



# **Nexus Hawk™ User Manual**



**ANY NETWORK, ANYTIME, ANYWHERE**

**Please read the complete User Manual before starting your Nexus Hawk.**

# Table of Contents

<b>INTRODUCTION</b>	<b>1</b>
WHAT'S INCLUDED WITH THE NEXUS HAWK?	1
<b>GETTING STARTED</b>	<b>1</b>
CONNECTING TO POWER	1
STAYING CONNECTED	1
10/100 ETHERNET DATA CONNECTION	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>LOGIN</b>	<b>2</b>
ACCESSING THE MANAGEMENT CONSOLE	2
<b>SETUP   PCMCIA</b>	<b>2</b>
CELLULAR WAN	2
PREFERRED WIRELESS CARDS	2
WWAN WATCHDOG	3
<b>SETUP   WIFI</b>	<b>3</b>
AP/CLIENT CONFIG	3
CLIENT	4
MAC FILTERING	4
<b>SETUP   10/100 ETHERNET</b>	<b>5</b>
ETH0 (WAN) PORT	5
ETH1 (LAN) PORT	5
<b>SETUP   SERIAL</b>	<b>6</b>
GPSD	6
GPS AGGREGATION	6
DATA CACHING	7
GPS BEACON	7
<b>SECURITY   VPN CLIENT</b>	<b>7</b>
IPSEC	7
IPSEC (CISCO XAUTH)	8
OPENVPN	8
<b>SECURITY   VPN SERVER</b>	<b>9</b>
OPENVPN	9
<b>APPLICATIONS   WAN PORTS</b>	<b>10</b>
PORT FORWARDING	10
DMZ HOST	10
REMOTE ACCESS	10
<b>APPLICATIONS   ADVANCED ROUTING</b>	<b>11</b>
STATIC ROUTES	11
DEFAULT ROUTE	11
<b>ADMINISTRATION   MANAGEMENT</b>	<b>11</b>
PASSWORD	11
DDNS	12
STATIC DHCP	12
FAILOVER	12

NTP	12
<b>ADMINISTRATION   DEBUG FILE DOWNLOAD</b>	<b>13</b>
<b>ADMINISTRATION   RESET</b>	<b>13</b>
REBOOT SYSTEM	13
RESTORE DEFAULTS	13
<b>ADMINISTRATION   FIRMWARE UPDATE</b>	<b>13</b>
<b>ADMINISTRATION   SAVE/RESTORE SETTINGS</b>	<b>13</b>
SAVE CURRENT SETTINGS	14
RESTORE SETTINGS	14
<b>IP LOOPBACK</b>	<b>14</b>
<b>SETTINGS PERSISTENCE</b>	<b>14</b>
<b>STATUS</b>	<b>14</b>
WAN CONNECTIVITY	14
PCMCIA SLOTS	14
WiFi	15
10/100 ETHERNET	16
SERIAL	16
SECURITY	16
<b>HELP</b>	<b>16</b>
<b>TECHNICAL SPECIFICATIONS</b>	<b>17</b>
<b>TROUBLESHOOTING</b>	<b>18</b>
<b>INDEX</b>	<b>20</b>
PRODUCT LIMITED WARRANTY	23
FEDERAL COMMUNICATIONS COMMISSION	25

# Introduction

Congratulations on your purchase of a Nexus Hawk™! This literature is intended as a primary reference for normal configuration and operation of the Nexus Hawk. The information presented within should allow most users to easily configure the device to their preferences. As with any product from Nexus iSR, should you encounter any difficulties, technical support is standing by to help you.

## What's Included with the Nexus Hawk?

- Nexus Hawk
- WiFi Antenna
- Ethernet Crossover Cable
- Power Supply
- QuickStart Guide

# Getting Started

## Connecting to Power

The Nexus Hawk accepts DC power input ranging from 11-48V. Upon power-up, both the **green** Power-LED and the **red** Status-LED will illuminate. **Allow the unit approximately 90 seconds to complete its startup sequence.** During this time, it is performing a Power On Self Test (POST). When the **red** Status-LED begins pulsing, your Nexus Hawk is fully powered up and ready!

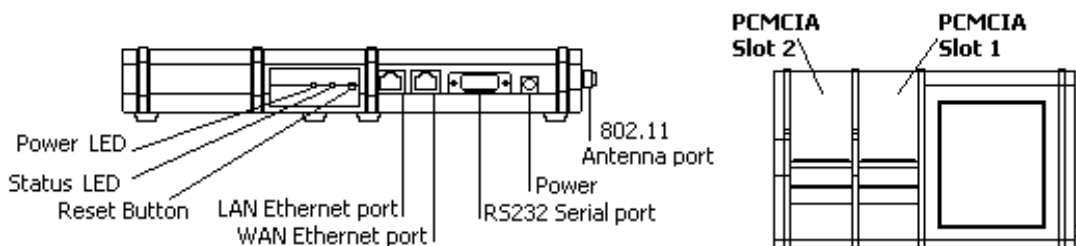
## Staying Connected

The Nexus Hawk has four possible paths to the Internet/WAN: 10/100 WAN (Eth0), WiFi Client (connected to a WAN-connected WiFi Access Point), Cellphone Card 1 (Slot 1), Cellphone Card 2 (Slot 2). Connectivity is prioritized in this order. If a higher priority connection is established, the data stream will automatically transfer to it. If a connection is lost, the Nexus Hawk will attempt to transfer WAN functions to the next lowest priority connection (if one exists).

## WiFi Connection

The Nexus Hawk's WiFi port is enabled by factory default with WEP security. This allows users to access the Nexus Hawk without an Ethernet crossover cable and without creating an "open" access point for others to exploit.

The SSID includes the last 10 characters of the Hawk's serial number. The WEB pre-shared key is the last 10 characters of the Hawk's Eth0 MAC address. Note: The MAC address (hence, pre-shared key) is calculated by subtracting "1" from each character of the Hawk's serial number (e.g. - S/N 112233445C, MAC= 001122334B)



# Login

## Accessing the Management Console

Launch a web browser (e.g. - Internet Explorer, Firefox, etc.) and enter the following address: **192.168.1.1** (the factory default value). The "splash page" will give you the option of either viewing or changing the configuration of your Nexus Hawk.

You may view configuration without being authenticated.

To change the configuration, authentication is required. Factory defaults for authentication are:

Username: **manager**

Password: **manager**

# Setup | PCMCIA

## Cellular WAN

The Nexus Hawk card slot(s) support only Cellular Data Cards. The Cellular WAN option allows the Nexus Hawk to provide access to the internet through the services of a major mobile telephone service carrier.

Insert your Nexus Hawk preferred cellular data card into a card slot.

The Nexus Hawk will automatically detect which data carrier your cellular card is on and connect to the network when the card is inserted, eliminating interaction from you the customer.

