter key, or arm-disarm buttons.

If the appropriate partitions are armed or in alarm, entering a valid PIN code will disarm the system. If the partitions are disarmed, entering a valid PIN code will arm these in the Away mode.

Notes

- It is recommended (but not required) to disable the Idle PIN and Display partition list options to take all advantages of Simplified arm-disarm mode.
- If the Display partition list option is enabled, it is not required in the Simplified arm-disarm mode to press Enter after selecting the partitions to operate. If any partition is selected, the selection is automatically confirmed 5 seconds after the last key is pressed.
- The screensaver is not deactivated automatically. If the screensaver is active, press any button first to deactivate the screensaver, and then start entering your PIN.
- The operation to perform in Simplified arm-disarm mode is chosen based on the state of all partitions that the user has the permission to disarm (relevant only if custom users are configured).
- If the Simplified arm-disarm mode is enabled and any partition is armed, you cannot access the keypad menu by pressing the Enter key.

Example:

User PIN is 1234, Simplified arm-disarm mode is set to 4-digit mode, Idle PIN is disabled.

To arm or disarm the partitions, follow these steps:

1. If the screensaver is active, press any button to deactivate it.
2. Press 1, 2, 3, 4.

System arms or disarms, depending on its current state.

Arm/Disarm Your System with NXG-1832 / NXG-1833-EUR keypad and user card

The system can be armed/disarmed by presenting a card or tag to the NXG-1832 / NXG-1833-EUR keypads, which are equipped with a built-in Mifare card reader. The following configuration steps must be taken to allow arming and disarming via a user card or tag:

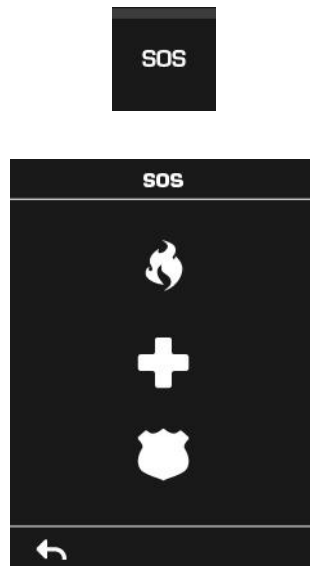
- A card must be properly secured, assigned to a User, and enabled. See “Configuring cards or tags using the NXG-1832 / NXG-1833-EUR keypads” on page 160 for details.
- The user must have permissions to execute the desired operation (arming away, arming stay, disarming).
- The keypad must be configured to trigger the desired action when a card or tag is presented. There are three card beep functions available (single, double, and triple beeps), which can be configured separately for desired actions. See *NXG-183x-EUR Series Keypad User Manual* for details.

In order to trigger the configured function, the card must be presented to the keypad, preferably close to the center of the LCD screen, and the keypad must be either in screensaver mode, or showing the main screen.

Note: It is possible to configure the same card function for both arm and disarm operation. If the partition is armed or in alarm, presenting the card will disarm it. If the partition is disarmed, presenting the card will arm the partition. See *xGenConnect Door Access Programming Guide* for more details.

Activate SOS Feature (NXG-1820-EUR only)

Touch the SOS button to display the SOS feature:

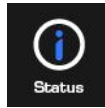


On this screen touch and hold the appropriate button for 2 seconds to activate Manual Fire Alarm, Manual Medical Alarm, or Manual Panic Alarm.

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.

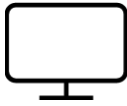
If silent alarm is enabled, then the keypad will not display any signs that the panic button was pressed.

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 xGenConnect 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-18xx keypad offers a programming menu allowing full system configuration. Refer to the appropriate keypad installation manual. *xGen 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 an 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.

WiFi Router

xGenConnect Router can open a WiFi Access Point to allow an installer to connect a mobile phone / tablet / laptop to the router and program the panel using a web browser.

Quick Connect using an NXG-1820 / NXG-1830 keypad:

1. Unlock the keypad and access the Programming menu.
2. Navigate to Advanced > Communicator > IP Configuration > IP Options.
3. Navigate to Enable WiFi Internal Access Point.
4. Toggle the option on.
5. Exit menu.

On your mobile phone / tablet / laptop:

1. Navigate to WiFi settings.
2. Connect to NXG_x_xx_EU_serial number. The password is identical to the SSID shown.
3. Open a web browser.
4. Navigate to 192.168.33.1.
5. Login to the panel.
6. Change the default password.
7. Log out.
8. Reconnect to the SSID with the new password.
9. Program required settings.

The access point will remain until the installer turns it off.

Alternatively, to manually create the WiFi Internal Access Point:

1. Default the panel.
2. Unlock the keypad and access the Programming menu.
3. Navigate to Advanced > Communicator > IP Configuration > IP Options.
4. Navigate to WiFi Internal Access Point SSID.
5. Program a valid SSID name.
6. Navigate to WiFi Internal Access Point Password.
7. Program a valid WiFi password.
8. Navigate to Enable WiFi Internal Access Point.
9. Toggle the option on.
10. Exit menu.

Method 1: DLX900 Management Software

DLX900 is an ideal tool for programming xGenConnect 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)

Connect to xGenConnect using DLX900 on LAN

1. Turn on power to your system
2. Connect an Ethernet cable to the J13 Ethernet port on the xGenConnect and wait 10 seconds for the local router to assign the xGenConnect 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.

Connect to xGenConnect using DLX900 on UltraSync

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

Note: The system needs to be provisioned in UltraSync.

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. Select Connection method: UltraSync.
6. Click Save.
7. Click Connect via TCP/IP.
8. Click Read All.

Method 2: Web Server

xGenConnect 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 xGenConnect Web Server over LAN

1. Turn on power to your system
2. Connect an Ethernet cable to the J13 Ethernet port on the xGenConnect and wait 10 seconds for the local router to assign the xGenConnect 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 xGenConnect login screen should appear. Some browsers may require you to enter http://

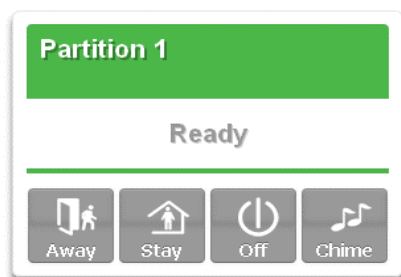
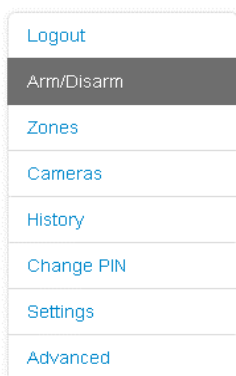


Sign In:
Enter Your Name:

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

Note: On EN Grade 3 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.

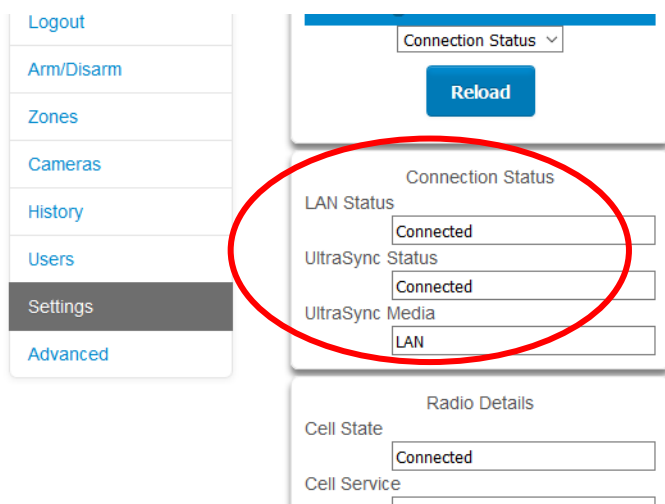
- Check your router settings and try again.
- On an NXG-1820 touchscreen keypad press Menu, PIN, ENTER, go to Installer > Communicator > IP Configuration > IP Options. “Enable DHCP” should be ticked, “Disable Web Pages on LAN” should be unticked.

Check LAN Connection to UltraSync

UltraSync is a cloud-based service that allows remote management and remote access to a xGenConnect system if enabled. This includes secure connections between the UltraSync+ app, xGenConnect, 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 xGenConnect via 4G Cellular and Wi-Fi Router Module

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

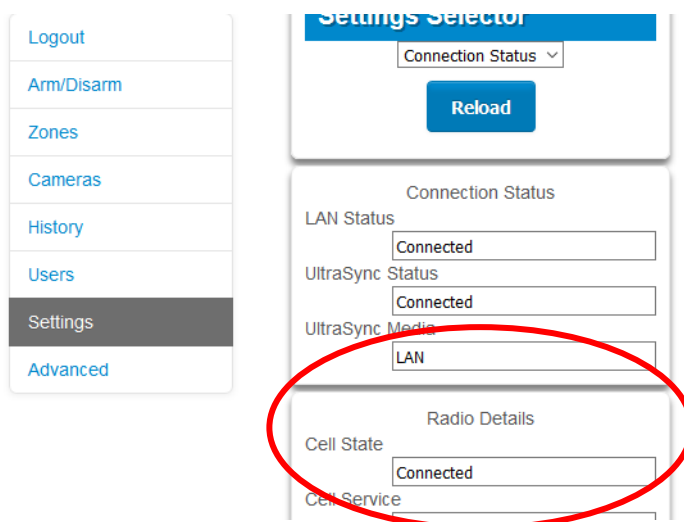
An optional 4G Cellular and Wi-Fi Router Module provides dual path reporting over Wi-Fi/Ethernet and 4G. If the primary path (Wi-Fi/Ethernet) is not working, the module will switch to 4G back-up reporting path to the central monitoring station.

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 xGenConnect panel, it will automatically register on available mobile network(s). Refer to the 4G Cellular and Wi-Fi 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.



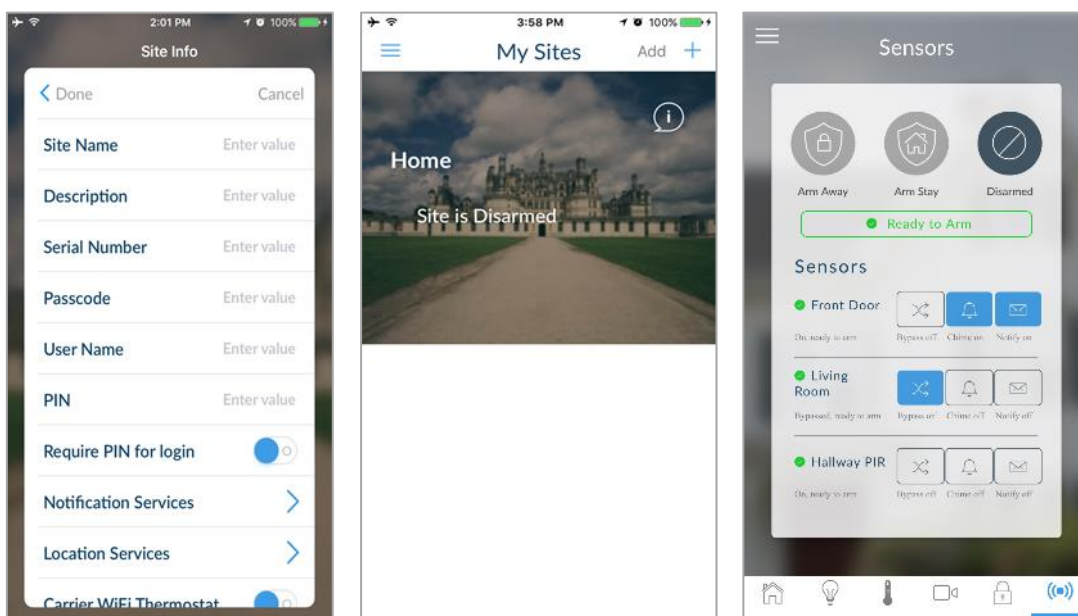
If it does not, check the 4G connection:

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 –105 to –51.
4. Check module is correctly installed.
5. Check that 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 xGenConnect system is connected to your network and UltraSync. It is now ready to be programmed. Refer to “Programming with Web Pages” on page 52.

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 xGenConnect 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 xGenConnect via UltraSync+ app

UltraSync+ is an app that allows you to control your xGenConnect system from an Apple® iPhone/iPad, or Google Android device. First set up the xGenConnect 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 xGenConnect circuit board. Alternatively log in to xGenConnect 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 xGenConnect 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”

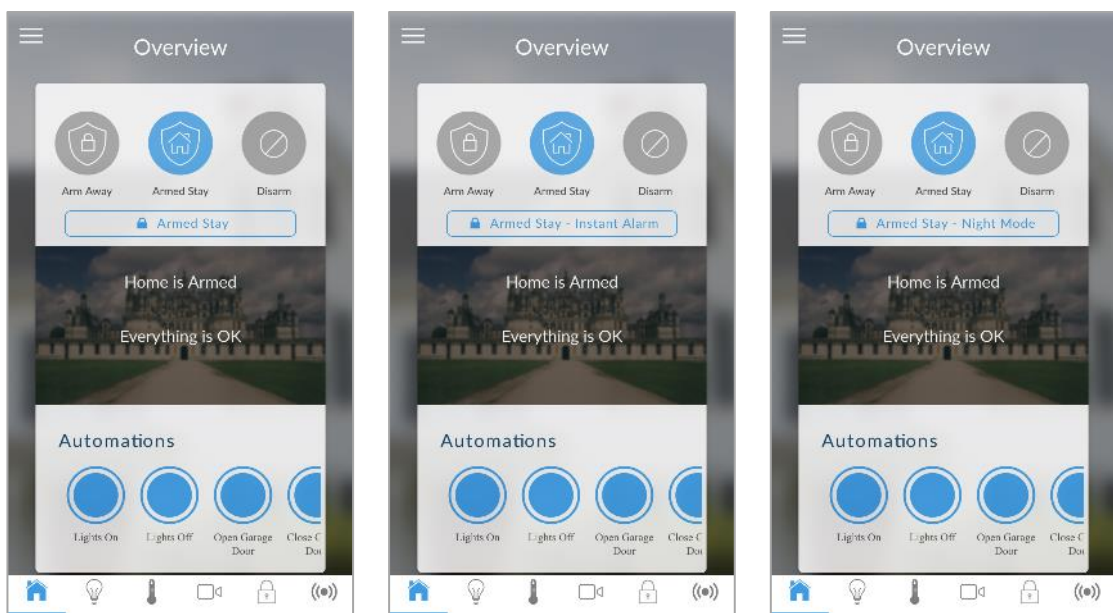
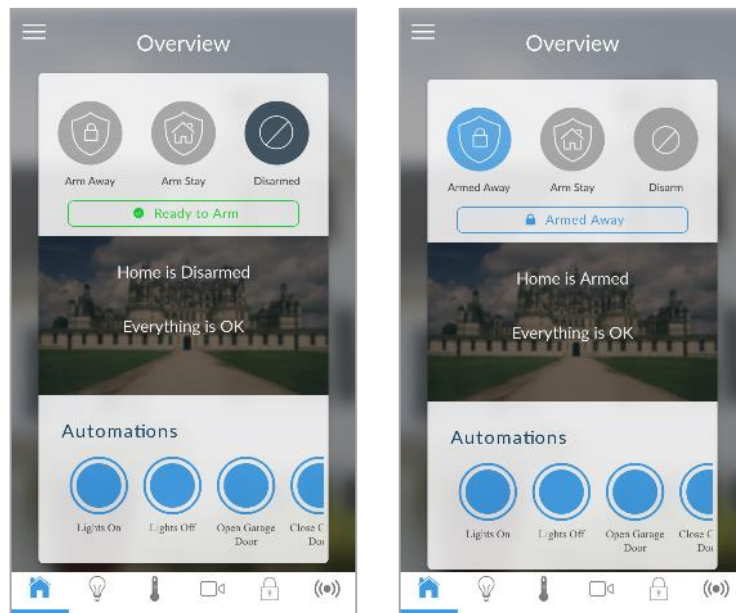
and “1”. You may also use any other valid user account. Only menus a user has access to will be displayed.

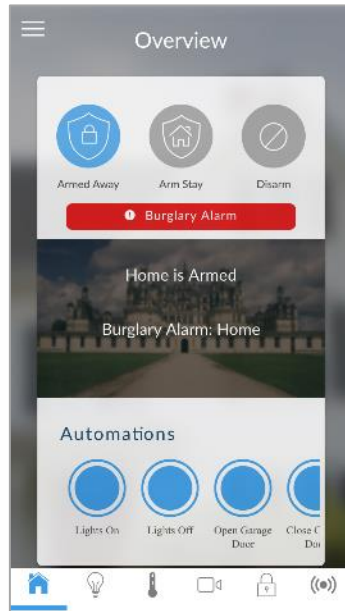
Note: EN 50131 Grade 3 default codes are 971300, 123400.

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 xGenConnect.

Using the App

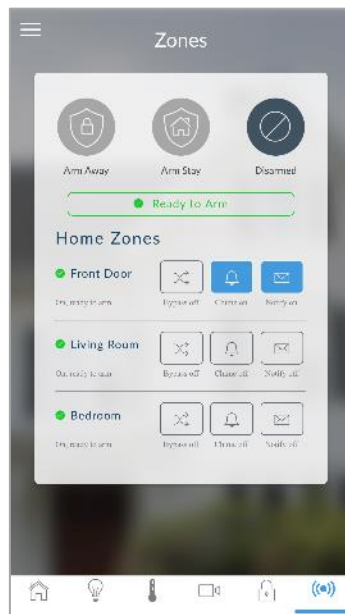
The first screen that will appear once you connect is the Overview screen. This will display the status of your system and allows you to arm or disarm partitions by touching Arm Away, Arm Stay, or Disarm. It also allows you to activate programmed automation scenes.





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.

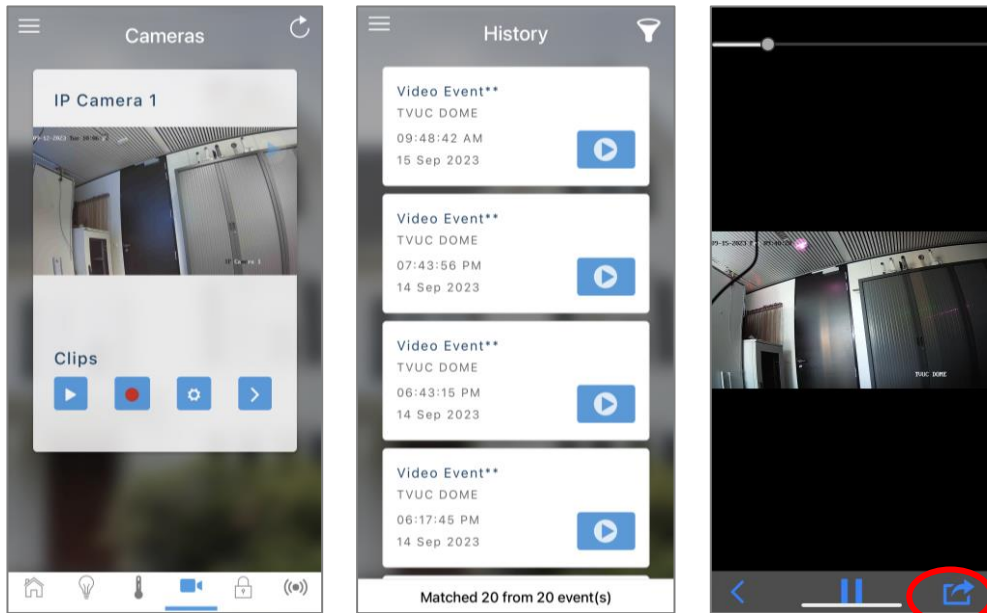



Touch the Camera icon to view cameras connected to your system.

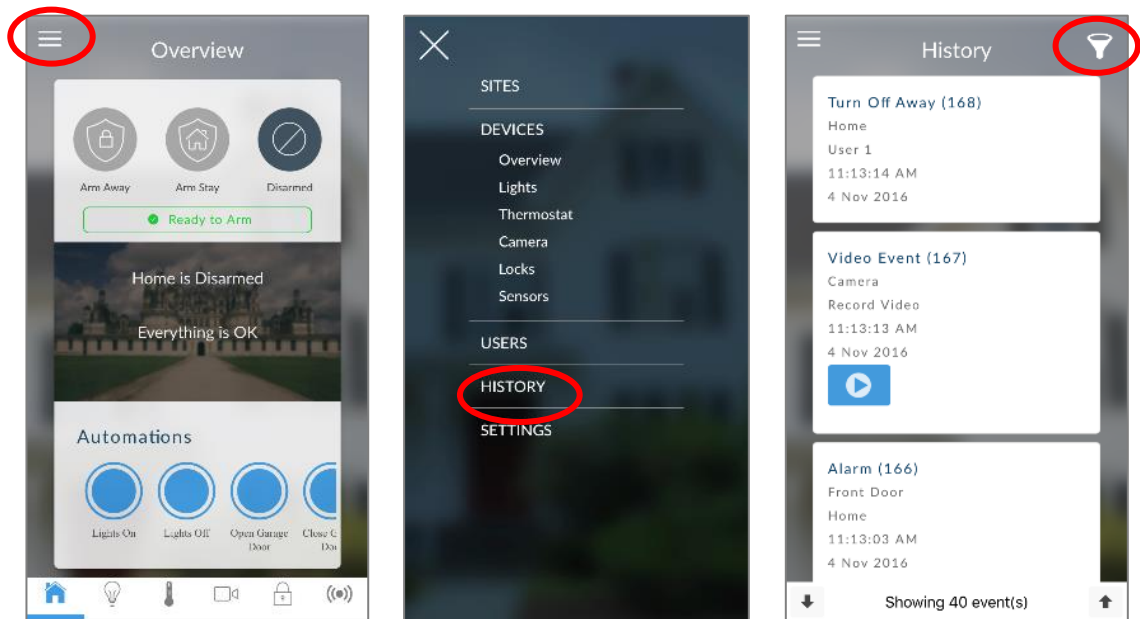
Live snapshots from each camera will be shown.

- Touch the snapshot to open the live stream in full screen. Touch the screen then Back to return to the Camera screen.

- Touch the Play button under each camera to show the history log with all latest recorded clips from that camera. Press the event to watch the recorded clip. Touch the Share button to save or forward the clip.
- Touch the Record button to request that camera to record a short clip which can be retrieved afterwards.




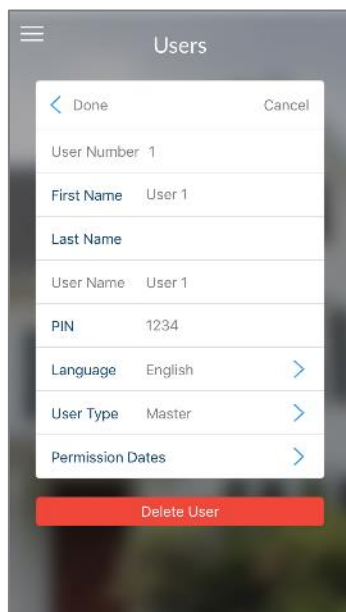
Video clips can also be accessed from the History screen. Touch Menu , HISTORY, then change Selected Events to Video. Touch “Press to Play Video” to retrieve the clip from the camera. Once downloaded, you can save or forward the clip.



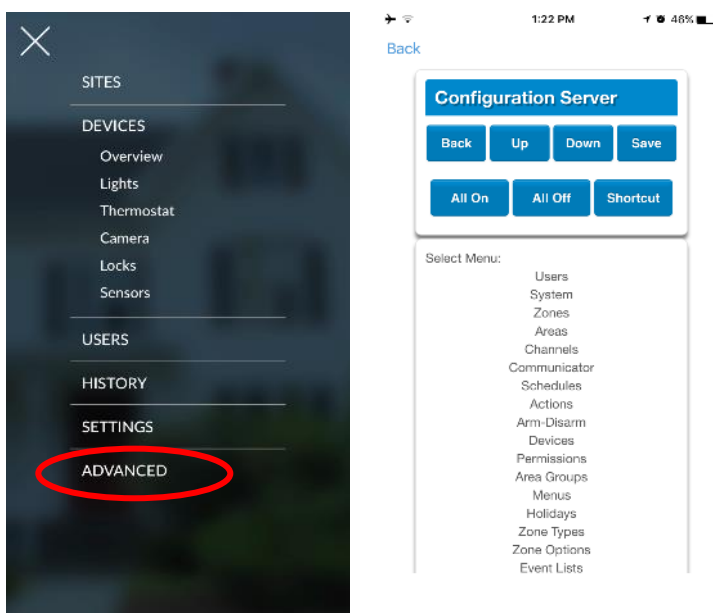
This History screen displays the event log of the xGenConnect, recording important events and allowing authorized users the ability to audit the system. Changing the Selected Events to Alarms will display the filtered Mandatory Event Log.

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 xGenConnect. Refer to *xGen 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 xGenConnect.

- 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 – eu1.ultraconnect.com:443
 - Ethernet Server 2 – eu1.zerowire.com:443
 - Wireless Server 1 – eu1w.ultraconnect.com:8081
 - Wireless Server 2 – eu1w.zerowire.com:8081
- Power cycle connected equipment including xGenConnect 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 4: Advanced Menu Tree” on page 156.
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 no access to xGenConnect programming menus.

Programming with Web Pages

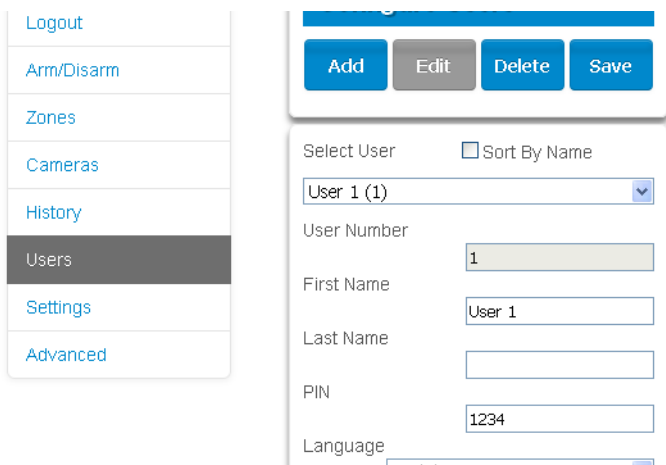
Most commonly used features can be programmed from the xGenConnect Web Server > Settings menu. The same menus are displayed from the UltraSync+ app by clicking Menu > Settings.

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 3 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 xGenConnect Web Server and UltraSync+ app.



- **Web Access Passcode.** This provides access to the xGenConnect 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:

The screenshot shows the 'Settings Selector' interface. On the left is a sidebar menu with options: Logout, Arm/Disarm, Zones, Cameras, History, Users, Settings (highlighted), and Advanced. The main content area is titled 'Settings Selector' and has a dropdown menu set to 'Network' and a 'Save' button. Below this are three sections: 'LAN configuration', 'Remote Access PINS', and 'Options'. The 'Remote Access PINS' section has a red circle around the 'Web Access Passcode' and 'Download Access Code' fields, both containing '00000000'. The 'Options' section has several checkboxes: 'Enable Ping' (checked), 'Enable UltraSync' (checked), 'Monitor LAN' (unchecked), 'Always Allow DLX900' (checked), and 'Enable Web Program' (checked).

LAN configuration				
IP Host Name	<input type="text"/>			
Enable DHCP	<input checked="" type="checkbox"/>			
IP Address	192	168	1	222
Gateway	192	168	1	1
Subnet	255	255	255	0
Primary DNS	192	168	1	1
Secondary DNS	0	0	0	0

Remote Access PINS	
Web Access Passcode	<input type="text" value="00000000"/>
Download Access Code	<input type="text" value="00000000"/>
Automation User Name	<input type="text"/>
Automation PIN	<input type="text" value="00000000"/>

Options	
Enable Ping	<input checked="" type="checkbox"/>
Enable UltraSync	<input checked="" type="checkbox"/>
Monitor LAN	<input type="checkbox"/>
Always Allow DLX900	<input checked="" type="checkbox"/>
Enable Web Program	<input checked="" type="checkbox"/>

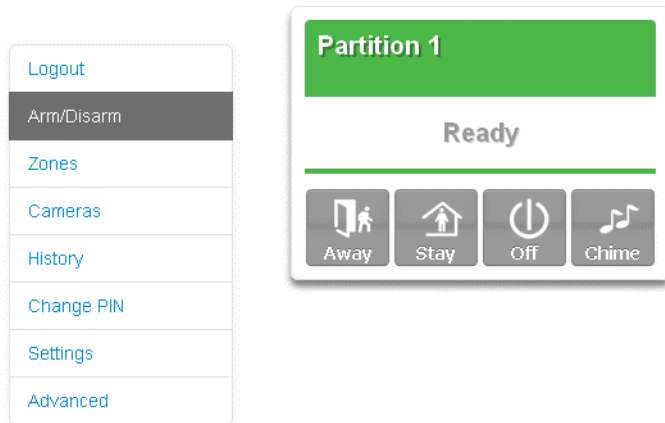
Learning Wireless Zones

1. Log in to the Web Server.

The screenshot shows the 'Sign in' page. It has a title 'Sign in' and two input fields: 'Enter your username:' with the value 'installer' and 'Enter your password:' with four dots. Below the fields is a blue 'Sign In' button.

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

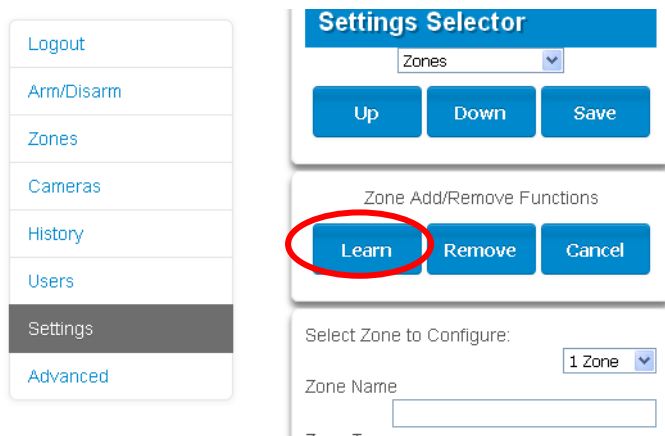
3. You should now see a screen similar to the one shown below.



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 xGenConnect.

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
19	Fire Reporting Only	Fire	Silent	N	N	Y	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
19	Fire Reporting Only	Fire	Silent	N	N	Y	N	N	N

Zone Options Table

Default Number	Default Name	Zone Options													Zone Reporting	Zone Contact Options						
		Bypassed Stay Mode	Forced Arm Enabled	Bypass	Cross Zone	EOL	Automatic Zone Test	Night Mode	Zone Inactivity Test	Follow Any Armed Partition	Final Set Door	Single EOL	Delayed in Stay	Fire Reporting Only	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 Partition	Final Set Door	Single EOL	Delayed in Stay	Fire Reporting Only	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	Bypass Stay	Y	Y	Y		Y																132:BA
20	Request-to-Exit					Y									Y	Y	Y	Y	Y			130:BA
21	Fire Reporting Only											Y		Y	Y	Y	Y	Y	Y			110: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

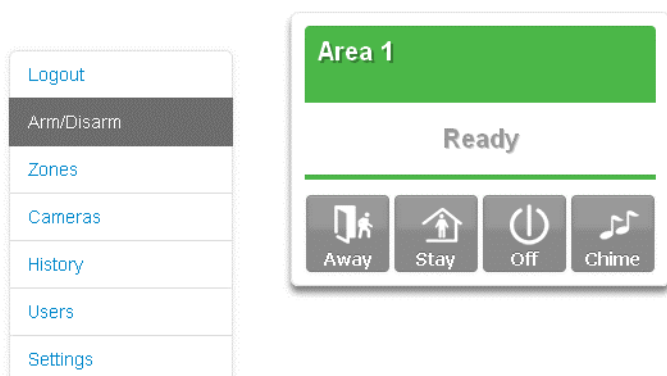
The xGenConnect system supports up to 256 users. Each user is assigned a PIN code and a user number. This allows them to interact with the system.

1. Log in to the Web Server.

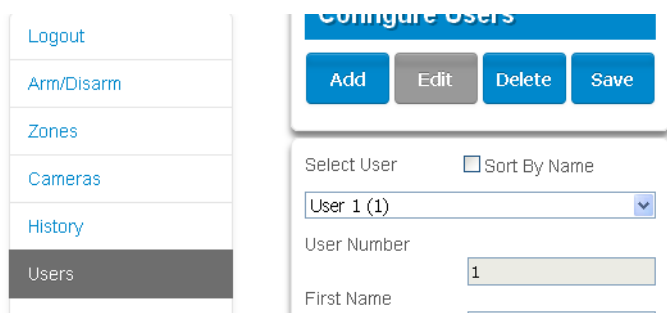
Sign In:

Enter Your Name:

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.

