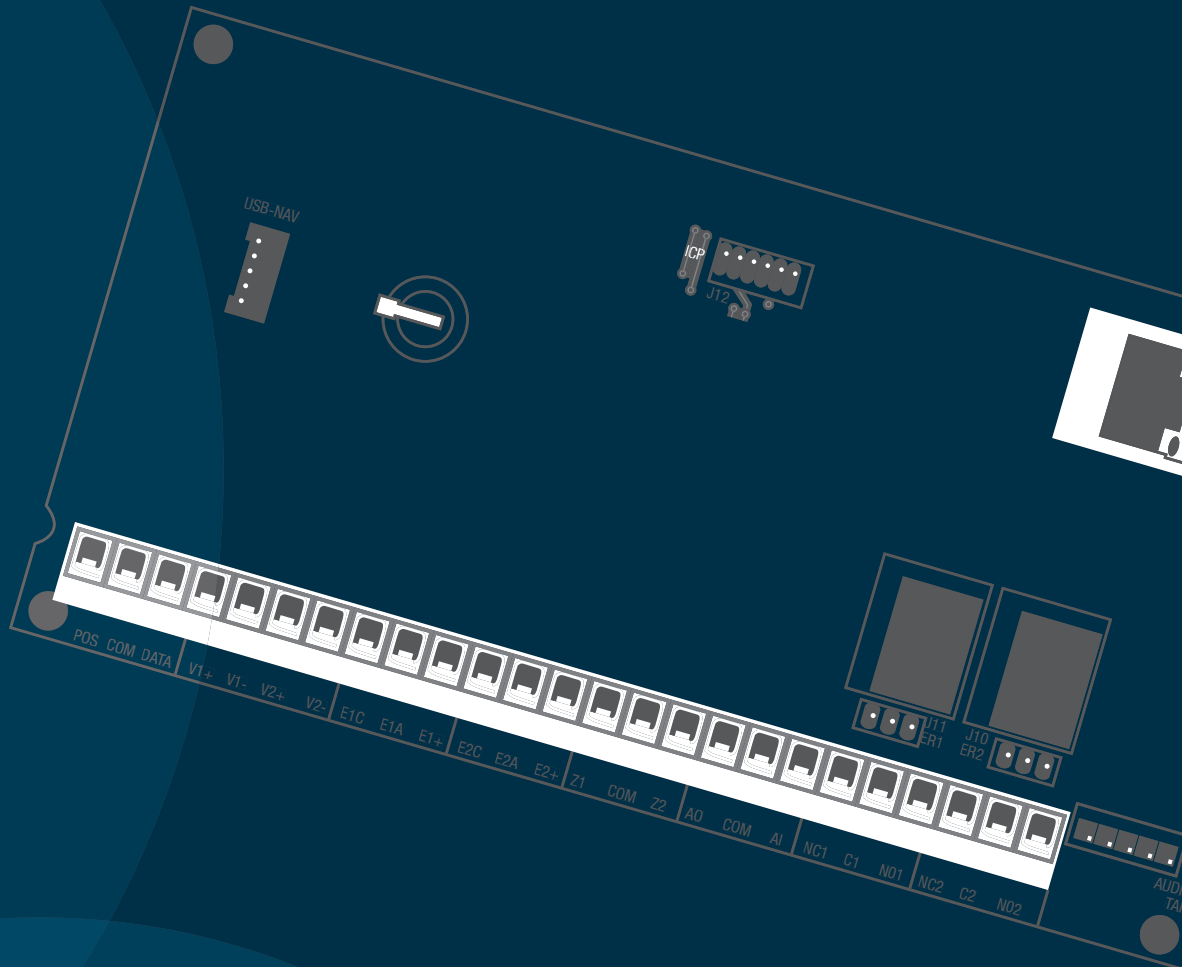


ComNav User Manual


CROWN

AIR CONDITIONING - AUDIO VISUAL - ELECTRICAL - SECURITY



HILLS™

DAS

Copyright	<p>© 2016 UTC Fire & Security Americas Corporation, Inc. All rights reserved.</p> <p>This document may not be copied in whole or in part or otherwise reproduced without prior written consent from UTC Fire & Security Americas Corporation, Inc., except where specifically permitted under US and international copyright law.</p>
Trademarks and patents	<p>ComNav name is a trademark of UTC Fire & Security Americas Corporation, Inc.</p> <p>Android, Google and Google Play are registered trademarks of Google Inc.</p> <p>iPhone, Apple, iTunes are registered trademarks of Apple Inc. App Store is a service mark of Apple Inc.</p> <p>Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.</p>
Manufacturer	<p>Placed on the market by: UTC Fire & Security Americas Corporation, Inc. 3211 Progress Drive, Lincolnton, NC, 28092, USA</p> <p>Authorized EU manufacturing representative: UTC Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands</p>
Compliance	<p>CE</p>
EU directives	<p>UTC Fire & Security hereby declares that this device is in compliance with the applicable requirements and provisions of one or more of the Directives 1999/5/EC, 2014/30/EU and 2014/35/EU. For more information see: www.utcfireandsecurity.com or www.interlogix.com</p>
	<p>2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.</p>
Contact information	<p>www.hills.com.au</p>
Customer support	<p>Hills Technical Support 1800 252 213 or hts@hills.com.au</p>

Content

Important information	4
Introduction	7
Glossary of Terms	8
Answering an incoming ComNav call	9
Accessing the ComNav via Web Pages	10
Navigating to the ComNav	10
Sign in Menu.....	10
Access Levels.....	11
Status and Partition Control	12
Zones.....	13
Output Control.....	13
History.....	14
Users	14
Email Reporting	15
Voice Reporting	17
Name Editor.....	18
Access via UltraConnect App	19
Troubleshooting	20
System Status Messages	20

Important information

Thank You

We hope that ComNav will provide you with ease of access and convenient control of your NetworX security system with the UltraConnect app.

All users of your security system should read and follow the instructions and precautions in this manual before operating your security system. Failure to do so could result in the security system not working as intended.

This manual should be kept in an accessible location for the life of the security system. If you do not understand any part of this manual, you should ask your service provider for further clarification. Read the entire manual and if possible, practice on the ComNav whilst your security provider is on site.

Product Warnings

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

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

ANY PRODUCT, SOFTWARE, SERVICE OR OTHER OFFERING MANUFACTURED, SOLD OR LICENSED BY INTERLOGIX, MAY BE HACKED, COMPROMISED AND/OR CIRCUMVENTED AND INTERLOGIX MAKES NO REPRESENTATION, WARRANTY, COVENANT OR PROMISE THAT ITS PRODUCTS (INCLUDING SECURITY PRODUCTS), SOFTWARE, SERVICES OR OTHER OFFERINGS WILL NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED.