## Preferred Wireless Cards

- Cingular - Options GT Max (1.8)
- Cingular - Sierra Wireless 875
- Sprint - Novatel Wireless Merlin S720
- Sprint - Pantech PX-500
- Sprint - Sierra Wireless 595
- Verizon - Kyocera KPC-650
- Verizon - PC-5750
- Verizon - V740 (Express Card)

**Detected:** This field will display the manufacturer's model name of the detected card.

**Connect:** Pressing this button connects the inserted card to the cellular network.

**Disconnect:** You **must** either power-down, or press this button before removing your cellular data card from the Nexus Hawk. Failure to do so may cause malfunction.

**Dialup parameters:** The dialup parameters options are used for connecting to

- **Auto:** Use this option to automatically connect the the cellular network. **(DEFAULT)**
- **Manual:** Use this option if your air card needs to specify specific parameters to connect to the cellular network.
  - **Username, Password:** Check this option if a username and password is required to connect
  - **Phone Number:** Check this option and enter the password required to connect
  - **APN Identifier:** Check this option and enter the APN Identifier required to connect
  - **Port Speed:** Check this option and select the desired port speed when connecting

After pressing the Connect button the Cellular WAN configuration page will briefly refresh and indicate with the available button selections that a connection has been initiated.

Your selections may be verified by navigating to the **Status** page on the top navigation bar. Once a connection has been established, the carrier, signal strength *of signal upon initial connection*, and connection IP address will be displayed on the status page.

**NOTE:** Some cellular data cards will report 'No signal strength returned' for the signal strength of the card; this is normal operation of the card and/or network.

**NOTE: For best results power down before removing card.**

### **WWAN Watchdog**

**Enabled:** Enables the WWAN Watchdog functionality

**Ping host:** Host to ping in determining connectivity status

or

**Use PPP connection peer:** This option pings the closest available host on the cellular PPP link: the opposite end of the connection. If checked, the Ping host entry will be disregarded.

**Packet size:** Enter the size of the packet to ping in bytes. **DEFAULT: 56 bytes**

**Interval:** Enter the number of milliseconds between pings. **DEFAULT: 1000 milliseconds**

**Sample size:** Enter the number of pings to send before evaluating results. **DEFAULT: 10 packets**

**Packet loss exceeds:** Enter the packet loss percentage at which the watchdog will trip.

and/or when selecting both packet loss **and** latency, determines if both or only one criteria will trip the watchdog.

**Average latency exceeds:** Enter the average latency in milliseconds for the ping set beyond which the watchdog will trip.

**Watchdog action:** From the dropdown box specify what the watchdog should do when it trips.

- Redial connection
- Reboot Hawk

**Slot 2, Use same settings as Slot 1:** This option allows you to have Slot 2 use exactly what you specified for Slot 1 without having to re-enter it all.

## **Setup | WiFi**

### **AP/Client Config**

#### **AP**

This selection will enable the Nexus Hawk to function as a WiFi Access Point (AP), sharing its connections with others (Clients) who may connect to it. The Nexus Hawk may serve as either an AP or Client of another AP, *but not both at the same time*.

**NOTE:** When in WiFi AP mode, the Nexus Hawk's WiFi port and LAN (Eth1) port are bridged together at the physical layer as a single virtual device. This means that all IP information is the same (192.168.1.1, for instance). As a result, all LAN clients share the same DHCP pool, subnet, and can access each other. Firewalling and port forwarding may be done to any device on this shared virtual network. This occurs only in WiFi AP mode, and not in WiFi Client mode.

**SSID:** This is the name of your wireless network. This option has a 32 alphanumeric character limit. For more information click [here](#)

**Broadcast SSID:** Check this option to broadcast the name of your AP's WiFi network to others. Doing so makes discovery and attachment to your AP easier. Failing to broadcast it makes your AP somewhat more secure, by requiring trusted clients (people who will attach to it) to know the SSID without being prompted.

**Channel:** Select the channel on which your AP will operate. Channels 1-11 coincide with 802.11b/g (2.4 GHz) while channels 36 and up coincide with 802.11a (5.8GHz). Effort should be made to select a channel that is not in use in the immediate vicinity of the Nexus Hawk in order to minimize interference and maximize the WiFi efficiency.

**Security:** This specifies the security mode of the Nexus Hawk's WiFi AP.

**None:** Selecting this option creates an "open" or unsecured AP.

**WEP:** *Wireless Equivalent Privacy* is available in two modes; **64-bit** (shorter key) and **128-bit** (longer key). Selecting this option requires you to enter a private key that is known only to you and trusted others that you want to allow to connect to your AP. For more information click [here](#)

**WPA-PSK, WPA2-PSK, WPA/WPA2-PSK:** This stands for: *WiFi Protected Access*. Selecting this option requires you to enter a pre-shared key to secure the AP connection. The WPA/WPA2-PSK option allows for dual operation of both WPA and WPA2 for connected clients. For more information on WPA click [here](#) For more information on WPA2 click [here](#)

**Pre-shared key:** This is a passphrase that is used by the selected security mode. For WEP-level security, this must be a hexadecimal value using the digits 0-9 and letters from A-F. For the 64-bit option the value must be 10 characters. For 128-bit option the value must be 26 characters. For WPA/WPA2-level security, the value must be alphanumeric and a minimum of 8 characters and may be a maximum of 63 characters.

The AP's IP address is the same one that is specified for the **10/100 Ethernet LAN** configuration (Eth1). For example, if the 10/100 Ethernet LAN IP is set to the factory default of 192.168.1.1, this will also be the IP address for the WiFi port of the Nexus Hawk. They are considered "bridged".

## Client

The Nexus Hawk may connect to an 802.11a/b/g compliant WiFi Access Point (AP). This function may be found by navigating to the "**Setup | WiFi**" page. Check the "**Client**" box to enable the AP Client.

**SSID:** Enter the known SSID of the 802.11 a/b/g network that you wish to connect to. Once this option is selected and applied, it remains active. The Nexus Hawk will continue to scan for an AP with the entered SSID until it is able to locate it, at which point it will connect. If that AP disappears, the Nexus Hawk will resume its scanning function in an attempt to connect when one appears. For more information click [here](#)

**[Scan]:** Select this option to view any in-range AP's that are broadcasting their SSID's. Simply click the hyperlink to make your selection. To find out more about the AP hardware click on the MAC Address link which will perform a MAC Address lookup.

**Security:** This is defined by the AP, not the Nexus Hawk. Select the type of security set by the AP. NOTE: Some AP's differentiate between WPA-PSK and WPA2-PSK. The Nexus Hawk does not. If the AP uses either, simply select the **WPA/WPA2-PSK** option.

**Pre-shared key:** Enter the AP's pre-shared security key. This field is required if security is set to WEP or WPA.

**DHCP Client:** This allows the Nexus Hawk to be automatically configured to function on a network provided by another AP.

