

ComNav Installation Manual

Copyright	© 2023 Aritech. All rights reserved. This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Kidde Global Solutions (KGS), except where specifically permitted under US and international copyright law.
Trademarks and patents	Reliance and ComNav are trademarks of Dicker Data Limited. UltraSync is a trademark of KGS. iPhone, Apple, iTunes are registered trademarks of Apple Inc. App Store is a service mark of Apple Inc. IOS is the registered trademark of Cisco Technology, Inc. Android, Google and Google Play are registered trademarks of Google Inc. 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: KGS Fire and Security Products Level 4.01, 2 Ferntree Place, Notting Hill, Victoria 3168
EU compliance	
EU directives	KGS 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.aritech.com.
	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.
Disclaimer and Product Warnings	
Distributor	Dicker Data is an authorised distributor of KGS.
Contact information	www.dickerdata.com.au
Customer support	1800 327 457 or email DAS.TechSupport@dickerdata.com.au
Version	Manual updated for firmware P004000-17

Contents

Important information.....	7
Specifications.....	10
Introduction	11
Installing the ComNav into the enclosure	12
Wiring the ComNav	13
Terminal descriptions	14
Status LED.....	14
Preparing the ComNav for configuration.....	15
Enrolling, Defaulting and Retrieving the IP Address for the ComNav	16
Using a NX-181xx Voice keypad.....	16
Using a TouchNav keypad	17
Using a Standard Keypad (Icon or LCD).....	17
Accessing the ComNav via the Web pages	18
Enable LAN Web Page Access	18
Find the IP Address	18
Enable Features.....	18
Set the IP Address	19
Navigating to the ComNav	19
Main Menu – Installer Code	20
Programming the ComNav with the Web Pages	21
Status and Partition Control	21
Zones.....	22
Output Control.....	22
History.....	23
Users	23
Email Reporting	25
Feature Setup	26
Network Settings.....	27
Output Settings	29
IP Reporting	31
Name Editor	33
Enabling Smartphone App.....	35
Installing UltraSync+ app.....	37
Smartphone Push Notifications.....	38
Change Destination Name	38

Troubleshooting	39
Programming Worksheets	40
System Status Messages	43
FAQ - Frequently Asked Questions.....	44

Important information

Limitation of liability

KGS's sole obligation or liability is the repair or replacement of the product according to the limited warranty. To the maximum extent permitted by applicable law, in no event will KGS be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, lost savings, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise, even if KGS has been advised of the possibility of such damages, nor for any claim by any third party. 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 KGS 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 KGS 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, KGS assumes no responsibility for errors or omissions.

Disclaimers

A level of TCP IP knowledge is required by the installer/s to set up some of the ComNav functionality. KGS limits support to ComNav setup only, and is unable to offer further assistance on your client's DSL modem, router, firewall or any other 3rd party software. Please consult your customer's IT department or qualified IT professional about implementing this product onto your client's network.

The information in this document is subject to change without notice. KGS 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.

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.

Limited Warranty

KGS 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. KGS assumes no liability for consequential or indirect damage, and accepts no responsibility for repairing damage to the product caused by misuse, careless handling, or where repairs have been made by others. KGS does not warrant that the operation of this product will be uninterrupted or error-free.

No other guarantee, written or verbal, is authorised by KGS.

Product Warnings

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

THE ABILITY OF INTEROGIX'S PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH KGS HAS NO CONTROL AND FOR WHICH KGS 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 AUTHORISED PRODUCTS (INCLUDING ALARM OR OTHER CONTROL PANEL AND SENSORS).

ANY PRODUCT, SOFTWARE, SERVICE OR OTHER OFFERING MANUFACTURED, SOLD OR LICENSED BY KGS, MAY BE HACKED, COMPROMISED AND/OR CIRCUMVENTED AND KGS 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.

KGS 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.

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.

Cybersecurity Notice

The security of a whole system is only as strong as it's weakest point. In most homes this is the home WiFi router.

We highly recommend securing the WiFi router. This includes using a newer router which supports upgraded security protocols and setting a complex WiFi password. The router login name and password should be changed from the default. For more advanced users, firewall and client filtering should be enabled along with applying firmware updates from the router manufacturer.

The installer name for the ComNav should be changed from the default. All PIN codes should be changed from the defaults and use longer 6-digit PIN codes.

To protect your phone, always have a PIN/passcode/biometric lock enabled. Apply security patches as recommended.

Specifications

Compatibility	NetworX control panels as of version V2 (NX-4, NX-6, NX-8, Reliance 8, Reliance 12, and Reliance 128)
Operating Voltage	12 VDC, supplied from control panel
Current Draw	250 mA nominal, 320 mA (both relays energized)
Maximum Relay Current	1 A (per relay)
Maximum Relay Voltage	24 VDC, 30 VAC
Operating Temperature	0°C~49°C
Storage Temperature	-34°C~49°C
Maximum Humidity	90% relative humidity non-condensing
Dimensions (L x W x H)	152 x 81 x 13 mm

Introduction

The ComNav is an IP communication module that can be added to the NetworX panel range (NX-4v2, NX-6v2, NX-8v2, Reliance 8, Reliance 12, and Reliance 128) to provide remote access and alarm notification with a smartphone app or web browser.

The security panel can be configured for alarm reporting exclusively over IP when PSTN connectivity is no longer available.

The ComNav provides a web browser interface accessible via a local computer, smart phone or tablet to configure the device. UltraSync+ is an Apple® iOS® and Android® application for remote configuration and end user control of the security system.

Up to four zones are also supported with zone doubling (not available on NX-4 panels). Three email addresses can be programmed into the ComNav to allow alarm and trouble events to be emailed to the end user.

This manual assumes the installer is familiar with the NetworX family of security products and is capable of programming the security system. It also assumes that the installer is familiar with basic IP networking and Apple iOS or Android smart devices.

Setup Process

1. Install the ComNav into the Reliance panel.
2. Enrol the ComNav into the Reliance panel.
3. Minimum configuration is required:
 - a. Enable Feature 19 – Option 6 to show programming menus
 - b. GMT time zone and daylight savings (Feature Menu)
 - c. Enable UltraSync app by setting the Web Access Passcode (Network Settings Menu)

Important notes before proceeding

- By default, the panel must be in program mode before you can configure the ComNav with a web browser
- Access to the ComNav is with existing user accounts stored in the Reliance panel. Use the **existing PIN** for the **installer** to login to the ComNav.
- Record the following information during the installation process:
 - ComNav serial number (12 characters)
 - Web Access Passcode (8 digits)

Installing the ComNav into the enclosure

Inside the Reliance enclosure, several 2-hole insertion points have been constructed. This allows for either vertical or horizontal placement of the modules. **Notice that the insertion points have two sizes of holes - a larger hole and a smaller hole.**

Figure 1: The black plastic PCB guides are grooved on one edge where the PC Board will be seated. The end with the half-moon protrusion fits into the larger hole. The smaller hole is for the screw.