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

Limited Warranty

UTC Fire & Security Americas Corporation, Inc. guarantees this product against defective parts and workmanship under normal use for twenty-four (24) months from the date of purchase. If any defect appears during the warranty period contact your service provider.

Warranty Disclaimers

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

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

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

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

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

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

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

User Warnings

Keep in mind, the level of security you will obtain with this system relates specifically with two major factors:

- The quantity, quality, and placement of security devices attached to this security system.
- The knowledge you have of the security system and how that knowledge is utilized in a weekly test of the complete system.

This product is to be installed by qualified SERVICE PERSONNEL only

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 service provider for replacement batteries.

Advisory messages

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

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

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

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

Keep in mind, the level of security you will obtain with this system relates specifically with two major factors:

- The quantity, quality, and placement of security devices attached to this security system.
- The knowledge you have of the security system and how that knowledge is utilized in a weekly test of the complete system.

This product is to be installed by qualified SERVICE PERSONNEL only

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

Introduction

The ComNav is an optional module that may be added to your NetworX security system to provide remote access and reporting features. You can also integrate the security system to devices such as lighting and air-conditioning via low-level relays.

You can access ComNav using these methods:

- Built-In Web Server - provides remote access from a web browser. It allows users to arm / disarm individual partitions, check system status, enable / disable user codes, modify email accounts and voice phone numbers from any standard web browser.
- Smartphone app – provides access from an easy to use smartphone app without needing to set up port forwarding.

The ComNav can interact with you with one or more of these:

- Push Notifications - will send push notifications to smartphones with the UltraConnect app installed.
- Voice Reporting - will call up to three phone numbers and announce alerts in plain English
- Email Reporting - will email up to three addresses, no mail server needs to be configured

ComNavs built in web server allows users to arm / disarm individual areas, check system status, enable / disable user codes, modify email accounts, and voice phone numbers from any standard web browser.




