HILLS Reliance

ComNav User Manual

S2096A

P/N 230672 • REV K • ISS 01DEC21

Trademarks and patents

Hills Reliance and ComNav are trademarks of Hills Limited.

UltraSync is a trademark of Carrier Corporation.

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:
Carrier
3211 Progress Drive, Lincolnton, NC, 28092, USA

Authorised EU manufacturing representative:
CARRIER
Kelvinstraat 7, 6003 DH Weert, Netherlands

EU compliance

CE

EU directives

Carrier 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.

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

Hills is an authorised distributor of Carrier

Contact information

www.hills.com.au

Customer support

Hills Technical Support 1800 252 213 or hts@hills.com.au

Version

Manual updated for firmware P004000-12

Contents

Important Information

Thank You

We hope that ComNav will provide you with convenient control of your Hills Reliance security system with the UltraSync+ smartphone 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 INTEROGIX'S PRODUCTS, SOFTWARE OR SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH CARRIER HAS NO CONTROL AND FOR WHICH CARRIER SHALL NOT BE RESPONSIBLE INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND OPERATING SYSTEM COMPATIBILITY; MONITORING SERVICES; ELECTRONMAGNETIC OR OTHER INTERFERENCE, AND PROPER INSTALLATION AND MAINTENANCE OF AUTHORISED PRODUCTS (INCLUDING ALARM OR OTHER CONTROL PANEL AND SENSORS).

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

CARRIER 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

Carrier 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

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

CARRIER 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 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 MAKES NO REPRESENTATION OR WARRANTY WITH RESPECT TO SUCH SERVICES INCLUDING WHETHER OR NOT THEY WILL BE COMPATIBLE WITH THE PRODUCTS, SOFTWARE OR SERVICES MANFUFACTURED, SOLD OR LICENSED BY CARRIER.

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.

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.

Introduction

The ComNav is an optional module that may be added to your Hills Reliance security system to provide remote access and reporting features:

- Remote access – UltraSync+ app provides remote access to your security system from your Apple or Android smartphone. Users can arm / disarm individual areas, check system status, edit users and PIN codes.
- Push Notifications and Email Reporting – ComNav can send push notifications or emails to up to 3 devices with the UltraSync+ app.

Glossary of Terms

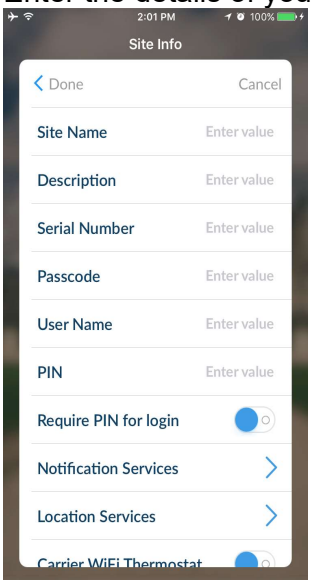
Authority Level	The level of access assigned to a user's PIN code
Arm	To turn your security system On.
Partition	Multiple "zones" (detection devices) can be allocated into "partitions" to permit users to selectively "arm" the security system. For example there may be 3 zones in a partition called Downstairs, 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. Hills Reliance 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.

Installing UltraSync+ app

UltraSync+ is an app that allows you to control your panel from an Apple® iPhone/iPad, or Google Android device. First set up the ComNav 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.



The serial number is on the back of the ComNav unit.

The default Web Access Passcode of 00000000 disables remote access. An installer can change it under Menu - Settings - Network.

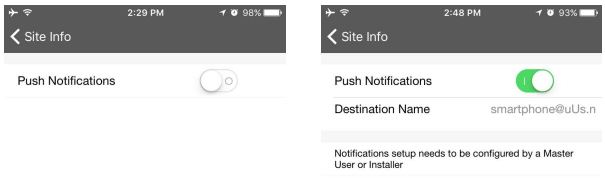
The username and PIN code is for any authorised user on the system. The default username and PIN code is "User 1" 1234 (for a user). Please note that there is a space between "User" and "1".

7. Click Done button to save the details, then Sites to go back.
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. At factory default only User 1 can add destinations to the ComNav. This is because User 1 has “master” permission. You will need an account with “master” permission to proceed.
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 connected to ComNav 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.

ComNav Settings

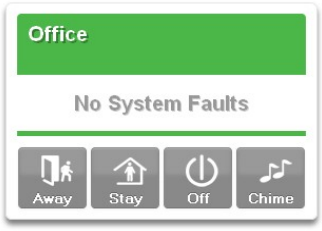
Changes to ComNav settings should be performed using the UltraSync+ app.

Access Levels

There are two access levels available to users – master code or standard user codes.

Master codes have greater authority and can change settings and add/remove users.