Figure 2: Place the *first* black plastic PCB guide in the top insertion point, grooved edge downward. The half-moon protrusion will be in the large hole. It does not require force. Insert one of the provided screws into the smaller hole (from inside the can) to secure it in place. A screwdriver should reach through the notch that runs the length of the guide to tighten the screw. The *second* PCB guide should be positioned opposite of the first (grooved edge up) and placed in the lower insertion point, using the same procedures described above. Once mounted, screw it in securely.

Figure 3: The PC board should slide freely in the grooves of both guides.

Figure 1

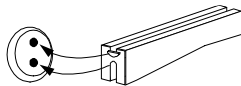


Figure 2

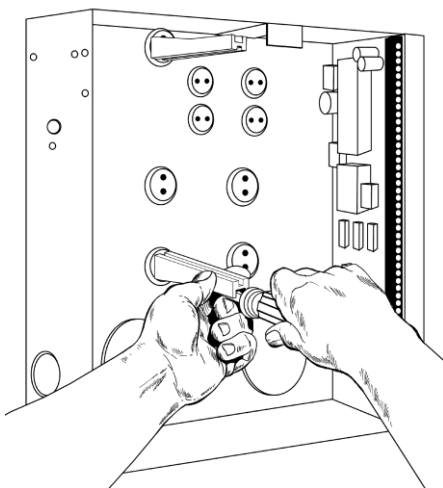
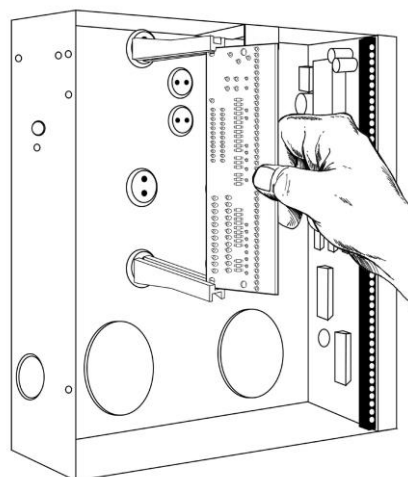


Figure 3

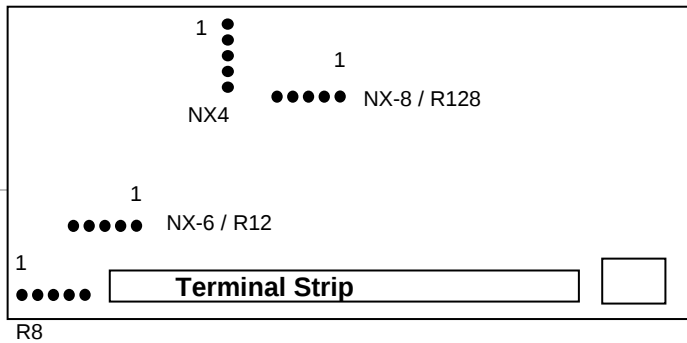


Wiring the ComNav

Remove all power (AC and battery) to the Reliance security system and connect ComNav's terminals POS, COM & DATA to the NetworX bus.

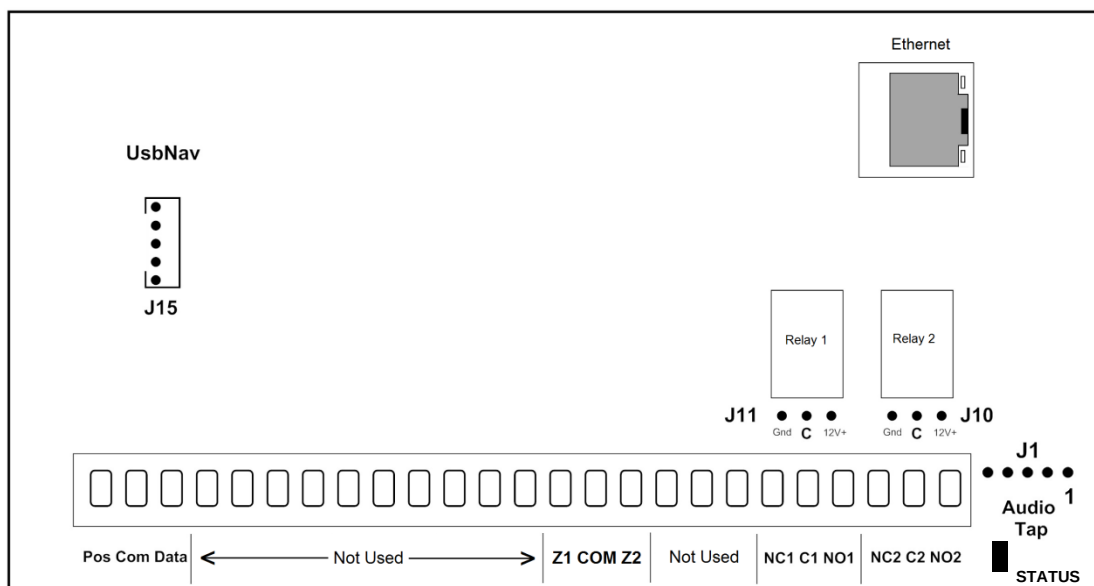
1. Connect J14 (RJ45) to available network port via a patch cable.

Figure 4



2. Connect zone inputs if required:
 - 3.3K Single EOLs
 - 3.7K Lower zone EOLs (when zone doubled)
 - 6.9K Higher zone EOLs (when zone doubled)
3. Select relay contact requirements via jumpers J10 and J11. Place link between GND and C for negative switch, and 12 V+ and C for positive switch, remove link for dry contact switching. Relay is rated 30 VAC @ 1 A, 24 VDC @ 1 A.

Figure 5. ComNav Connector Layout



Note: The USBNAV connector is used for upgrading the firmware. Please contact your local branch for the latest USB upgrade tool and firmware files.

Terminal descriptions

Terminal	Description	
1 Pos	Panel Bus	Positive terminal on the Reliance panel
2 Com		Common terminal on the Reliance panel
3 Data		Data terminal on the Reliance panel
14 Z1	Additional Zones	1 st / 3 rd Zone
15 Com		Common (-) return for Zone loop
16 Z2		2 nd / 4 th Zone
20 NC1		Normally closed
21 C1	Relay 1	Common
22 NO1		Normally open
23 NC2	Relay 2	Normally closed
24 C2		Common
25 NO2		Normally open

3.3K = Single EOLs
3.7K = Low zones
6.9K = High zones

This relay can be controlled from the UltraSync app when programmed

This relay can be controlled from the UltraSync app when programmed

Status LED

A red Status LED is positioned on the bottom right edge of the ComNav near the audio tap.