Advanced user settings

In case more advanced user operation is required, following options can be enabled or changed:

- **Partition Group:** Select to which partition or group of partitions, the user needs access to. By default each user has access to all partitions.

- **Door Group:** Select which door or group of doors, the user has access to. By default each user has access to all doors.
- **Display Partition List:** Applies to arm and disarming operations from the keypad. When enabled, entering a PIN to arm or disarm on the keypad will list all available partitions on which the user can then individually arm or disarm. When disabled, the system will always arm or disarm all partitions.
- **Partition Type Override:** Applies to non-standard partition types Time Disarm, Man Down, Guard Tour. When set, disables the feature for the user.
- **Disable Zone Bypass:** User cannot bypass zones
- **Disable Arm Disarm Reports:** Arm or disarm events from the user will not be reported
- **Disable App Scene Buttons:** When enabled, all scene buttons on the home screen of the UltraSync+ app will be hidden for the user.
- **Start Date:** The first date when this user can interact with the system. Future start dates can also be set here. The user will only be able to interact with the system between the start date and end date.
- **End Date:** The last date when this user can interact with the system. Future end dates can also be set here. The user will only be able to interact with the system between the start date and end date.

Adding Cards to Users

The xGenConnect system supports dedicated Mifare user cards and tags, which can be added to users.

The card or tag can be presented to the Mifare reader available on the keypad models NXG-1832 / NXG-1833-EUR and may trigger the functions as configured in the keypad options. See *NXG-183x-EUR Series Keypad User Manual* for details.

The card or tag can be used to arm and disarm the system, enter the keypad menu, execute system logic (Action or Scene), unlock doors, or any combination of these.

Every user may have only one card assigned. A single card cannot be assigned to multiple users.

The card can be added to existing users only. Create users before adding cards, if necessary. See “Adding a User” on page 57 for details.

To make the card usable in the system:

- **Assign a card to the user.** This operation can be done by entering the card ID.
- **Secure the card.** This assigns a system-specific security key to the card. The card must be presented to the reader to perform this operation.

It is recommended to perform the initial card configuration using the NXG-1832 / NXG-1833-EUR keypad. Adding and securing a card or tag will be done at the same when going to Add/Edit User Card in the user menu.

The keypad menu also allows you to add cards to users sequentially, which simplifies the configuration process. See *NXG-183x-EUR Series Keypad User Manual* for more details.

Alternatively, use the panel web page to configure cards.

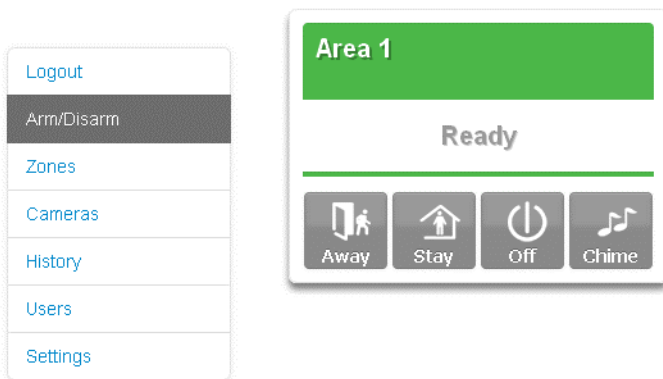
1. Log in to the Web Server.



Sign In:
Enter Your Name: _____

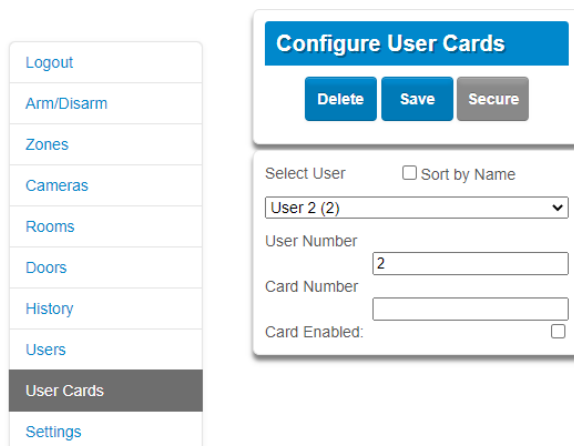
2. Enter your username and password. A master code is required to add cards. By default the user name is “User 1” (with a space between “User” and “1”), and the password is “1234”. Next, click Sign In.

3. The Arm/Disarm screen will appear:



The image shows two parts of the web interface. On the left is a vertical menu with options: Logout, Arm/Disarm (highlighted), Zones, Cameras, History, Users, and Settings. On the right is the 'Area 1' screen, which is 'Ready'. It features four buttons: 'Away' (with a person icon), 'Stay' (with a house icon), 'Off' (with a power icon), and 'Chime' (with a musical note icon).

4. Click User Cards.



The image shows two parts of the web interface. On the left is a vertical menu with options: Logout, Arm/Disarm, Zones, Cameras, Rooms, Doors, History, Users, User Cards (highlighted), and Settings. On the right is the 'Configure User Cards' form. It has buttons for 'Delete', 'Save', and 'Secure'. Below these are fields for 'Select User' (a dropdown menu showing 'User 2 (2)'), 'Sort by Name' (checkbox), 'User Number' (input field with '2'), 'Card Number' (input field), and 'Card Enabled:' (checkbox).

5. Select a user to assign the card.
6. Type the card number (eight digits) as printed on the card. The card number cannot be reused for more than one user.
7. Check the Card Enabled parameter.
8. Press Save button.

The card is now configured for the user. If the card has already been used for the other user, the relevant error message appears.

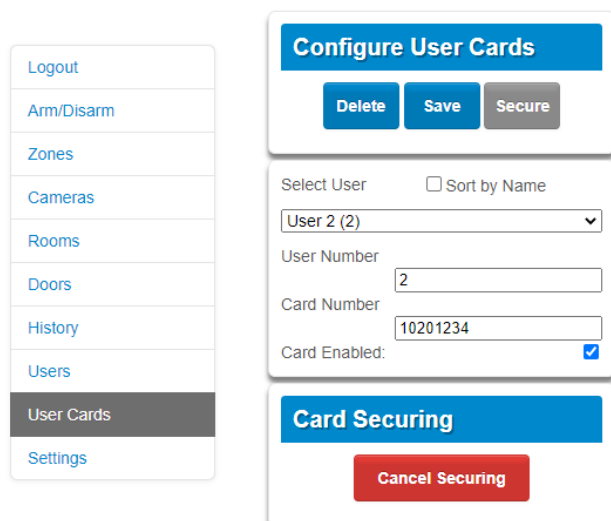
If the card had been secured before (for example, using the keypad menu), the card is ready to use.

Otherwise, if the card is new, or the system card security key has been changed in the panel, perform the following steps to secure the card:

1. Press the Secure button. The button is automatically enabled after successful saving of card data.

Note: Card Enable parameter must be checked.

Card securing process will start and an additional button will appear to allow cancelling the process of securing the card or tag if needed.



2. Present the card or tag to any NXG-1832 / NXG-1833-EUR keypad in the system. The keypad must display the main screen (screen saver is not active).

Keep the card or tag close to the keypad for a few seconds until the relevant message appears both on the keypad screen (“Card Secured, number”) and on the web page (“Securing Successful”). The keypad also generates a two-tone sound to confirm the card is successfully secured.

The card is ready for use.

Note: You can also assign cards to users using the NXG-1832 / NXG-1833-EUR keypad menus which may be more convenient as the card has to be presented to keypad reader anyway. Adding a card or tag to an existing user via the keypad menu will automatically secure the card, if not already the case. The keypad User Card menu also allows you to sequentially add and secure multiple cards to users. See *NXG-183x-EUR Series Keypad User Manual* for details.

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 Partition 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. Partition 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 Partition Group. The arm and disarm buttons on the keyfob will arm/disarm all partitions in the Partition 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 Partition Groups. Each one has a set of selected partitions.
- e. Modify the Permission and assign the appropriate Partition Group to the Control Groups displayed. For example, the Permission can Away Arm both Partition 1 and 2, but Disarm only Partition 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 xGenConnect 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 xGenConnect 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.

AB Alarm Confirmation

The partition option AB alarm verification enables a set of various options in relation to alarm verification. When enabled, the first alarm is reported as a standard burglar alarm (A-alarm, or unverified alarm). A second zone has to raise an alarm within a certain period to report a confirmed alarm (B-alarm, or verified alarm), provided the first alarm in the partition did not occur in an entry/exit zone.

The AB verification time allows you to configure the maximum delay between A and B alarms, and is set to 30 minutes by default. If the second alarm happens within this time, the alarm is reported as a verified alarm (B-alarm). When the AB time has expired, any next alarm is another unverified alarm (A-alarm).

The System Confirm option defines if the AB alarm confirmation works in separate partitions only, or allows for system-wide validity. If this option is enabled, an A-alarm in one partition can be confirmed by a B-alarm in another partition. If disabled, the A-alarm can only be confirmed by a B-alarm in the same partition.

The EE Confirm option configures the AB alarm confirmation during entry time. If the option is enabled, alarm confirmation is suspended during entry time. All alarms during the entry time are A-alarms. When the entry time has expired, alarm confirmation is active again. However, entry/exit zones cannot generate B-alarms.

If the TA Confirm option is enabled, a tamper alarm (TA) can report a B-alarm for burglary alarm (BA), and vice versa.

AB alarm verification can be enabled per partition.

Country

Out of the box, the xGenConnect panel will contain the EMEA default configuration. Selecting another country will make the panel load different panel settings. Loading country defaults will take about 30 seconds to complete, and during this time the keypads will be offline, but will turn online again when the process is complete.

Notes

- The country defaults contain control panel settings only.
- Loading country defaults will not remove enrolled devices.

Performing a panel factory default will make the panel turn back to the factory settings with EMEA defaults.

Programming Doors

The xGenConnect panel supports door control functionality which allows to control and monitor up to 16 doors depending on the panel model. **Note:** See “xGenConnect Specifications” on page 2 for maximum doors per system.

Basic options and timers related to door configuration are shown in the panel Settings menu. In case more advanced programming setup is required, all programming features are accessible from the panel advanced settings. Detailed description of all door-related parameters is available in *xGenConnect Reference Guide*.

Setting Menu > Door Settings

- **Door Name:** Program up to a 32-character custom name for the selected door. This name appears in every list in the system, including keypad controlling doors.
- **Door Type:** Select this submenu to enable the door with the desired combination of Door Input Zone Shunting (Shunt), Forced Door Monitoring (Forced), Door Left Open (DLO) monitoring.
- **Door Inputs:** Choose desired system zone inputs for the door zone, and the Request-to-Exit (RTE) zone. The door zone input can be part of the alarm system and can have any appropriate zone type. The RTE zone should not be used by the alarm system except for exit requesting buttons.

Note: Door zone should not be configured if Door type is Lock or Disabled. All other door types require Door zone to be properly set.

Both Door zone and Request-to-Exit can be wired to the NXG-1832 / NXG-1833-EUR keypad Input, using a special triple-EOL resistor configuration (see the keypad Installation Sheet for details).

In this case, the following parameters must be set properly:

- panel Door Zone parameter must be set to a particular desired zone number (for example, 1).
 - panel RTE Zone parameter must be set to the next consecutive zone number (for example, 2).
 - keypad parameter Zone must be set to the same value as Door Zone (for example, 1)
 - keypad parameter RTE as Next Zone must be enabled
 - Timers: This submenu contains all the timers associated with a door. Access this menu to adjust times if the application needs times other than the default time.
 - Door Unlock Time: The number of seconds the door remains unlocked when a user presents credentials to access the door. The user can open the door during this time.
 - Door Zone Shunt Time: The time the door can remain open before the zone creates an alarm.
 - Door Zone Warning Time: The time remaining in the shunt timer when a door warning condition becomes active. Keypad sounders and relay outputs can then be programmed to sound a sounder to notify the user of a pending shunt expiration.
 - Door Options: Use the option to select the desired behaviour of the door.
 - Door Forced Reporting: When the selected Door type supports the Forced Door feature, ticking this box causes the Forced Door Alarm to be reported off premises.
 - Door Left Open Reporting: When the Door Type selected supports the DLO feature, ticking this box causes the DLO Alarm to be reported off premises.
 - Log Door Access: Ticking this box will cause a logging event when the door is unlocked. This event identifies the Door and the user that opened it.
 - Mag Lock: Enable the option to prevent the lock from engaging until the door is closed for the Pre-Lock time. If enabled, the door will remain unlocked until it is closed.
- Note:** Door relay may be wired either to a dedicated Door Lock output on NXG-1832 / NXG-1833-EUR keypad, or to any output in the system (on the panel or on an output expander).
- The door relay wired to the NXG-1832 / NXG-1833-EUR keypad
- Set the Door parameter in keypad's programming settings, to the desired door number. The dedicated keypad output would follow the Unlock state of the selected door.

- Door relay wired to a system output

Configure an Action as follows:

- Function: Follow
- Event1: Category: Doors
- Event1: Type: Door Unlocked
- Event1: Start/End Range: door numbers.
- Events2,3,4: Type: disabled

Configure the output and assign it with this Action.

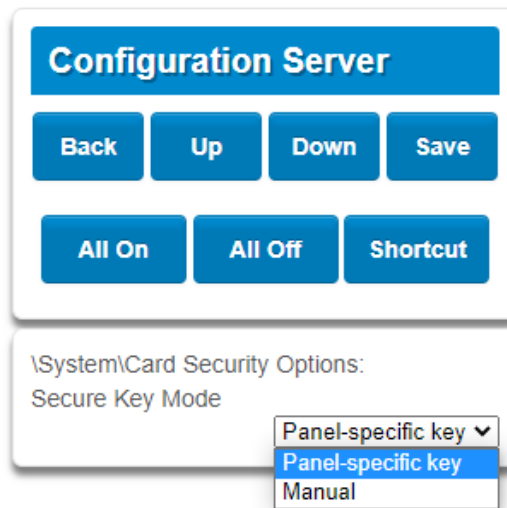
Programming Card Security

If the system contains keypads NXG-1832-EUR or NXG-1833-EUR, the dedicated Mifare cards can be used to authenticate and trigger user-defined operations in system.

The card security mode is configured by the two system parameters:

- System > Card Security Options > Secure Key Mode
- System > Card Security Options > Secure Key [8-40 characters]

There are two available card security modes, selectable by Secure Key Mode parameter:



- Panel-specific key. Every panel has a unique, pre-programmed card security key. Cards used in one system cannot be used in another system. *This is a default and recommended security mode, which provides the best security.* The second parameter ("Secure key" [8-40 characters]) is not used.
- Manual. Card security key can be programmed by the installer in the option Secure Key [8-40 characters]. The key must be entered as a text, 8 to 40 characters long.

This mode allows for using the same cards in two or more systems, provided that the same card encryption key is configured to all these systems.

The security key can be changed but *cannot* be read-out of the configured panel.

Notes

- Manual mode should be used only if same cards must be used in multiple systems. Otherwise, it is recommended to keep the default settings.
- The Cards used in the system must be secured before use. Securing is a process of applying the selected security mode and key to the cards. The operation can be performed either before, or along with the attaching Cards to Users. Securing must be performed by Master User. See relevant chapter on User Card configuration.

Securing process requires the card to be presented to the card reader during the operation, so it is recommended to perform this operation using menus of NXG-183x keypad. Keypad menus allows also a sequential adding and securing multiple cards to multiple users, which simplifies the configuration process.

Programming Cameras

Adding Cameras Using the New Device Setup (preferred)

The UltraSync+ app has a built-in guide to help an installer add cameras. It is required that the UltraSync cameras are connected to the same network as the xGenConnect.

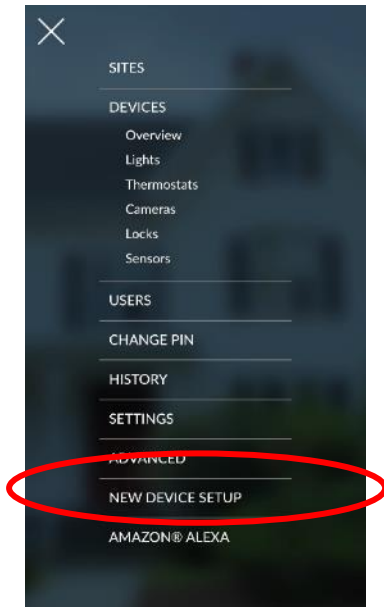
Before adding cameras:

- The xGenConnect 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 Wi-Fi 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 using the panel installer login credentials.

4. Click Menu – New Device Setup



5. Follow the application on-screen prompts to do the following:

- Connect your mobile device to the camera.
- Set up a camera user name and password.
- Sync the camera to the panel.
- Change camera names and view camera status.

The camera password should meet the following requirements:

- 8 to 16 characters long
- At least one uppercase and one lowercase letters
- At least one number
- At least one special character (- , . * & @ / \$? _ space)

Adding Cameras using the Camera 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

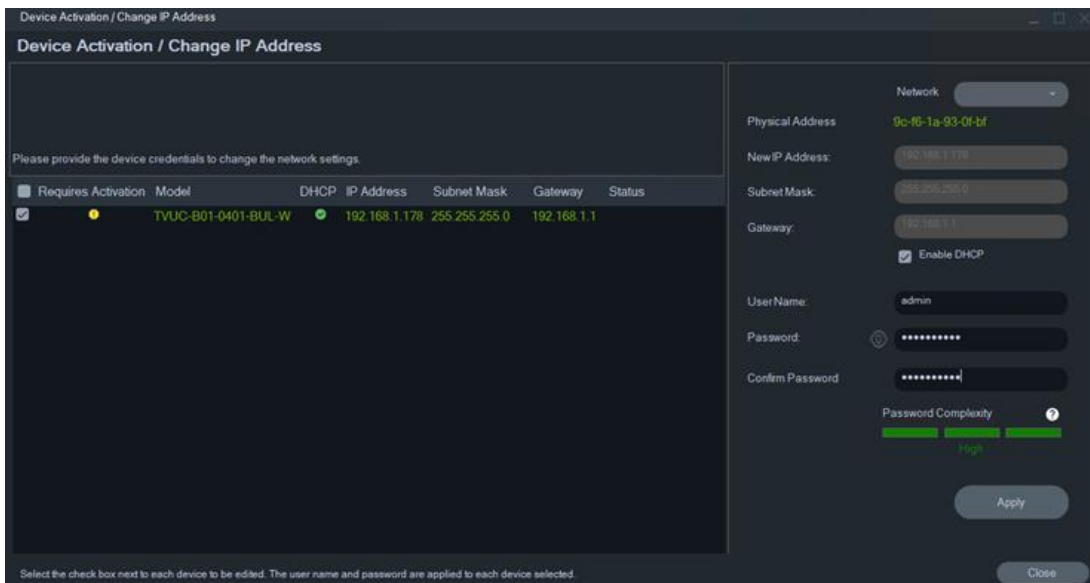
Only perform these steps if you are familiar with the operation of the camera. Incorrect settings may cause the camera to perform poorly. Default the camera to factory settings if this occurs.

Adding camera to the local LAN network:

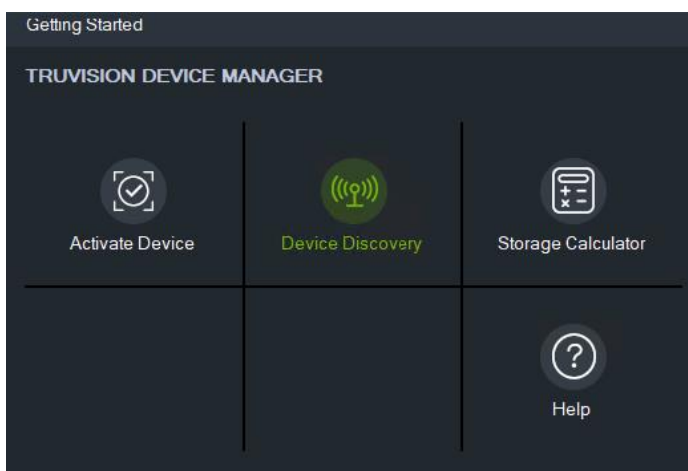
1. Power up the camera using the 12 VDC power supply that is included with the camera.
2. Make sure the camera is connected to the LAN network using an Ethernet cable.
3. Wait at least 2 to 3 minutes for the camera to start up. When no LAN cable plugged in, the camera will say “Please connect to Wi-Fi”, indicating it is ready to be configured. There will be no voice prompt when a LAN cable is plugged in.
4. Open TruVision Device Manager 9.2 or newer.
5. Device manager will show a non-activated camera.



6. Click the Activate Device button and select the checkbox of the camera that requires activation. Make sure “Enable DHCP” is checked unless you want to use a fixed IP address for the camera. Now Enter user name ‘admin’ and set a strong admin password for the camera meeting following requirements:
 - Minimum 8 characters and maximum 16 characters
 - Minimum 1 capital letter
 - Minimum 1 small letter
 - Minimum 1 number
 - Minimum 1 special character among - , . * & @ / \$? _ space.



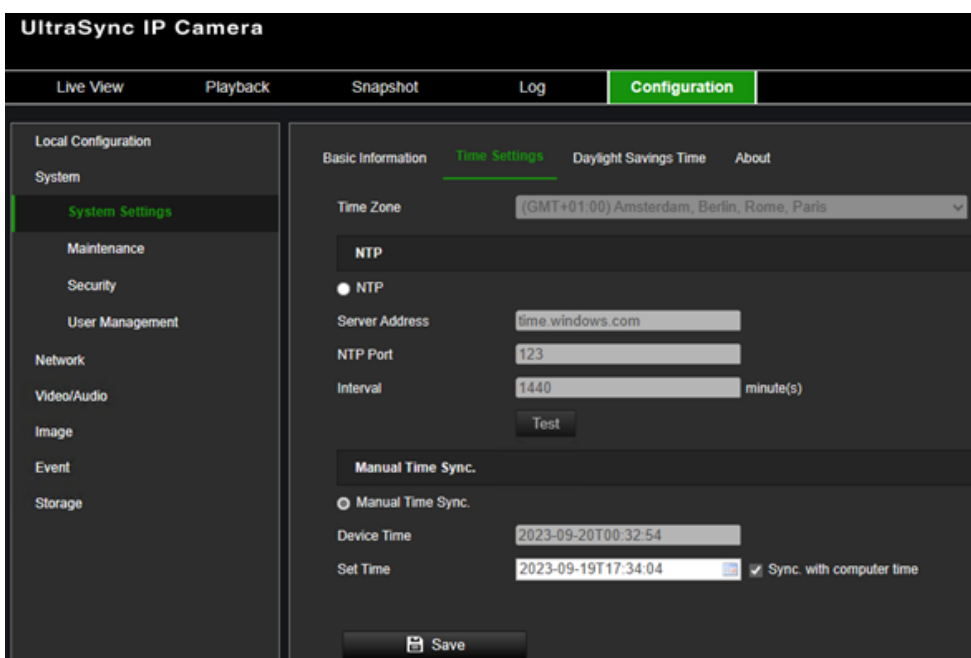
7. Click Apply to save settings and wait for Device Manager to confirm activation of the camera.
8. Click Close to leave the activation page.
9. From the Device Manager main screen, click now Device Discovery to show all cameras on the network.



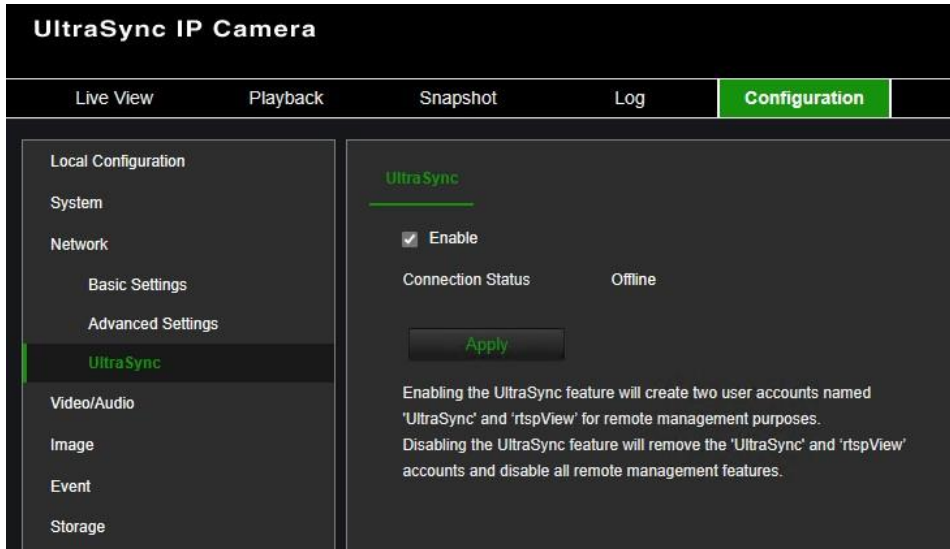
10. Double-click on the activated camera to open its web page.

Model	IP Address	Subnet Mask	Gateway	DHCP	Start Time
<input checked="" type="checkbox"/> TVUC-B01-0401-BUL-W	192.168.1.178	255.255.255.0	192.168.1.1	<input checked="" type="checkbox"/>	2023-09-20 00.30.11
<input type="checkbox"/> TVT-5609H	192.168.1.12	255.255.255.0	192.168.1.1	<input type="checkbox"/>	2023-09-10 17:01:00

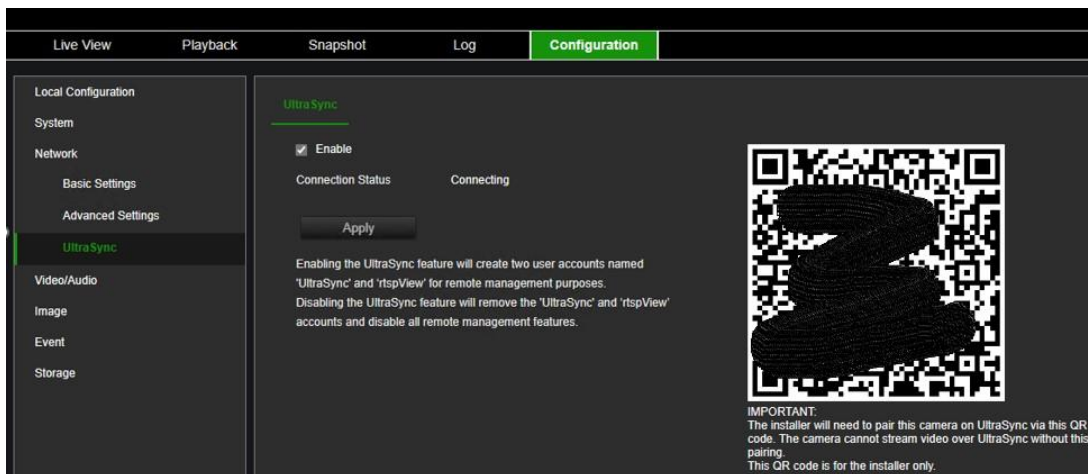
11. Login with the admin credentials you defined in step 6.
12. Go to camera menu Configuration > System > System Settings > Time Settings and select “Sync. with computer time” to set date and time. This is needed to establish a connection to UltraSync.



13. Go to Configuration > Network > UltraSync and check Enable to activate UltraSync connection. Click Apply to save settings.



After a short while a QR should appear indicating the camera is successfully connected to UltraSync. Don't scan this QR code as this is not needed for using the camera in combination with xGenConnect.



14. Now close the camera web page.

Adding camera to the local Wi-Fi network:

Repeat steps 1 to 11 above.

12. Go to Configuration > Network > Advanced > Wi-Fi and Search for local Wi-Fi networks.

- Select the desired local Wi-Fi network from the list of available networks. Only 2.4 GHz networks will work. After selecting the network, check the enable checkbox, fill in the Wi-Fi network password in field Key 1, and save settings.

The screenshot shows the configuration interface for an UltraSync IP camera. The 'Configuration' tab is selected, and the 'Wi-Fi' sub-tab is active. A 'Wireless List' table displays the following data:

No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)	Connection Status
1	Orange-d8e06	Manage	WPA2-personal	6	51	150	Disconnected
2	Guest-Orange-d8e06	Manage	WPA2-personal	6	49	150	Disconnected
3	devolo-384	Manage	WPA2-personal	1	20	150	Disconnected
4	AP_1612686624	Manage	not-encrypted	1	19	150	Disconnected
5	devolo-384	Manage	WPA2-personal	1	17	150	Disconnected
6	[REDACTED]	Manage	WPA2-personal	11	17	150	Disconnected
7	Proximus Public Wi-Fi	Manage	WPA2-enterprise	11	17	150	Disconnected
8	Proximus Public Wi-Fi	Manage	WPA2-enterprise	6	16	150	Disconnected
9	WIFI-2.4-0CB0	Manage	WPA2-personal	11	16	150	Disconnected
10	[REDACTED]	Manage	WPA2-personal	11	14	150	Disconnected
11	[REDACTED]	Manage	WPA2-personal	6	12	150	Disconnected
12	devolo-384	Manage	WPA2-personal	1	11	150	Disconnected


Below the table, the 'Wi-Fi' configuration fields are visible:

- SSID: WIFI-2.4-0CB0
- Network Mode: Manage (selected)
- Security Mode: WPA2-personal
- Encryption Type: TKIP
- Key 1: [REDACTED]

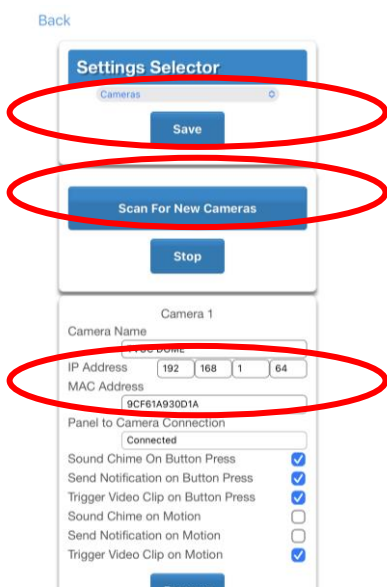
A 'Save' button is located at the bottom of the configuration area.

- Upon successful connection to the Wi-Fi network the camera shows status "Connected" in the table.
- Unplug the LAN cable and rescan in TruVision Device manager the network for new cameras. The camera should still show up since it is now connected via Wi-Fi. It will probably have a different Wi-Fi IP address than the previous LAN IP address we used.

Linking camera to the panel:

- From your iOS or Android device, open the UltraSync+ app.
- Add the panel details with the installer account / PIN.
- Log in to the site as the installer.
- Touch Menu  then Settings.

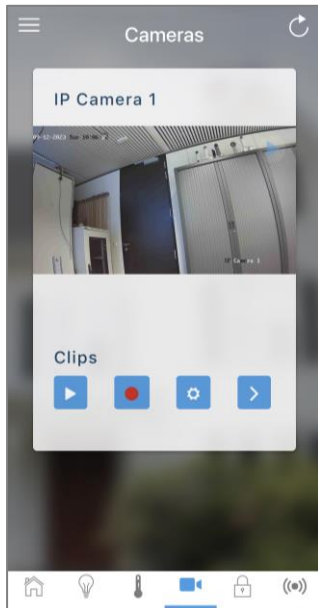
5. Select Cameras under the Settings Selector.



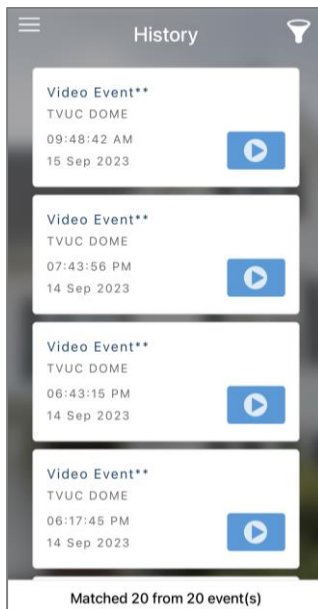
6. Click Scan for New Cameras. “Scanning...” will appear on the button, please wait for the message to disappear. The MAC Address will automatically be filled in.
7. Enter a Camera Name.
8. Optionally, enable notifications, trigger video clips in case of motion detection of doorbell button press.
9. Click Save.
Note: The camera may take up to 3 minutes to finalize the link with the panel and display on the Cameras screen of the app.
10. Close and relaunch the app.
11. 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. Touch the Play button under each camera to show the history log with all latest recorded clips from that camera. Press the event to watch the recorded clip.