If **Enabled** the Nexus Hawk will attempt to obtain configuration information from a DHCP enabled AP.

If **Disabled**, the Nexus Hawk will require manual IP assignment (also known as "Static IP") and the following console options will come into play:

**IP Address:** Enter the manually assigned (static) IP address. For more information click [here](#)

**Netmask:** Select the desired netmask from the drop down list. For more information click [here](#)

**Gateway:** Enter the desired gateway. For more information click [here](#)

**DNS1:** Enter the desired primary Domain Name Server's address. For more information click [here](#)

**DNS2:** Enter the IP address for an optional (not required) Secondary DNS.

Settings may be verified by navigating to the **Status** page on the top navigation bar. The wireless client status section will show a connection status, the SSID of the connected network, and a signal strength indicator.

## MAC Filtering

The Nexus Hawk supports MAC Filtering of wireless devices. MAC Filtering allows specified wireless devices to connect by allowing or denying each specified MAC addresses.

**Enabled:** Enables MAC Filtering functionality.

**Allow:** This option allows *only* the specified MAC addresses entered to connect to the Hawk

**Deny:** This option denies the specified MAC addresses access from connecting to the Hawk

**MAC:** Enter the desired MAC addresses. For more information on MAC click [here](#)

**Delete:** Deletes the specified address

**Apply Changes:** Saves the changes that were made.

## Setup | 10/100 Ethernet

### Eth0 (WAN) Port

The Nexus Hawk has two Ethernet ports. The port that is closest to the DC power jack is **ETH0** -- and is exclusively reserved to allow the Nexus Hawk to connect to devices that provide Wide Area Network (WAN) connectivity. Connection is by a standard RJ-45 Ethernet patch cable.

**DHCP Client:** This allows the Nexus Hawk to attempt to obtain configuration information from a DHCP enabled WAN device. For more information click [here](#)

**Enabled:** The Nexus Hawk automatically obtains configuration parameters from a DHCP server on the WAN.

**Disabled:** The Nexus Hawk will allow the Console Operator to manually configure networking parameters as follows:

**IP Address:** Enter the assigned (static) IP address. For more information click [here](#)

**Netmask:** Select the desired netmask from the drop down list. For more information click [here](#)

**Gateway:** Enter the IP address of the desired gateway. For more information click [here](#)

**DNS1:** Enter the IP address of the desired Primary Domain Name Server (DNS). For more information click [here](#)

**DNS2:** Enter the IP address for an optional (not required) Secondary DNS.

**Apply Changes:** Saves the changes that were made.

Settings may be verified by navigating to the **Status** page on the top navigation bar. A well configured **Eth0** status will display as "Connected" with a properly formatted IP address.

### Eth1 (LAN) Port

The Nexus Hawk has two Ethernet ports. The port that is closest to the <RESET> button is ETH1 -- and is exclusively reserved to allow local network (LAN) connection to the Nexus Hawk (such as used by a locally connected computer). Direct-connection to a computer will require a Category-5 (minimally) Ethernet crossover cable (a **RED** crossover cable is supplied with your purchase and is included in the packaging). For more information click [here](#).

**Warning**, if you are using this port to configure the Nexus Hawk : Changes here can cause you to lose connectivity to the Nexus Hawk. **Proceed with caution.** If at any time, you lose connection and are unable to recover, you may regain control by resetting the Nexus Hawk to factory defaults.

**IP Address:** The default address is 192.168.1.1 It may be manually changed here. Note: Changing this address, while connecting through this port will cause loss of connectivity. To regain connectivity, perform a DHCP IP renewal on your client. From your computer's command prompt:

**Windows2000/XP:**

```
ipconfig /release <enter>
```

```
ipconfig /renew <enter>
```

**Linux:**

```
ifconfig /release <enter>
```

```
ifconfig /renew <enter>
```

**Netmask:** Select the desired netmask from the drop down list. For more information click [here](#)

**DHCP Server:** For more information click [here](#)

**Enabled:** The Nexus Hawk will provide dynamic configuration parameters to LAN devices.

**Disabled:** The Nexus Hawk will not provide dynamic configuration parameters to LAN devices. This will require that all LAN devices be manually configured, individually.

**Apply Changes:** Saves the changes that were made.

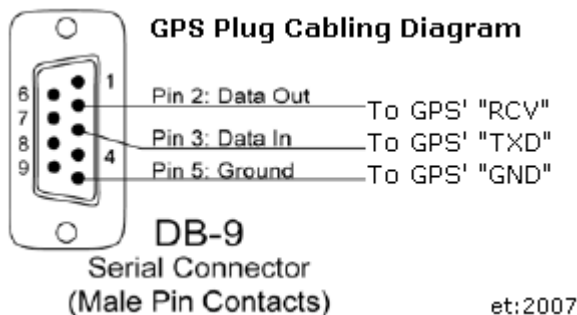
You may verify that the Nexus Hawk has been properly configured by navigating to the **Status** page on the top navigation bar. A well configured **Eth1** status will display as "Connected" with a properly formatted IP address.

## Setup | Serial

### GPSd

NOTE: The Serial Port supports only Global Positioning System (GPS) functionality in this firmware revision. The GPS must be both serial (RS-232c) and capable of providing NMEA-0183, Rockwell or Garmin Binary data streams (all of which are converted into NMEA-0183 on the selected port). The Nexus Hawk's firmware will auto-detect the communication settings (baud rate, parity, etc.) of the connected GPS.

Only three wires are needed for data connectivity, TXData, RXData and Ground. The diagram below shows the cabling from the perspective of a plug that is attached to the GPS.



**Enable GPSd:** Enables the described function. For more information on GPSd click [here](#)

**TCP Port:** This is the TCP port that will interface with the GPS. Most simply, one may use TELNET to attach to the port and manage the GPS (including the receipt of NMEA sentences, once the GPS is commanded to send data). By default, this is **192.168.1.1:2947** though it may also be accessible remotely by DNS if a dynamic DNS service has been subscribed to. For more information on TCP click [here](#)

**Apply Changes:** Updates are applied only when this button is pressed.

Upon pressing **Apply Changes**, the Nexus Hawk will immediately open the designated port to/from the GPS. Some GPS's may appear to sit idle until a user sends a command to activate their data stream. The most often used code is simply "r", at which point the port will present raw NMEA strings. For more information on how to use GPSd-presented data for mapping and navigation applications, visit <http://www.penguin-soft.com/penguin/man/1/gpsd.html>.

**Note:** With only this selected, the GPS data stream is available only to LAN and WiFi connected clients. You may present the GPS data stream to the WAN port by additionally selecting the [Access to GPS Port](#) option.