- Off – not connected, check cable and internet connection
- Blinking – connecting to cloud servers
- On – connected to cloud servers

WARNING: THE EQUIPMENT SHOULD ONLY BE OPERATED WITH AN APPROVED POWER ADAPTER WITH INSULATED LIVE PINS. OPERATION OF THE EQUIPMENT WITH A POWER ADAPTER THAT DOES NOT MEET THESE STANDARDS COULD POSE AN ELECTRICAL HAZARD THAT MIGHT RESULT IN SERIOUS INJURY OR DEATH.

Caution: Remove all power (AC and battery) to the Reliance security system before proceeding. Failing to do so could result in possible damage to the product.

Caution: Do not exceed the Maximum Load ratings above for the relay configuration. Exceeding the maximum rating could result in possible damage to the product. Relay is rated 30 VAC @ 1 A, 24 VDC @1 A.

WARNING: DO NOT CONNECT MAINS VOLTAGE TO THE COMNAV. DOING SO COULD DAMAGE THE MODULE OR NETWORK PANEL AND POSE AN ELECTRICAL HAZARD THAT COULD RESULT IN A FIRE OR CAUSE SERIOUS ELECTRICAL SHOCK OR LOSS OF LIFE.

Current Limit Warning: Check the current requirements of your load before connecting! There is no overcurrent protection on the relays when providing bus ground or bus voltage (jumper between GND and C, or C and 12V +). You must ensure your load does not exceed the recommended limits above. Exceeding limits can damage the module and pose an electrical hazard that could cause a fire or electrical shock that might result in property damage, serious injury, or loss of life. Reliance panels do have overcurrent protection on the bus and may disconnect the bus to provide temporary protection. If enabled, your panel will report "Overcurrent Fault" or "Expander Overcurrent". Repeated overcurrent conditions can result in permanent damage to the panel or connected devices.

Preparing the ComNav for configuration

Before you can configure the device, you must:

1. Enrol the ComNav into the Reliance panel.
2. Default the ComNav.
3. Retrieve the IP address from the ComNav.

You can accomplish these three steps via any LCD (NX-148xx), Voice (NX-181xx) or TouchNav keypad.

Enrolling, Defaulting and Retrieving the IP Address for the ComNav

The ComNav is set to **device address 191** and programming is carried out like all other Reliance modules.

Default the ComNav following these instructions depending on the type of keypad you are using. When you exit program mode, the ComNav will be automatically enrolled.

Using a NX-181xx Voice keypad

Step

1. **[MENU]-[0]** Selects main menu - Option 0, Advanced system configuration.
 ◀ *Enter your code, touch menu to exit.*
2. **[?]-[?]-[?]-[?]** Enter your 4 or 6 digit Programming code
 Touch 1 for keypad configuration
 Touch 2 for panel and device configuration
 ◀ *Touch 3 to configure service provider phone number*
 Touch menu to exit.
3. **[2]** Selects Panel and Device configuration.
 ◀ *Select a device number followed by enter*
 Touch menu to go back.
4. **[1][9][1]**
 [ENTER] Connects to device 191 (ComNav)
 Selected device 191 is connected.
 ◀ *Select a Location number followed by enter*
 Touch menu to go back.
5. **[9][1][0]**
 [ENTER] Defaults the device. **Note:** only required once.
6. **[2][1]**
 [Enter] This keypad will announce the first number of the IP address.
7. **[MENU]** This keypad will announce the second number of the IP address.
8. **[MENU]** This keypad will announce the third number of the IP address.
9. **[MENU]** This keypad will announce the fourth number of the IP address.
- 10.. **[MENU]** Moves back to step 4, select a device number.
11. **[MENU]** Moves back to step 3, Advanced system configuration selection.
12. **[MENU]** Exits from Advanced system configuration (exiting program mode automatically enrolls the ComNav).

Using a TouchNav keypad

Step

1. **[MENU]** Press the Menu button.
2. **[Settings]** Press the Settings button.
3. **[?]-[?]-[?]-[?]** Enter your 4 or 6 digit Programming code.
4. **[Program]** Press the Program button.
5. **[1][9][1]**
[ENTER] Connects to device 191 (ComNav).
6. **[9][1][0]**
[ENTER] Defaults the device. **Note:** only required once.
7. **[2][1]**
[ENTER] Access location 21 to retrieve the IP address of the ComNav. Scroll through the segments with the ► button and record the IP address (e.g. 192.168.1.2).
8. **[Exit]** Press the Exit button. (exiting program mode automatically enrolls the ComNav).

Using a Standard Keypad (Icon or LCD)

Step

1. **[*][8]** Selects Panel and Device programming.
2. **[?]-[?]-[?]-[?]** Enter your 4 or 6 digit Programming code.
3. **[1][9][1] - [#]** Connects to device 191 (ComNav).
4. **[9][1][0] - [#]** Defaults the device. **Note:** only required once.
5. **[2][1][#]** To discover the IP address of the ComNav (Press * to scroll through each segment of the IP address. Record the IP address (e.g. 192.168.1.2).
6. **[Exit]** Moves back to step 3.
7. **[Exit]** Exits programming (exiting program mode automatically enrolls the ComNav).

Accessing the ComNav via the Web pages

Enable LAN Web Page Access

Enter program mode on a local keypad to allow web page access for 15min.

After 15min the web page will be disabled. Re-enter program mode on a keypad to allow access for another 15min.

Find the IP Address

DHCP is enabled by default which means an IP address will be assigned automatically if your network supports DHCP.

To discover the IP address – use a keypad connected to the alarm system, enter program mode, and navigate to device **191**, Location **21**. Navigate through the segments to view the IP address.

If the IP address is empty (Location 21, Segment 1 will be 0) then either:

- ComNav has not connect yet to the customer router,
- DHCP is not functioning \ enabled on the customer router,
- or static IP needs to be configured manually.

Enable Features

ComNav firmware P004000-12 and above disables programming menus for cybersecurity reasons. To enable programming menus permanently, turn on Feature Location 19 Option 6.

Location 19 – IP Location Settings

- Enable option 1 to turn on DHCP which will allow your router to assign the ComNav and IP address automatically. Disable this option to manually assign an IP address.
- Enable option 4 to allow ping command for troubleshooting.
- Enable option 5 to automatically update the clock.
- **Enable option 6 to show the ComNav programming menus. At factory default it is disabled for increased security.**
- Enable option 7 to allow DLX900 access.
- Enable option 8 to allow remote / web programming.