Glossary of Terms

Authority Level	The level of access assigned to a user's PIN code
Arm	To turn your security system On.
Partition	Multiple "zones" (detection devices) can be allocated into "partitions" to permit users to selectively "arm" the security system. For example there may be 3 zones in a partition called Downstairs, and two zones in another partition called Upstairs. Users can only arm and disarm partitions they have authority level to. Partitions are also called "areas".
Away Mode	To turn your security system on when you are leaving the premises.
Bypass	Isolate / remove selected zones from your security system. A bypassed zone is not capable of activating an alarm, as it is temporarily removed from your system.
DHCP	Dynamic Host Configuration Protocol, is a computer network protocol used by devices to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing networks to add devices with little or no manual intervention
Disarm	To turn your security system Off.
Exit Delay	The time allowed to exit the premises after the security system is armed.
Entry Delay	The time allowed to disarm your security system after the first detection device has been activated.
Master Code	A four (4) or six (6) digit PIN code that is used by a user to arm or disarm the security system. Its main feature is the ability to create, alter and delete user PIN codes. Can also be used as a function code for all features. NOTE: Your security system may have either four (4) digit PIN codes or six (6) digit PIN codes, but not a mixture of both.
Outputs	Where external devices are configured. These devices can be controlled from your security system.
Relay	An electrically operated switch. Common uses include being used to open the front gate to let a visitor in, or to turn lights on and off.
RTC	RTC stands for Real Time Clock - your ComNav has a built in clock with backup battery that saves the time and date in case your security system loses power for an extended period of time.
Self Monitored	Back-to-Base monitoring companies provide a 24/7 service with trained security staff to respond to any incidents. Having a Self Monitored system is more economical, however it does not provide as many features. NetworX security systems support both Back-to-Base Monitoring and Self Monitoring.
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 for arming just the perimeter of the premises.
Service Provider	The installation / maintenance company servicing your security system.
User Code	A four (4) or six (6) digit PIN code that is used by a user to arm or disarm the security system. Codes may be required for certain features. NOTE: A system may have either four (4) digit PIN codes or six (6) digit PIN codes, but not a mixture of both.
Zone	An individual detection device or sensor is called a "zone". For example a Passive Infra Red (PIR) motion detector in the lounge room is a single zone.

Answering an incoming ComNav call

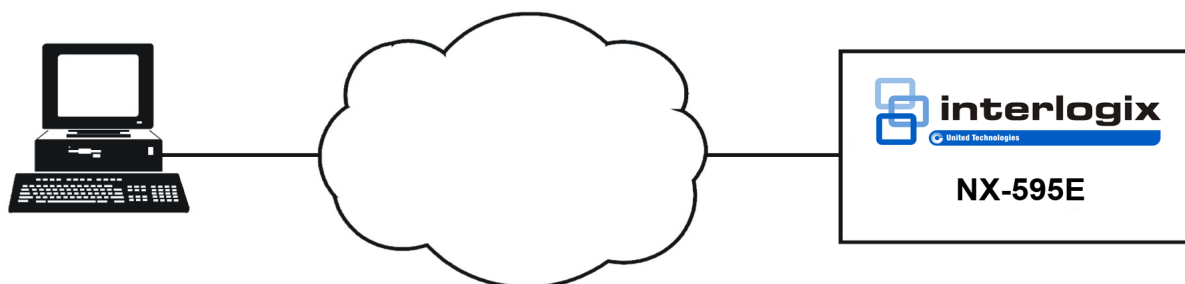
If voice reporting has been enabled, the ComNav can make a voice call to notify you of a system event.

Step Example Answering an alarm call from your security system at one of the three alarm phone numbers.

1.  Answer the incoming call. ComNav will announce:
Call from (system name).
Alarm condition active.
Enter your code.
Press star to cancel.
2. **[PIN]** Enter your PIN code to gain access.
ComNav will now announce the current alarm condition.
Please refer to the System Status Messages Table for additional information.
3.  * Return to the ComNav main menu.
4.  # Disconnects call.

Accessing the ComNav via Web Pages

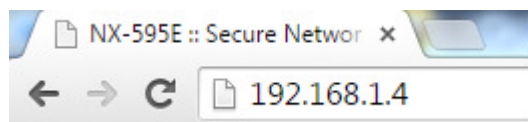
The ComNav has a built-in web server that allows users to change settings and control their security system. Please speak with your security provider regarding how your system has been configured.



Navigating to the ComNav

Open your web browser and enter the ComNav's IP address directly into the browser (Figure 1). This number may change depending on your router and whether a static IP address has been assigned to the ComNav. To find the IP address of your ComNav, login to your router and find the device connected, or ask your installer for assistance.