5. Click the Share button to download or forward the clip.

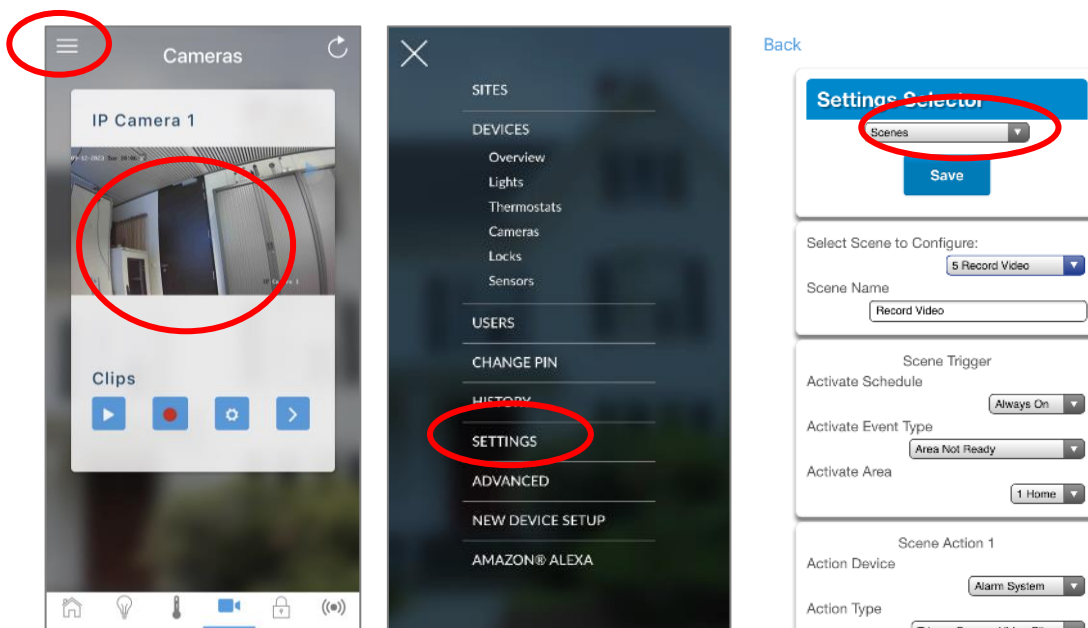
Programming event triggered camera clips


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.

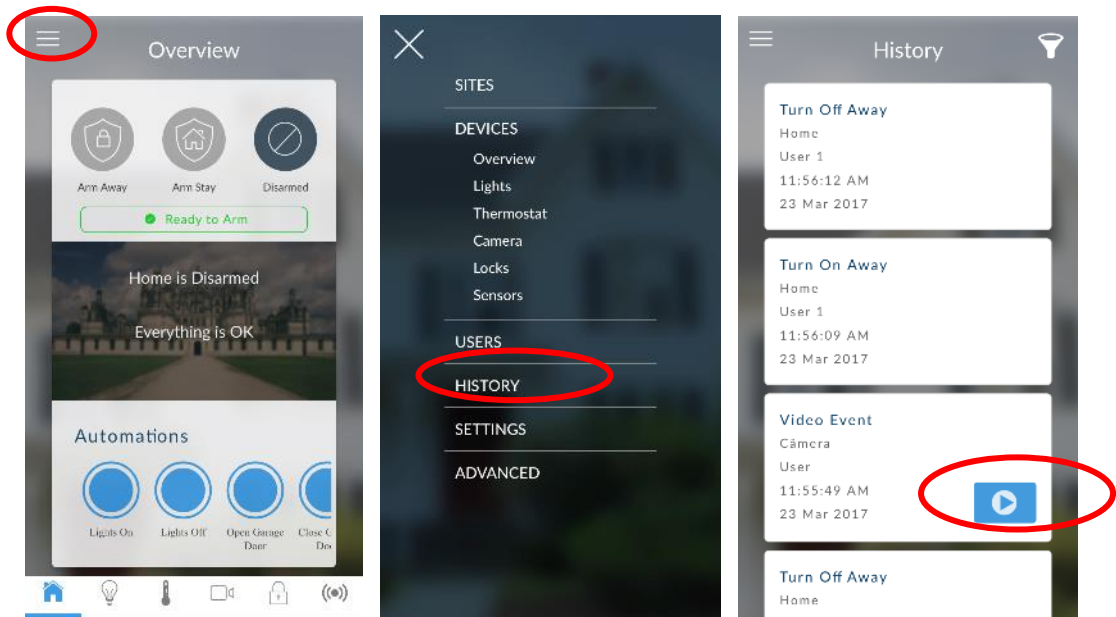
Note: Ensure you can view the Live Stream from the camera before continuing.



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/Partition/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

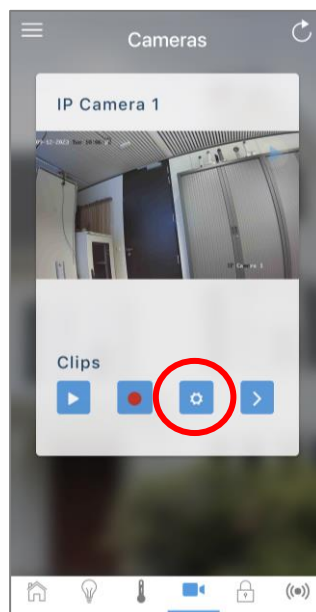
1. Touch Menu  then HISTORY.
2. Find the video event by using the navigation buttons and scrolling down.



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

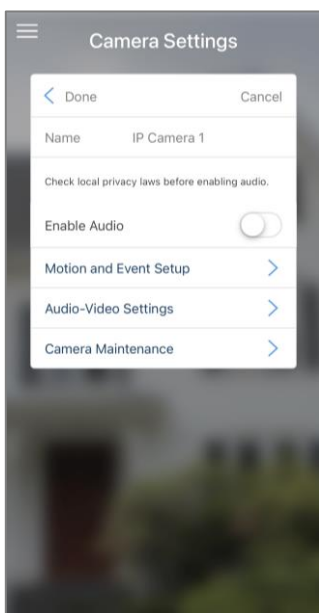
3. Tap the event to play the video.
4. Click the Share button to download or forward the clip.

Camera configuration

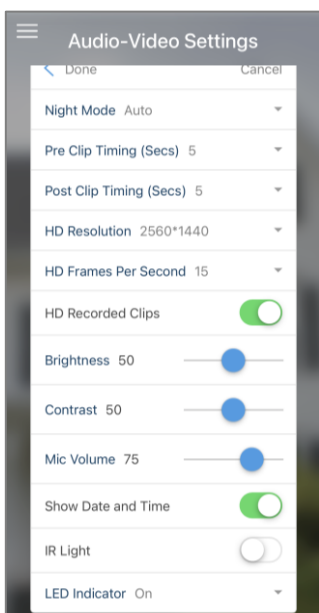


A number of optional camera settings can be configured from the application. Tap the camera icon on the bottom of the screen. Tap on the Configuration icon for the camera that needs to be configured.

- Enable Audio enables the camera 2-way audio. This feature allows you to listen in, talk from the mobile device through the camera speaker, as well as have recorded audio with the clips being stored on the SD card.

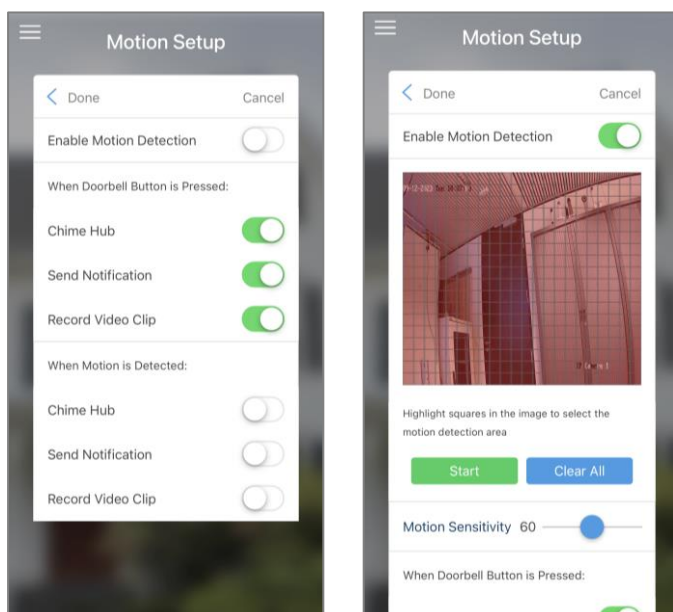


- Audio-Video settings allow you to change basic settings from the camera, such as pre-post recording time, image brightness and contrast, and microphone volume, enable or disable date and time, IR light, and LED indicator.

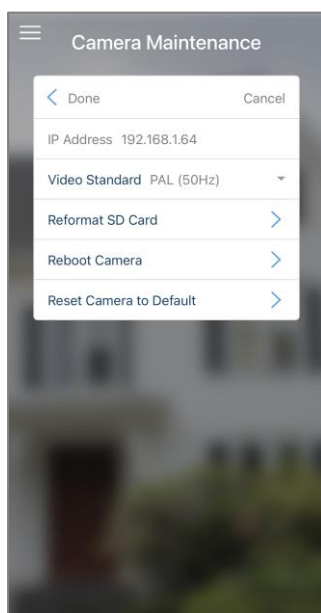


- Motion and Event setup allows you to enable the built-in camera motion detection feature. Select if a video clip should be recorded, and should push

notification be received. Define the detection area and modify the motion sensitivity as required.



- From the Camera Maintenance menu the camera can be rebooted or reset to factory settings. Also, the SD card can be formatted.



Notes

- Video and log files are stored on the microSD card inside the UltraSync camera and can only be accessed using the UltraSync+ app when validated with the panel.
- For security reasons, the microSD card will be encrypted when the camera has been successfully added through the App setup wizard. Stored video files cannot be retrieved from the microSD card in case it would be removed from the camera.

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 requires to be “provisioned” and added to the web portal in order to authenticate to the cloud servers which the cameras will connect to.

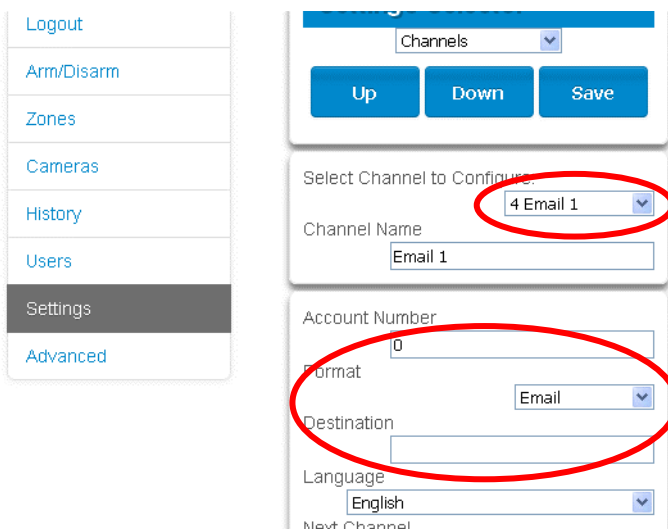
Only cameras specified for use with your panel will work. These cameras have additional encryption and security to protect against unauthorised 3rd party access.

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

Configuring Email Reports

Note: The system needs to be provisioned in UltraSync.

1. Log in to xGenConnect. 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 xGenConnect can be configured to support Osborne-Hoffman Reporting. This is done by entering specially formatted text in Channel > Destination.

Setting Up OH Reporting

Note: The system needs to be provisioned in UltraSync.

Go to <https://webportal.ultra-sync.com/> and log in with your dealer account.

Create New User Request

Site type

Central Station

End User Name

Address

Country

Flemish Region

City

ZIP

Phone

Mobile

SID

Timezone

Service Grade

Add-on services (additional charges may apply)

SMS Notification (SMS)
(This feature is subject to additional fees, please contact your sales representative for further details. It's currently supported only by xGenConnect, ZeroWire, NX500E and xGen.)

OH Reporting (OHR)

1. Select Site Type: Panel.
2. Select Central Station: Self Monitoring.

3. Select Service Grade: Core Intrusion (for Dual or Cellular only) or Core Intrusion IP (for LAN only).
4. From the Add-on services section, enable OH Reporting.
5. Click on Create when complete.

In addition, change the panel configuration in the Channels menu:

1. Click Settings > Channels to view Channel 1.
2. Select one the OH options in the channels report format field. Between CID and SIA; and between Cellular, IP, and Dual path.
3. 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.

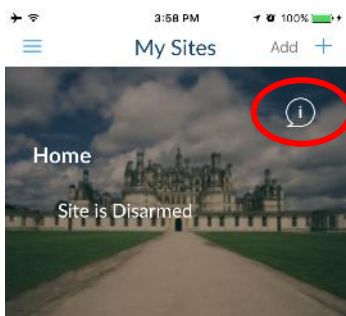
You will need to have a:

- Fully configured and online xGenConnect system.

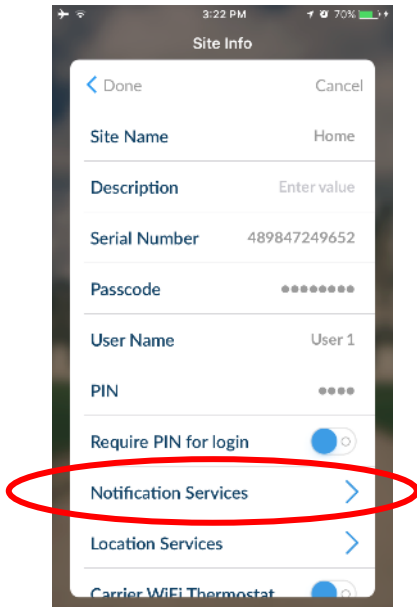
Note: The system needs to be provisioned in UltraSync.

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

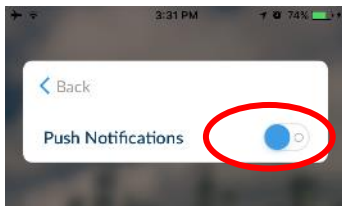
1. Open the UltraSync+ app.
2. Click the edit button next to the site you wish to receive notifications from.



3. Click Notification Services.



4. Enable Push Notifications.

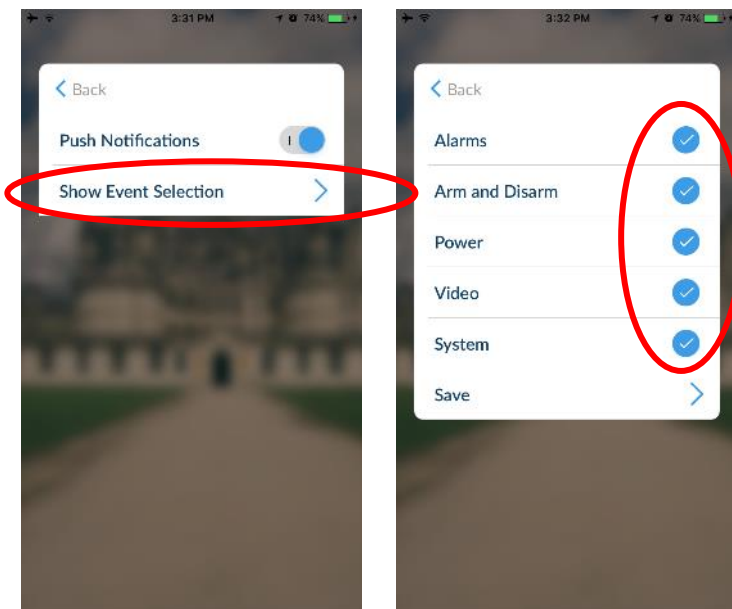


5. Wait for the registration process to complete.

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.

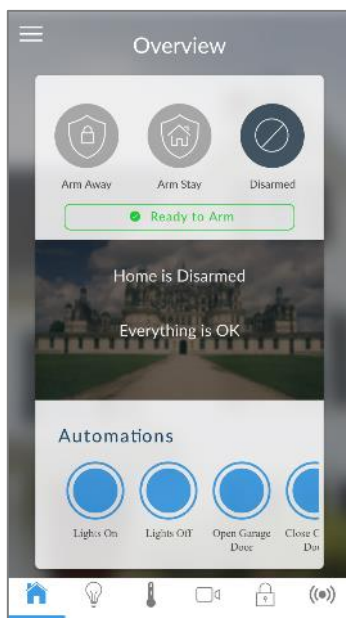
- c. Click Save >.
- d. Click Back.
- 7. Click Back.
- 8. Click Done.

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.

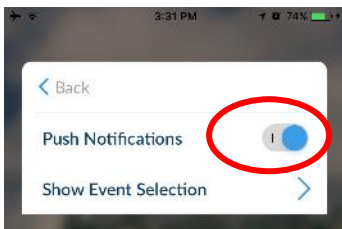
Troubleshooting Notifications

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 xGenConnect.



- Check the xGenConnect 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).

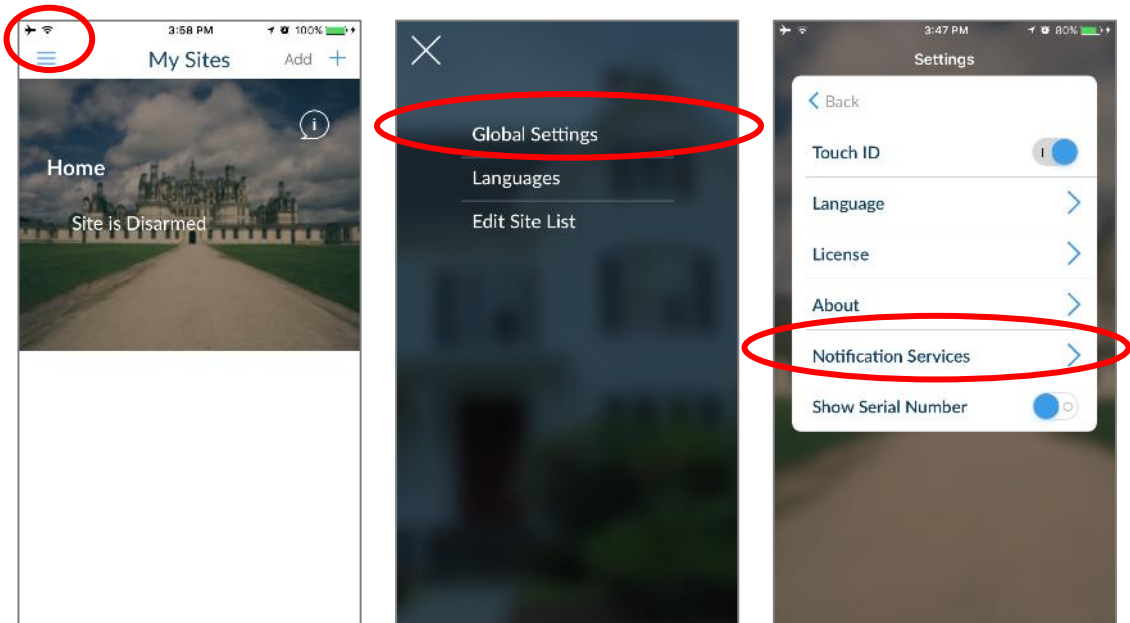


- Check your smartphone has notifications enabled (on Apple iOS click Settings, Notifications, scroll down and click UltraSync, check “Allow Notifications” and “Show in Notification Centre” are enabled, optionally select the Alert Style as Banners or Alerts).

- If you are on iOS, ensure your phone is logged into your Apple account under iTunes or iCloud.

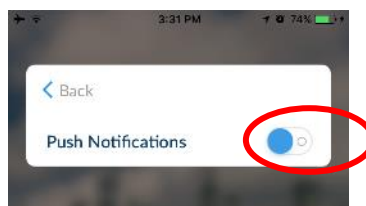
If you are on Android, ensure your phone is logged into your Google account under Google Play or Settings. This is required as UltraSync sends the push notification to Apple and Google servers for delivery to your device. “Rooted” or “Jailbroken” phones may not have the required software to receive push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



If you do not have access to the device, the xGenConnect 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.

The screenshot shows the 'Settings Selector' interface. On the left is a sidebar menu with options: Logout, Arm/Disarm, Sensors, Cameras, Rooms, History, Change PIN, Settings (highlighted), and Advanced. The main panel has a 'Channels' dropdown menu. Below it are 'Up', 'Down', and 'Save' buttons. A section titled 'Select Channel to Configure:' contains a dropdown menu with the following options: 4 smartphone_u1 (circled in red), 1 Central Station Primary, 2 Central Station Backup 1, 3 Central Station Backup 2, 4 smartphone_u1, 5 Email 2, 6 Email 3, 7 Email 4, 8 Email 5, 9 Email 6, 10 Email 7, 11 Email 8, 12 Email 9, 13 Email 10, 14 Email 11, 15 Email 12, 16 Email 13, and disabled. Below this are fields for Account Number, Format, Destination, Language, Next Channel, Event List, and Attempts.

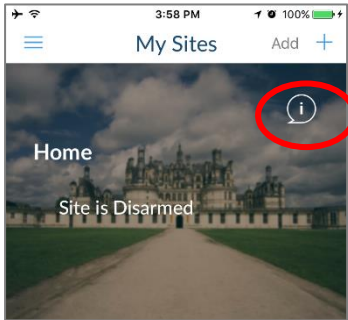
5. Delete the content of the Destination field.

This screenshot shows the same 'Settings Selector' interface. The 'Channels' dropdown is still selected. The '4 smartphone_u1' option is now selected in the 'Select Channel to Configure:' dropdown. The 'Channel Name' field contains 'smartphone_u1'. The 'Destination' field is circled in red and contains the text 'smartphone@u1'. Other fields like Account Number (0), Format (Email), Language (English), Next Channel (disabled), Event List (4 Event List), and Attempts (3) are visible.

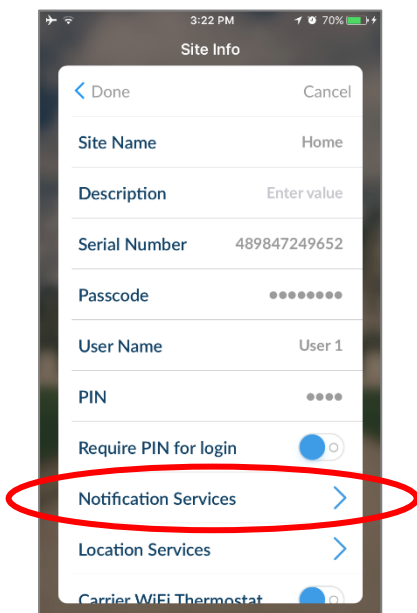
6. Click Save.
7. Your device will no longer receive notifications from this xGenConnect and the Channel is available to be reused.

Enable SMS Notification

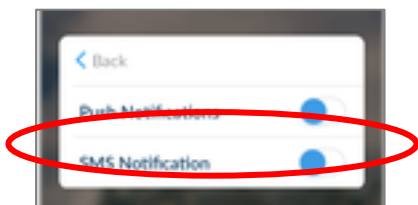
1. Open the UltraSync+ app.
2. Click the edit button next to the site you wish to receive notifications from.



3. Click Notification Services.



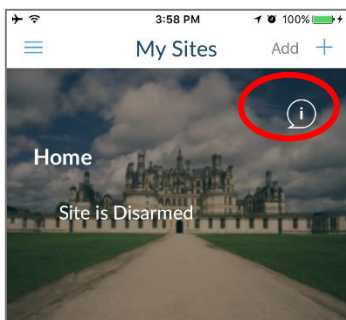
4. Enable SMS Notifications.



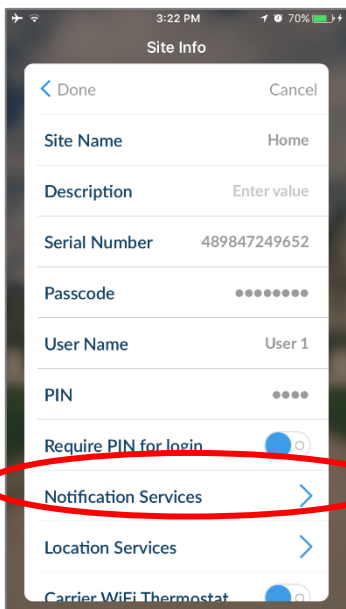
5. Type in the destination mobile phone number.
6. Tap Back.
7. Tap Done.

Disable SMS Notification

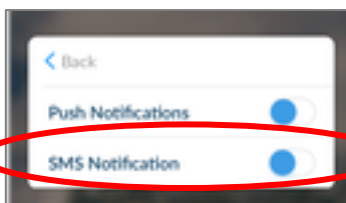
1. Open the UltraSync+ app.
2. Click the edit button next to the site you wish to stop SMS notifications from.



3. Click Notification Services.



4. Disable SMS Notifications.



5. By switching off SMS Notification, the mobile phone number will be deleted from this device's Channel.
6. Tap Back.
7. Tap Done.

Programming Scenes

xGenConnect can perform automation features such as turning on a device 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 *xGen 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, “Partition Not Ready” and “Partition 1”.
8. Under Scene Action 1, select Alarm System 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 behaviour is desired.

[Back](#)

The screenshot shows a 'Settings Selector' interface with the following sections:

- Scenes:** A dropdown menu showing 'Scenes' and a 'Save' button below it.
- Select Scene to Configure:** A dropdown menu showing '5 Record Video' and a text input field containing 'Record Video'.
- Scene Trigger:** Three dropdown menus: 'Activate Schedule' (Always On), 'Activate Event Type' (Area Not Ready), and 'Activate Area' (1 Home).
- Scene Action 1:** Two dropdown menus: 'Action Device' (Alarm System) and 'Action Type' (Trigger Camera Video Cam).

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.

User Reporting

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

Programming Instructions

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 xGenConnect to send diagnostic emails then check email is set up correctly under Communicator > Email and xGenConnect is connected to a network.

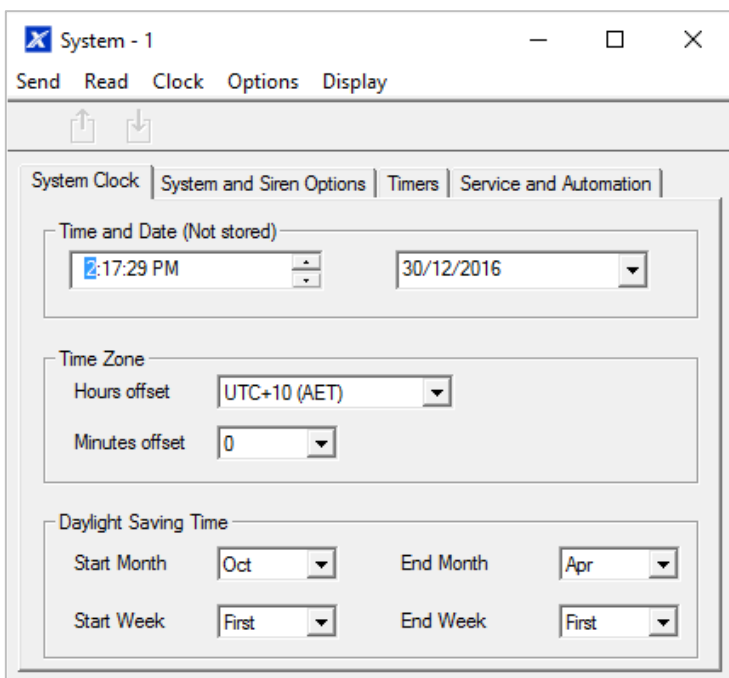
Note: Ensure you set the correct time zone here.

Programming Sequence

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

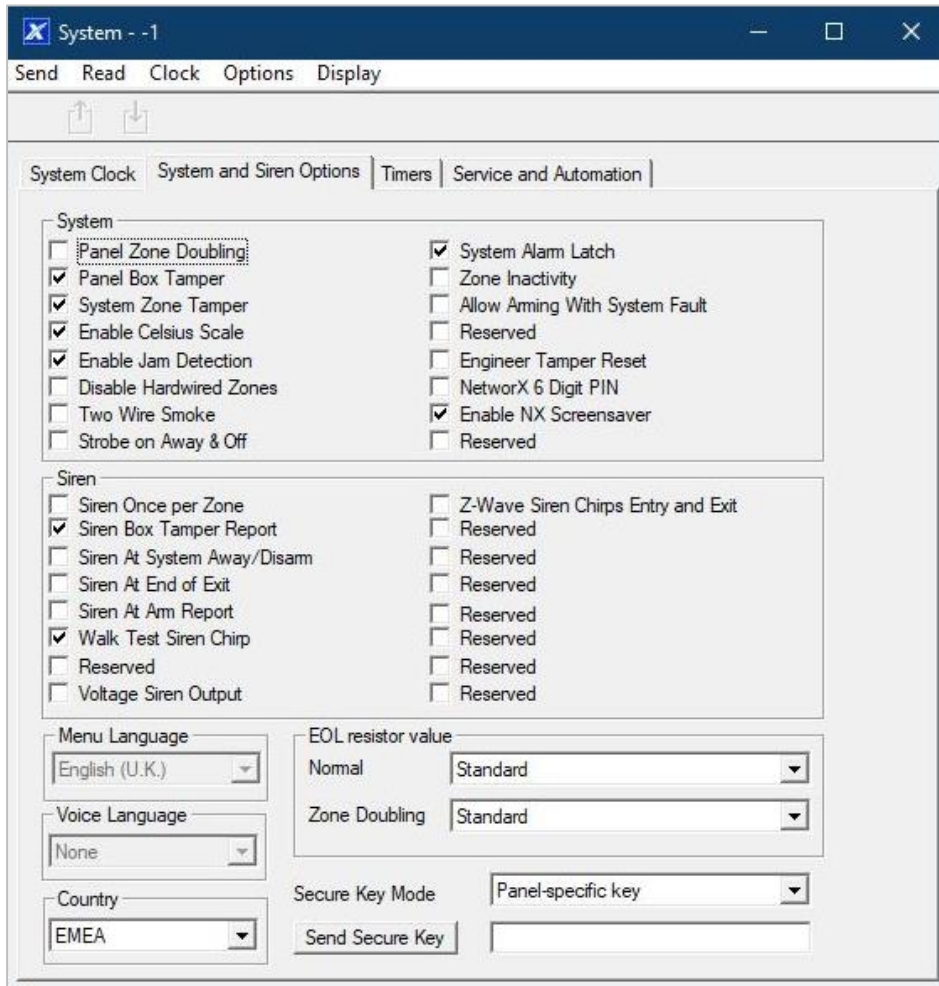
Instructions

1. Open System



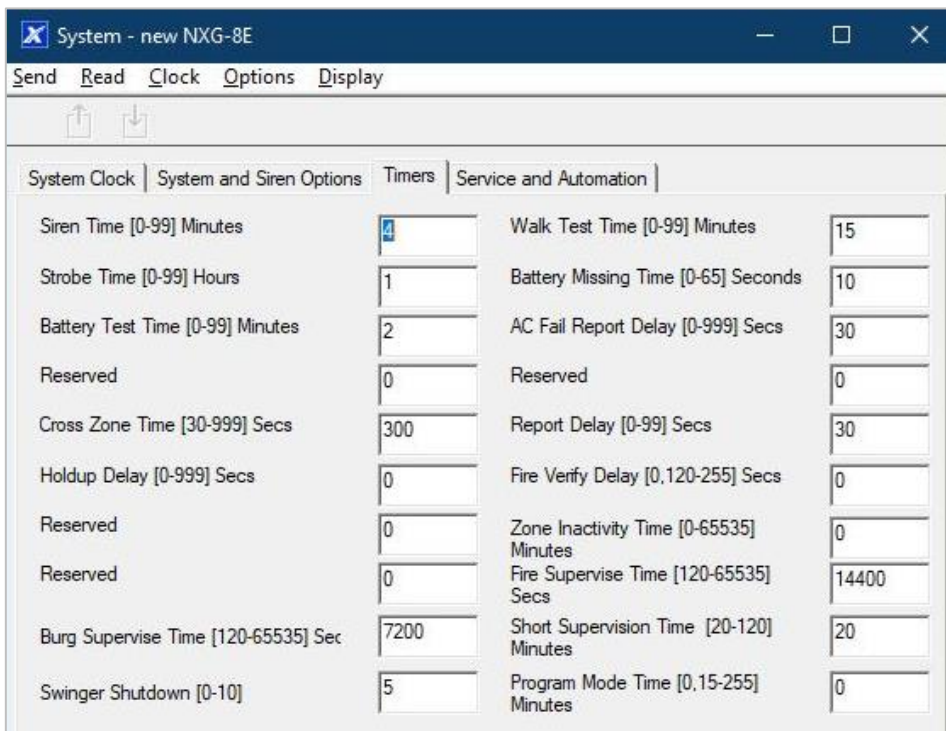
2. Select the right Time Zone using the Hours and minutes offset