Set the IP Address

If static IP needs to be programmed, enter the details in these locations:

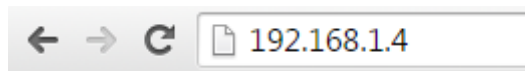
Location 20 – IP Gateway

Location 21 – ComNav IP Address

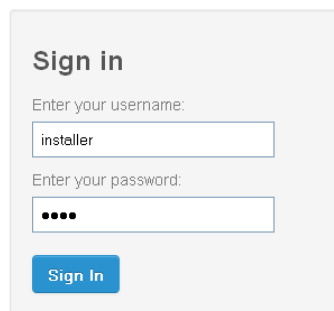
Location 22 – Subnet Mask

Navigating to the ComNav

Enter the IP address of your ComNav into a compatible web browser.



Sign in Page

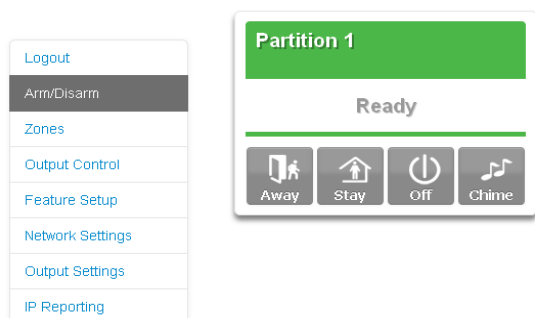
A screenshot of a 'Sign in' form. It has a title 'Sign in' and two input fields: 'Enter your username:' with the text 'installer' and 'Enter your password:' with masked characters '••••'. A blue 'Sign In' button is at the bottom.

When successfully connected, the ComNav will display the “Sign in Page”. Panel must remain in Program Mode using a keypad. Enter the correct username/password combination to login.

Default Installer Username: **installer** (username is case sensitive)

Default Password: **9713** (the panel Go To Program code)

Main Menu – Installer Code

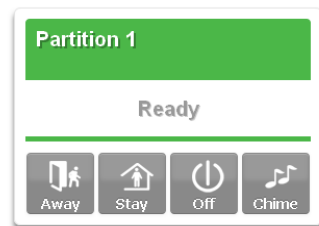


Programming menus will be available when ComNav is accessed via the default installer code while the panel is in program mode.

Feature Setup, Network Settings, Output Settings, and IP Reporting will only be displayed when the main panel is in program mode. Alternatively, enable Location 19, Option 6 to always show these menus to the installer.

Programming the ComNav with the Web Pages

Status and Partition Control



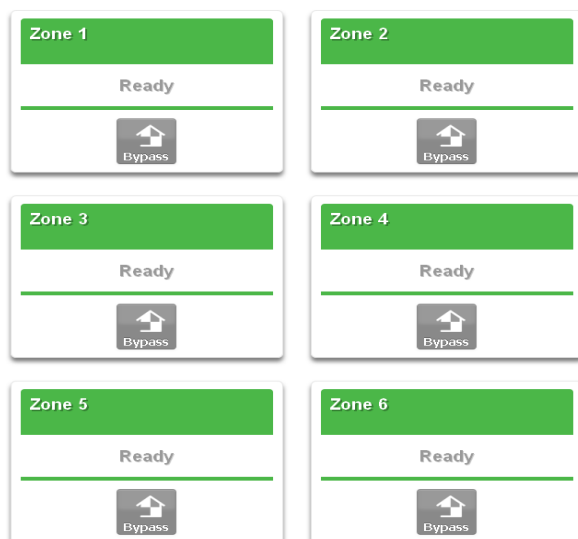
Partition Colour	Status
Green	Partition is active, and all zones are secure
Yellow	Partition is armed in the stay mode
Red	Partition is armed in the away mode
Blue	System condition present
Grey	Partition not ready, zone(s) open

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

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

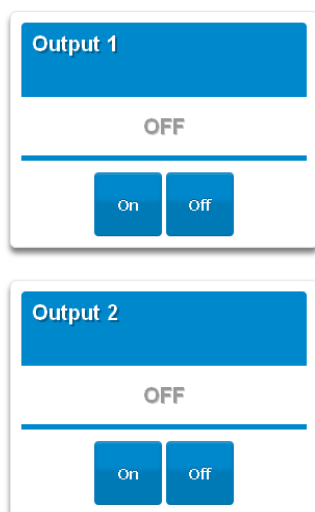
To disarm a partition from either stay or away arming modes, click the Off button.

Zones



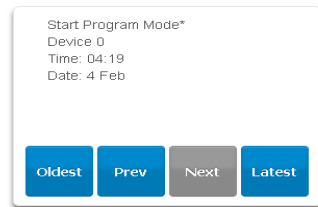
From the Zones menu you can view zone status and bypass zones.
Maximum zone count for the specific Reliance panel will be displayed.
The two extra zones on the ComNav will not be displayed here.

Output Control



If you have outputs connected and programmed as Manual Control, you can turn them on and off from this menu.

History

A screenshot of the History menu. It displays the following text: "Start Program Mode*", "Device 0", "Time: 04:19", and "Date: 4 Feb". Below this text are four buttons: "Oldest", "Prev", "Next", and "Latest".

Start Program Mode*			
Device 0			
Time: 04:19			
Date: 4 Feb			
Oldest	Prev	Next	Latest

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

Oldest – Will display the oldest event available.

Prev – (Previous) will display an older event.

Next – Will display a newer event.

Latest – Will display the most recent event.

Users

A screenshot of the Users menu. It contains the following fields and options:

- Select a User:** A dropdown menu showing "1 User 1".
- Displaying User:** A text field containing "1".
- User Name:** A text field containing "User 1".
- PIN:** A text field containing "1234".
- Pin Digits:** A text field containing "4".
- User Authority:** A list of checkboxes:
 - ☐ Reserved
 - ☐ Arm Only
 - ☐ Arm Only After Close
 - ☒ Master
 - ☒ Arm/Disarm
 - ☒ Bypass
 - ☒ Report
 - ☐ Activate aux outputs
- User Areas:** A list of checkboxes:
 - ☒ NX au area 1
- Buttons:** "Clear User" and "Save User".

Users on the control panel can be assigned a User Name on this menu to provide access to the UltraSync+ app. The default is "User 1" and should be changed for security.

Note: TouchNav keypads have their own database of text labels including User Names. These are stored under Menu – Settings – Text – Users.

To synchronise existing text labels:

- To copy from the ComNav to all TouchNav keypads, login to the webpage, click Name Editor, click Copy All
- To copy from a TouchNav keypad to the ComNav (and all other TouchNav keypads), on the keypad press Menu – Settings – Text – Copy – Copy All.