Figure 1



Sign in Menu

The screenshot shows a 'Sign in' form with the following fields and elements:

- Sign in** (Section Header)
- Enter your username:
- Enter your password:
-

When successfully connected the ComNav will display the “Sign in” Menu.

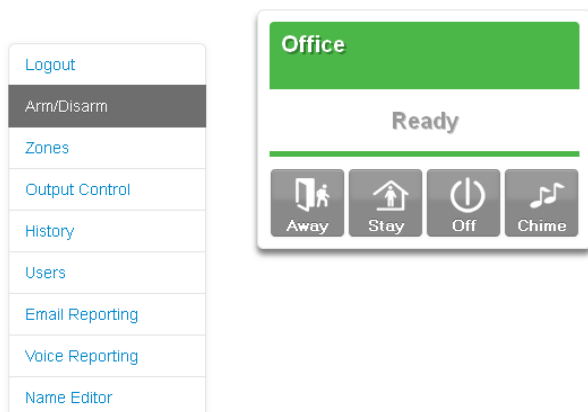
To access the main menu enter the username and password as supplied by your security provider. These details should be on the back of this manual.

Note: Username is case sensitive

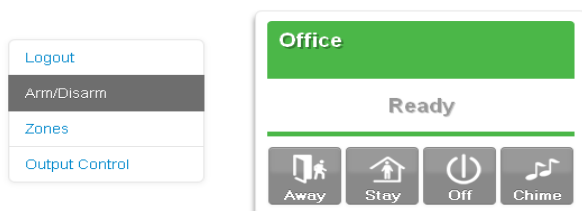
Access Levels

There are two access levels available to users - master code or standard user codes. Master codes have greater authority and are able to access more features.

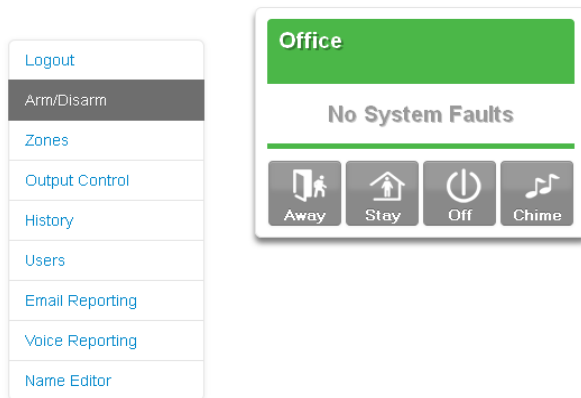
Main Menu – Master Code



Main Menu – Standard User Code



Status and Partition Control



Area Colour

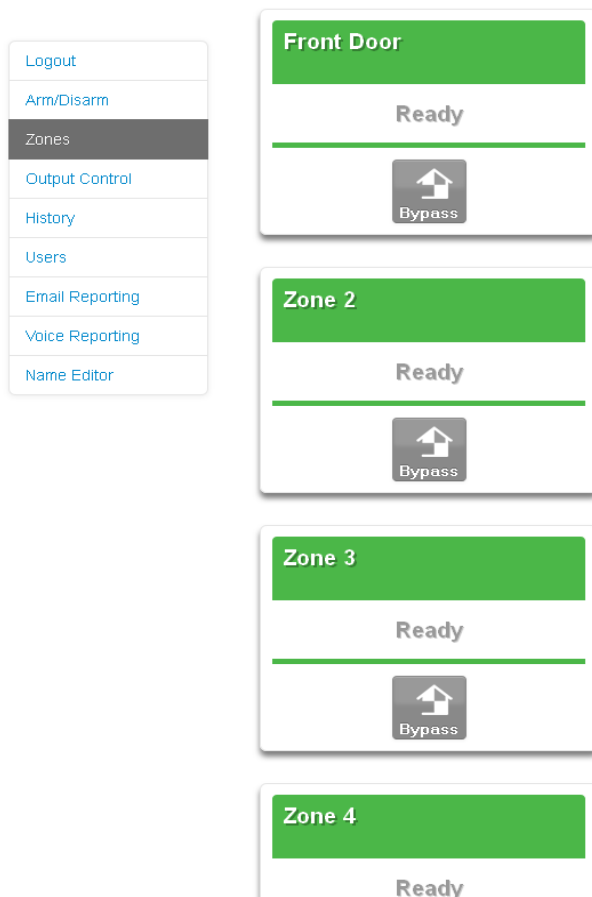
Green	Area is active, and all zones are secure
Yellow	Area is armed in the stay mode
Red	Area is armed in the away mode
Blue	System condition present
Grey	Area not ready, zone(s) open

Up to 8 active areas can be displayed, and control can be individual or as a group.