### GPS Aggregation

The GPS Aggregation page enables the Nexus Hawk to send GPS data updates to an aggregator. Updates may be sent at timed intervals or continuously and GPS data will be cached for later delivery in the event of a disconnect. Supports APRS standard or raw NMEA data streams. **GPSd must be enabled for aggregation to be available.**

**Connect to aggregator:** Enables the GPS to connect to the aggregator specified

**Host:** Enter the host IP address of the aggregator

**Port:** Enter the port number to connect to on the host

**Continuous:** Select the Continuous option to send continuous data without stopping

**Timed:** Select the Timed option to send data at the interval specified

**Cache GPS data when aggregator is unavailable:** Check this option to enable the caching of GPS data when the aggregator is unavailable.

**APRS:** Sends out APRS data. APRS is a trademark of APRS Engineering, LLC, Bob Bruninga President.

- **Callsign/ID:** Enter the callsign/ID to represent the GPS. The callsign/ID must contain at least one number.
- **Icon:** Select the icon to represent the GPS

- **Overlay:** Eleven of the icons support overlay. GPSOD - Digi; GPSOG - HF Gateway; GPSA0 - Circle; GPSNV - Car; GPSAA - Box; GPSDV - Aircraft; GPSDW - WX station - Green; GPSSN - Triangle; GPSSS - Ship/Boat; GPSSU - Truck; GPSSV - Van.

**Raw (default):** Send out raw NMEA data

- **Header:** Enter the custom header to send in front of the NMEA strings
- **Force APRS-style authentication:** Check this option to send a valid APRS-style authentication string to the specified aggregator.

## Data Caching

The Nexus Hawk will cache GPS data upon loss of a path to the target host (either an aggregator or a single host) but the cache is not used as long as there *is* an active path in effect. Upon restoration of the path the cache will be sent to the target host.

## GPS Beacon

The GPS Beacon is used to send specified GPS sentences to the source specified. This feature is useful when trying to keep bandwidth usage down.

**Enable GPS Beacon:** Enables the GPS Beacon functionality

**Host:** Enter the host IP address

**Port:** Enter the port number to connect to on the host

**Interval:** Enter the interval in seconds at which you want the Hawk to send data to the host

**TCP:** Select this option to send the data via TCP. For more information on TCP click [here](#)

**UDP:** Select this option to send the data via UDP. For more information on UDP click [here](#)

**Bind sockets/datagrams to LAN IP address:** Forces outgoing GPS Beacon data to originate from the Nexus Hawk's LAN IP address. Should only be selected if the GPS Beacon destination is on the other end of a standard IPsec tunnel (not Cisco Xauth). **DEFAULT: Disabled**

**NMEA Sentences to report:** Check which sentences you want to send out.

- GPRMC - Recommend minimum specific GPS data
- GPGGA - Global positioning system fix data
- GPGSA - GPS DOP and active satellites
- GPGSV - GPS satellites in view

**Custom Header:** Enter the custom header to send in front of the NMEA-0138 string

# Security | VPN Client

## IPsec

IPsec is a protocol allowing VPN connectivity from a client to a central location, providing secure access to a private LAN over a WAN. The Nexus Hawk supports IPsec client functionality and will route traffic from connected client devices over the VPN as well, thus replacing the need for many IPsec clients with one. For more information on IPsec click [here](#)

**Enabled:** Enables IPsec client connectivity

**Server IP/Hostname:** Enter the hostname/ IP address of the IPsec server or concentrator

**Server subnet:** Enter the server subnet

**Phase 1:** The first phase of authentication and handshaking to establish an IPsec session.

**DH Group:** Diffie-Hellman key group. Options are Group 2 or Group 5

**Encryption:** Encryption algorithm to be used for Phase 1 handshaking.

3DES: Triple Data Encryption Standard. For more information click [here](#)

AES-128: Advanced Encryption Standard 128-bit. For more information click [here](#)

**Authentication:** Authentication hash to be used for Phase 1 handshaking.

MD5: Message-Digest algorithm 5. For more information click [here](#)

SHA1: Secure Hash Algorithm. For more information click [here](#)

**Phase 2:** The second phase of authentication and handshaking to establish an IPsec session.

**Encryption:** Encryption algorithm to be used for Phase 2 handshaking.

3DES: Triple Data Encryption Standard. For more information click [here](#)

AES-128: Advanced Encryption Standard 128-bit. For more information click [here](#)

**Authentication:** Encryption algorithm to be used for Phase 2 handshaking.

MD5: Message-Digest algorithm 5. For more information click [here](#)

SHA1: Secure Hash Algorithm. For more information click [here](#)

**Authentication Type:** Select the type of authentication that you want to use for IPsec

X.509 Certificates: Select this option to use the X.509 encryption type. For more information click [here](#)

Pre-shared Key: Select this option to use a pre-shared key for authentication

**Pre-Shared Key:** Enter the pre-shared key defined by your network administrator

**CA Certificate:** Certificate of the Certificate Authority used to sign the other certificates in use. Enter the CA certificate here. Please ensure that the certificate is copy-pasted correctly.

**Public Server Certificate:** Enter the certificate assigned to the IPsec server here. Please ensure that the certificate is copy-pasted correctly.

**Public Client Certificate:** Enter the certificate assigned to the IPsec client here. Please ensure that the certificate is copy-pasted correctly.

**Private Client Key:** Enter the client key here.

**Private key passphrase:** Enter the private key passphrase here.

## **IPsec (Cisco Xauth)**

The Nexus Hawk supports IPsec login to Cisco VPN concentrators with group and username credentials.

**Enabled:** Enables the IPsec (Cisco Xauth) functionality.

**Server IP/Hostname:** Enter the server IP or hostname on which the Cisco VPN concentrator resides.

**IPsec Group ID:** Enter the IPsec group id

**IPsec Group Secret:** Enter the IPsec group secret

**Xauth Username:** Enter the Xauth username required by the Cisco VPN concentrator

**Xauth Password:** Enter the Xauth password required by the Cisco VPN concentrator

**DPD Interval:** Time between dead peer detection messages sent from the VPN client to the concentrator.

There is a known incompatibility between this feature and Cisco PIX devices. Nexus recommends disabling this option when connecting to a PIX. **DEFAULT: 300, DISABLED: 0.** For more information on DPD click [here](#)

**NAT-T Mode:** Mode in which the Nexus Hawk's VPN client will traverse NAT firewalls.

- **Auto:** The Nexus Hawk will auto-detect NAT-T mode
- **None:** Use no NAT-T
- **Force NAT-T (DEFAULT):** highly recommended for Cisco PIX re-key compatibility
- **Cisco UDP:** Uses Cisco proprietary UDP encapsulation

**Cisco UDP Port:** Local port for Cisco UDP encapsulation. Only relevant if Cisco UDP is selected for NAT-T mode. **DEFAULT: 10000**

**Maximum Session Length:** Maximum amount of time the Nexus Hawk will allow a VPN session to continue before terminating it and redialing. Especially useful when re-key problems with the concentrator are encountered. **DEFAULT: 0**