PIN codes can be modified here. A user PIN code allows arming and disarming partitions. PIN codes are four to six digits in length. Refer to the Reliance panel installation manual to change PIN length.

The User Authority determines the options available to that user:

- Arm Only – allows the user to only arm partitions and prevents disarming
- Arm Only After Close – allows the user to only arm partitions after closing window and prevents disarming
- Master – allows this user to create delete or modify user codes. Master access always allows arming and disarming. Users can only assign partitions to users they have access to.
- Arm/Disarm – allows this user to arm and disarm partitions they have access to
- Bypass – allows this user to bypass zones
- Report – send open and close reports when this user arms and disarms partitions
- Activate aux outputs – allows this user to control outputs
- User Partitions – select the partitions the user will be allowed to access and control.

Email Reporting

Email Reporting

The screenshot shows a configuration window titled "Email Reporting". At the top left is a blue "Save Config" button. Below it are three labels: "Email 1 Address:", "Email 2 Address:", and "Email 3 Address:", each followed by a text input field. Below these is a section titled "Email 1 Events:" containing a list of events, each with a checked checkbox: Alarms, Restores, Opening/Closing, Bypass, Zone Trouble, Power Trouble, Tamperers, Test Reports, System Trouble, Failure To Report, Sensor Trouble, Start/End Program Mode, Cancel, Recent Close, Reserved, and another Reserved.

Email Addresses 1, 2 and 3: Enter up to three destinations to receive emails or push notifications when the selected event(s) are activated. A max of three destinations for email or push notification are supported.

Return Address: Email client or push notification in UltraSync app will display this text field as the sender. This does not have to be a valid email address.

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

Feature Setup

Save Config

Language

English

☐ Enable Zone Doubling

Start Zone:

disabled

Installer Name:

installer

Service Number:

GMT Offset:

0 (GMT)

0

Daylight Saving Time Start:

Disabled

First Sunday

Daylight Saving Time End:

Disabled

First Sunday

Save Config

Device ID:

1

Firmware:

A55P004000-12

Hardware:

206180IX10

Bootload:

B0402003

Web Version:

CN_0.109-A

Voice:

0.7

Language:

0

Zone-doubling: This feature will allow the two on-board zones to double to four zones.

Single EOL	Zone Doubled EOL's	
3K3	Lower Zone 3K7	Higher Zone 6K9

Start Zone: Used to enter the starting zone number of the additional zones on the ComNav. Applicable only on panels which support 16 or more zones.

Data	Zones	Data	Zones	Data	Zones	Data	Zones
9	= 9 - 12	41	= 41 - 44	73	= 73 - 76	105	= 105 -108
17	= 17 - 20	49	= 49 - 52	81	= 81 - 84	113	= 113 - 116
25	= 25 - 28	57	= 57 - 60	89	= 89 - 92	121	= 121 - 124
33	= 33 - 36	65	= 65 - 68	97	= 97 - 100		

Installer Name: Default installer name is **installer** and is case sensitive. This is the username to sign in via a web browser or the UltraSync app. Installer level access will also show these additional menus: Network Settings, Feature Setup, Output Settings, and IP reporting. The Installer Name will display as the “Service Provider” when the Help icon is pressed on a TouchNav.

Service Number: The system service number will be announced on keypads that support voice when a system fault is present, and displayed on keypads with a screen. Your customer service telephone number is the recommended setting. The Service Number will display when the Help icon is pressed on a TouchNav.

GMT Offset Hours/Minutes: Sets local GMT (Greenwich Mean Time).

DST Start / End month: Selects the months, daylight savings begins and ends for the particular installation region.

DST Start / End week: Selects which Sunday daylight savings begins and ends for the particular installation region.

Device ID, Firmware, Hardware, Bootloader, Web Version, Voice, and Language: Displays the current versions loaded on the connected ComNav.

Network Settings

Save Config

MAC Address: D8:80:39:19:03:57

Host Name: COMNAV

☒ Enable DHCP

☒ Enable Ping

☐ Enable NTP Server Time Updates

☒ Enable DLX900 Server

☒ Enable Web Access

IP Address: 192.168.66.68

Gateway: 192.168.66.1

Subnet Mask: 255.255.255.0

Primary DNS: 192.168.66.1

Secondary DNS: 0.0.0.0

Web Access Passcode: 12345678

Web Access Server 1:

Web Access Server 2:

DLX900 Port: 41796

Save Config

MAC Address: Media Access Control address (MAC address) is a unique identifier assigned by the manufacturer.

Host Name: Fixed as “ComNav”.

Enable DHCP: DHCP, or Dynamic Host Configuration Protocol allows networks to obtain configuration information and add devices automatically.

Enable Ping: The “ping” command is always functional whilst the ComNav is in program mode and is defaulted to NOT operate whilst the ComNav is in the normal run mode. Enable this option to allow the ComNav to respond to “ping” commands in normal operation.

Enable NTP Server Time Updates: This feature will update the panel time using the internet. This can automatically resolve the “Loss of Date/Time” alarm message.

Enable DLX900 Server: Enable remote access via DLX900.

Enable Web Access: This enables email and IP reporting. If Web Access Code is enabled then email and IP reporting will function.

Features	Email and IP Reports	UltraSync App
Enable Web Access = OFF Web Access Code = 00000000	No	No
Enable Web Access = OFF Web Access Code = not 00000000	Yes	Yes
Enable Web Access = ON Web Access Code = 00000000	Yes	No
Enable Web Access = ON Web Access Code = not 00000000	Yes	Yes

IP Address: An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network. If DHCP is enabled and supported by your network, the ComNav's IP address will be automatically assigned, otherwise you will be required to enter your unique IP address here.

Gateway: IP address of the router the ComNav is connected to which provides access to the internet. For end users this is usually their modem/router.

Subnet Mask: Allows a network to be divided into subnets, and allows the flow of network traffic between hosts to be segregated based on a network configuration. Applying the subnet mask to an IP address splits the address into two parts, an "extended network address" and a host address. A typical subnet mask is 255.255.255.0

Primary DNS: IP address of the primary DNS server which will allow the ComNav to discover the IP address of the servers it needs to connect to.

Secondary DNS: IP address of the secondary DNS server which will allow the ComNav to discover the IP address of the servers it needs to connect to when the Primary DNS server is not working.

Web Access Passcode: This code allows the smartphone app to connect to this ComNav. When set to 00000000 the app will not function.

Web Access Server 1: This server address should not be changed, it enables the remote web access, smartphone app and email services without requiring port forwarding. It requires the Primary DNS and Secondary DNS servers to be functioning.

Web Access Server 2: This server address should not be changed.

DLX900 Port: IP port used to accept connections from DLX900 desktop software.