To arm (turn on) an individual area/s, click on Away or Stay button for that area.

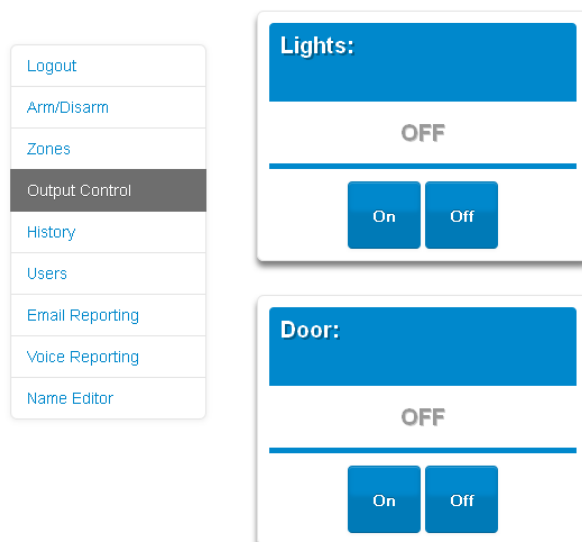
To disarm area/s from either the stay or away arming modes, click on the Off button.

Zones



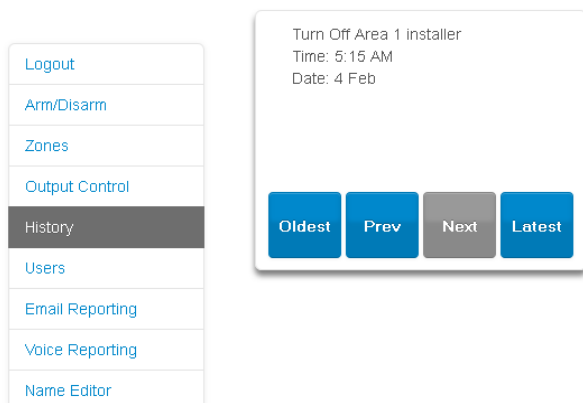
From the Zones menu you can view zone status and bypass zones.

Output Control



If you have outputs connected, you can control them from the Output Control menu.

History



Current system faults will be displayed in the Arm/Disarm page and the system's past 512 event log can be accessed via the History menu.

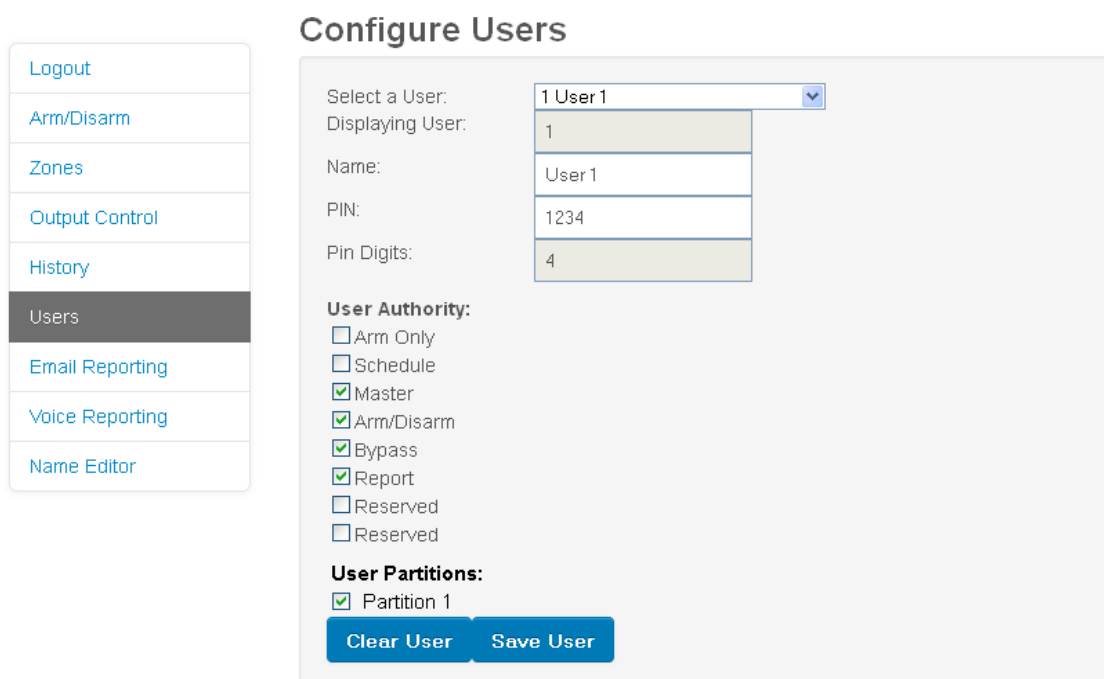
Oldest – Will display the last event stored in the internal event log.