Status and Partition Control



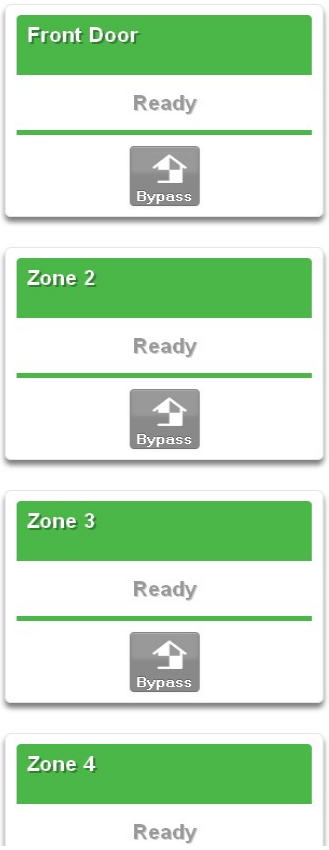
Area Colour	
Green	Area is active, and all zones are secure
Yellow	Area is armed in the stay mode
Red	Area is armed in the away mode
Blue	System condition present
Grey	Area not ready, zone(s) open

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.

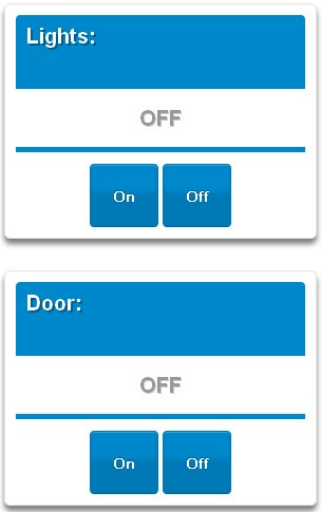
To disarm area/s from either the stay or away arming modes, click on the Off button.

Zones



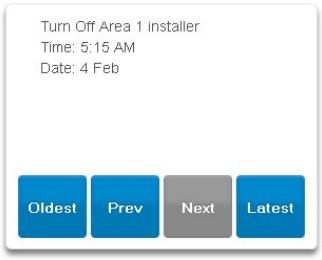
From the Zones menu you can view zone status and bypass zones.

Output Control



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

History



Current system faults will be displayed on the Status page and the system's 512-event log can be accessed via the History menu.

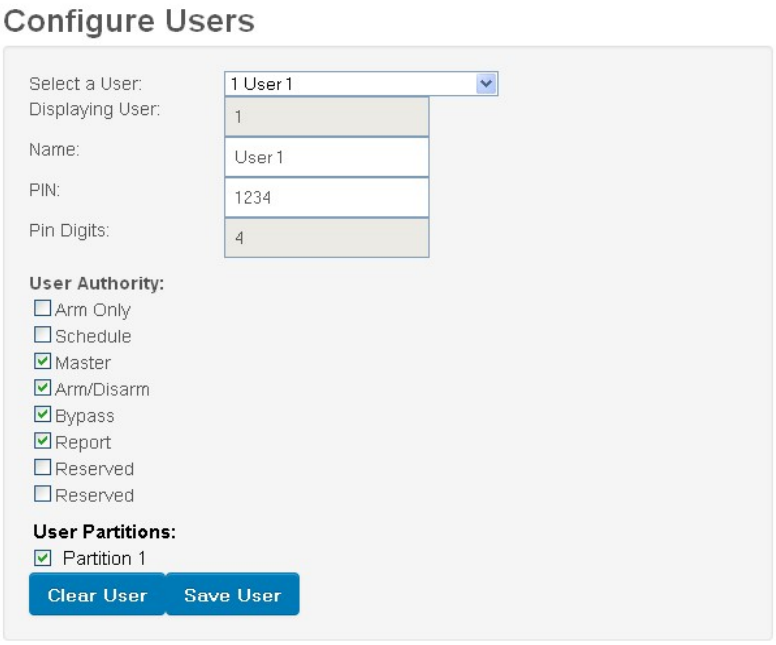
Oldest – Will display the oldest event available.

Prev – (Previous) will display an older event.

Next – Will display a newer event.

Latest – Will display the most recent event.