Output Settings

Configure Outputs

Save Config

Output 1 Programming:

Activation Event:Manual Control

Activation Time:5

☐ Minutes☐ Latch

Output 1 Options:

☐ Code Reset☐ Invert

Output 1 Partitions:

☒ Partition 1☒ Partition 2☒ Partition 3☒ Partition 4☒ Partition 5☒ Partition 6☒ Partition 7☒ Partition 8

Output 1 Schedule:

☐ Open Schedule☐ Close Schedule

Output 1 Schedule Times:

Open Hour:8

Open Minute:0

Close Hour:17

Close Minute:0

Output 1 Schedule Days:

☐ Sun☒ Mon☒ Tue☒ Wed☒ Thu☒ Fri☐ Sat

Output 2 Programming:

Activation Event:Manual Control

Activation Time:5

☐ Minutes☐ Latch

Output 2 Options:

☐ Code Reset☐ Invert

Output 2 Partitions:

☒ Partition 1☒ Partition 2☒ Partition 3☒ Partition 4☒ Partition 5☒ Partition 6☒ Partition 7☒ Partition 8

Output 2 Schedule:

☐ Open Schedule☐ Close Schedule

Output 2 Schedule Times:

Open Hour:8

Open Minute:0

Close Hour:17

Close Minute:0

Output 2 Schedule Days:

☐ Sun☒ Mon☒ Tue☒ Wed☒ Thu☒ Fri☐ Sat

Save Config

The two on-board relays can be controlled through various system events or manually controlled by a user from the web page or smartphone app.

Note: From the activation event drop down list “Output 1 Trigger” and ”Output 2 Trigger” are fixed X10 module commands 0 and 1. This allows you to send an X10 module command 0 or 1 remotely by using Menu 4-Output Control on the ComNav.

Drop down Event	X10 Module Number
Output 1 trigger	0
Output 2 trigger	1

Activation Event: Select the required event from the drop down list that will activate the corresponding relay. Select Manual Control to allow end-users to control the relay from the Output Control Menu (also displays in UltraSync app).

Activation Time: Time the relay will be active, options 0-255. Default is in seconds unless the Minutes box is checked.

Minutes: On if output should be timed in minutes; off if timed in seconds

Latch: On if output should latch; off if output should be timed.

Code Reset: On if output should stop timing upon code entry; off if output should follow timer.

Invert: On if output should be inverted

Open Schedule: On if output should only activate between the opening and closing time.

Close Schedule: On if output should only activate between the closing and opening time.

Output Partitions: Is used to select the partition(s) the event must occur in before the output will activate.

Schedule Times: Sets the Opening / Closing hours and minutes (24 hour format) and the days of the week the event must occur in before the output will activate.

IP Reporting

IP Reporting

Save Config

Serial Number:

123412341234

Receiver 1 Format:

disabled

Use PSTN for Failover:

☐

Receiver 1 Selectors:

☒ Alarms

☒ Restores

☒ Opening/Closing

☒ Bypass

☒ Zone Trouble

☒ Power Trouble

☒ Tamperers

☒ Test Reports

☒ System Trouble

☒ Failure To Report

☒ Sensor Trouble

☒ Start/End Program Mode

☒ Cancel

☒ Recent Close

☒ Reserved

☒ Reserved

Receiver 2 Format:

disabled

Receiver 2 Selectors:

☒ Alarms

☒ Restores

☒ Opening/Closing

☒ Bypass

☒ Zone Trouble

☒ Power Trouble

☒ Tamperers

☒ Test Reports

☒ System Trouble

☒ Failure To Report

☒ Sensor Trouble

☒ Start/End Program Mode

☒ Cancel

☒ Recent Close

☒ Reserved

☒ Reserved

Save Config

Serial Number: The serial number of the ComNav.

Receiver format: Select the reporting format to match the IP receiver. Contact the control room for the correct settings.

Receiver Selectors: Select the events you want to report to the IP receiver. Note that event selection must be configured in the ComNav, not in the app.

Non-Provisioned OH Reporting

In certain applications, the panel can be configured to support non-provisioned Osborne-Hoffman Reporting.

1. The panel must not be provisioned in the UltraSync Servers.
2. Login to the NX-595 / ComNav as installer.
3. Click IP Reporting.
4. Select one the OH reporting options in the Receiver 1 Format field:
OH CID IP Format or OH SIA IP Format.
5. In the Receiver 1 Address field, enter the OH receiver IP address
6. In the Receiver 1 Port field, enter the OH receiver port number. This is set to 9999 at default.
7. Click Save Config.
8. Alarm panel will now report events to UltraSync and they will be delivered to OH receiver specified.

The screenshot shows the 'IP Reporting' configuration page. On the left is a sidebar menu with options: Logout, Arm/Disarm, Zones, Output Control, Feature Setup, Network Settings, Output Settings, and IP Reporting (which is highlighted). The main content area is titled 'IP Reporting' and contains a 'Save Config' button at the top. Below the button are several input fields: 'Serial Number' (229332390066), 'Receiver 1 Format' (OH CID IP format), 'Receiver 1 Address' (empty), 'Receiver 1 Port' (9999), 'Receiver 1 Account' (empty), 'Receiver 1 Number' (55), and 'Receiver 1 Line Number' (1). At the bottom is a checkbox for 'Use PSTN for Failover' which is currently unchecked.

Receiver Address: public IP address of the OH Net Receiver.

Receiver Port: port number of the OH Net Receiver.

Receiver Account: account number is forwarded to your automation software, may be up to 6 digits.

Receiver Number: one or two hexadecimal characters (0-9, A-F), default is one (1) if left blank.

Receiver Line Number: must be single hexadecimal character (0-9, A-F), default is one (1) if left blank.

Name Editor

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

Edit Names Then Click Save

Save

Copy

Copy All

Partition Names:

Partition1

Zone Names:

ZN1

ZN2

ZN3

ZN4

ZN5

ZN6

ZN7

ZN8

ZN9

ZN10

ZN11

ZN12

ZN13

ZN14

ZN15

ZN16

Output Names:

OP1

OP2

OP3

OP4

OP5

OP6

OP7

OP8

OP9

OP10

OP11

OP12

OP13

OP14

OP15

OP16

Entry Message:

Exit Message:

Edit Names Then Click Save

Save

Copy

Copy All

To load text labels **from** a TouchNav, 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 TouchNav to other TouchNav keypads and the ComNav.