**Redial pause:** Amount of time the Nexus Hawk will wait between VPN connection attempts to the concentrator. **DEFAULT: 10**

## **OpenVPN**

For advanced users, the Nexus Hawk supports functioning as an OpenVPN endpoint. For more information on OpenVPN click [here](#). For a how-to guide in setting up a VPN server click [here](#)

**Enabled:** Enables OpenVPN functionality.

**Interface Type:**

- **tap:** Simulates an Ethernet device and operates with Layer 2 packets. Used to create a Network bridge
- **tun:** Network Tunnel simulates a network layer device and operates with Layer 3 packets. Used with Routing. For more information on tun click [here](#)
- For more on tap and tun information click [here](#)

**Server IP/Hostname:** Enter the server IP address or hostname

**Port:** Enter the port number of the VPN tunnel

**Protocol:** Select which protocol you wish to use.

- **TCP:** Select this option to use TCP. This option transfers packets and checks the packets for errors. For more information click [here](#)
- **UDP:** Select this option to use UDP. This option is an alternative protocol to TCP, it is faster than TCP because it does not use packets, it also does not provide error checking. For more information click [here](#)

**TUN MTU:** Enter the maximum packet size that the VPN is capable of transmitting. For more information click [here](#)

**TUN MTU Extra:**

**TCP MSS:**

**Public Server Certificate:** Enter the public server certificate here. Please ensure that the certificate is copy-pasted correctly.

**Public Client Certificate:** Enter the public client certificate here. Please ensure that the certificate is copy-pasted correctly.

**Private Client Key:** Enter the client key here.

**Apply Changes:** No updates are applied unless this button is pressed. Once pressed, the screen changes are saved.

You can verify the connectivity status of the OpenVPN tunnel by navigating to the **Status** page and checking the connectivity status for "Security|OpenVPN Client Tunnel." If the status is indicated as "Connected" and shows a properly formatted IP address, the Nexus Hawk is acting as an OpenVPN client to the remote network.

## Security | VPN Server

### OpenVPN

For advanced users, the Nexus Hawk supports functioning as an OpenVPN server. For a how-to guide in setting up a VPN server click [here](#)

**Enabled:** Enables OpenVPN server functionality.

**Interface Type:** tap: Simulates an Ethernet device and operates with Layer 2 packets. Used to create a Network bridge.

**Port:** Enter the port number of the VPN tunnel. **DEFAULT: 1194**

**Protocol:** Select which protocol you wish to use.

- **TCP:** Select this option to use TCP. This option transfers packets and checks the packets for errors. For more information click [here](#)
- **UDP:** Select this option to use UDP. This option is an alternative protocol to TCP, it is faster than TCP because it does not use packets, it also does not provide error checking. For more information click [here](#)

**Keepalive:** Enter the number of seconds that you want the server to send a keep alive string. **DEFAULT: 10 seconds**

**Timeout:** Enter the number of seconds that the server will continue to attempt to maintain a session with an unresponsive client. **DEFAULT: 120 seconds**

**Address Range:** Enter the address range that the sever will assign to incoming client connections. NOTE: This range should not overlap onto the DHCP address range if enabled (Setup | 10/100 Ethernet).

**Public CA Certificate:** Enter the public ca certificate here. Please ensure that the certificate is copy-pasted correctly.

**Public Server Certificate:** Enter the public server certificate here. Please ensure that the certificate is copy-pasted correctly.

**Private Server Key:** Enter the server key here.

**Diffie-Hellman Key Parameters:** Enter the Difie-Hellman key parameters here.

**Apply Changes:** No updates are applied unless this button is pressed. Once pressed, the screen changes are saved.

# Applications | WAN Ports

## Port Forwarding

The Nexus Hawk supports forwarding of specific port ranges from the WAN to a client on the LAN.

**Enabled:** Enables the specified port

**From:** Enter the port number that you want to begin forwarding

**To:** Enter the port number that you want to end forwarding

**TCP/UDP:** Transmission Control Protocol/User Datagram Protocol Options

**Both:** Select this option to use both TCP and UDP protocol

**TCP:** Select this option to use TCP. This option transfers packets and checks the packets for errors. For more information click [here](#)

**UDP:** Select this option to use UDP. This option is an alternative protocol to TCP, it is faster than TCP because it does not use packets, it also does not provide error checking. For more information click [here](#)

**Internal Host:** Enter the LAN client IP address of the host

**Delete:** Deletes the specified port

**Apply Changes:** Changes are applied only after pressing this button.

To input a single port, simply enter it as both the **From** and **To** port. If both the port forwarding and DMZ options are enabled, port forwarding will take priority, with the remaining ports allocated to the DMZ IP address.

Do not enter overlapping port ranges for different IP addresses, as this configuration does not translate to a logical port forwarding structure. Please note that some cellular carriers will firewall the connections to their networks. As such, a public WAN IP address does not guarantee universal accessibility from the internet.

## DMZ Host

The Nexus Hawk supports a LAN client which can be placed in the DMZ (de-militarized zone) to allow access from the connected WAN.

**Enabled:** Enables the DMZ host option.

**IP address:** Enter the address of the client on the LAN which will accept the WAN connection.

**Apply Changes:** Updates are applied only upon pressing this button.

If port forwarding and DMZ values conflict, port forwarding will always be given priority. The DMZ host will receive only the ports not allocated in the forwarding table. **Caution: Forwarding all traffic to a specific host may cause the undesired effect of losing Internet-based connectivity to the Management Console. This is because all data will be forwarded to the host specified. The Management Console will still be accessible to devices attached to the LAN (Eth1) and WiFi AP.**

The LAN client will now be accessible from any connected WAN interface. Please note that some cellular carriers firewall the connections to their networks, and a public WAN IP address does not guarantee universal accessibility from the internet.

## Remote Access

Allow certain LAN services to be accessible to WAN users, here. **NOTE:** This connection will be available if the target network allows outside connections. Target network cannot be firewalled.

## Access to the Management Console

**HTTP Enabled:** The Management Console is now available by WAN (i.e. - Internet) connected users on port :80. If using a cellular data card, it is presented on that card's IP address. If using DynDNS.org's services, it is presented on the URL's port :80 (i.e. - <http://MyHawk.dyndns.org:80> ).

**Port:** The port that the data will be presented on. Default is 80

**HTTPS Enabled:** The Management Console is now available by WAN (i.e. - Internet) connected users under a secure certificate on the port specified.