Prev – (Previous) will display the previous consecutive event from the internal event log to what is currently displayed.

Next – Will display the next consecutive event from the internal event log to what is currently displayed.

Latest – Will display the current existing event from the internal event log.

Users



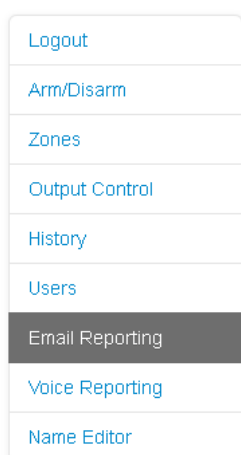
Users must be given a User Name on this menu to be able to login to the web pages and the smartphone app.

The user configuration menu is where user PIN codes are assigned to users. A user code is used to arm and disarm areas within your security system. They are generally four digits in length, but can be configured to be six digits in length if this level of security is required (contact your security provider to enable 6 digit PINs).

The User Authority determines the options available to that user. Tick the Master box to allow that user codes to create delete or modify user codes. Users can only assign areas to users they have access to.

Email Reporting

Select the events and email addresses to send events to. Note: reporting must be enabled on the main panel to enable email reporting.



Email Reporting

Save Config

Email 1 Address:

Email 2 Address:

Email 3 Address:

Email 1 Events:

- Alarms
- Restores
- Opening/Closing
- Bypass
- Zone Trouble
- Power Trouble
- Tamper
- Test Reports
- System Trouble
- Fail To Report
- Sensor Trouble
- Start/End Program Mode
- Cancel
- Recent Close
- Reserved
- Reserved

Email 2 Events:

- Alarms
- Restores
- Opening/Closing
- Bypass
- Zone Trouble
- Power Trouble
- Tamper
- Test Reports
- System Trouble
- Fail To Report
- Sensor Trouble
- Start/End Program Mode
- Cancel
- Recent Close
- Reserved
- Reserved

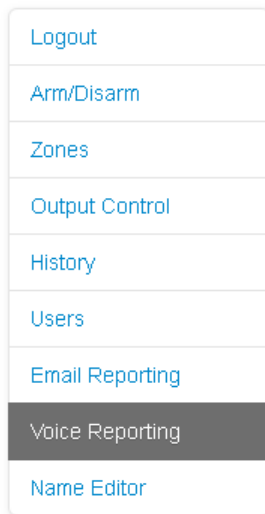
Email addresses 1, 2 and 3: Enter up to three email addresses, which will receive emails when the selected event(s) are activated.