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

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

Enabling Smartphone App

To enable UltraSync+ app access for your customer:

1. Look for the serial number label on the back of the ComNav PCB.
PROVIDE THIS SERIAL NUMBER TO THE END-USER.
2. Enter program mode on a keypad. Panel must remain in program mode to allow access to the web pages.
3. Find the IP address of your ComNav under Device 191, Location 21.
4. Enter the IP address into a web browser then login:
Username: **installer** Password: **9713**
Make sure your computer is on the same network as the ComNav.
5. Go to Menu > Network Settings and change the Web Access Passcode.
This 8-digit passcode grants access to the UltraSync+ app.
PROVIDE THIS CODE TO THE END-USER.
The default passcode is 00000000 and it disables remote access.
You must change this to allow end-users to use the app.

Network Settings

The screenshot shows the 'Network Settings' page with a 'Save Config' button at the top left. The settings are organized into two columns. The left column contains labels for various network parameters, and the right column contains their corresponding values. A red circle highlights the 'Secondary DNS' field, which has the value '0.0.0.0'. Below the 'Secondary DNS' field is the 'SSL Port' field with the value '443'. At the bottom of the form is another 'Save Config' button.

MAC Address:	00:1E:4C:0C:19:5E
Host Name:	Nx595E
☒ Enable DHCP	
☒ Enable Ping	
☐ Enable NTP Server Time Updates	
☒ Enable DLX900 Server	
☒ Enable Web Access	
IP Address	192.168.1.99
Gateway	192.168.1.1
Subnet Mask	255.255.255.0
Primary DNS	192.168.1.1
Secondary DNS	0.0.0.0
SSL Port	443
Web Access Passcode	00000000
Web Access Server 1	s1.zerowire.com:443
Web Access Server 2	s2.zerowire.com:443
DLX900 Port	41796

6. Add a Username to your Reliance System.
This example shows “User 1”.
PROVIDE THIS USERNAME AND PIN TO THE END-USER.

Configure Users

Select a User:	1 User 1
Displaying User:	1
User Name:	User 1
PIN:	1234
Pin Digits:	4

User Authority:

- ☐ Arm Only
- ☐ Schedule
- ☒ Master
- ☒ Arm/Disarm
- ☒ Bypass
- ☒ Report
- ☐ Reserved
- ☐ Reserved

User Partitions:

- ☒ Partition 1

7. Check red STATUS LED on ComNav is lit solid to indicate it is connected to the cloud servers. If it is blinking then it is still trying to connect, this should take less than 1 minute.

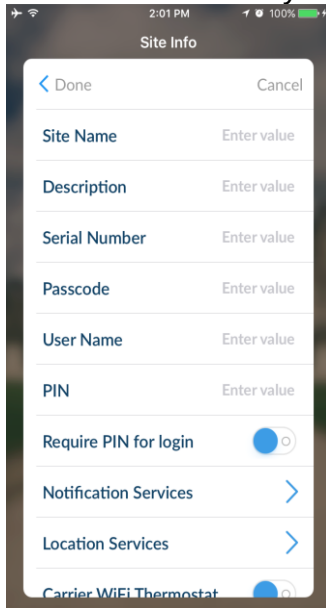
Installing UltraSync+ app

UltraSync+ is an app that allows a user to control the panel from an Apple® iPhone/iPad, or Google Android device. First set up the ComNav then download this app. Data 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.



The serial number is 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 Settings - Network.

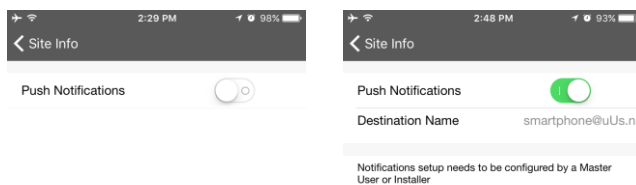
*The default username and PIN code is "**installer**" **9713** (for an installer) and "**User 1**" **1234** (for an end-user). Please note that there is a space between "User" and "1". You may also use any other valid user account.*

7. Click Done button to save the details.
8. Click the name of the Site to connect.

Smartphone Push Notifications

Register the smartphone

1. Open UltraSync+ on the smartphone that should receive push notifications.
2. Click the (i) symbol next to the ComNav you wish to receive push notifications from.
3. Scroll down and click “Notification Services”.
4. Click the slider button to register for Push Notifications.



5. Make a note of the Destination Name, it is case-sensitive.
6. Click Back.
7. Click Done.

Add smartphone as destination

8. You will need an account with “master” permission to proceed. This is controlled by the panel user permissions. User 1 and installer have master permission at factory default.
9. Open UltraSync+.
10. Click the site name to connect.
11. Click More, then Email. This will only be visible to accounts with “master” permission.
12. Type the Destination Name into one of the Email Address fields.
13. Click Save Config.
14. Click Sites and close the app. ComNav will now send push notification messages to that smartphone.
15. Arm / Disarm your security system using the alarm panel keypad (not from the app).
16. The smartphone specified should receive a push notification.
17. To disable push notification messages, repeat the steps above and delete the Destination Name from the Email Address field.

Change Destination Name

Each smartphone must have a unique name so that the ComNav can send push notifications to it. To change your smartphone name:

1. Open the app.
2. Click the Menu button on the top left.
3. Click Global Settings.

4. Click Notification Services.
5. The device name is displayed. Click it to change it.
6. Click Save.
7. Click Back to return to the home screen.

Troubleshooting

- If a username is changed after activating notifications on a smartphone then push notifications will not be delivered to that device. To fix, disable and re-enable push notifications on that device. Then update the destination field in the ComNav as described in “Smartphone Push Notifications”.
- Check the red STATUS LED on the ComNav is lit solid which indicates it is successfully connected to the cloud servers. If it is off or blinking, then check your cables and access to the internet. For example, unplug the Ethernet cable from the ComNav and connect it to a laptop to verify the laptop can access the internet. If the internet connection is functioning correctly, default the ComNav, power cycle the panel, and try again.
- Power cycle the customer’s router.
- Use a 3rd party network app (eg fingo) to verify the ComNav is connected to the customer network.
- Check you can connect to the ComNav while on the same network. For example, if the ComNav is connected to a WiFi router, then connect your smartphone to that WiFi network, enter the installer code on a keypad to enter Program Mode, then enter the IP address of the ComNav into a web browser on your mobile device. The ComNav login page should appear. This confirms if the ComNav is powered on and functioning correctly.
- 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.
- Confirm that other devices on the same network can connect to the internet.
- Check all access codes are correct (12-digit serial number, 8-digit Web Access Passcode is not 00000000, case-sensitive username, 4-8 digit PIN).
- Check that port forwarding is NOT configured on the network for the ComNav.
- When performing troubleshooting, ensure your device (smart phone, laptop, tablet, etc) is connected to the same network as the ComNav.
- Turn off WiFi on your mobile device and try using the app again while using mobile data.