3. If you wish to update the time and date
4. Go to System and Siren Options



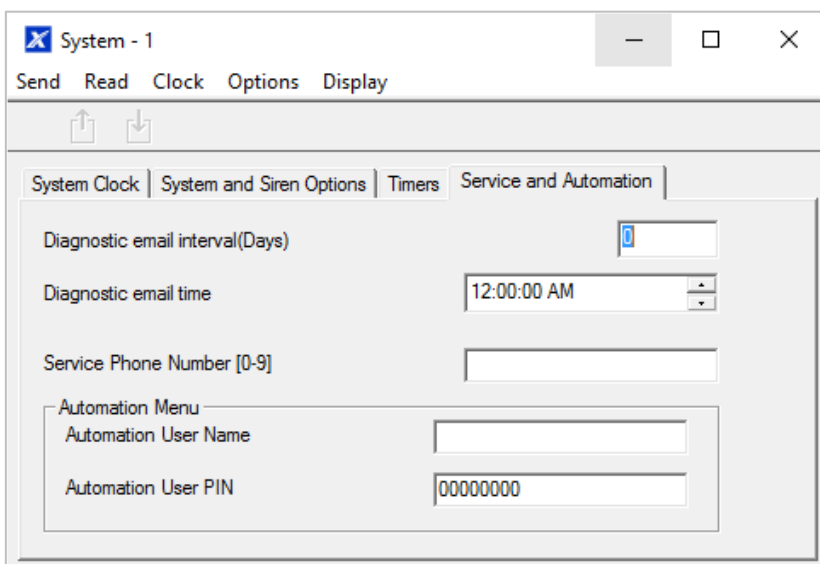
5. Select the settings you want to enable

6. Go to Timers



7. Enter the settings for global timers. Note Entry/Exit times are not here, go to Partitions > Partition 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

UpDownSave

Control Name

Language

Voice Language

System Date and Time

Date:

Time (hh:mm:ss) :

System Time Zone

Hours Offset

Minutes Offset

System Daylight Saving Time

Start Month

Start Week

End Month

End Week

System Timers

Siren Time [0-99] Minutes

Battery Test Time [0-99] Minutes

Battery Missing Time [0-65] Seconds

AC Failure Report Delay [0-999] Seconds

Cross Zone Time [0-999] Seconds

Zone Inactivity Time [0-65535] Minutes

Fire Supervise Time [120-65535] Seconds

Burg Supervise Time [120-65535] Seconds

System Options

Panel Zone Doubling

Panel Box Tamper

System Zone Tamper

Disable Hardwired Zones

Zone Inactivity

System Reporting

System Channels

Programming Instructions for Permissions

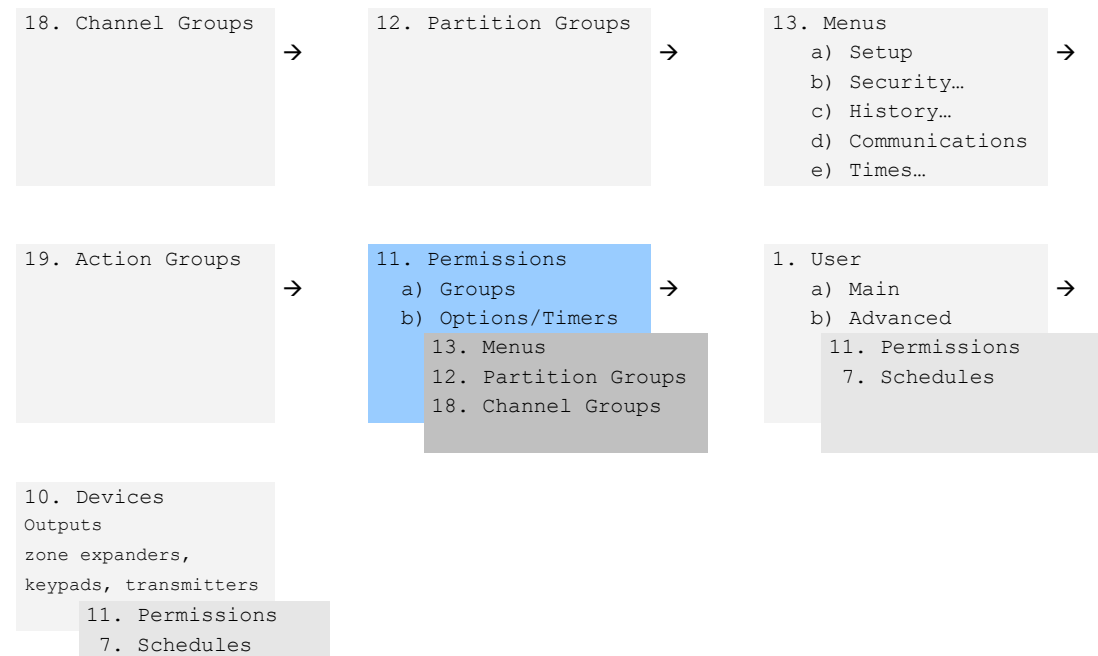
Goal

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

Pre-conditions

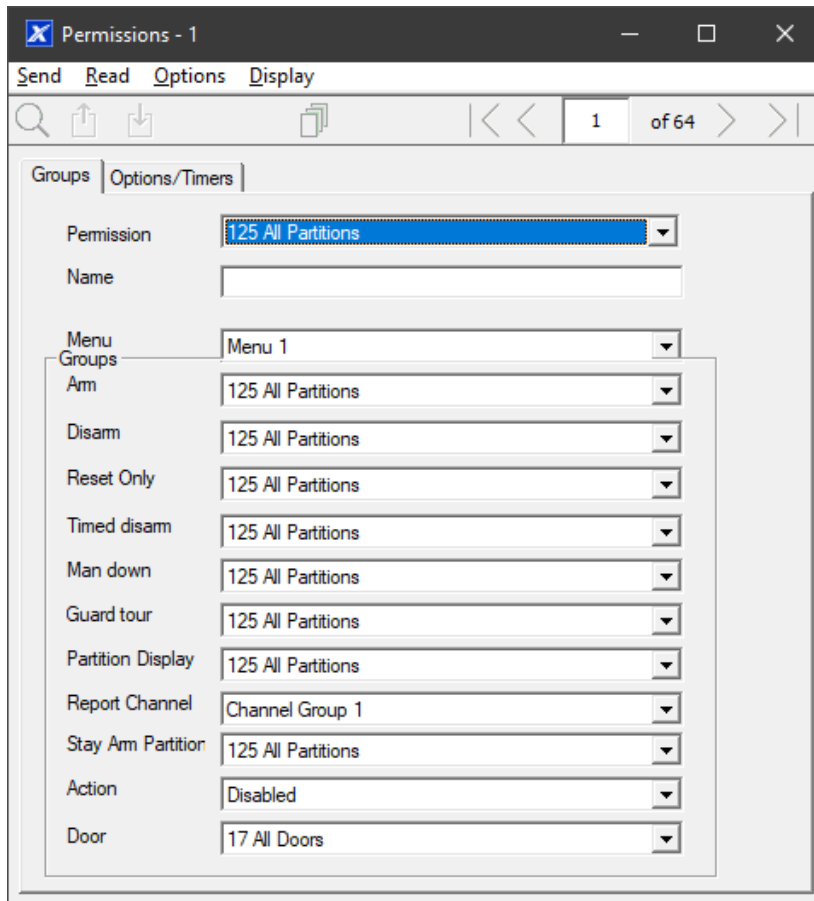
Have programmed or customized Channel Groups, Partition Groups, Door Groups, Menus, and Action Groups. Alternatively you can use the preset groups.

Programming Sequence



Instructions

1. Open Permissions

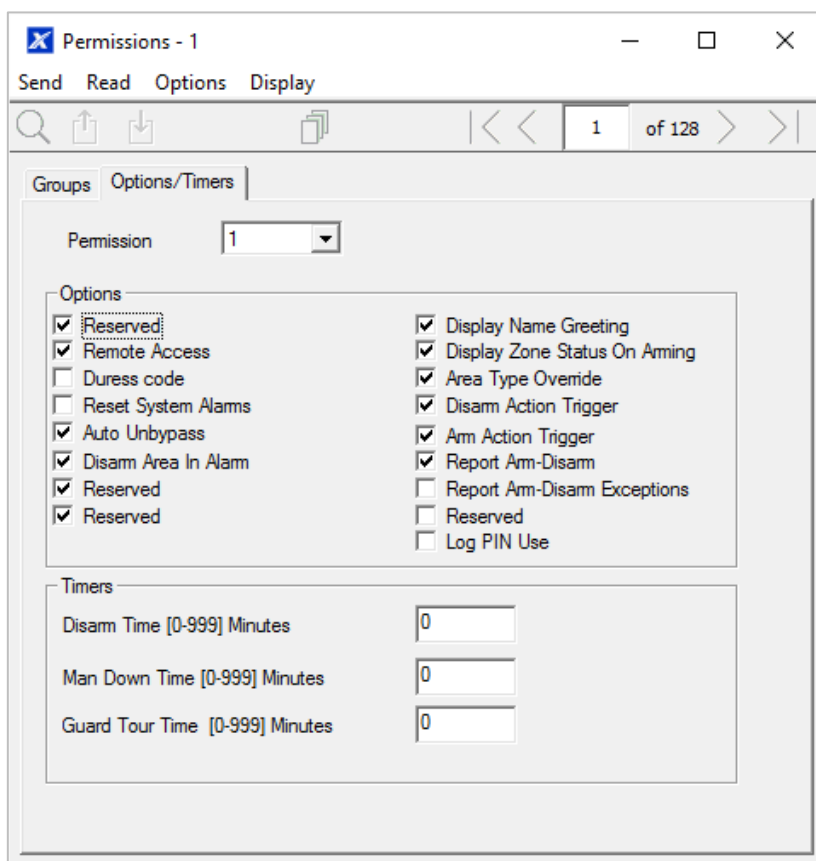


The screenshot shows a window titled "Permissions - 1" with a menu bar containing "Send", "Read", "Options", and "Display". Below the menu bar is a toolbar with search, upload, download, and copy icons, and a page indicator showing "1 of 64". The main content area has two tabs: "Groups" (selected) and "Options/Timers". The "Groups" tab contains a form with the following fields:

Permission	125 All Partitions
Name	
Menu Groups	Menu 1
Arm	125 All Partitions
Disarm	125 All Partitions
Reset Only	125 All Partitions
Timed disarm	125 All Partitions
Man down	125 All Partitions
Guard tour	125 All Partitions
Partition Display	125 All Partitions
Report Channel	Channel Group 1
Stay Arm Partition	125 All Partitions
Action	Disabled
Door	17 All Doors

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 Partitions that are selected inside the Partition 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 *xGen 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 xGenConnect system.

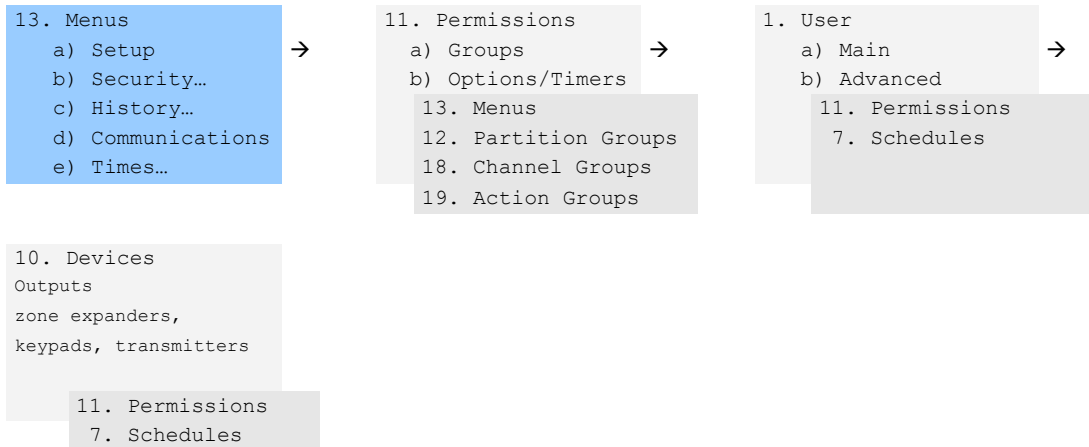
Pre-conditions

None.

Notes

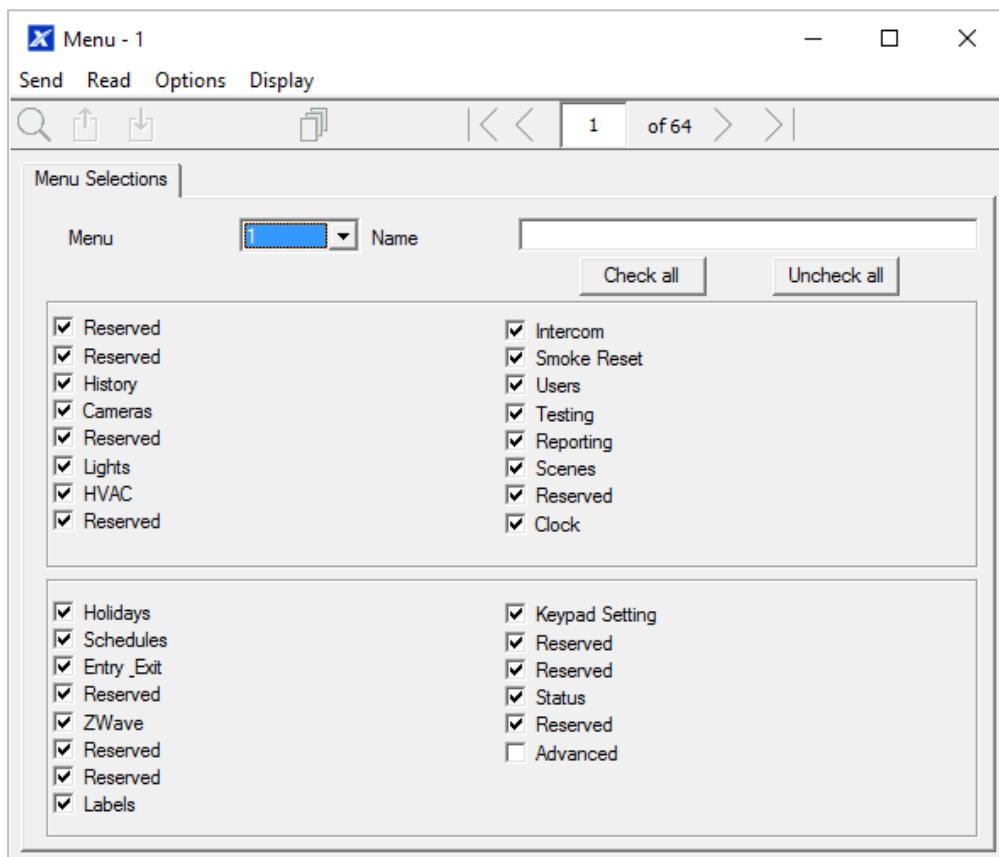
- The menus that will be available are the ones that the device has permission to display AND the ones that a user has access to, at the specified time and date which is controlled by Schedules.
- Users have up to 4 levels of access and devices have up to 2. This allows very sophisticated and fine grained 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



Instructions

1. Open Menu



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 xGenConnect system on the specific dates.

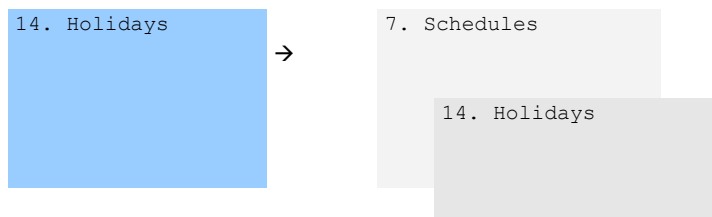
Pre-conditions

None.

Notes

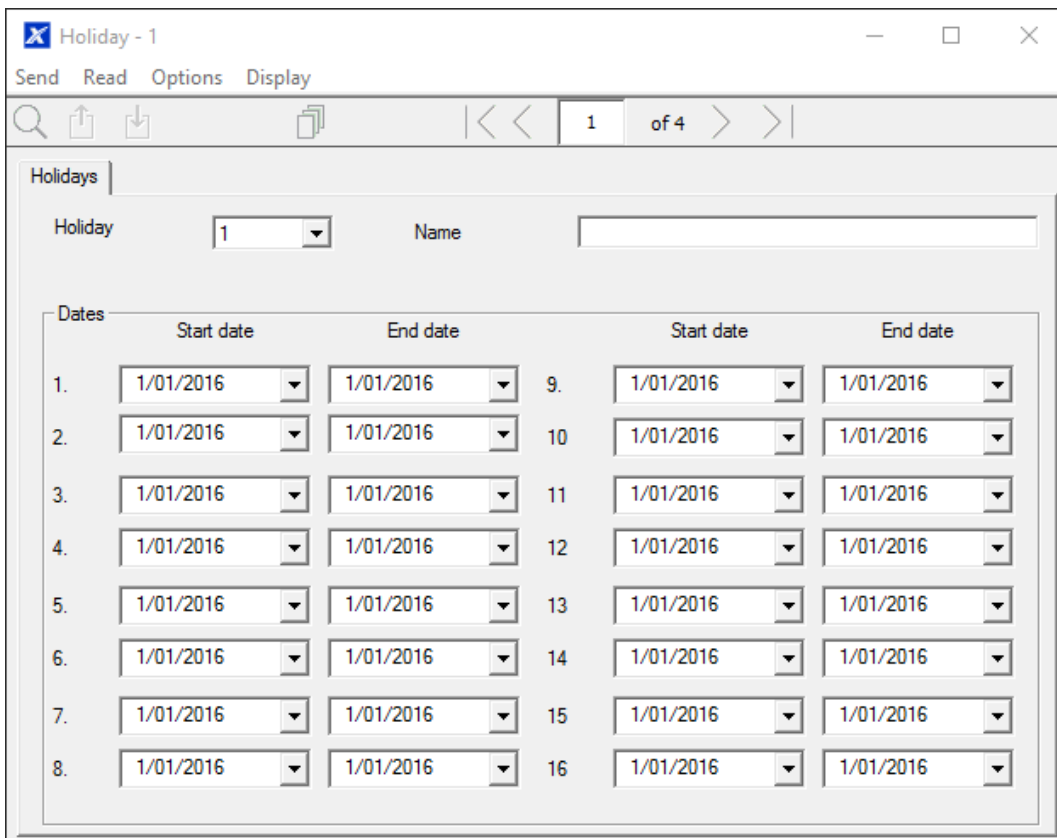
- Ticking Holidays in a Schedule for a permission PREVENTS access.
- Holiday schedules may impact automation features such as Actions if they are in use. For example, you may not want an Action to play on a holiday, so take care in programming the associated Schedule and permissions.

Programming Sequence



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 Partitions

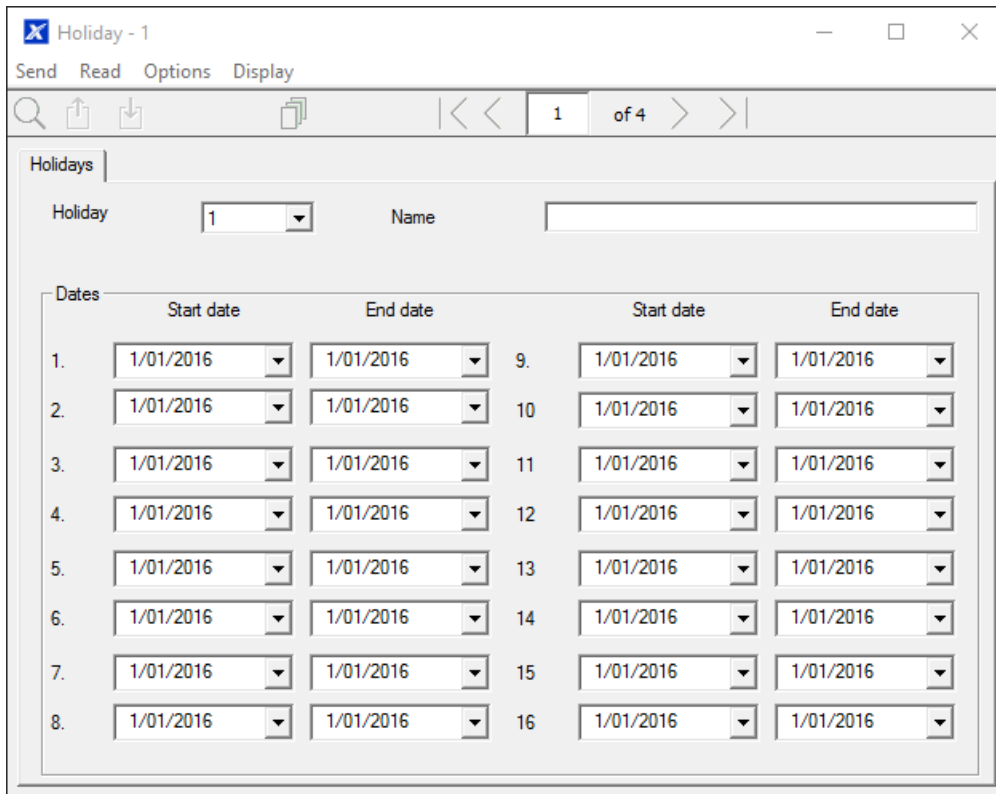
Office Schedule 1 – 8am-8pm M-F, Holidays 1 (ticked)

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

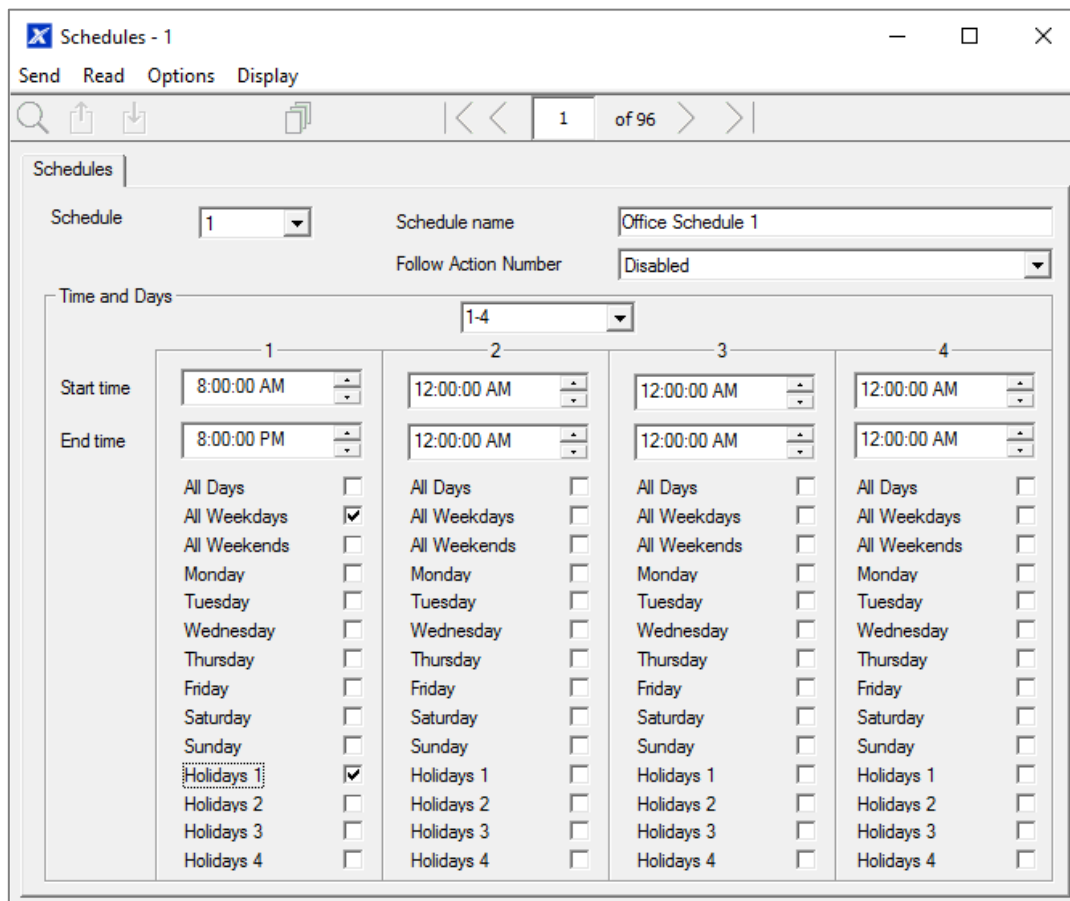
The public holidays in NSW, Australia for 2019 are:

- 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

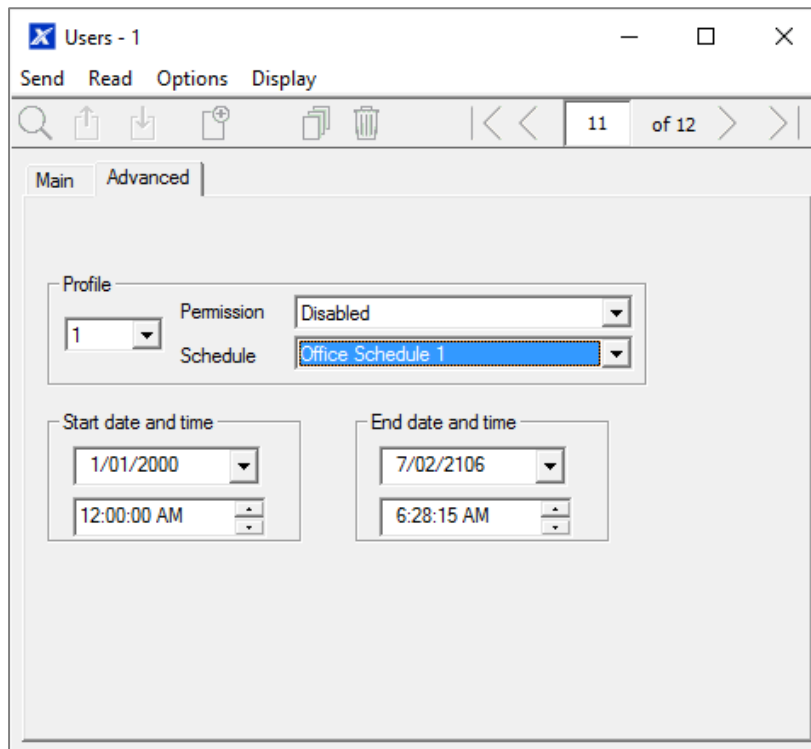
Open Holidays and program the date ranges.



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 xGenConnect system.

Pre-conditions

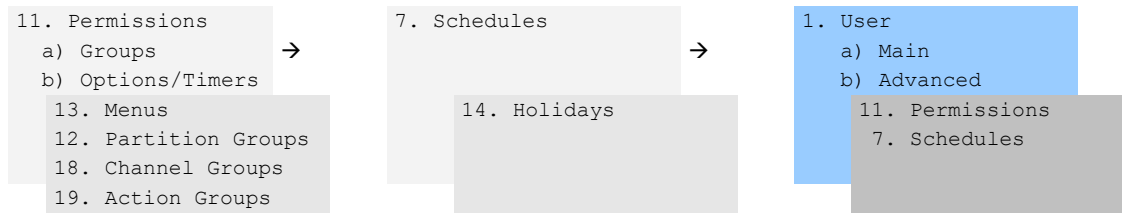
- Have programmed or customized Permissions. Alternatively you can use the defaults.
- Have programmed or customized Schedules. Alternatively you can use the defaults.

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 3 required settings are 6 digits minimum.
- User name must be assigned to give that user access to UltraSync+ app or xGenConnect 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.
- EN 50131 Grade 3 default codes are 971300, 123400, 567800.

Programming Sequence



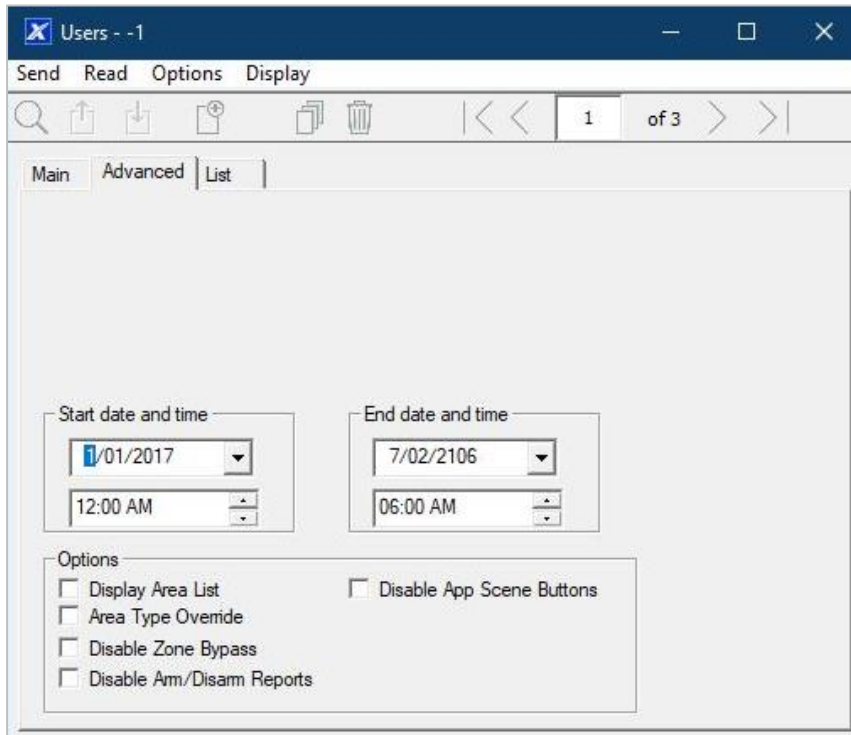
Instructions

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 *xGen Reference Guide*.
6. If the user type is not Custom, select the desired Partition Group and Door Group.
7. Card number and Card Enabled parameters may be set. **Note:** DLX900 does not allow securing cards or fobs remotely. It is recommended to use the NXG-1832 / NXG-1833-EUR keypad or panel web browser to assign cards to users.
8. Click the Advanced tab.



9. 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.

10. You can program up to 4 levels of access for each user. Permission 1 is applied when Schedule 1 is true. **Note:** Available for Custom user type only.

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 *xGen Reference Guide* for more details.

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

Web Page

Configure Users

Add Edit Delete Save

Select User Sort By Name

User 1 (1) ▼

User Number: 1

First Name: User 1

Last Name:

PIN: 1234

Language: English ▼

User Type: Custom ▼

Start: 2000-01-01 Midnight ▼

End: 2106-02-07 6:00 AM ▼

Profile 1: Always On ▼
All Partitions ▼

Profile 2: Always On ▼
disabled ▼

Profile 3: Always On ▼
disabled ▼

Profile 4: Always On ▼
disabled ▼

Programming Instructions for Zones

Goal

Program zones and add them to Partitions.

Pre-conditions

None.

Notes

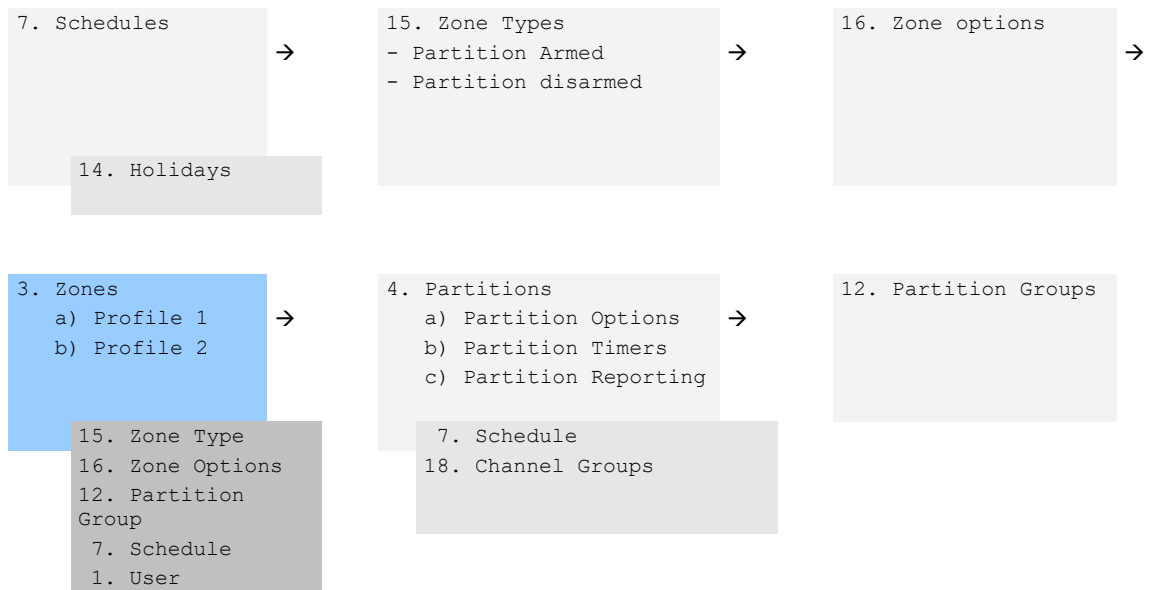
Use defaults for Zone Types and Zone Options to quickly set up your system.