Email Reporting – examples

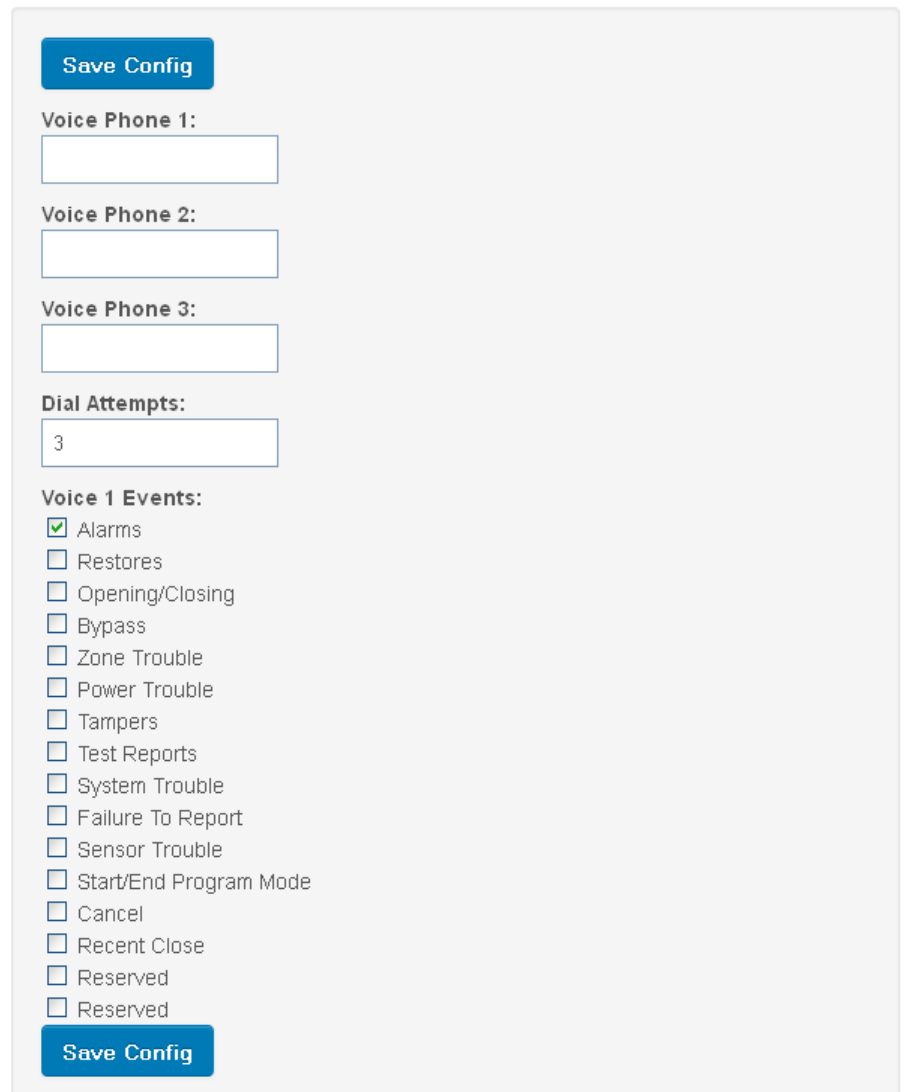
User Arming: Security Report From Account 0001
Turn on
Partition 1
Fred
Time: 11:55 AM
Date: 19 Jun

Panic Button on keypad: Security Report From Account 0001
Keypad Panic Alarm
Partition 1
Time: 11:55 AM
Date: 19 Jun

Voice Reporting



Voice Reporting



Alarm phone numbers 1, 2, and 3 will receive a phone call announcing the events selected on this screen. The voice events selected apply to all three alarm phone numbers.

When the call is answered, the ComNav will announce:

“Alarm condition active. Enter your code. Press star to cancel”.

Enter your PIN code to hear the full alarm condition. You may then disarm or re-arm your security system.

The ComNav will attempt to call phone number 1, if it is unanswered or a valid PIN code is not received, it will hang up and try phone 2, then 3. This will repeat for the number of times entered in Dial Attempts.

Name Editor

A built in Name Editor allows you to enter custom names for areas, zones, and outputs which will appear on the NX-1820 screen.

To load text labels **from** a NX-1820, go to that keypad:

1. Touch Menu.
2. Touch Settings.
3. Enter an authorised PIN code.
4. Touch Text.
5. Touch Copy.
6. Touch Copy All – all text labels (including user names) will be copied from this NX-1820 to other NX-1820 keypads and the ComNav.

The screenshot displays the Name Editor interface. On the left is a vertical menu with the following items: Logout, Arm/Disarm, Zones, Output Control, History, Users, Email Reporting, Voice Reporting, and Name Editor (highlighted in dark grey). To the right, the main interface is titled "Edit Names Then Click Save" and contains three buttons: Save, Copy, and Copy All. Below this are two sections: "Partition Names:" with two input fields labeled "Partition1" and "Partition2"; and "Zone Names:" with a list of 16 input fields labeled "ZN1" through "ZN16".

After making changes on the Name Editor, you must copy the updates **to** connected NX-1820 keypads:

1. Click Save.
 2. Click Copy All to send all text labels to NX-1820 keypads, or Copy to send only changed items (faster).
- Copy and Copy All includes all User Names entered on the Users Menu