**Port:** The port that the data will be presented on. Default is 443

### Allow access by manufacturer for diagnostics

**Enabled:** This option enables *trusted Nexus ISR technical staff* to remotely access to your Nexus Hawk securely, via SSH. Providing delightful support to you is our top priority. For more information click [here](#)

### Access to GPS port

**Enabled:** Present GPS access to WAN (i.e. - Internet) users. Note: Control of the GPS is governed by the framework provided by the GPSd daemon. Local clients still have the ability to access the GPS information. For more information, click [here](#)

## Applications | Advanced Routing

### Static Routes

Static routes allow the Nexus Hawk to always use a specified gateway to access a certain host or network. For more information click [here](#)

**Show Current Routes:** Press this button to show the currently defined routes

**Enabled:** Check this box to enable a static route

**Name:** Enter the name of the static route

**Destination:** Enter the desired destination IP Address of the static route

**Netmask:** Enter the desired netmask. For more information click [here](#)

**Gateway:** Enter the desired gateway

**Default for Interface:** Check this option to use the default gateway rather than one manually specified

**Interface:** Select the desired interface or use 'Best Available' and the Nexus Hawk will choose the best available interface

**Delete:** Check this box to delete the selected route

**Apply Changes:** Press this button to apply the changes

**Cancel Changes:** Press this button to cancel changes made

### Default Route

The default route option allows you to order the path of your default route. If there is a WAN connection that you don't want made available for your default route move it under the ---DO NOT USE BELOW HERE--- line.

## Administration | Management

### Password

The Nexus Hawk uses the defaults of Login=manager, Password=manager. It does not follow the Admin/Admin standard used by other manufacturers specifically to make unintended access more difficult. These values may be changed here.

**Login name:** Displays the current login name. If you wish to change the login name enter the new name.

**Current password:** Enter the current configuration password.

**New password:** Enter the new password

**Re-enter new password:** Enter the new password again for verification purposes

**Password-protect status page:** Normally, the Status page is viewable by anyone who attaches to your Nexus Hawk. Check this option if you wish to restrict that page, requiring login authentication before being able to view its contents.

**Apply Changes:** Updates are applied only after pressing this button.

**NOTE:** Once saved, you will be required to login with the new login information.

## **DDNS**

The Nexus Hawk supports a dynamic DNS update with dyndns.org. If you have a dyndns.org account, this function may be useful for finding the Nexus Hawk from the internet when it is connected to a WAN interface. Contact your Network Administrator for system-specific settings. For more information click [here](#)

**Username:** Enter your dyndns.org account username.

**Password:** Enter your dyndns.org account password; must be at least five characters

**Hostname:** Enter the hostname associated with your dyndns.org user account. Currently, only hostnames provided by dyndns.org are supported. NOTE: Hostnames are controlled by the dyndns policy. For more information click [here](#)

**Apply Changes:** No updates are applied unless this button is pressed. Once pressed, the screen changes are saved.

Once saved, the Nexus Hawk will attempt to update the specified dyndns.org entry whenever it initiates a new connection to a WAN interface. NOTE: Only dynamic hosting by DynDNS.org is supported at this time.

## **Static DHCP**

The Nexus Hawk supports static DHCP leases and allows configuration of the router to provide the same IP address to a specific client via DHCP upon every connection. For more information on DHCP click [here](#)

**MAC:** Enter the media access control address of the client device. For more information click [here](#)

**Hostname:** Enter the hostname of the client device. Using DNS masquerading, this device may be referenced by other LAN-connected clients by its assigned Hostname rather than it's assigned IP address. For more information click [here](#)

**LAN IP:** Enter the IP address which will be provided to the client device by DHCP. For more information click [here](#)

**Delete:** Check this option to delete the specified entry(s)

**Apply Changes:** Updates are applied only when this button is pressed.

**Example:** Use this option to assure that the same IP address is always served to a device with a particular MAC address.

## **Failover**

Arrange available WAN links in the order that you would prefer that the Hawk uses them. The Hawk will then automatically and dynamically use the highest available link on the list.

**Priority List:** Lists the possible internet connection types.

**Up Button:** Select an item in the Priority list and press this button to move the item up in the list.

**Down Button:** Select an item in the Priority list and press this button to move the item down in the list.

## **NTP**

The Network Time Protocol (NTP) interface page allows you to update the Nexus Hawk's internal clock.

**Enable NTP Client:** Enables the NTP service on the Nexus Hawk

**NTP Host:** Enter the name of the NTP host

## **Asset Label**

Enter up to 16 alphanumeric characters as an "Asset Label". This text will appear under the Nexus Hawk logo in the upper left-hand corner of all Management Console screens. This field is used for no other purpose and is provided to assist human administrators to more easily identify Nexus Hawk assets.

**Asset Label:** Enter the label used to define the Nexus Hawk.

**Apply Changes:** Updates are applied only when this button is pressed.

## Administration | Debug File Download

The Nexus Hawk allows the user to download a debug file to provide to technical support in the event of a system malfunction. This will allow Nexus ISR engineers to inspect the status of your problem and more quickly determine its cause.

Press the "**Download**" button to save the "debug.bin" file. Simply e-mail it to the email address provided by your administrator, along with as much detail about the issue as possible.

## Administration | Reset

### Reboot System

This is the equivalent to pressing the <Reset> button on the back panel of your Nexus Hawk. You will be presented with a warning. Press the "**Reboot**" button to reboot the Nexus Hawk. **Note:** This operation will take up to 2 minutes to complete.

**Note: The system will be unavailable while rebooting!**

### Restore Defaults

Select this option to restore your Nexus Hawk to Factory Default settings **without** the need to reboot. The changes will take effect immediately, without delay.

Note: If you have changed your Eth1 IP address from the default you will lose connectivity through that port upon restoring defaults. To regain connectivity, perform a DHCP IP renewal on your client. From your computer's command prompt:

**Windows2000/XP:**

```
ipconfig /release <enter>  
ipconfig /renew <enter>
```

**Linux:**

```
ifconfig /release <enter>  
ifconfig /renew <enter>
```

**WARNING: All settings will be reset to factory defaults, all custom settings will be.**

## Administration | Firmware Update

The Nexus Hawk allows the user to update to the latest firmware version. The current firmware version is displayed at the top right corner of the Management Console.

**Browse:** Press this button to locate a locally stored firmware file to upload to the device. **This firmware file must come directly from <http://www.nexusisr.com>** Navigate to the Support page and click the Nexus Hawk Firmware Downloads link

**Update:** Press this button to upload the firmware file to the Nexus Hawk. The Nexus Hawk will attempt to apply the firmware update and report on the success or failure of the operation. A successful firmware update will be immediately followed by a reboot (which may take up to 2 minutes to complete).

## Administration | Save/Restore Settings

## Save Current Settings

**Save:** Pressing this button will save the 'settings.bin' file to the directory you specify.

## Restore Settings

**Browse:** Press this button to locate a locally stored settings file 'settings.bin' to upload to the device. This settings file must be the file that a Nexus Hawk wrote.