Users



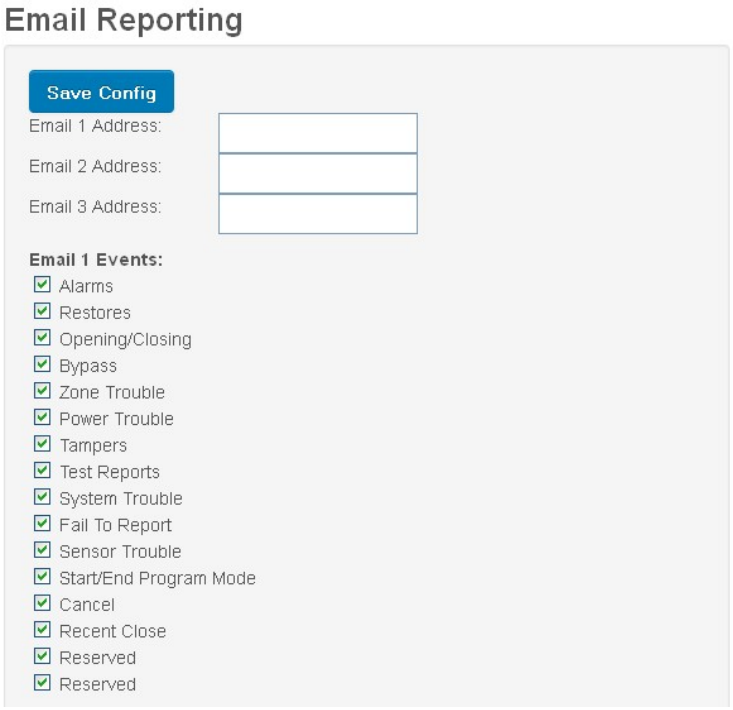
Users must be given a User Name on this menu to provide access to the UltraSync app.

PIN codes are also assigned to users on this screen. A user PIN code is required to arm and disarm areas in your security system. They are generally 4-digits long but should be increased to 6-digits for more security. 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 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.

Email Reporting – examples

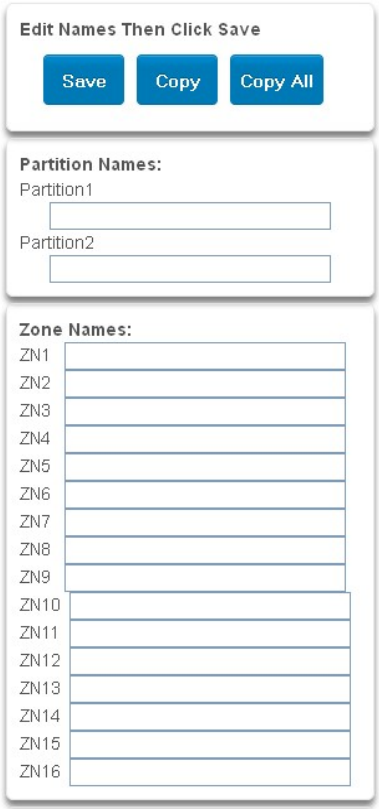
User Arming:	Security Report From Account 0001 Turn on Partition 1 Fred Time: 11:55 AM Date: 19 Jun
Panic Button on keypad:	Security Report From Account 0001 Keypad Panic Alarm Partition 1 Time: 11:55 AM Date: 19 Jun

Name Editor

If you have touch screen keypads installed for your security system, the Name Editor on the ComNav allows you to customize the names that appear on the screen for areas, zones, and outputs.

To load text labels **from** a touch screen keypad, 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 touch screen keypad to other touch screen keypad and the ComNav.



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

1. Click Save.
2. Click Copy All to send all text labels to touch screen keypads, or Copy to send only changed items (faster).

- Copy and Copy All includes all User Names entered on the Users Menu

Troubleshooting the smartphone app

- If you change a username after activating notifications, disable and re-enable notifications. Then perform the steps described in “Smartphone Push Notifications” using this new Destination Name.
- 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).
- ComNav depends on having access to a reliable internet connection via its Ethernet port. Turn your internet router off and on to reset the connection to ComNav.
- 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.
- Temporarily disable your internet router security settings or firewall. These can block the ComNav from accessing the internet.
- If you have access to the physical ComNav and box tamper is not enabled – check the STATUS light on the ComNav is lit red and stays on. This indicates successful connection to the cloud servers to enable the app. A flashing STATUS light indicates the ComNav is trying to connect to the internet.
- Reboot your internet router.
- Contact your installation company for further assistance.

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

Hills Branches		
Alexandria (NSW) Bldg 5, 85 O'Riordan Street ALEXANDRIA 2105 Phone: 02 9311 8700	**Seven Hills (NSW)** 18/24 Abbott Road via Costello Place, SEVEN HILLS 2147 Phone: 02 97490994	**Fyshwick (ACT)** 40 Kembla Street Fyshwick ACT Phone: 02 6228 1477
Banyo (QLD) Lot 2, 12 Huntington Place BANYO QLD Phone: 07 3623 0900	**Nerang (QLD)** 65 Lawrence Drive Nerang QLD 4211 Phone: 07 5500 7250	**Torrensville (SA)** Unit 1, 107-109 Hayward Ave Torrensville SA 5031 Phone: 08 8150 9400
Coburg (VIC) 51 Moreland Road Coburg Victoria 3058 Phone: 03 9381 3400	**Notting Hill (VIC)** 41-43 Normanby Road Notting Hill VIC 3168 Phone: 03 8542 5100	
Balcatta (WA) 11 Abrams Street Balcatta WA 6021 Phone: 08 6240 9500	**Moonah (TAS)** 33 Sunderland Street Derwent Park TAS 7009 Phone: 03 6272 0211	