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



Instructions

1. Go to Zones.

Zone: 1

Zone Name:

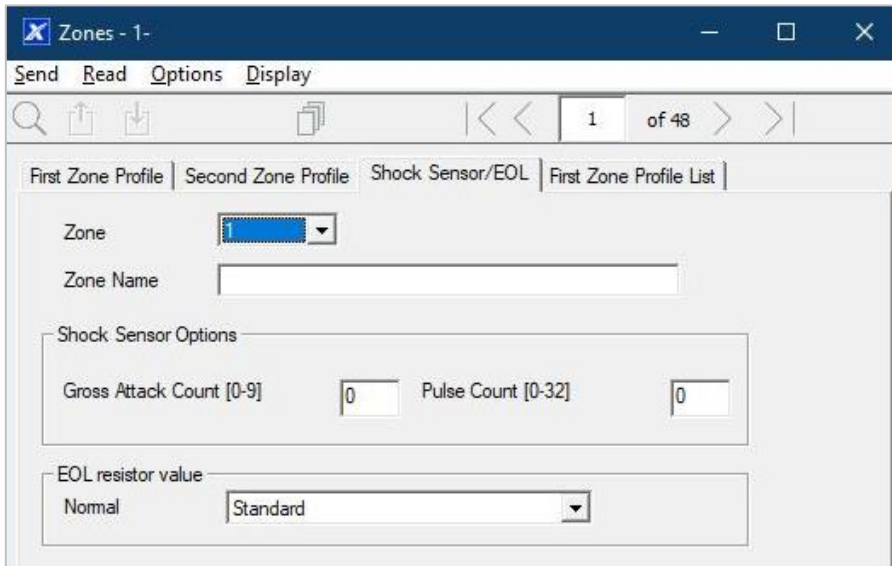
Zone type: 3 Entry Exit Delay 1

Zone Options: 1 Bypass

Partition Group: 1 Partition 1

Schedule: Always On

User number: 0



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 option preset.
6. Select a Partition group for the zone. If you want a zone to be in its own Partition, then select a Partition group with only one Partition. To create a zone in a common Partition, select a Partition group with multiple Partitions. 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

Logout
Arm/Disarm
Zones
Cameras
Rooms
History
Change PIN
Settings
Advanced

Settings Selector

Zones ▼

Save

Zone Add/Remove Functions

Learn **Cancel**

Transmitter Type Zone ▼

Select Zone to Configure: 1 Zone ▼

Zone Name

Zone Type 3 Entry Exit Delay 1 ▼

Zone Options 1 Bypass ▼

Partition Group 1 Partition1 ▼

Serial Number

Tamper

Disable Internal Reed

Disable Supervision

Wired Shock Sensor Settings:

Gross Attack Count [0-9]

Pulse Count [0-32]

Next

Zones are assigned to one or more Partitions using Partition Groups. If necessary, program Partitions and Partition Groups, then assign a Partition Group to each zone (step 6).

Programming Instructions for Custom Zones

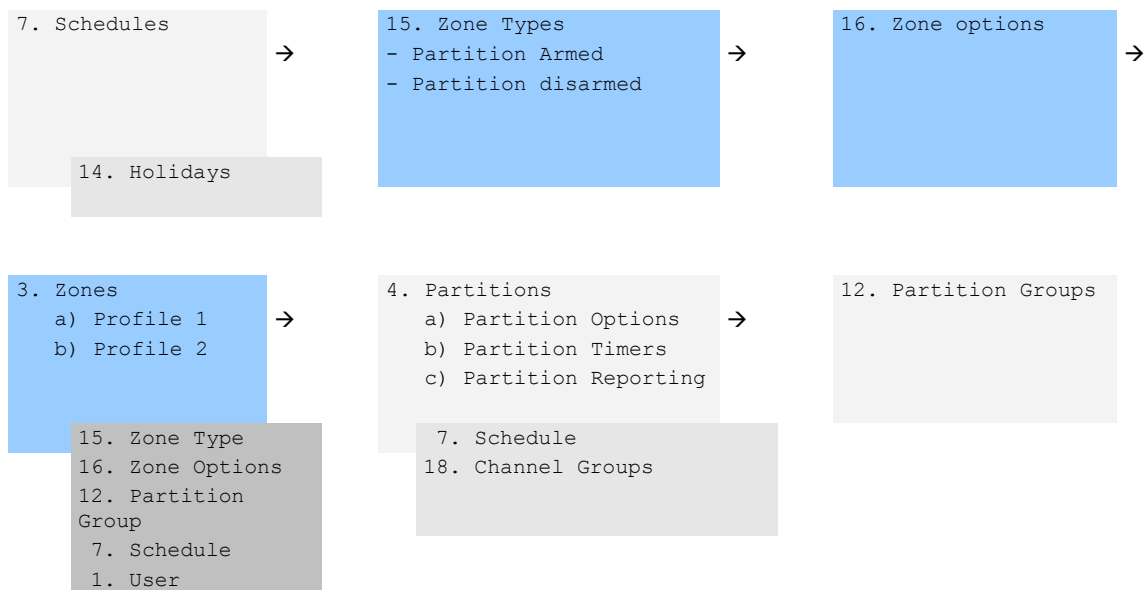
Goal

Program zones with advanced customization, including setting zone behaviour 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.

The screenshot shows a window titled "Zone types - 1" with a menu bar containing "Send", "Read", "Options", and "Display". Below the menu bar is a toolbar with search, copy, and navigation icons, and a page indicator showing "1 of 32". The main content area is titled "Zone Type Profiles" and contains two sections: "Area Armed" and "Area Disarmed".

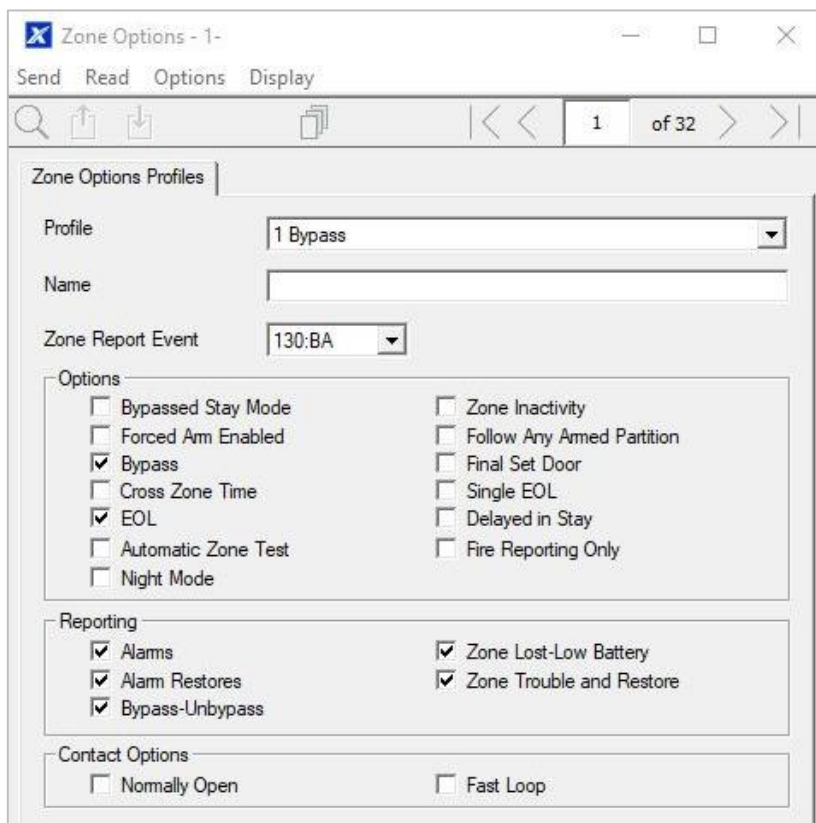
Area Armed:

- Profile: 1 Day Zone
- Name: [Empty text box]
- Zone Attribute: Instant
- Siren Attribute: Yelping
- Code Pad Sounder:
- Report delay:
- No Code Pad Display:
- Momentary Switch:
- Zone Inhibit:
- Swinger Shutdown:

Area Disarmed:

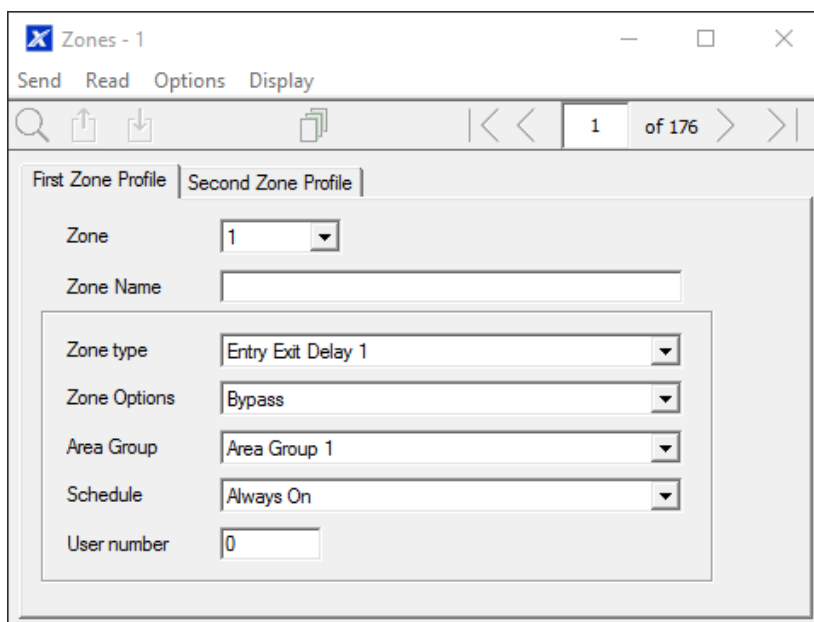
- Zone Attribute: Trouble Zone
- Siren Attribute: Silent
- Code Pad Sounder:
- Report Delay:
- No Code Pad Display:
- No Latching:
- Zone Inhibit:
- Swinger Shutdown:

2. Go to Zone Options.



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

4. Go to Zones.

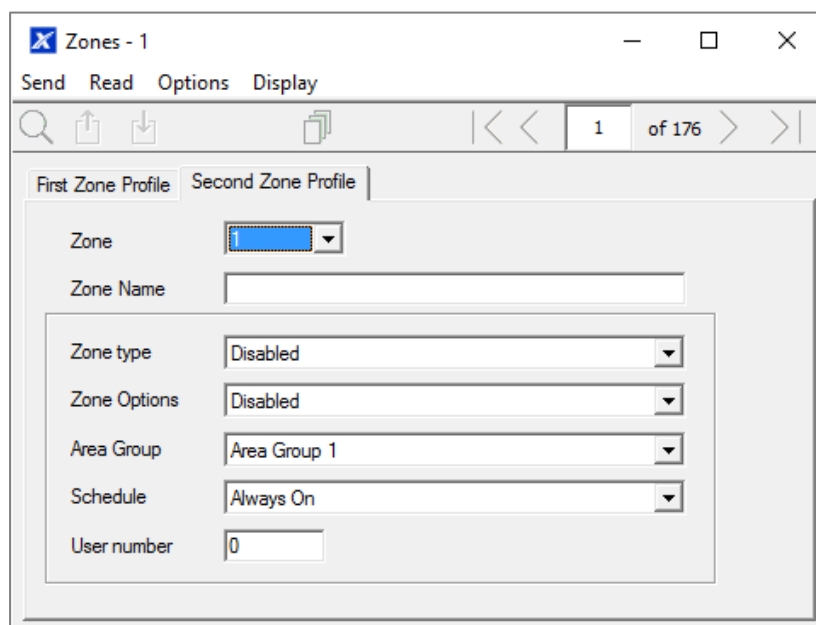


5. Select a zone number you want to program.
6. Enter a name for the zone.
7. Select the zone type profile you just created.
8. Select the zone options profile you just created.

9. Select a Partition Group for the zone. If you want a zone to be in its own Partition, then select a Partition Group with only one Partition. To create a zone in a common Partition, select a Partition Group with multiple Partitions. 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 Partitions using Partition Groups. If necessary, program Partitions and Partition Groups, then assign a Partition Group to each zone (step 8).

Programming Instructions for Partitions

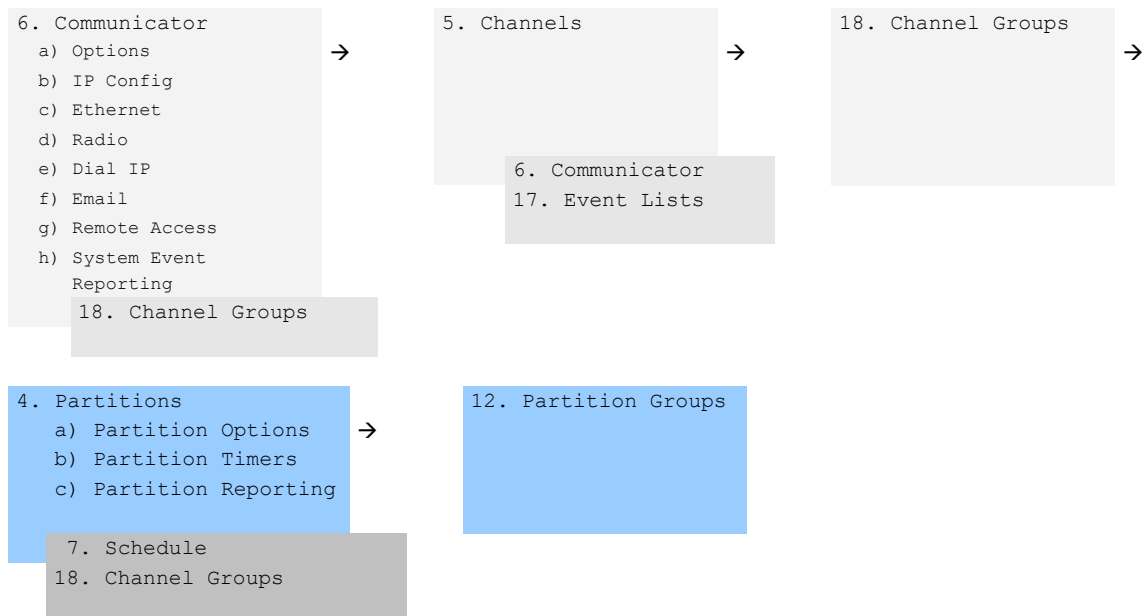
Goal

Program Partitions, Entry/Exit Times, Reporting Options, and Partition Groups.

Pre-conditions

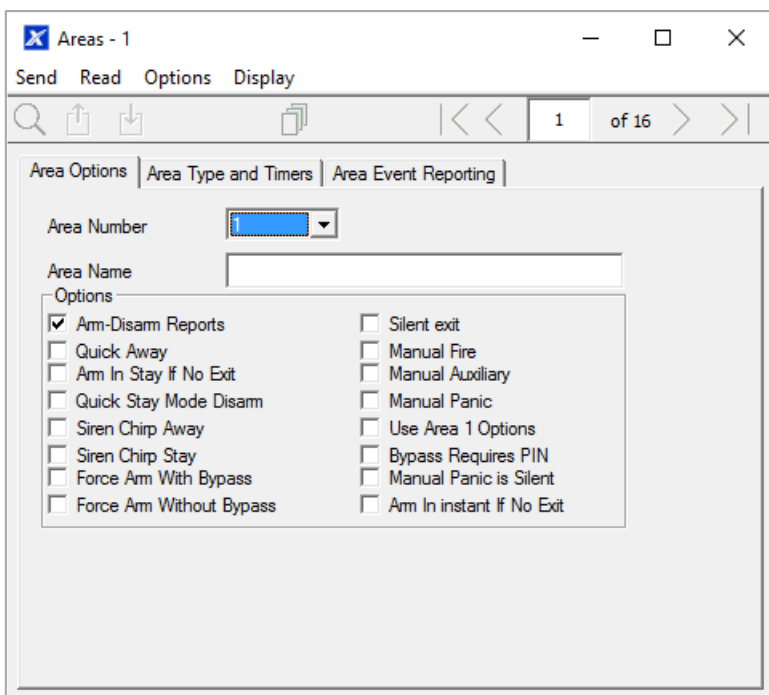
Programmed Communicator, Channels, and Channel Groups.

Programming Sequence



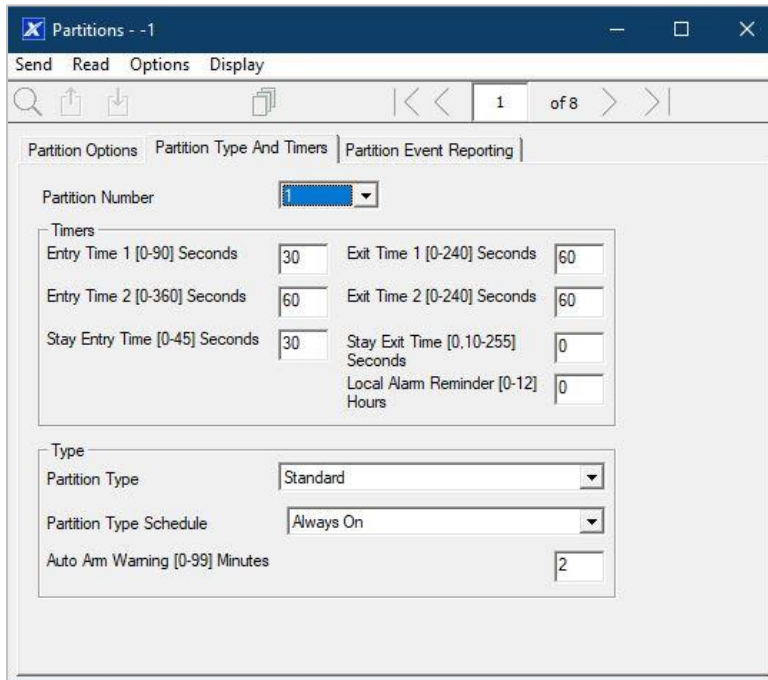
Instructions

1. Go to Partitions.

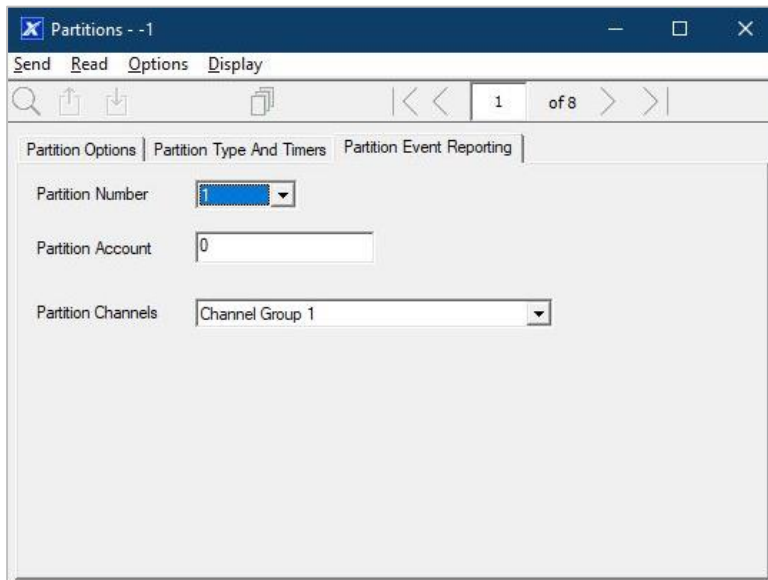


2. Select a Partition Number.
3. Enter a descriptive name.
4. Select the Options you want to enable for this Partition. Partition 2 and above have "Use Partition 1 Options" ticked to allow faster programming of your system. Untick this box if you want to customize options for Partition 2 and above.

- For advanced programming you can assign a Schedule and a Partition Time Disarm function to occur according to the schedule. Refer to *xGen Reference Guide* for more details.
- Go to Partition Timers.



- Enter the timers that apply to this Partition.
- Go to Partition Reporting.



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

Next

Customize Partition Groups if needed.

Webpage

Logout

Arm/Disarm

Zones

Cameras

Rooms

History

Change PIN

Settings

Advanced

Settings Selector

Partitions ▼

Save

Select Partition to Configure:

Partition Name: 1 Partition ▼

Partition Timers

Entry Time 1 [0-90] Seconds: 10

Exit Time 1 [0-240] Seconds: 10

Entry Time 2 [0-360] Seconds: 10

Exit Time 2 [0-240] Seconds: 10

Stay Entry Time [0-90] Seconds: 10

Stay Exit Time [0,10-255] Seconds: 0

Partition Options

Quick Arm

Quick Stay Mode Disarm

Manual Panic

Manual Panic is Silent

Manual Fire

Manual Auxiliary

Force Arm With Bypass

Partition Reporting

Partition Account: 0

Partition Channels: 1 Channel Group ▼

Programming Instructions for Schedules

Goal

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

Pre-conditions

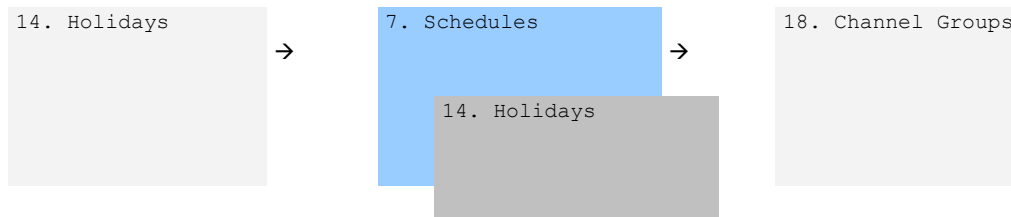
Holidays have been programmed if needed.

Notes

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

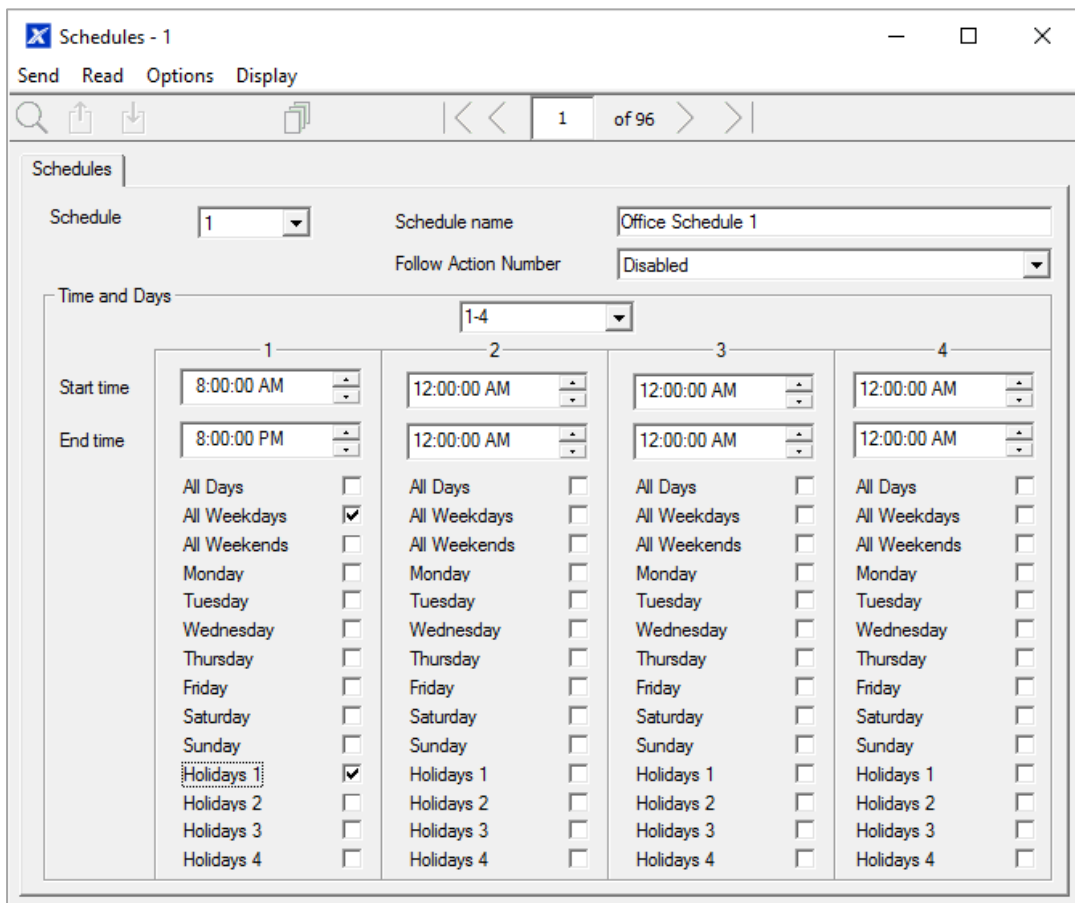
- xGenConnect automatically handles schedules that span midnight (for example, bakers hours), do not tick the following day of the AM hours. (See *xGen Reference Guide* for more details.)

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 an NXG-18xx, 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

UpDownSave

Select Schedule to Configure:

Schedule Name: 1 Schedule

Time and Days 1

Start Time (hh:mm) : 00 00

End Time (hh:mm) : 00 00

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Holidays 1

Holidays 2

Time and Days 2

Start Time (hh:mm) : 00 00

End Time (hh:mm) : 00 00

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Holidays 1

Holidays 2

Time and Days 3

Start Time (hh:mm) : 00 00

End Time (hh:mm) : 00 00

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Holidays 1

Holidays 2

Time and Days 4

Start Time (hh:mm) : 00 00

End Time (hh:mm) : 00 00

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Holidays 1

Holidays 2

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 xGenConnect system.

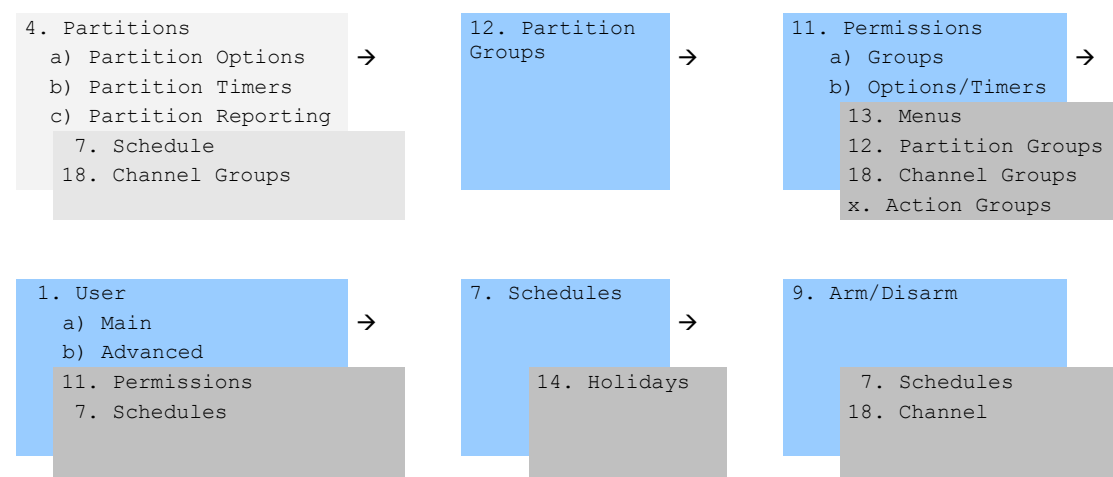
Pre-conditions

Partitions have been programmed.

Notes

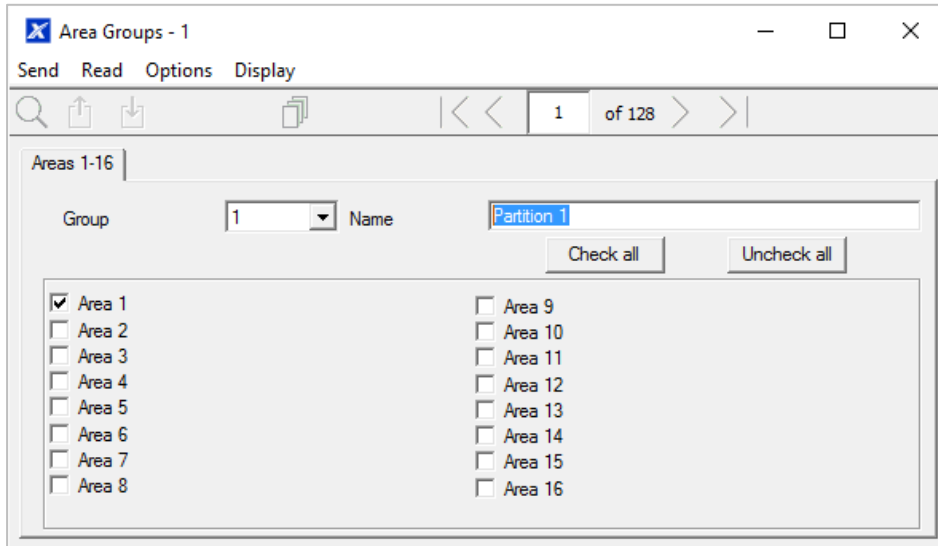
- The Arm-Disarm will function as if it is the user you select. You will need to program valid user permissions including Partition Groups, User Schedule, Profile levels, and active date and time.
- Creating a new user only for the purpose of Arm-Disarm will make it easier to maintain.
- Use defaults for Schedules, Partition Groups and Permissions for faster programming.
- xGenConnect will sound a warning prior to the Arm-Disarm from arming a Partition. This is set in Partitions > Partition Timers > Partition Type Delay.
- If a user with Partition Type Override option disarms a Partition with Arm-Disarm, then the Arm-Disarm will no longer function on that Partition. To re-enable Arm-Disarm that Partition must be manually armed.

Programming Sequence

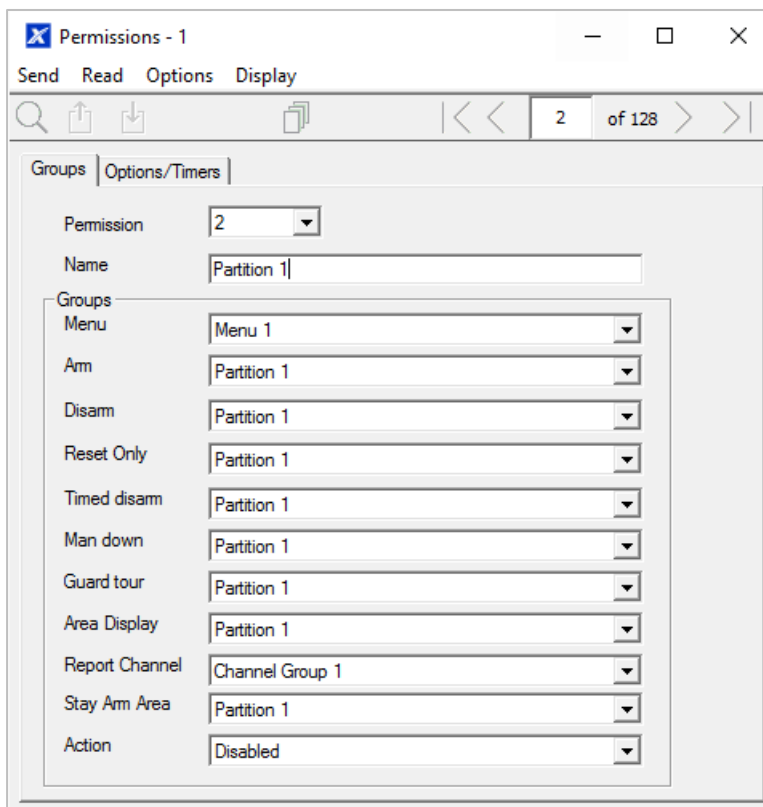


Instructions

1. Create a Partition Group and select the Partitions you want to be Armed according to the schedule you will create later.



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



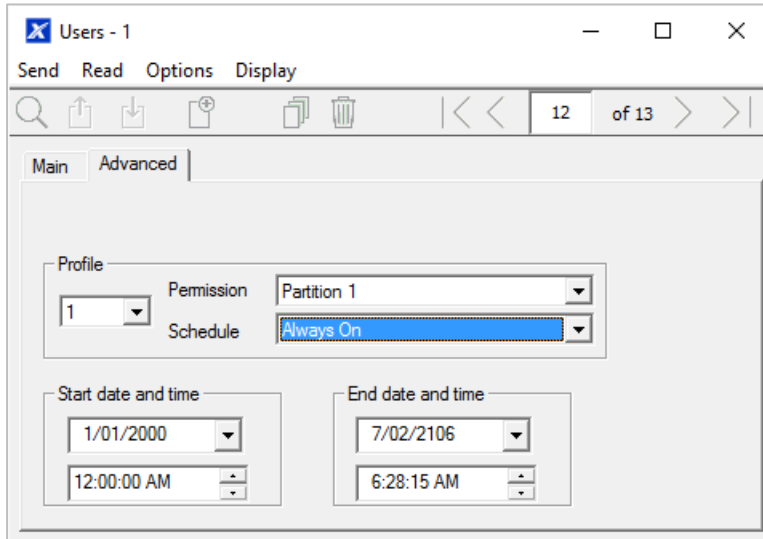
4. Open Users and create a new user. Suggested you provide a descriptive name such as “Auto Arm User” to make troubleshooting in the future easy.