**Restore:** Press this button to upload the settings file to the Nexus Hawk.

**WARNING: Restoring settings from a file may affect accessibility of the Nexus Hawk from your current location by changing settings such as LAN IP address, WAN connectivity, port forwarding, and other configuration items.**

# IP Loopback

The Nexus Hawk supports IP Loopback. IP Loopback allows users on the LAN to access a service on the same LAN by connecting to the appropriate forwarded port using the WAN IP address. This is especially helpful for client applications which are only aware of the server/peer's WAN IP address.

### **Example:**

Host A is connected to a Hawk LAN with an IP address of 192.168.1.2. The Hawk has a WAN IP address of 10.0.0.1, and has a port forwarding entry to route all incoming TCP traffic on port 23 to a telnet service on Host A at 192.168.1.2. Host B is on the same Hawk LAN with an IP address of 192.168.1.3. Host B can access the telnet service on Host A by referencing the Hawk's WAN IP address of 10.0.0.1 and TCP port 23, which the Hawk will route appropriately to 192.168.1.2 without generating any WAN traffic.

For more information on loopback click [here](#)

# Settings Persistence

Beginning with firmware version 1.2.0 user-entered the settings will persist (no re-keying necessary) as users upgrade Hawk firmware to keep up-to-date. Said another way, performing a firmware upgrade will no longer automatically reset the Nexus Hawk to factory default settings.

**Note: Settings Persistence is supported for (1) all firmware upgrades and (2) firmware roll-backs that share the same Firmware Family (identified by the first and second identifiers in the firmware version numbers (e.g. - 1.2.9, 1.2.13, 1.2.18 are in the same Firmware Family while 1.2.9, 1.3.7 are not)**

# Status

The status page displays the status of the Nexus Hawk. The contents of this page are updated every 20 seconds (note the timer at the top of the page).

## WAN Connectivity

This area displays how the Nexus Hawk is connected to the "outside world" (most often, the Internet).

## PCMCIA Slots

This area displays the status of Cellular card(s) in the card slot(s).

**Signal Strength:** Displays the strength of the signal

**Carrier:** Displays the name of your cellular service carrier

**Card Name:** Displays the model name of the connected card

---

**WAN IP Address:** Displays the IP that the carrier has assigned to the Nexus Hawk's cellular card(s)

## **WiFi**

### **AP**

This area displays the status of the Access Point.

**[xx:xx:xx:xx:xx:xx]:** Displays the MAC address of the WiFi access point; this will always be the same as the WiFi client.

**SSID:** Displays its SSID

**Security:** Displays the type of security in effect

## Client

This area displays the status of the client.

**[xx:xx:xx:xx:xx:xx]:** Displays the MAC address of the WiFi client; this will always be the same as the WiFi access point.

**Signal strength:** Displays the signal strength of the connection

**IP Address:** Displays the IP Address assigned to the Nexus Hawk's WiFi port by the AP's DHCP server

**SSID:** Displays the SSID of the network that it is connected to (through the remote AP)

**Security:** Displays the security of the network that it is connected to (through the remote AP)

## 10/100 Ethernet

### WAN Port

This area displays the status of the WAN Port (Eth0) port.

**[xx:xx:xx:xx:xx:xx]:** Displays the MAC address of the Eth0 port.

**IP Address:** Displays the IP address either delivered from a WAN DHCP server or manually configured through the Management Console.

### LAN Port

This area displays the status of the LAN Port (Eth1) port.

**[xx:xx:xx:xx:xx:xx]:** Displays the MAC address of the Eth1 port.

**IP Address:** Displays the IP address of the connection.

## Serial

This area displays whether or not a GPS device is connected

## Security

This area displays the connection state of the OpenVPN Client Tunnel and IPSec Client Tunnel.

# Help

You can find all the user documentation files for the Nexus Hawk on this page.

**User Manual:** This is a printable version (PDF) of this file with the added features of an index and technical specifications chart.

**QuickStart Guide:** This is a guide in PDF format for initializing the Nexus Hawk

**QuickConfig Guide:** This is a guide in PDF format for setting up the Nexus Hawk

**QuickFix Guide:** This is a guide in PDF format for fixing common problems while using the Nexus Hawk

## Technical Specifications

	Model			
	1000	1000-WG	2000-WG	
<b>POWER CONSUMPTION</b>	.	.	.	6W idle, 15W max @ 14VDC
<b>INPUT POWER INTERFACE</b>	.	.	.	14 VDC ±10 percent AC: 120 VAC 60 Hz power adapter
<b>INTERFACE PORTS</b>	.	.	.	❖ 1 – DB9 EIA232 asynchronous serial
	.	.	.	❖ 2 – Fast Ethernet (100Mbps)
	1	1	2	❖ 32-bit Cardbus/PCMCIA card slots
<b>COMPATIBLE NETWORKS</b>	.	.	.	❖ Integrated 802.11 a/b/g
	.	.	.	❖ CDMA EV-DO/1xRTT Rev A
	.	.	.	❖ GSM EDGE/GPRS/UMTS/HSDPA
	.	.	.	❖ Satellite via RJ-45 or PCMCIA adapter
	.	.	.	❖ Future Cardbus/PCMCIA Connectivity – 3G, 3.5G, 4G, IEEE 802.16 (WiMAX), IEEE 802.15.3a (UWB)
	.	.	.	❖ GPS
<b>MANAGEMENT / CONFIGURATION</b>	.	.	.	Web-based Management Application
<b>802.11 ANTENNA</b>	.	.	.	RP-TNC Port with tri-band omni antenna included
<b>SUPPORTED DATA RATES</b>	.	.	.	CDMA EV-DO rev A: 2.4Mbps downlink burst 1.8Mbps up.
	.	.	.	CDMA EV-DO: 2.4Mbps downlink burst 0.15Mbps up.
	.	.	.	CDMA 1xRTT: 155kbps
	.	.	.	GSM UMTS/HSDPA: 2.0Mbps downlink burst
	.	.	.	GSM EDGE: 115kbps
	.	.	.	Fast Ethernet: 100 Mbps
	.	.	.	802.11g WiFi: 54Mbps
	.	.	.	802.11b WiFi: 11Mbps
	.	.	.	802.11a WiFi: 54Mbps
<b>SECURITY</b>	.	.	.	Supports WEP, WPA, WPA2
	.	.	.	Supports IPSec pass-through
<b>WARRANTY</b>	.	.	.	Two-year limited Warranty

### \*Feature Variations by model

Model	32Bit CardBus	WiFi 802.11 a/b/g	GPS	Dimensions L x W x D		
<b>1000</b>	1	No	No	7.62"	6.1"	1.6"
<b>1000-WG</b>	1	Yes	Yes	7.62"	6.1"	1.6"
<b>2000</b>	2	No	No	10.12"	6.1"	1.6"
<b>2000-WG</b>	2	Yes	Yes	10.12"	6.1"	1.6"