Programming Worksheets

Location 1 - ComNav Features

Option 1 is used to set the zone-doubling feature. This feature will allow the two on-board zones to double to four zones. Please refer to Location 18 for starting zone number. If this feature is unselected, both on-board zones remain as single end of line zones and require 3K3 resistors.

When Zone doubling is enabled:

Lower zones = 3K7

Higher zones = 6K9

Segment 1	
(1)	Zone doubling
(2)	[Do not change]
(3)	[Do not change]
(4)	[Do not change]
(5)	[Do not change]
(6)	[Do not change]
(7)	[Do not change]
(8)	[Do not change]
Segment 2	
Segment 3	

Location 18 - Zone Starting Number

Location 18 is used to enter the starting zone number of the additional zones on the ComNav (also, see Location 1).

Data	Zones	Data	Zones	Data	Zones	Data	Zones
9	= 9 - 12	41	= 41 - 44	73	= 73 - 76	105	= 105 - 108
17	= 17 - 20	49	= 49 - 52	81	= 81 - 84	113	= 113 - 116
25	= 25 - 28	57	= 57 - 60	89	= 89 - 92	121	= 121 - 124
33	= 33 - 36	65	= 65 - 68	97	= 97 - 100		

Note: Starting Zone Number has an effect on panels supporting over 8 zones, otherwise it is ignored.

Segment 1	
-----------	--

Location 19 - Network Settings

Location 19 is used to set required network settings.

Enable DHCP: DHCP, or 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.

Enable Ping in the run mode: The “ping” command is always functional whilst the ComNav is in program mode and is defaulted to NOT operate whilst the ComNav is in the normal run mode. Enable this option to allow the ComNav to respond to “ping” commands in normal operation. For security reasons it is recommended this option remain disabled during normal operation.

Enable NTP Server Time Updates: The ComNav will check its internal clock and use the internet to compare it against GMT time. This is done every 15 minutes and will update itself if the variance is greater than 3 minutes. Note that if the ComNav is connected to the cloud servers for email or other services, this time update will occur automatically regardless of this setting. A backup battery holds the time and date during power outage.

Enable All Program Access from Web: When enabled an installer can always access Network Settings, Feature list, Outputs and IP Reporting via the ComNav's web pages. This option is not visible from the Web Server and can be changed from a keypad.

Enable DLX900 Server: Enabled by default, do not change.

Enable Web Access: When enabled, email and IP reporting will function.

Segment 1	
(1)	Enable DHCP
2	[Do not change]
3	[Do not change]
(4)	Enable Ping in run mode
5	Enable NTP Server Time Updates
6	Enable All Program Access from Web
(7)	Enable DLX900 server
(8)	Enable Web Access
Segment 2	

Location 20 - IP Gateway

The 4 segments in Location 20 are used to set the IP address of the networks gateway.

In homes, the gateway is usually the Internet Service Provider (ISP) device that connects the user to the internet, such as the WiFi modem.

In commercial settings, the gateway is typically the device such as a router/firewall that connects the internal LAN to the outside WAN (Internet).

Segments 1 - 4				
----------------	--	--	--	--

Location 21 - ComNav IP Address

The 4 segments in Location 21 are used to set the IP address of the ComNav so as it can be identified on the network.

Segments 1 - 4				
----------------	--	--	--	--

Location 22 - Subnet Mask

The 4 segments in Location 22 are used to set the Subnet mask.

Segments 1 - 4				
----------------	--	--	--	--

Location 23 - DNS Server 1

The 4 segments in Location 23 are used to set the networks DNS server address.

Segments 1 - 4				
----------------	--	--	--	--

Location 24 - DNS Server 2

The 4 segments in Location 24 are used to set the networks DNS server address.

Segments 1 - 4				
----------------	--	--	--	--

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

FAQ - Frequently Asked Questions

1. Do I need port forwarding?
No, built-in cloud services automatically configure remote connections.
2. Do I need an email server?
No, ComNav will send emails using a cloud service. This is automatically configured and you only need to specify the destination email address.
3. How do I connect/program the ComNav?
 - a. Default the ComNav.
 - b. Ensure the router supports DHCP (most do out of the box).
 - c. Connect the ComNav to the router using an Ethernet cable. The router should automatically assign the ComNav module an IP address.
 - d. On a keypad connected to the Reliance security system, enter *8 [Master PIN] 0# 191# 21# which will display the IP address of the ComNav. Press * to scroll through each segment of the IP address.
 - e. On a computer enter the IP address into a web browser to bring up the login page. The ComNav must remain in program mode to allow access.
 - f. Login to the ComNav. The default username/password is **installer 9713**. The PIN code is the installer PIN stored in the main control panel.
 - g. You can now program any additional settings you require via the web interface. As a minimum set the Web Access Passcode so the end-user can access it.
4. What if I cannot connect to ComNav with my computer?
 - a. Check that the router has DHCP enabled; refer to the router manual for details.
 - b. Default the ComNav. This will ensure DHCP is enabled.
 - c. Check that the customer's router has allocated an IP address to the ComNav in Location 21 of the ComNav. If it is 0.0.0.0 then DHCP is not working correctly. You should manually assign the ComNav a static IP address in Location 21. Make sure that it is on the same subnet as your computer and that the IP address is not used by another device.
 - d. Put the ComNav into program mode by using a keypad and enter device 191. By default this is an extra layer of security to prevent unauthorised remote access. Then try again from a web browser. You can also enable web access permanently on the ComNav in Location 19, Segment 1, Option 6 = On

- e. While the ComNav is in program mode: On a windows computer, click Run, type `cmd`, press Enter, then `ping [ip address]`. If there is an error it will show “timed out” and you should check your network. If you see a time then your computer can talk to the ComNav. You can also enable ping permanently on the ComNav in Location 19, Segment 1, Option 4 = On.
5. I’m not receiving any emails!
- a. Perform testing using a standard user PIN, the installer account by default does not send all reports.
 - b. Check that the emails are not being captured in your SPAM folder or blocked by a firewall.
 - c. Check the email address is correct.
 - d. Check that the event is ticked in the ComNav settings.
 - e. Check that you are receiving other emails.
 - f. Check that the relevant reporting options are enabled in the panel programming.
 - g. Try using UltraSync app to verify your system is connecting to the servers.
 - h. Try using another email provider to confirm the ComNav is sending emails.
6. I’m not receiving any push notifications!
- a. Enable push notifications on the smartphone.
 - b. Then enter the smartphone Destination Name into an email address field on the ComNav.
 - c. The Destination Name / email address is case sensitive.
 - d. Check the smartphone has notifications enabled. New features, privacy updates, and security updates by Google and Apple may hide push notifications. Follow steps to deactivate and re-enable push notifications.