The screenshot shows a window titled "Users - 1" with a menu bar containing "Send", "Read", "Options", and "Display". Below the menu bar is a toolbar with icons for search, copy, paste, and delete, along with navigation arrows and a page indicator "12 of 13". The main content area has two tabs: "Main" (selected) and "Advanced". In the "Main" tab, there are several input fields and dropdown menus: "User Number" is set to "99"; "Name" is "Auto Arm User"; "PIN" is "9999"; "Type" is set to "Custom"; and "Language" is set to "English (Australia)".

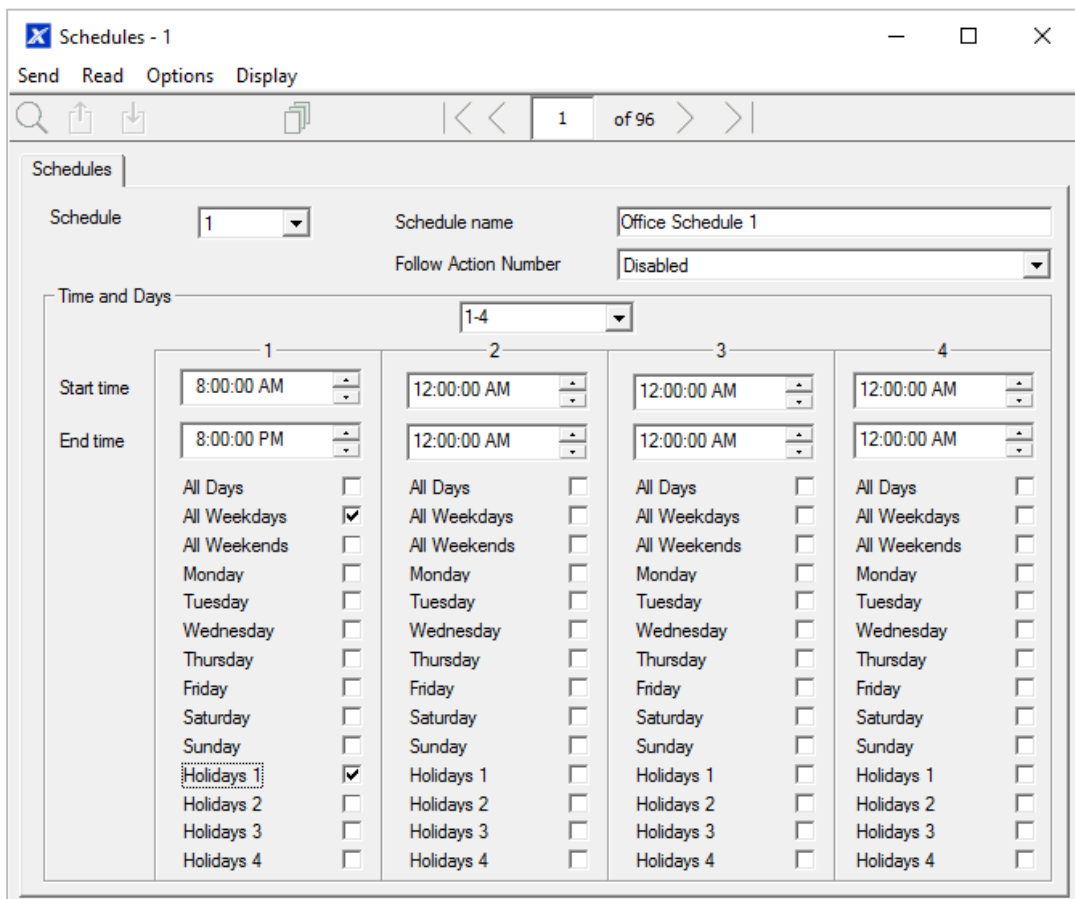
5. Go to the Advanced tab.

The screenshot shows the same "Users - 1" window, but now the "Advanced" tab is selected. The "Main" tab is still visible but not active. In the "Advanced" tab, there are two main sections: "Profile" and "Start date and time". The "Profile" section has a dropdown menu for "Profile" (set to a blue icon), "Permission" set to "Disabled", and "Schedule" set to "Always On". The "Start date and time" section has "Start date and time" set to "1/01/2000" and "12:00:00 AM". The "End date and time" section has "End date and time" set to "7/02/2106" and "6:28:15 AM".

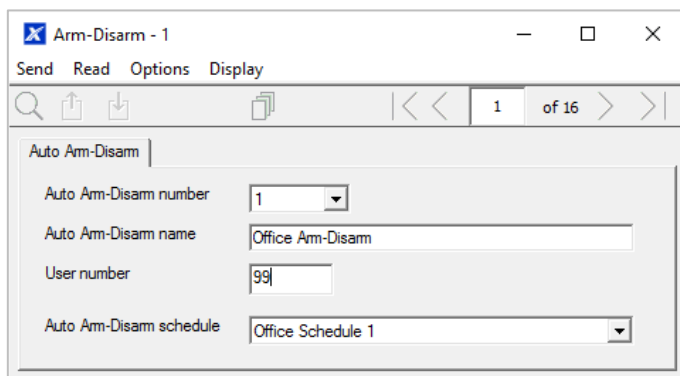
- Select the Permission you created above. If you want a simple Arm-Disarm then leave the Schedule here as Always On. The Schedule selected here is only for the **User**. It determines when the User is allowed to perform an Arm-Disarm, not when the Arm-Disarm will occur.



- 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 Partitions 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 Partition 1, 2, and 3 at any time or day.

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

Arm-Disarm Number 1 – Arm-Disarm Example

Schedule 4 – Office Hours
Mon – Fri
9 AM – 5 PM

→ See “Programming Instructions for Schedules” on page 118 to program

User 55 – Arm-Disarm User

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

Permission 99 – Full Access

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

Arm Partition Group 1
1, 2, 3

Disarm Partition Group 1
1, 2, 3

Schedule 1 – Full Access
7 days, 24 hours

→ See “Programming Instructions for Schedules” on page 118 to program

Programming Instructions for Communicator

Goal

Configure each communication path for delivering event messages.

Pre-conditions

None.

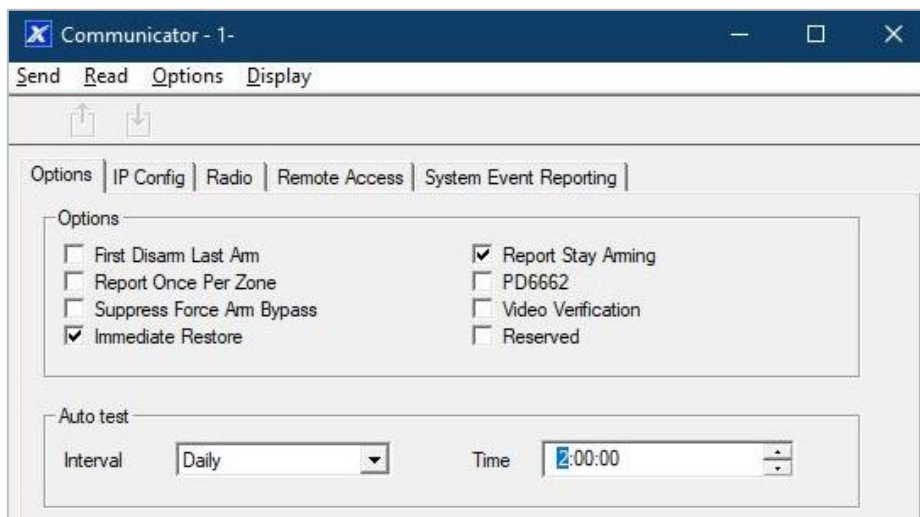
Programming Sequence

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

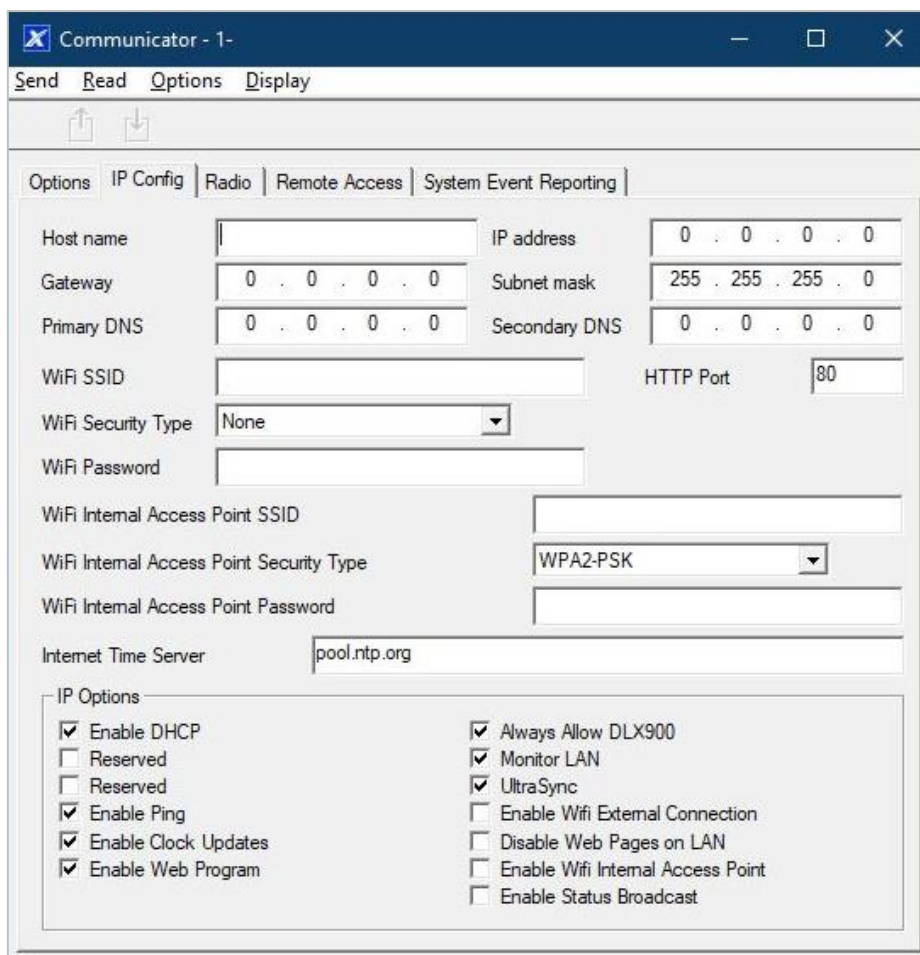
```
18. Channel Groups
```

Instructions

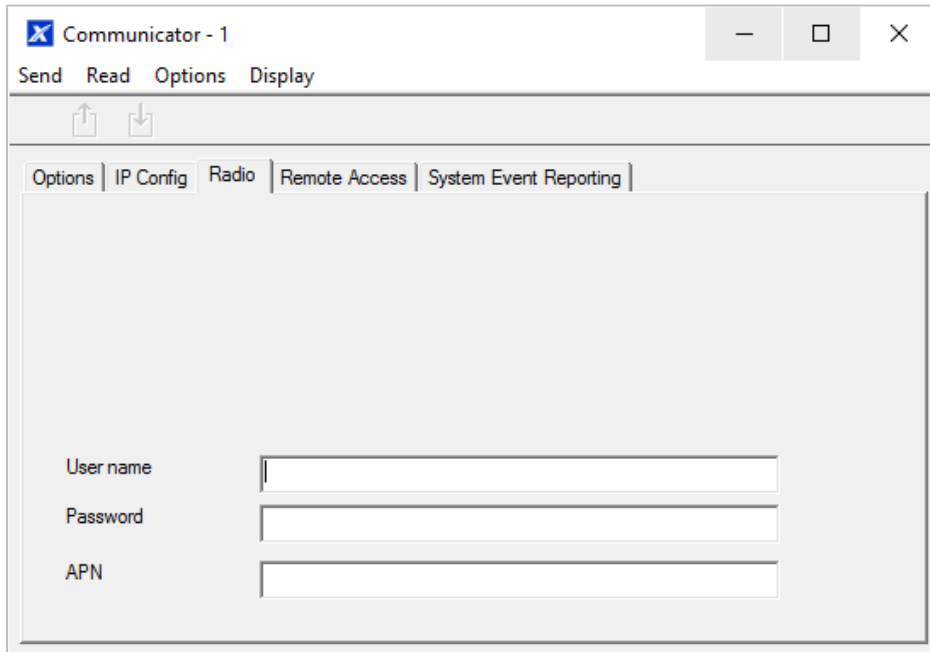
1. Open Communicator.



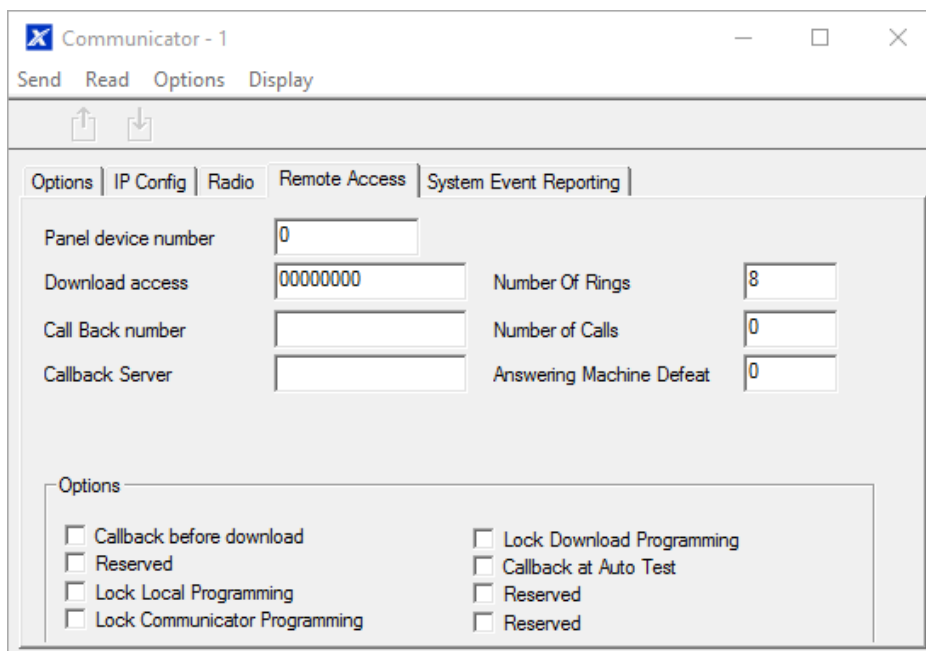
2. Select reporting options.
3. Select when you want xGenConnect to perform an automatic communication test.
4. Click IP Config.



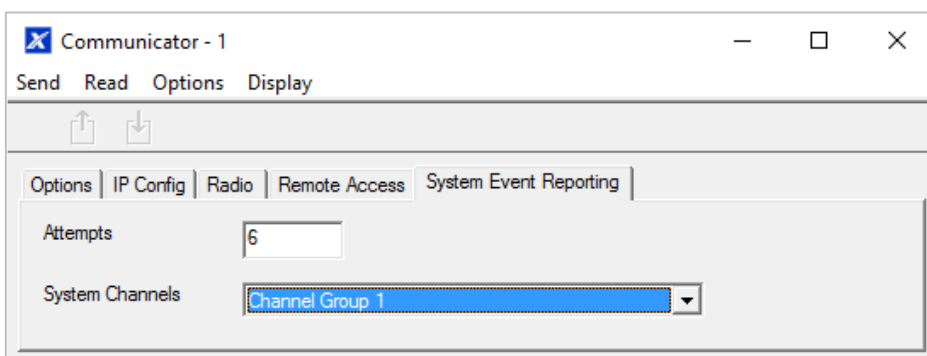
5. Edit IP settings for the xGenConnect system, if DHCP is enabled on the xGenConnect and a DHCP server is available, then this screen will automatically be filled in.
 - Enable Clock Updates: Will keep the time and date correct using the provided Internet Time Server, no manual adjustment will be needed 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.



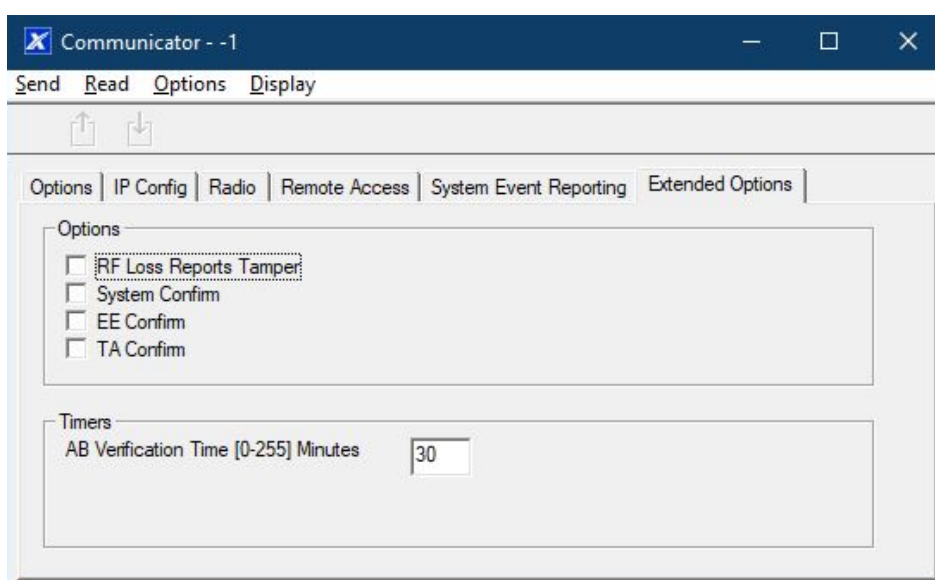
7. Click Remote Access



8. Edit Remote Access settings for the xGenConnect system.
 - Download Access Code: Gives access to DLX900 to access the xGenConnect panel programming.
9. Click System Event Reporting.



10. Click Extended Options.



- RF Loss Reports Tamper: A sensor loss of wireless supervision will report as tamper instead of trouble.
- System Confirm, EE Confirm, TA Confirm, AB Confirmation time: settings for AB alarm confirmation. See “AB Alarm Confirmation” on page 64 for details.

11. 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).

xGenConnect is connected to internet and has been allocated an IP address (see “Programming Instructions for Communicator” on page 127, IP Config).

Notes:

UltraSync provides a secure VPN connection to your xGenConnect system over the internet. You will need to provide your xGenConnect serial number, Web Access Passcode, and a valid Username and PIN code that exists in your xGenConnect 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

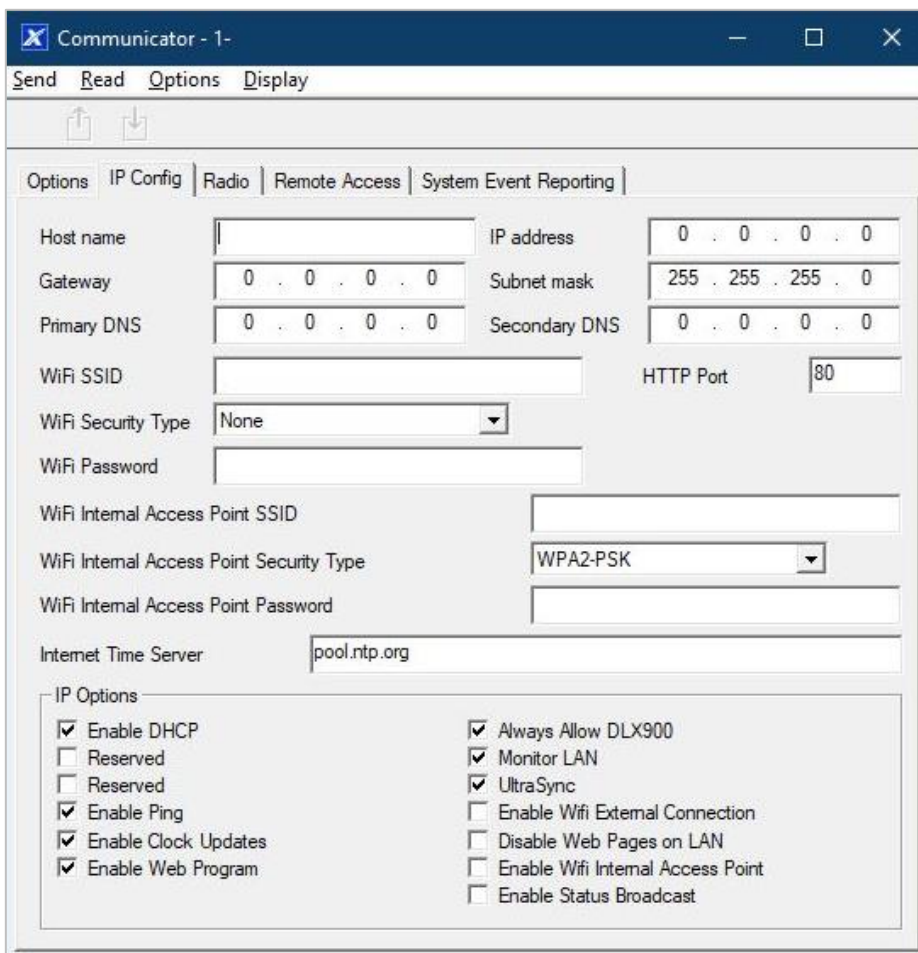
The Web Access Passcode is NOT needed for:

- Email services
- Web console over a local LAN connection

Once UltraSync is set up, you may connect to your xGenConnect 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

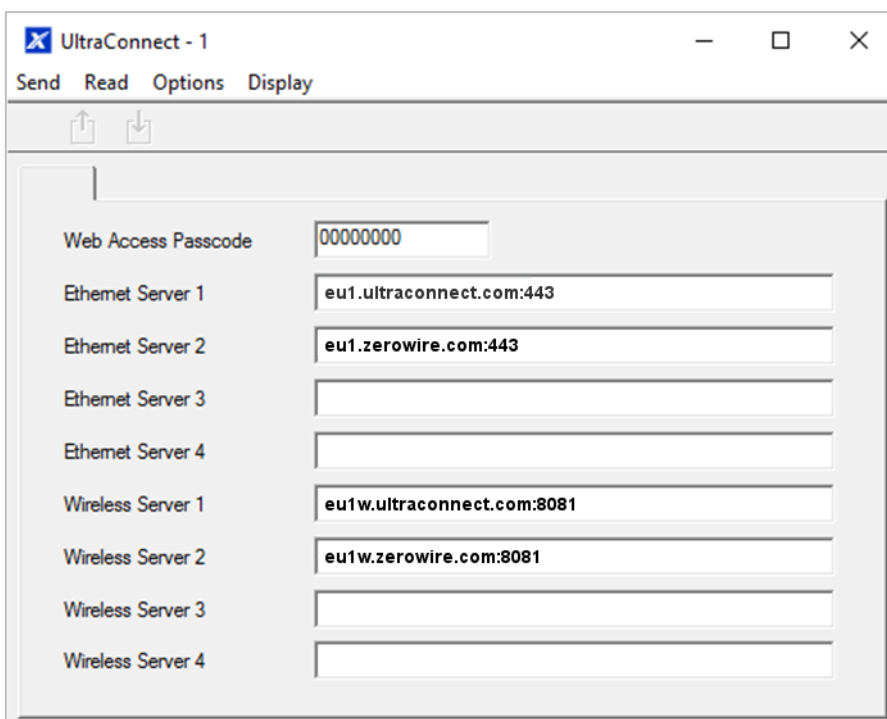
1. Go to Menu 6. Communicator > 3. IP Config.



The screenshot shows the 'Communicator - 1-' window with the 'IP Config' tab selected. The window has a menu bar with 'Send', 'Read', 'Options', and 'Display'. Below the menu bar are two arrows pointing up and down. The main content area has several tabs: 'Options', 'IP Config', 'Radio', 'Remote Access', and 'System Event Reporting'. The 'IP Config' tab is active and contains the following fields and options:

- Host name: [Empty text box]
- IP address: [0 . 0 . 0 . 0]
- Gateway: [0 . 0 . 0 . 0]
- Subnet mask: [255 . 255 . 255 . 0]
- Primary DNS: [0 . 0 . 0 . 0]
- Secondary DNS: [0 . 0 . 0 . 0]
- WiFi SSID: [Empty text box]
- HTTP Port: [80]
- WiFi Security Type: [None]
- WiFi Password: [Empty text box]
- WiFi Internal Access Point SSID: [Empty text box]
- WiFi Internal Access Point Security Type: [WPA2-PSK]
- WiFi Internal Access Point Password: [Empty text box]
- Internet Time Server: [pool.ntp.org]
- IP Options section with the following checked/unchecked boxes:
 - Enable DHCP
 - Reserved
 - Reserved
 - Enable Ping
 - Enable Clock Updates
 - Enable Web Program
 - Always Allow DLX900
 - Monitor LAN
 - UltraSync
 - Enable Wifi External Connection
 - Disable Web Pages on LAN
 - Enable Wifi Internal Access Point
 - Enable Status Broadcast

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



The screenshot shows the 'UltraConnect - 1-' window with the 'Options' menu open. The window has a menu bar with 'Send', 'Read', 'Options', and 'Display'. Below the menu bar are two arrows pointing up and down. The main content area has the following fields:

- Web Access Passcode: [00000000]
- Ethernet Server 1: [eu1.ultraconnect.com:443]
- Ethernet Server 2: [eu1.zerowire.com:443]
- Ethernet Server 3: [Empty text box]
- Ethernet Server 4: [Empty text box]
- Wireless Server 1: [eu1w.ultraconnect.com:8081]
- Wireless Server 2: [eu1w.zerowire.com:8081]
- Wireless Server 3: [Empty text box]
- Wireless Server 4: [Empty text box]

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 xGenConnect serial number, Web Access Passcode, and a valid Username and PIN code. The xGenConnect 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 xGenConnect 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 xGenConnect module.
- Check that the user permissions are currently valid.

See also “Appendix 2: App and Web Error Messages” on page 153.

Programming Instructions for Event Lists

Goal

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

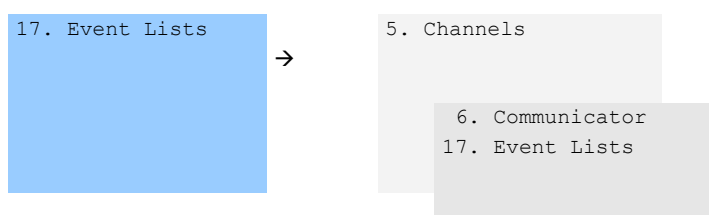
Pre-conditions

None.

Notes

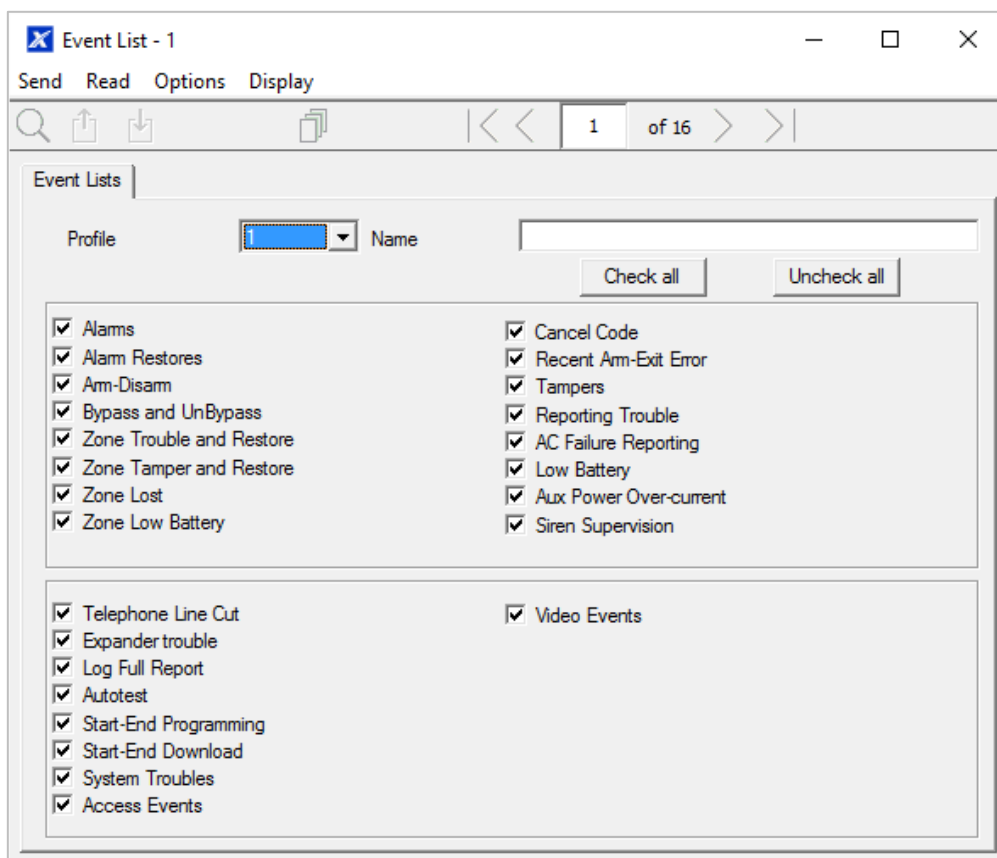
- If an event message is enabled in an Event List, then the Channel will attempt to deliver it. If an event message is not enabled on the Event List, the Channel will not attempt delivery even if the message has been sent to it.
- Event List set up for push notifications is automatically performed by 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.

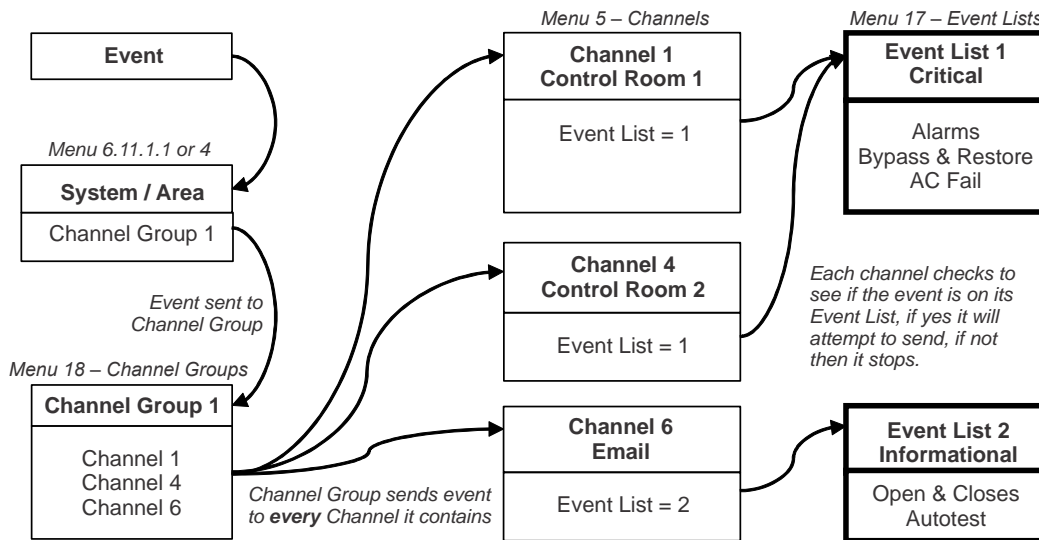
3. Check the events you want to include in the list.

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 127).

Event Lists must be programmed (see “Programming Instructions for Event Lists” on page 133).

Notes

- Partition Account Number will take priority over Account Number entered here for Zone events. If no Partition 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 xGenConnect 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.