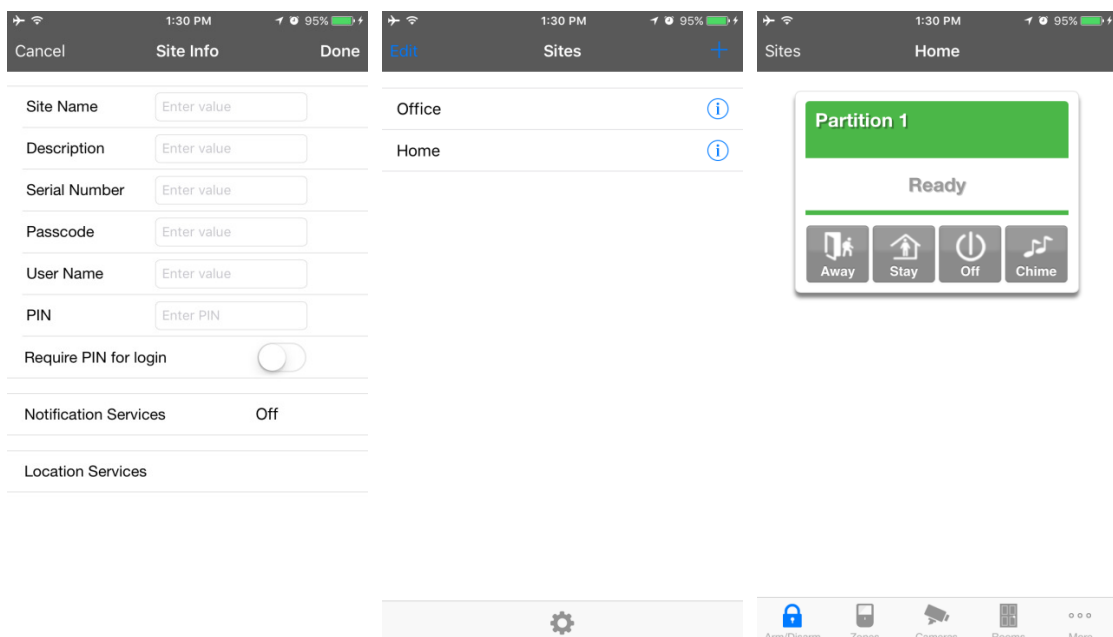
Access via UltraConnect App

UltraConnect is an app that allows you to control your control panel from an Apple® iPhone/iPad, or Google® Android® device.

1. On your smartphone, go to the Apple® App StoreSM or Google Play® Store.



2. Search for **UltraConnect**.
3. Install the app.
4. Click the icon on your device to launch it.
5. Click + on the top right to add a new account, or the blue arrow to edit an existing site.
6. Enter the details of your security system – this should be on the back of this manual, if not please contact your security installation company or builder for assistance.
The serial number is printed on the back of the ComNav unit. Alternatively login to ComNav Web Server and go to IP Reporting to view it.
The default Web Access Passcode of 00000000 disables remote access. To change it, login to ComNav Web Server and go to Network Settings.
The username and PIN code is for any authorized user on the system. To change these details, login to ComNav Web Server and go to Users (requires master access).
7. Click Done button to save the details, then Sites to go back.
8. Click the name of the Site, the app will now connect you to the ComNav.



Troubleshooting

- ComNav may not work on corporate network due to firewalls, proxy servers, and other security settings. Connect it to a network port that can provide direct access to the internet.
- Check that other devices on the same network can connect to the internet, if they are working then confirm all access codes are correct (serial number, Web Access Passcode, username, PIN)

System Status Messages

Zone Number / Zone Name

In alarm – This zone has triggered a system alarm condition

Is bypassed – This zone is isolated (disabled) and will not activate an alarm

Chime is set – This zone is part of the chime group

Is not secure – This zone is not closed

Fire alarm – This zone has triggered a fire alarm

Tamper – This zone has triggered a tamper alarm

Trouble fault – This zone has an open circuit

Loss of wireless supervision – This zone is a wireless device and has lost its communication link with the control panel

Low battery – This zone is a wireless device and needs its battery changed

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

System

AC power fail – The security system has lost its electricity power

Low battery – The security systems back up battery requires charging

Battery test fail – The security systems back up battery requires changing

Box tamper – The security systems cabinet tamper input has activated

Siren trouble – The security systems external siren has a problem

Over current – The security system is drawing too much current

Time and date loss The security system time and date need resetting

Communication fault – The security system has detected a problem with the phone line

Expander

Low battery – A remote power supply's back up battery requires charging

AC power fail – A remote power supply has lost its electricity power

Box tamper – An expanders cabinet tamper input has activated

Keypad

Fire alarm – A fire alarm has been activated at the keypad

Panic – A panic alarm has been activated at the keypad

Medical – A medical alarm has been activated at the keypad

DAS Limited

Suite 2, Level 9
130 Pitt Street
Sydney NSW 2000

t +61 2 9216 5510
f +61 2 9216 5599
e info@das.com.au
w das.com.au

DAS