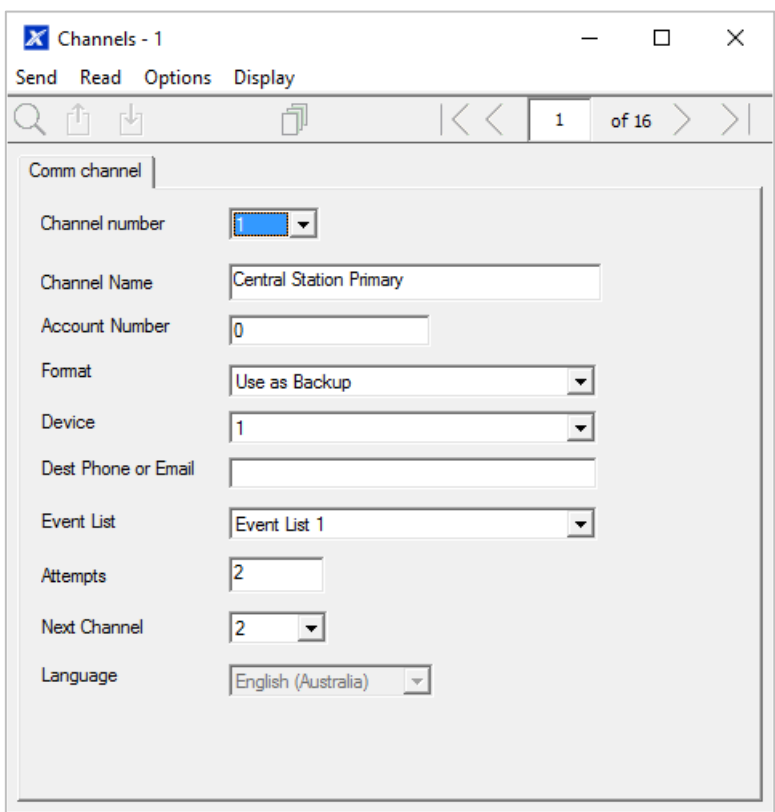
Programming Sequence



18. Channel Groups

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 xGenConnect 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

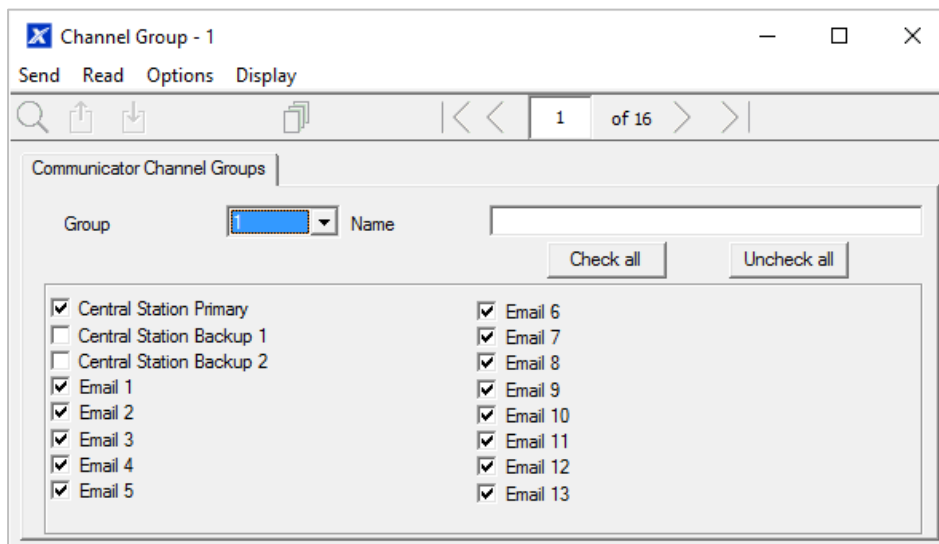
they on this Event List, if they are, then will be routed through this Channel. Events that arrive at this Channel which are not on this list will be blocked.

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 xGenConnect 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 xGenConnect will attempt to send it. If not, then xGenConnect 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

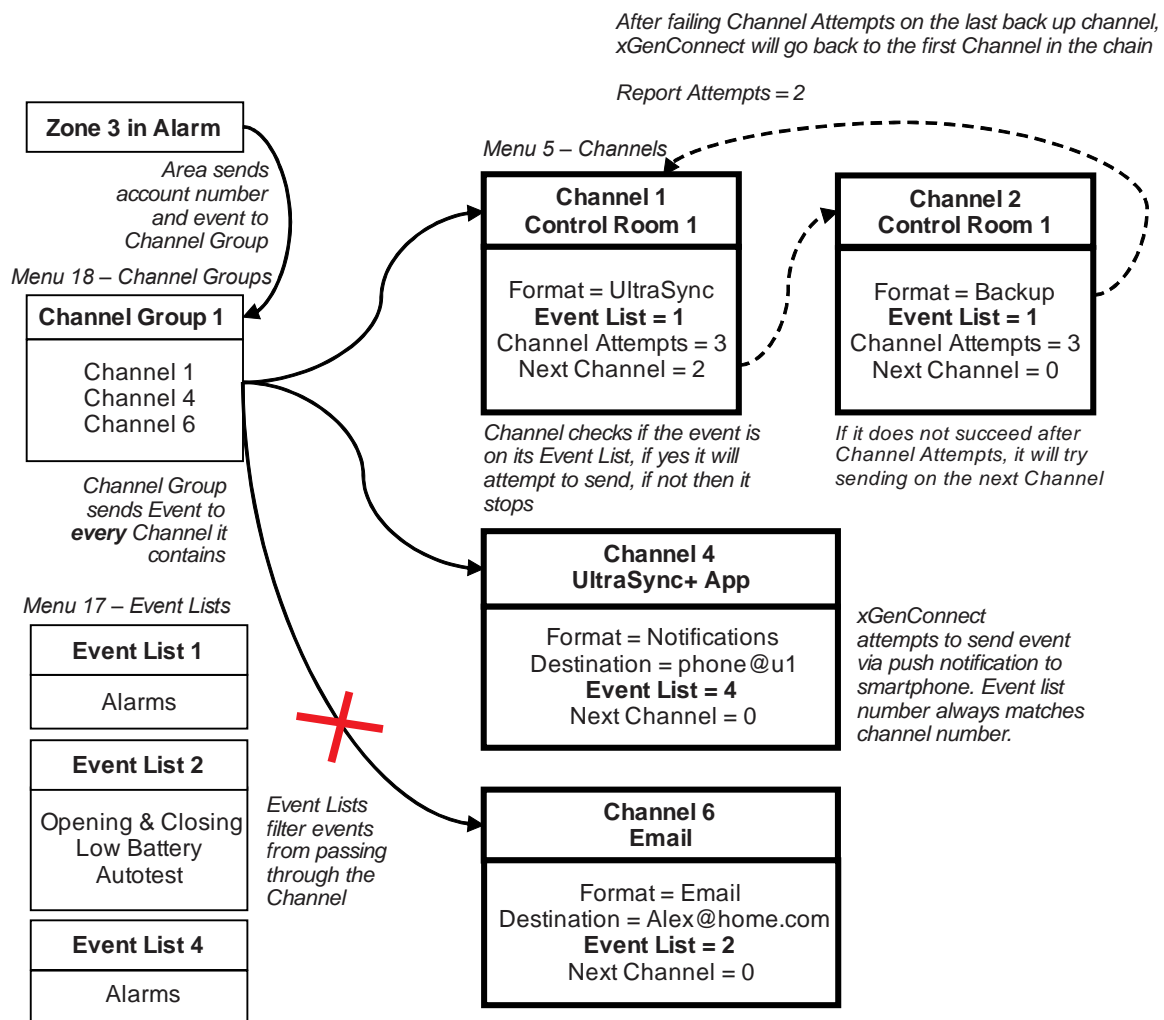
In this example we have multi-path, prioritised/selective event reporting via three reporting paths – one control room with backup, push notification to a smartphone, and an email address. These are grouped into “Channel Group 1”.

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, xGenConnect 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 xGenConnect will still deliver to this destination if Channel 1 cannot be reached. If Channel 2 was included in the Channel Group, then the control room will receive duplicate messages.

Next

Program your Partitions and Zones.

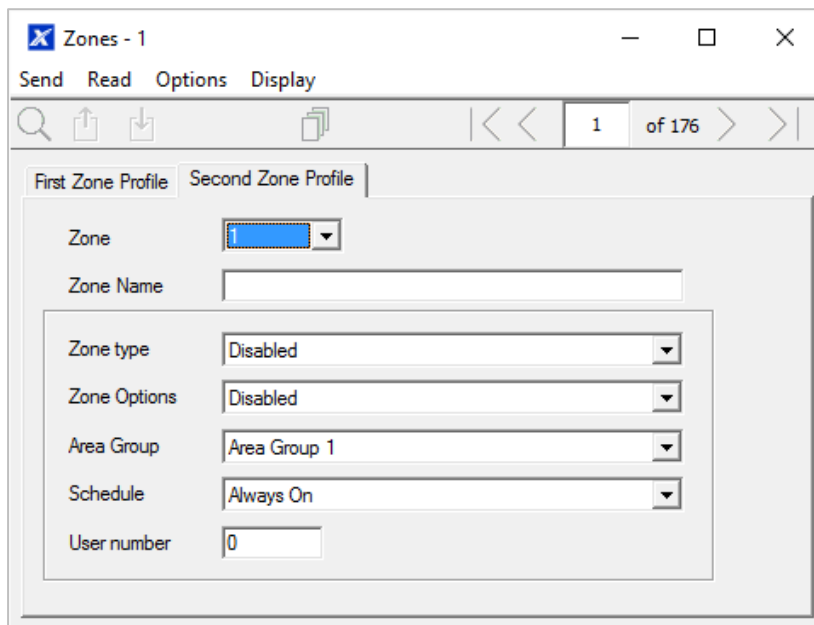
Programming Instructions for Zone Reporting

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 Partition Group (see “Programming Instructions for Zones” on page 108).

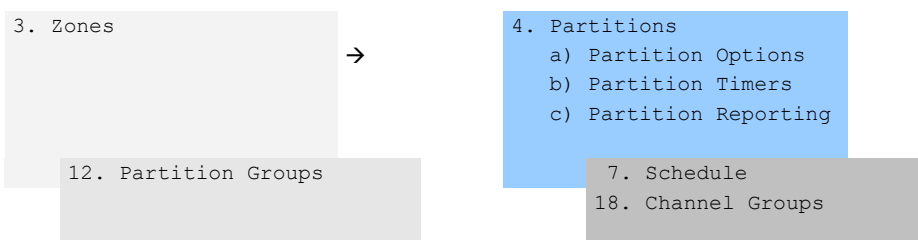


- Channels and Channel Groups must be programmed (see “Programming Instructions for Channels” on page 135).

Notes

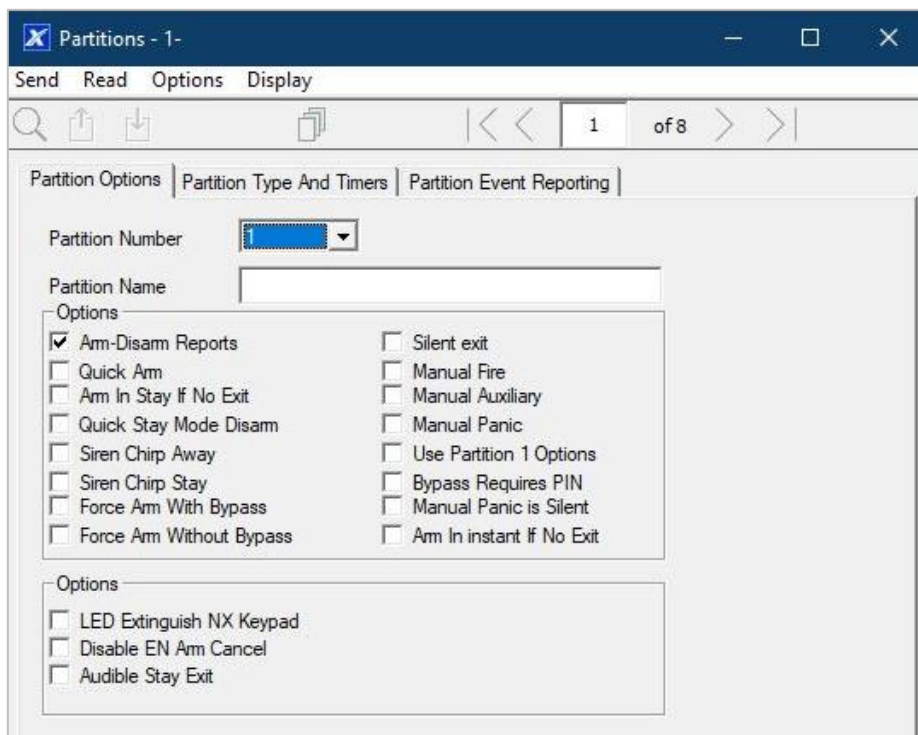
- Each zone may be allocated to multiple Partitions through a Partition Group.
- Events will be sent to the lowest numbered Partition in the Partition Group.
- A zone may have a Second Zone Profile, when this becomes active all events will be sent to the Partition Group programmed in the second profile.

Programming Sequence

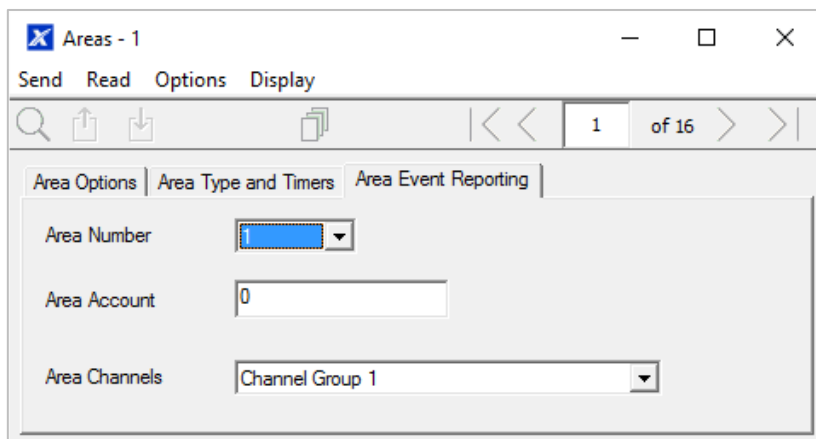


Instructions

1. Open the lowest Partition number for the Zone.



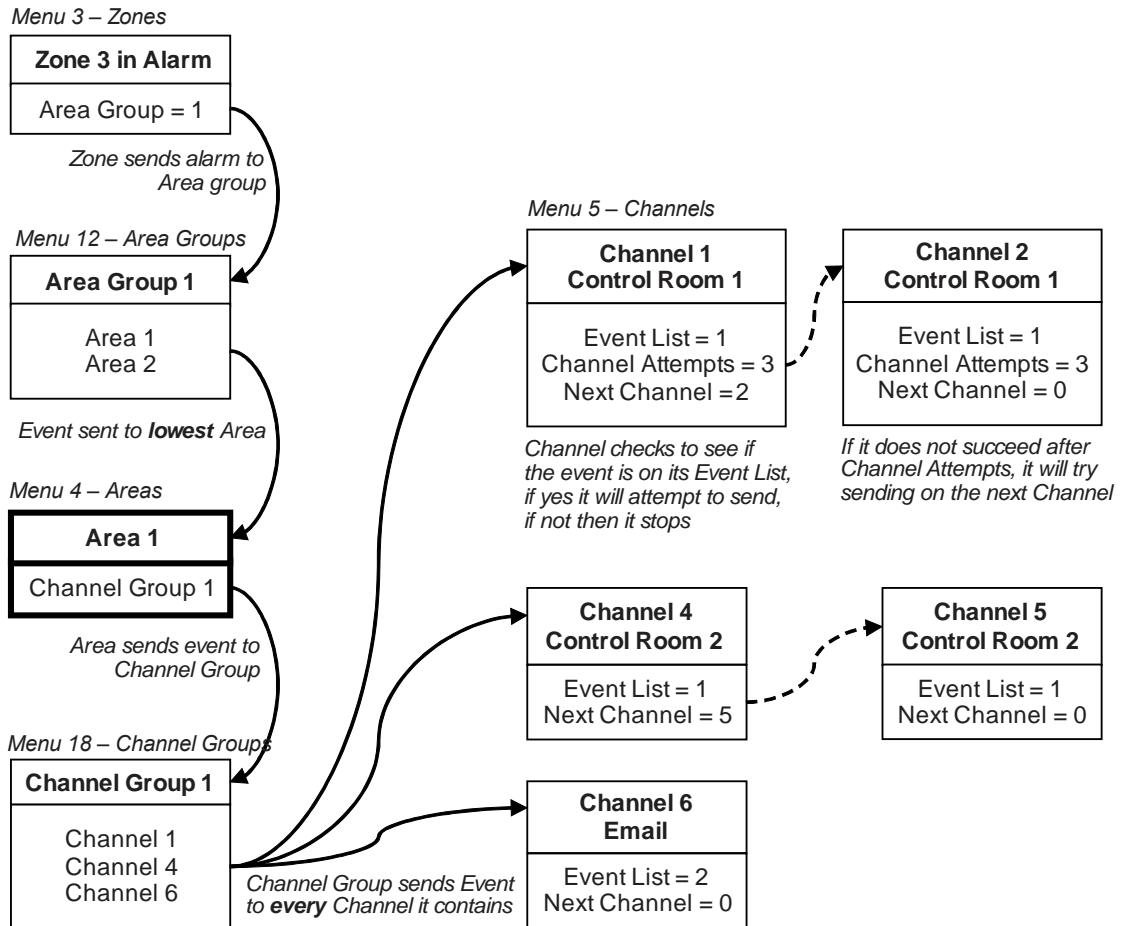
2. Go to Partition Reporting.



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

Done. All zones that are a part of that Partition 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 127).

Event Lists must be programmed (see "Programming Instructions for Event Lists" on page 133).

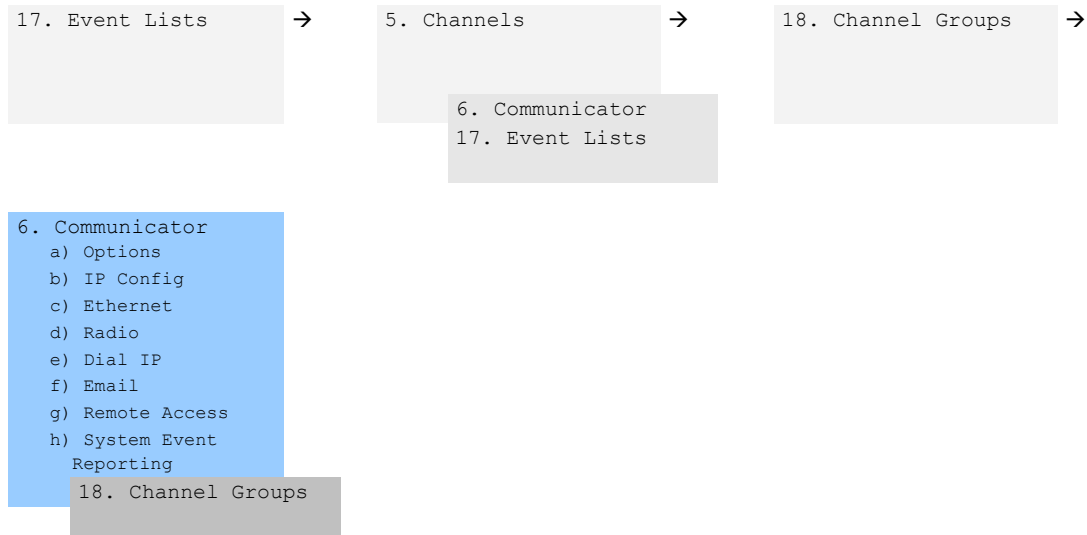
Channels and Channel Groups must be programmed (see "Programming Instructions for Channels" on page 135).

Notes

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

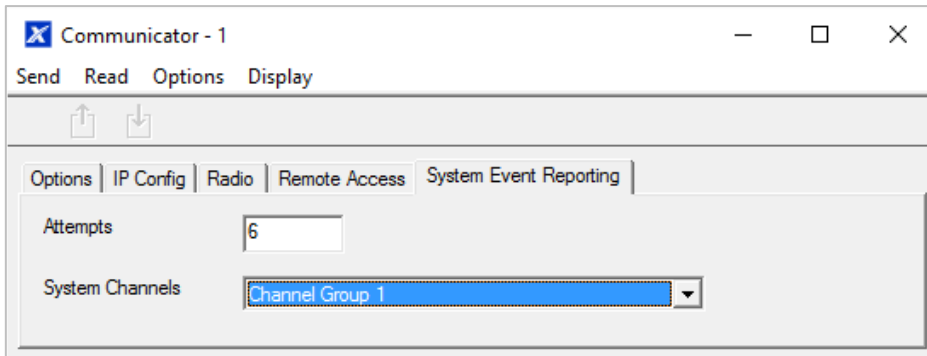
- Take note of the Sequence Attempts under Communicator > System Event Reporting (6.11.2). This is the number of times xGenConnect will attempt the sequence of Channels you set up in this section.

Programming Sequence



Instructions

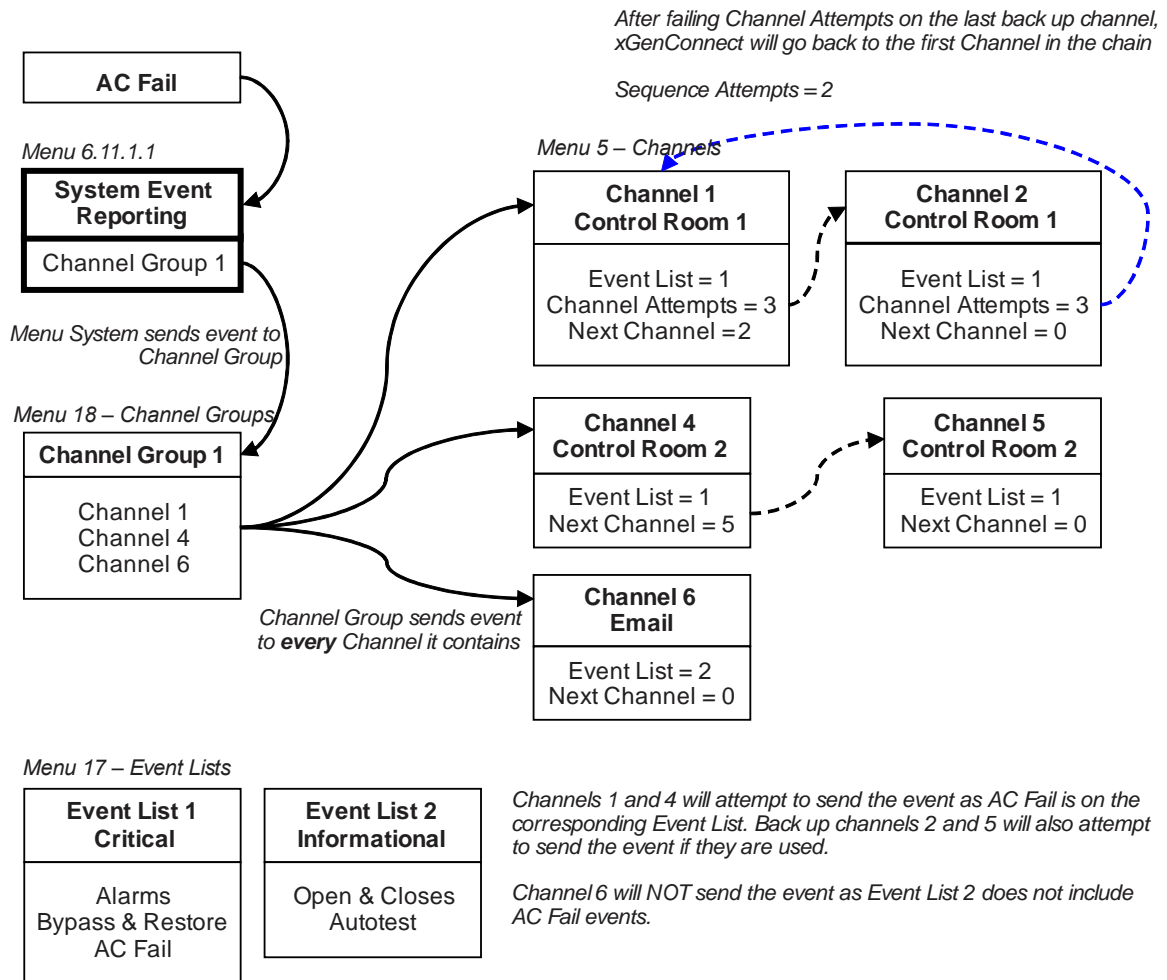
1. Go to Communicator, System Event Reporting.



2. Select a Channel Group.

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

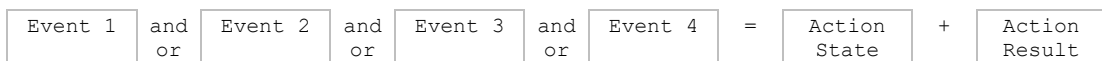
Example



Programming Instructions for Actions

Goal

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



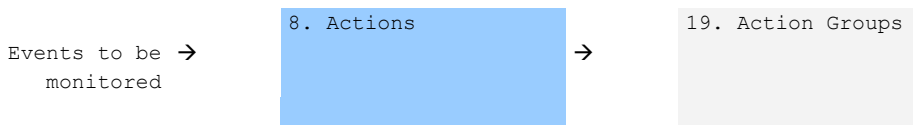
Pre-conditions

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

Notes

- See *xGen 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



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 Partitions 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.

The screenshot shows a software window titled "Actions - -1" with a menu bar containing "Send", "Read", "Options", and "Display". Below the menu bar is a toolbar with search, copy, and navigation icons, and a page indicator showing "33 of 64". The main area has two tabs: "Event" and "Result", with "Result" selected. The "Result" tab contains the following fields:

- Action Number: A dropdown menu showing "Action 33".
- Result Category: A dropdown menu showing "Zone Results".
- Result Type: A dropdown menu showing "Disabled".
- Start: A text input field containing "0".
- End: A text input field containing "0".
- User Number: A text input field containing "0".
- Options: A group box containing two checkboxes: "Log Trip" (unchecked) and "Log Restore" (unchecked).

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

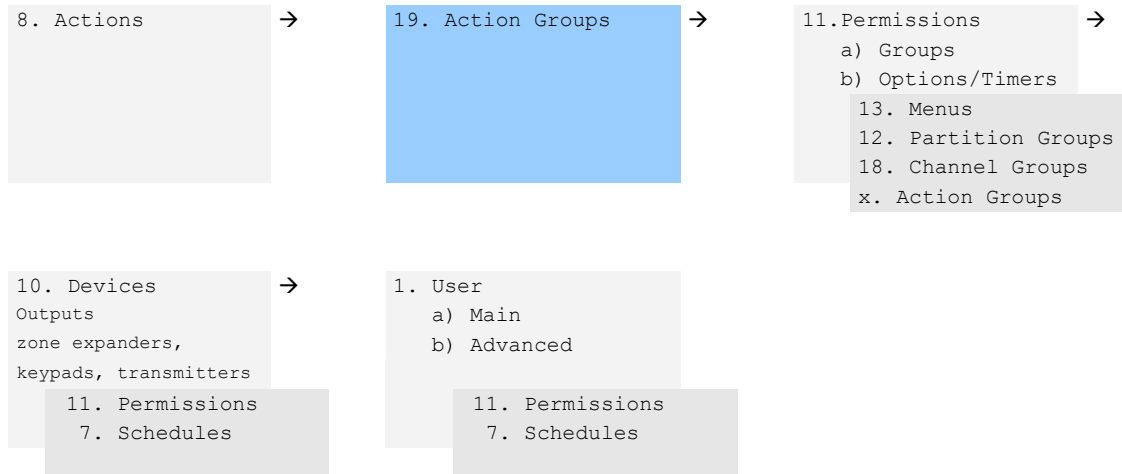
Program the actions you want to use.

Notes

- See *xGen 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 NXG-18xx.
- Permissions control what actions a User or Device has access to.

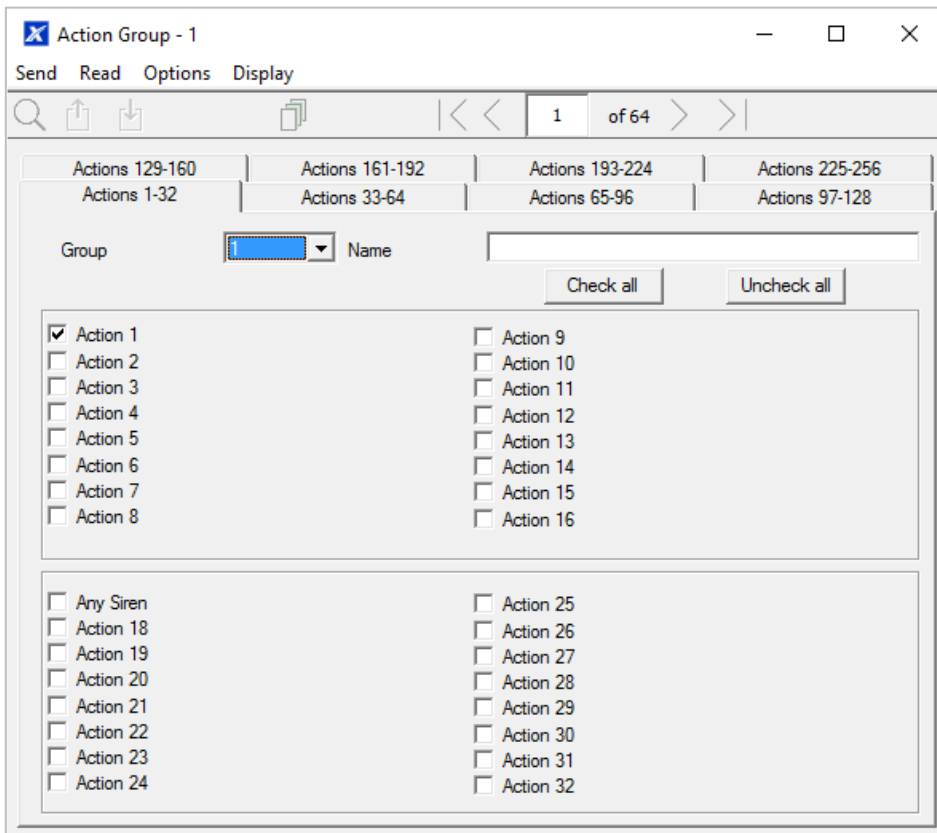
- Both the User AND Device need to have access to the desired Action for it to be displayed on an NXG-18xx screen.

Programming Sequence



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.

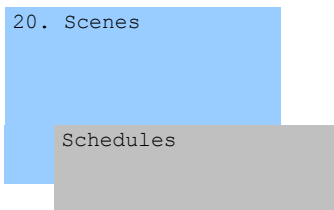
Pre-conditions

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

Notes

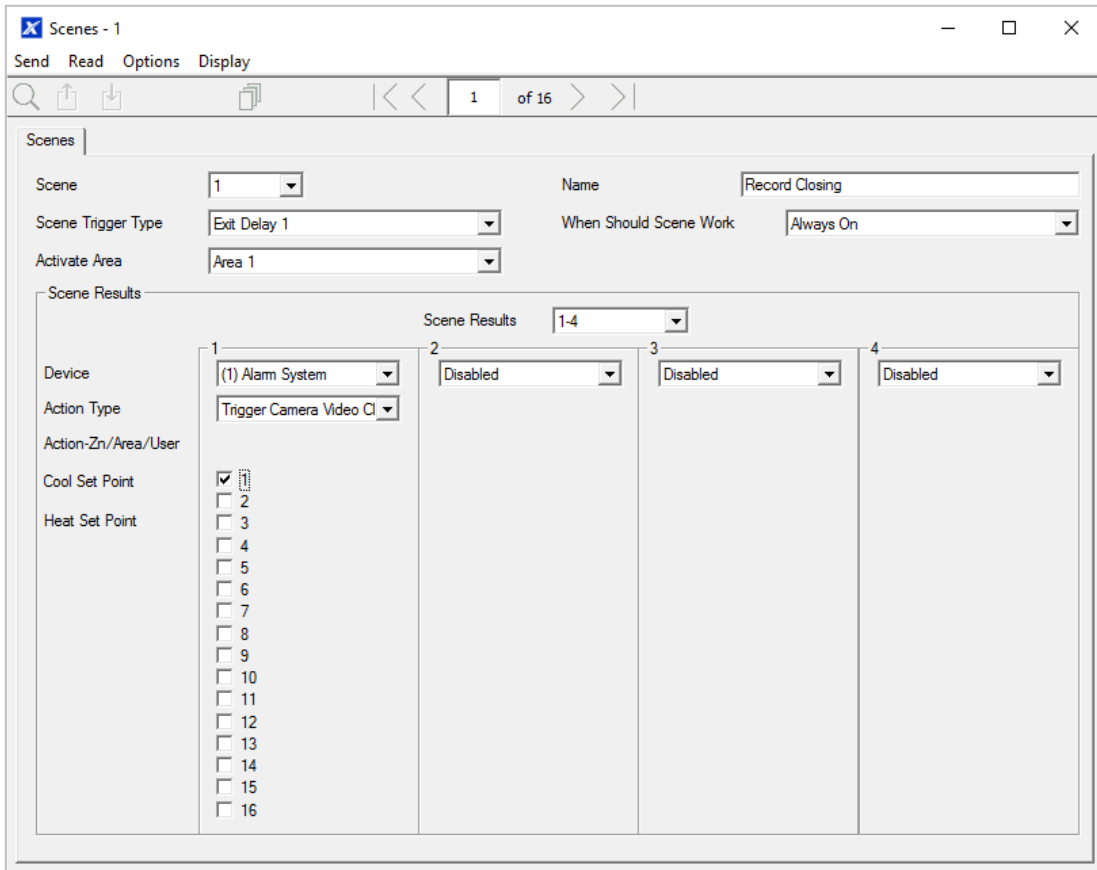
User 99 will be reported for alarm system control events.

Programming Sequence



Instructions

1. Open Scenes.



2. Select Event Type and the Partition.

3. Select the Schedule that will determine when this Scene is active.

4. Now program the sequence of actions that you want to happen.

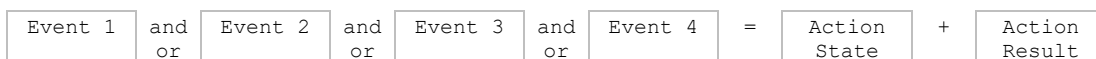
Example

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

Programming Instructions for Outputs

Goal

Turn an output on or off according to an Action.



Pre-conditions

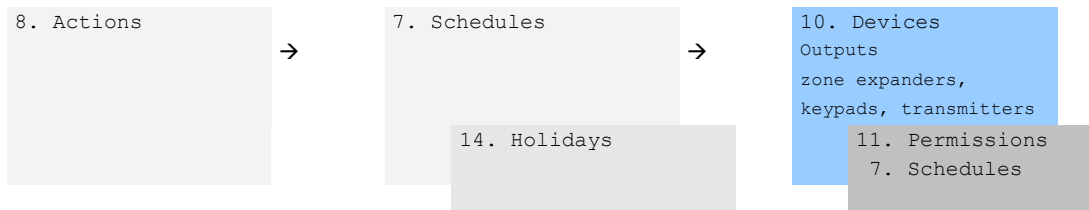
Program the Action and any associated components.

Notes

- See *xGen 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 xGenConnect are controlled by monitoring an Action State, no Action Result needs to be programmed.

Programming Sequence

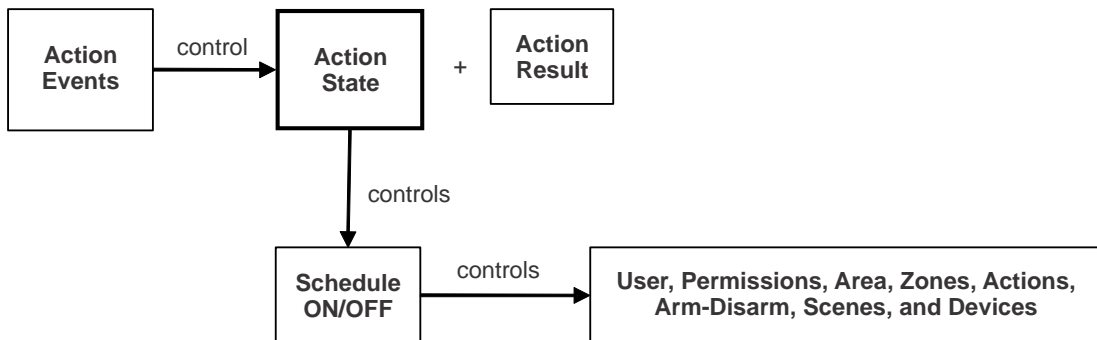


Instructions

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, Partitions, 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.

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 999 to the Central Monitoring Station. SOS functions also report as user 999.

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 xGenConnect 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.

Partition Number. Partition Name

- Is on in the away mode: This Partition is armed in the away mode.
- Is on in the stay mode: This Partition is armed in the stay mode.
- Is ready: This Partition is secure and ready to be armed.
- Is not ready: This Partition is NOT ready to be armed, a zone is not secure.
- All Partitions are on in the away mode: All Partitions in this multi partition system are armed in the away mode.
- All Partitions are on in the stay mode: All Partitions in this multi partition system are armed in the stay mode.
- All Partitions are ready: All Partitions in this multi partition system are secure and ready to be armed.

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 xGenConnect 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: NetworX Modules Compatibility

Module part number	Description	Supported by xGenConnect	Remarks
NX-7002N-V3	Plug on GSM module for NX-V3 control panels	No	Use NXG-7002
NX-535N	Voice speech module	No	
NX-535N-V3	Plug on Voice speech module for NX-V3 control panels	No	
NX-1048-R-D-EN	Multilingual LCD keypad, wireless 868 MHz GEN2, white, incl. batteries	No	
NX-1048-D-EN	Multilingual LCD keypad, wired, white	Yes	No programming, limited user functions
NX-848E	Transceiver in housing for mounting out of the box	Yes	Use NXG-868 for new installations Requires NX keypad for programming
60-904-43-48Z	48 zone wireless receiver, 433.92 MHz (NX-448E)	Yes	Use NXG-433 or NXG-9-RF-LB for new installations
NX-1xx	8 zone LED keypad without door	Yes	No programming, limited user functions
NX-13xx	16 zone LED design keypad with removable door	Yes	No programming, limited user functions
NX-15xx	16 zone LED vertical keypad with removable door	Yes	No programming, limited user functions
NX-1820E-EUR	Touch screen keypad, multi-lingual	No	Use NXG-1820-EUR or NXG-183x-EUR
NX-148	LCD design keypad with removable door	Yes	No programming, limited user functions
NX-587E	Virtual keypad	No	
NX-216E-EN	16 zone expander module for NX-8 and NX-8E, EN approved	Yes	
NX-508E	Output module with 8 open collectors	Yes	Requires NX keypad for programming
NX-507E	Output module with 7 relays and 1 OC	Yes	Requires NX keypad for programming
NX-534E-AL	Two-way voice module, including 3510	No	
NX-540E	Telephone interface module	No	
NX-320-I	Smart power supply and bus extender	Yes	Use NXG-320 for new installations Requires NX keypad for programming
NX-584E	Home automation module with two-way serial port interface	No	

Module part number	Description	Supported by xGenConnect	Remarks
NX-586E	Direct connect interface for DL900 Up and Download software	No	
NX-590NE	TCP/IP Internet/Intranet interface module	No	
NX-1701E	Proximity card reader	Yes	Requires NX keypad for programming
NX-1750	ProxPad proximity reader	Yes	Requires NX keypad for programming
NX-2192E-EUR	PinPoint Bus Interface Card	No	

See also “EN 50131 and INCERT certified components” on page 15.

Appendix 4: 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. Partition Group
 4. Schedule Number
 5. User Number
 4. Second Zone Profile
4. **Partitions**
 1. Partition Number
 2. Partition Name
 3. Partition Entry-Exit Times
 4. Partition Options
 5. Partition Timers
 6. Partition Type Settings
 7. Partition 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
 4. Tablet Keypads
 1. Name
 2. Serial Number
 3. Partition Group
 4. Keypad Options
11. **Permissions**
 1. Permission Number
 2. Permission Name
 3. Control Groups
 4. Permission Options
 5. User Timer Options
12. **Partition Groups**
 1. Partition Group Number
 2. Partition Group Name
 3. Partition 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
23. **UltraSync**
 1. Web Access PIN
 2. Ethernet Server 1
 3. Ethernet Server 2
 4. Ethernet Server 3
 5. Ethernet Server 4
 6. Wireless Server 1
 7. Wireless Server 2
 8. Wireless Server 3
 9. Wireless Server 4

Appendix 5: NXG-183x Keypad Features

Navigating through “Program” menu using NXG-183x-EUR keypad

NXG-183x-EUR allows the installer to configure all the configuration parameters exposed by the panel or other peripheral devices. In order to enter programming menu, one needs to press the ENTER key on the keypad, then enter the installer PIN followed by ENTER.

Once entered the installer programming menu, “Program” appears as the first submenu. The menu structure is identical to the Advanced menu structure from the panel web page. See also “Appendix 4: Advanced Menu Tree” on page 156.

Navigation through the Program menu is similar to operation within the user menu, with some additional extensions:

- Top line shows the full path of the current location (for example, Zones / Zone Number 1 / Zone Name, etc.). The path is usually too long to fit the screen – in such case it can be scrolled back and forth by pressing “i” key.
- If the current location is within the menu tree of enumerable objects (for example, within Zones, Partitions, Channels, Schedules, etc.), then the object number (for example, Zone number) can be instantly changed by either one of the following methods:
 - Pressing A button allows the installer to specify the new object by entering a number.
 - Pressing Left (4) or Right (6) buttons allows the installer to increase or decrease the current object number within the allowed limits.

Wireless sensor learning

There are two sensor learning modes:

- Single sensor learning.

To program a single sensor, go to the menu Program / Devices / Interlogix Transmitters, and select the sensor you want to learn. Enter value “1” in the transmitter serial number field, and then press Enter.
- Multiple sensors learning.

To program multiple sensors, go to the menu Program / Devices / Interlogix Transmitters, and select the starting number for multiple sensors learning. Enter value “2” in the transmitter serial number field, and then press Enter.

The keypad will show “Learn Mode Active / Activate Sensor” message.

Activate the wireless sensor. Refer to the appropriate sensor manual for information.

When a sensor is tripped for learning, the keypad shows “New Device Found / Number: X, SID: Y”. The sensor Y is now enrolled as a transmitter number X.

In the single sensor learning mode, the information disappears after 10 s, and you return to the Interlogix Transmitters menu.

In the multiple sensors learning mode, another sensor can be tripped and learned in the position X+1.

The multiple sensors learning mode will stop when the transmitter address reaches the limit for the particular control panel model, or when the Cancel button is pressed.

Note: Ensure that the particular device is enrolled in the proper transmitter number range, for example, in the NXG-8 panel variant, sensors must be enrolled within the range 1 to 48, and keyfobs must be enrolled within the range 49 to 64. Trying to enroll a device in the wrong transmitter range will cause an error “Invalid Device Type”.

Deleting wireless sensor

To delete a single sensor from the system, go to the menu Program / Devices / Interlogix Transmitters, and select the sensor you want to remove. Enter value “0” in the transmitter serial number field, and then press Enter.

The sensor is now permanently removed from the system.

Restoring factory defaults

Default settings of the panel or peripheral devices can be restored by pressing D button in the relevant System Device menus of the Program menu:

- The Panel factory defaults can be restored by pressing D button at the menu location:

/ Devices / System Devices / Control / Device number 1

This is equivalent to the operation Default ALL performed on the NXG-1820-EUR keypad.

- The factory defaults of a peripheral device can be restored by pressing D button at the menu location:

/ Devices / System Devices / TYPE / Device number X

where TYPE can be Keypad, Zone Exp, Output Exp, Power Supply, and X is the device number.

For example, pressing D button at the menu location “/ Devices / System Devices / Keypad / Device number 2” will restore the factory defaults of the 2nd keypad in the system.

Using this method, one can restore the factory defaults of the NXG-183x-EUR keypad itself.

In all the cases, the keypad asks for confirmation before loading the factory defaults in order to avoid accidental changes.

Logo customization

The NXG-183x-EUR keypad can display a company logo on the display when both the Enable Screensaver and the Show Logo options are enabled in the keypad settings. The logo will be shown only when the keypad screensaver mode is active.

Creating a customized company logo requires the following:

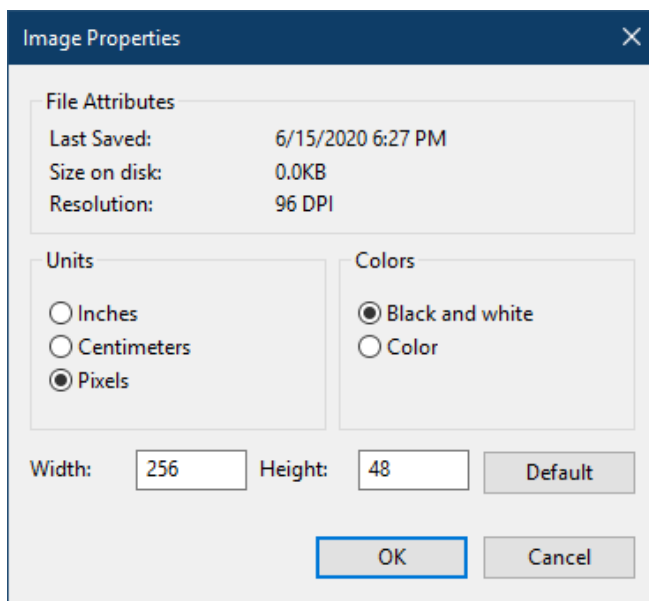
- Computer or laptop with application to edit and create .bmp files (for example, Microsoft Paint)
- DLX900 v5.15 or higher to create .MIF3 file out of the .bmp file
- USBUP-EUR-V2 (or DLX900) to flash the NXG-183x keypad with the company logo file (.MIF3)

The company logo file can be created by using a computer and a simple application like MS Paint. In order to create a company logo file and upload this file onto the keypad, follow these steps:

1. Create an image using any application capable of editing and saving .bmp files. In example, use Microsoft Paint on a Windows computer or laptop.

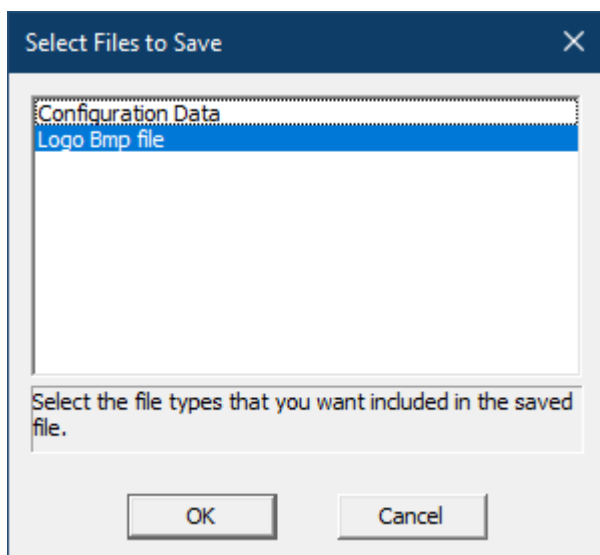
The image must be monochrome (black and white), no colours or shades of grey are supported. The image size should not exceed 256 x 48 pixels (full screen size of NXG-183x).

As an example, the picture below shows the file properties in MS Paint, with the relevant options properly set:



2. Save the prepared image as a black-and-white file type with .bmp extension. For MS Paint, select file type Monochrome Bitmap (*.bmp, *.dib).
3. Open DLX900 software (version 5.15 or higher), connect to the system or just open the DLX900 account for which there is the NXG-183x-EUR keypad and for which you want to upload the new company logo file.
4. Go to Devices / Device Info / Keypad. Select the NXG-183x keypad.

5. Click Create file button in USBUp section. Next, select Logo Bmp file option in the component selection window (see figure below). Press OK.



6. The Input file selection window appears. Select the .bmp file saved in step 2.
7. Resulting file selection window appears. Provide the location and name for a resulting .mif3 file. Click Save.

The resulting MIF3 file can now be used to flash one or more NXG-183x keypads with the customized company logo.

Loading of the file can be done either using the USBUP-EUR-V2 upgrade tool, or using DLX900 software and the Update Device button. In both cases, upgrading the company logo .MIF3 file uses the same procedure as upgrading the firmware of the device.

Configuring cards or tags using the NXG-1832 / NXG-1833-EUR keypads

A master user has access to the User Cards menu from an NXG-1832 / NXG-1833-EUR keypad with built-in Mifare reader.

The User Cards menu allows to add, delete, modify, and view a user card or tag assigned to an existing user.

The menu also contains the method to assign multiple cards to users in fast and convenient way. For more details, see *NXG-183x Series Keypad User Guide*.

Glossary

A-Alarm	A-alarm active (unverified alarm), reset after disarm or expiration of AB timer and no B-alarm.
Action	An action allows the system to perform automation functions. These can monitor the status up to 4 input conditions called Action Events, change state (Action State), and perform a function (Action Result) such as arming a range of partitions.
Action group	An action group is one or more actions that can be accessed by a device or user. They are assigned to a user or device via permissions.
Alarm	The state of a security system when a device connected to a zone is activated and the condition of the partition is such that activation should be signalled. For example, a door or window is being opened, causing a siren to sound.
Alarm control	The control over alarm functions.
Alarm reporting	A procedure to transmit alarm events or other events to the central station by means of a communicator and a set of rules called a protocol. Alarm reporting can also be provided my means of push notification towards an end-user smart phone
Arm	To turn your security system On.
Armed	The condition of a partition where a change in the status of any zone (from normal to active) causes an alarm. A partition or premise is only armed when it is unoccupied. Some zones (like vaults) can remain armed continuously.
Automatic arm-disarm	Automatically arm and disarm partitions by a specific user according to a specified schedule. The partitions armed and disarmed will be the ones that the user has access to via their permissions.
Away mode	To turn your security system on when you are leaving the premises.
B-alarm	B-alarm active (verified alarm), reset after disarm.
Burglar alarm	An alarm triggered by a security device like a motion detector or door contact, indicating someone has entered without authorized access. May also be referred to as an intrusion alarm.
Bypass	Zones can be temporarily disabled so they will not be monitored by the security system. For example, an interior door is left open, bypass it to temporarily ignore it and allow arming of the security system. Bypassed zones are not capable of activating an alarm. Zones will return to normal operation when the system is disarmed. This prevents unintentional permanent disabling of a zone.
Card	A medium holding credentials by which a user can be identified in a security system. A card is associated in the user configuration to a user by which the access rights are defined. Also referred to as a badge. Cards are used on readers or keypads with built-in readers.
Central station	A company to which alarm signals are sent during an alarm report. Also known as Central Monitoring Station (CMS) or Alarm Receiving Centre (ARC).
Channel	A channel is a communication path for events to be sent from the control panel to a selected destination. A channel has an associated event list which contains the events it is allowed to forward on.

Channel group	A channel group is one or more destinations for event messages to be sent to. When a message is sent to a channel group, it is sent to all the channels that it contains. It forms the basis of multi-path reporting.
Chime group	All the zones that will activate chime, when in chime mode.
Chime mode	An operational mode that will emit a ding-dong sound at the keypad when specific zones are activated.
Closed	A zone in a normal state is “closed”. The security system monitors each zone for changes in state from closed to open, and can respond with certain actions such as sounding the siren. For example, a reed switch on a front door may change from a closed state to an open state when the door opens.
Communicator	An electronic device that allows the control panel to transmit alarms and other events to a central station. It sends event messages to the specified destination including details such as where the event originated from and the type of event. The receiver will then log the time and date when it receives the event. For example, Alarm from Zone 2 in Partition 1 at 3:00am on 5/5/2022 from Account 1234.
Control panel	An electronic device that is used to gather all data from sensors in the premises. Depending on programming and status of partitions, it generates alarm signals. If required, alarms and other events can be reported to the central station. It stores all programming, may provide network or other connectivity options for reporting, provides physical terminals for connecting power, backup battery, zones, siren, strobe, outputs, and system bus for expansion devices.
Cursor	A flashing underline character on the liquid crystal display (LCD) that indicates where the next character entered on the keypad will appear.
Disarm	To turn your security system Off.
Disarmed	The condition of a partition when it is occupied, and normal activity does not set off an alarm.
DLO (Door Left Open)	Door kept open for the time longer than configured.
Door contact	A magnetic contact used to detect if a door or window is opened.
Door control	The control of entry to, or exit from, a security area through doors.
Door group	Door groups specify when access to a specific door is granted. Door groups are assigned to users. Each Door group may have a different time period (schedule) when access to the door may be granted.
Door shunt	Prevents from generation of intrusion alarm if the door was opened legitimately.
Dual	Dual detector. A security device used to detect intruders in a certain part of a partition or premises. The technique used is based on two techniques like PIR and RADAR or PIR and Ultrasonic.
Duress	A situation where a user is being forced to breach the system security (for example, forced at gunpoint to open the door). The security system duress facility allows a signal to be activated (for example, notification to a central station) by the user. This is done by entering a duress PIN.
Duress code	A predetermined user PIN that will arm / disarm the security system whilst sending a special code to the central monitoring station indicating the user is entering / leaving the premises under duress. Only applicable on monitored systems.

Engineer	Personnel from an installer that can install and service the control panel.
Entry delay	The time allowed to disarm your security system after the first detection device has been activated.
Event	Events are messages that are sent by the security system due to system or partition conditions. These include partitions in alarm, opening and closing, zone bypass, low battery, tamper, communication trouble, and power issues.
Event list	Event lists contain events that a channel is allowed to send to the specified destination. If a channel receives an event that is not in the associated event list, then the channel will ignore the event.
Exit delay	The time allowed to exit the premises after the security system is armed.
Fire alarm	An alarm triggered by fire or smoke detectors indicating a fire.
Fob	See keyfob.
Forced arming	An option that permits arming even when there are open zones. Generally assigned to zones that cover the security system (for example, motion zones, front door reed switches), allowing the user to arm the security system without the need to wait for those zones to be closed.
Forced door	Door opened without valid permission
History	A list of past alarm, door control, video, and other system events stored in memory that can be viewed from a keypad, from the application, or through DLX900 connections.
Hold-up	A silent alarm that is triggered by a hold-up button. Normally it does not trigger any siren, only sends a message to a central station. Sometimes also referred to as Panic button.
Installer	A company that installs and services security equipment.
Key switch	A device using a switch to arm or disarm partitions. The switch needs a key to switch.
Keyfob	A personal wireless device, which is used to perform programmed functions, for example, arm or disarm partitions.
Keypad	A device that is the user interface for security options for partitions or for access points (doors). The keypad can be a console (keypad used to program the control panel, perform user options, view alarms, etc.) or any other device that can be used to perform security function, such as arm or disarm partitions, open doors, etc.
LCD	Liquid crystal display. The part of a keypad where messages are displayed.
Local alarm	An alarm that is signalled only within premises and occurs when a partition is occupied. The circumstances that cause a local alarm may be checked and rectified by personnel on site and it is therefore unnecessary for the alarm to be reported to a central station.
Master code	A PIN that is used by a user to arm or disarm the security system. Its main feature is the ability to create, alter, and delete user PINs. Can also be used as a function code for all features.

Menus	<p>Security system has a large range of features sorted into various menus such as Users, System, and Zones. Each menu item can be seen when using the Web Server or the UltraSync+ app.</p> <p>Menus are used to restrict what is displayed by a device and what features a user has access to.</p>
Monitored	A security system that is configured to send all alarm signals to a central monitoring station.
Nuisance alarm	An alarm that is triggered by a security device, without any burglar. It could be caused by open windows, pets, or incorrect projection of security equipment.
Online / offline	Operational/non-operational. A device may be offline due to a malfunction in the device itself or it may be disconnected from the control.
Open	A detector which is triggered will turn the zone to open. The security system monitors each zone for changes in state from closed to open and can respond with certain actions such as sounding the siren. For example, when a PIR zone detects movement, the zone will change from a closed state to an open state.
Output	Outputs on the control panel can be connected to a siren and strobe, and activate when an alarm condition occurs in the system.
Panic button	See hold-up.
Partition	Zones are grouped into partitions which can be secured independently from each other. This allows you to split your security system into smaller components that can be separately managed. For example, your system can be divided into an upstairs partition and downstairs partition.
Partition group	A partition group is one or more partitions that can be accessed by a device or user. They are assigned to a user or device via permissions.
Perimeter	Typically, this refers to zones located around the boundary of the protected partition such as zones on doors and windows, and excludes interior motion zones.
Permission	A permission includes a list of features a user or device is allowed to access. This includes programming menus, partitions, reporting channels, actions, reporting options, access control options, special options, and special timers.
PIN	A 4 to 6 digit number given to, or selected by, a user. It is necessary to enter a PIN on a keypad as a prerequisite to perform most security system options. In the system configuration the PIN is associated with a user number, which identifies the PIN holder to the system.
PIR	Passive infrared detector. A security device used to detect intruders in a certain part of a partition or premise. The technique used is based on infrared detection.
Profile	Each user can have up to four (4) permission profiles. Each profile contains a set of permissions and a corresponding schedule. This allows advanced user programming and provides specific access to different features of the security system during specific dates/time. With advanced programming, profiles can be enabled or disabled in response to system conditions.
Quick arm	An option that allows you to turn on (arm) the security system by pressing the Away or Stay button on the keypad or UltraSync+ app.

Reader	A device used for door control that can read cards to allow access. May be integrated into a keypad.
Reporting	See Alarm reporting.
RTE (Request-to-Exit zone)	A zone that is programmed to open a door using a button or motion detector. Used to allow users to exit without using the door reader. Request to exit is often abbreviated to RTE. Also called egress.
Scene	Each scene can trigger up to 16 actions to create an automation event. This can save users time by automatically running multiple actions. A scene can be triggered manually, through a schedule, or via a system event.
Schedule	A schedule is a list of up to 16 sets of days and times. Typically, these are used to provide access to users only within the specified sets of days and times. Outside of the schedule a user will not have access to the system. Schedules are used to automatically arm and disarm specified partitions using the Arm-Disarm feature. Scenes can perform a set of actions according to a specified schedule. Schedules themselves can be enabled and disabled through actions. This powerful feature allows you to provide conditional access to various users and devices based on system conditions.
Screensaver	The screensaver activates on a keypad after a predefined idle time. In this mode, the information displayed on the keypad is very limited for security reasons. A user intervention is necessary to return to a normal display mode.
Service provider	The installation / maintenance company servicing your security system.
Shunt	A procedure that automatically bypasses a zone from generating an alarm when it is activated. For example, shunts stop a door generating an alarm when opened for a short time.
Stay mode	To turn your security system on when you are staying in the premises, this will automatically bypass pre-programmed zones and arm others. Often used to arm only the perimeter while allowing movement inside the premises.
Tamper	A situation where a zone, a keypad, control panel, expander or associated wiring are tampered with, or accidentally damaged. The security system tamper facility activates a signal when tamper occurs. Tamper alarms from zones are called zone tampers.
UltraSync	A secure cloud service with full redundancy to route encrypted alarm messages from your security system to a Central Monitoring Station. It also provides secure connections between the UltraSync+ app, control panel and cameras. No programming, email addresses, user names, or PINs are stored for security and data privacy reasons.
UltraSync+ app	Mobile app for smartphones to control the security system. View status, control zones and outputs, view cameras, program users and other alarm features.

User	An authorised person who can interact with the security system and perform various tasks according to the permissions assigned to them. Each user has a set of profile levels. These control what the user has access to, a list of functions, and when the user is allowed to perform these functions. A user is typically a person who is assigned a PIN and arms/disarms the system with this PIN, card, or keyfob device. Users can also be automatic functions of the system. For example, security system can automatically arm specific partitions a user has access to at a specified time. No human interaction is required, all the permissions of the programmed user will still be applied and enforced.
User code	See PIN.
User group	User groups define the options and permissions available to users.
Walk test	A test performed by a user or installer. To pass the test, the user or installer must walk past detectors, open doors and windows to activate these. The intention is to test the functionality of the security system.
Web Server	The control panel has a built-in web server which provides access to its features via a web browser interface (PC) or from UltraSync+ app. This allows you to program and control the system without being physically in front of a keypad.
Zone	A detection device such as a motion detector (PIR), reed switch, smoke detector, panic button, etc. Zones may be physically wired to the security system. Also known as an input or sensor on other security panels.

Index

4

4G antennas, 27

A

A-alarm, 64
AB alarm confirmation, 64
account access, 39
action groups, 145
actions, 143
adding cards to users, 59
adding keyfobs, 61
adding user, 57
advanced keyfob programming, 62
advanced user settings, 58
alarm transmission path, 15
alarm transmission system faults, 15
alarm verification, 64
antenna, 26
arming and disarming, 33
arming with NXG-1820-EUR keypad, 33
arming with NXG-183x-EUR keypad, 34
arming with NXG-183x-EUR keypad and user card, 36
arming-disarming, 122
auxiliary current, 6

B

B-alarm, 64
battery capacity, 6

C

cable requirements, 24
cam lock, 16
cameras
 programming, 68
card
 programming security, 67
channels, 135
combining actions with schedules, 149
communicator, 127
configuring cameras, 68
configuring email reporting, 80
configuring OH reporting, 81
country defaults, 64
current consumption, 5
current rating, 6
custom zones, 111

D

default settings, 64
delete modules, 32
disarming, 33

disarming with NXG-1820-EUR keypad, 35
disarming with NXG-183x-EUR keypad, 35
disarming with NXG-183x-EUR keypad and user card, 36

door
 programming, 64

E

email reporting, 80
EN 50131 certified components, 15
EN 50131 compliance precautions, 14
EN 50131-3 and EN50136-2 compliancy, 12
end-of-line resistor, 23
enroll modules, 30
environmental specifications, 7
EOL, 23
error messages, 153
event lists, 133

F

fuses, 8

G

general specifications, 4
geolocation, 92
geosphere, 92
gross attack count, 23
grounding, 24

H

hardwired shock sensor, 23
holidays, 102

I

INCERT certified components, 15
introduction, 1

K

keyfob
 adding, 61
 advanced programming, 62
keypress tamper, 33

L

learning zones, 53
LED indicator diagram, 20
lock out on invalid card, 33
lock out on invalid PIN, 33

M

- mains, 3
- maintenance, 8
- menu tree, 156
- menus, 100
- metal enclosure, 30
- modules
 - delete, 32
 - enroll, 30
- modules compatibility, 154

N

- NX modules, 26
- NX-003 housing, 25
- NX-003-CB housing, 28
- NXG-003-G3 enclosure, 30
- NXG-183x keypad, 157
 - sensor learning, 157
- NXG-320 enclosure, 29
- NXG-4 LEDs, 22
- NXG-4 terminals, 22
- NXG-4 wiring, 22
- NXG-8 panel, 25
- NXG-8(E) LEDs, 20
- NXG-8(E) terminals, 19
- NXG-8(E) wiring, 17
- NXG-8(E)-CB panel, 28
- NXG-9 LEDs, 21
- NXG-9 terminals, 21
- NXG-9 wiring, 21

O

- OH reporting, 81
- options affected by EN 50131 regulations, 13
- output
 - programming, 148
- output current rating, 6
- outputs, 148

P

- partition
 - programming, 115
- partitions, 115
- permissions, 98
- plastic enclosure, 29
- power requirements, 24
- power supply, 3
- product codes, 2
- programming
 - scenes, 91
- programming action groups, 145
- programming actions, 143
- programming arming-disarming, 122
- programming cameras, 68
- programming card security, 67
- programming channels, 135
- programming communicator, 127

- programming custom zones, 111
- programming doors, 64
- programming event lists, 133
- programming holidays, 102
- programming menus, 100
- programming methods, 39
 - DLX900 Management Software, 40
 - NXG-1820 keypad, 51
 - UltraSync+ App, 45
 - web pages, 52
 - xGenConnect Web Server, 42
- programming outputs, 148
- programming partitions, 115
- programming permissions, 98
- programming push notifications, 84
- programming scenes, 147
- programming schedules, 118
- programming system event reporting, 141
- programming system options, 94
- programming UltraSync, 131
- programming users, 105
- programming zone reporting, 139
- programming zones, 108
- pulse count, 23
- push notifications, 84

R

- reporting codes, 9

S

- scene
 - programming, 91
- scenes, 91, 147
- schedule
 - programming, 118
- schedules, 118
- sensor learning, 157
- service, 3
- shielding, 25
- shock sensor, 23
- SIA and CID reporting codes, 9
- SMS notification, 89
- SOS feature, 37
- specifications, 2
- sunrise, 92
- sunset, 92
- system capacity, 1
- system event reporting, 141
- system monitoring functions, 8
- system options, 94
- system status messages, 151

T

- terminal diagram, 19
- termination, 25

U

- UltraSync, 131
- UltraSync+ app messages, 153
- unverified alarm, 64
- user
 - add, 57
 - adding card, 59
 - advanced settings, 58
 - programming, 105
- users, 105

V

- verified alarm, 64

W

- walk test, 150
- Web Server messages, 153
- Wi-Fi antennas, 27
- Wi-Fi router, 39

- wireless sensor, 27
- wiring diagram, 17

X

- xGenConnect LED indicator diagram, 20
- xGenConnect product codes, 2
- xGenConnect terminal diagram, 19
- xGenConnect wiring diagram, 17

Z

- zone
 - end-of-line resistor, 23
 - EOL, 23
 - programming, 108
- zone options, 56
- zone reporting, 139
- zone types, 55
- zones, 108