# Troubleshooting

TROUBLESHOOTING Nexus Hawk		
Error	Cause	Solution
Power light is not on	Nexus Hawk is not receiving power	<ol style="list-style-type: none"> <li>1. Verify that the power supply is plugged in</li> </ol>
<b>Status</b> page is reporting "Attempting to Connect" to the Client for more than 5 minutes	The Nexus Hawk cannot receive a valid signal	<ol style="list-style-type: none"> <li>1. Move closer to AP</li> <li>2. Verify that the AP is still on and connected</li> <li>3. Verify that the security settings are the same between AP and Client</li> <li>4. Verify that the clients MAC address is allowed to connect to the AP by checking the <b>Setup   WiFi   MAC Filtering</b> configuration page</li> </ol>
<b>Status</b> page displays 'load error: Unknown'	Nexus Hawk is no longer connected to the PC or has no power	<ol style="list-style-type: none"> <li>1. Verify that the Crossover cable is connected to the PC</li> <li>2. Verify that the power source is connected to the Nexus Hawk</li> </ol>
Status light is not flashing at 1-second intervals	Nexus Hawk has not finished booting or doesn't have power	<ol style="list-style-type: none"> <li>1. Wait another 30-60 seconds for Nexus Hawk to finish booting</li> <li>2. Press and hold the "Reset" button for no more than 5 seconds to reboot the Nexus Hawk.</li> <li>3. Nexus Hawk should come up in a ready state.</li> </ol>
Unable to view <b>Status</b> Page or are receiving the "The page cannot be displayed" message	There is no connection between the Nexus Hawk and the PC	<ol style="list-style-type: none"> <li>1. Verify that the power source is connected to the Nexus Hawk</li> <li>2. Verify that the Crossover Cable is connected to the "<b>Eth1</b>" port</li> <li>3. Incorrect IP settings. Press and hold the "<b>Reset</b>" button for 5 on/off cycles to reset to factory defaults</li> </ol>
<b>Status</b> is reporting disconnected with the Cellular card	There is no cellular service	<ol style="list-style-type: none"> <li>1. Verify that the cellular card is plugged into Slot 1 or Slot 2 securely</li> <li>2. Verify that the correct cellular card is configured in the correct slot on the <b>Setup   PCMCIA   Cellular WAN</b> page</li> <li>3. Verify that the antenna is securely connected to the 802.11 port</li> </ol>
<b>Status</b> page is reporting "Attempting to Connect" to the cellular card for more than 5 minutes	The Nexus Hawk cannot receive a valid signal	<ol style="list-style-type: none"> <li>1. Verify that the cellular card is on the verified list of cellular cards</li> <li>2. Move the Nexus Hawk closer to a window.</li> </ol>
<b>Green</b> light on " <b>Eth1</b> " port is not lit up	Crossover cable is not connected to PC/Laptop	<ol style="list-style-type: none"> <li>1. Verify that the Crossover Cable is connected to both the Nexus Hawk and the PC/Laptop</li> </ol>
GPS device is not responding to commands	GPS device is not connected to the Nexus Hawk	<ol style="list-style-type: none"> <li>2. Verify that the serial cable is connected to the Nexus Hawk's Comm port</li> </ol>
Unable to connect to internet using Client but able to connect to AP	AP is configured incorrectly	<ol style="list-style-type: none"> <li>1. Verify that AP is configured to access the internet correctly.</li> <li>2. Verify that the AP can access the internet</li> <li>3. If connecting through Cellular WAN verify that the card</li> </ol>

		<p>is configured correctly</p> <ol style="list-style-type: none"> <li>4. Verify that the AP and Client don't have the same IP address</li> </ol>
"Limited or no connectivity" displayed on PC	Nexus Hawk is not connected to PC	<ol style="list-style-type: none"> <li>1. Verify that the Nexus Hawk has power</li> <li>2. Verify that the provided crossover cable not straight is being used</li> <li>3. Verify that the crossover cable is connected to the Eth1 port</li> </ol>
Unable connect to internet through Eth0 (WAN) port	Conflict with IP address or conflict within network	<ol style="list-style-type: none"> <li>1. If using DHCP make sure the DNS is not statically configured on the PC</li> <li>2. Verify that there are no more than 2 switches and 3 hubs in the network.</li> </ol>
The <Connect> and <Disconnect> buttons are non functional on the Cellular WAN configuration page	Cellular card is not being recognized by the Nexus Hawk	<ol style="list-style-type: none"> <li>1. Power-off the Nexus Hawk, unplug the cellular data card, firmly re-insert the cellular data card, power-up the Nexus Hawk.</li> <li>2. If the link light on the cellular card fails to blink, it is possible that the cellular card is not functional. Repeat the operation in the other slot (if the Nexus Hawk has multiple slots).</li> </ol>
Why won't my PC correctly renew my IP address when I change the Hawk's Eth1 subnet?	Conflict with IP address or conflict within network	<ol style="list-style-type: none"> <li>1. Your Hawk is probably plugged into a WAN on which it shares an IP conflict with another WAN-connected device. Disconnect the Hawk from the WAN prior to attempting to change the Hawk's Eth1 subnet.</li> </ol>
I can't 'surf the net', even though I have a data card plugged into the Nexus Hawk		<ol style="list-style-type: none"> <li>1. When a data card is functional...but is being used outside of its subscription area, it will get an IP address...but it won't surf</li> <li>2. When a data card is no longer functional (it is no longer provisioned due to non-payment, etc.), it will attempt to connect (twice, it seems) then disconnect itself from the Hawk. Here's what you'll see in the management console:             <ol style="list-style-type: none"> <li>a. Status: "No WAN", all slots empty</li> <li>b. Setup PCMCIA will show the card properly "discovered" and &lt;connect&gt; button dark (pushable)                 <ol style="list-style-type: none"> <li>i. If you press &lt;connect&gt; and go to the Status page...                     <ol style="list-style-type: none"> <li>1. It will attempt to connect twice, then give up, leaving you with the personality shown in (a.) and (b.) above</li> </ol> </li> </ol> </li> </ol> </li> </ol>

# Index

## 8

802.11, 3

## A

Access Point, 3  
Aggregator, 6  
AP, 3  
APN, 2

## B

Beacon, 7  
Broadcast, 3

## C

Caching, 7  
Callsign, 6  
Cellular WAN, 2  
Channel, 3  
Cisco, 8  
Client, 4  
Clock, 12  
Connection, 1

## D

DDNS, 12  
Debug File, 12  
DHCP, 4, 5, 12  
Dialup parameters, 2  
DMZ, 10  
DNS, 4  
dyndns, 12

## E

Ethernet, 1, 5

## F

Failover, 12  
Firmware, 13

## G

GPS, 6, 7  
GPSd, 6

## H

Help, 15  
HTTPS, 10

## I

IP Address, 5

IP Loopback, 14

IPsec, 7, 8

## L

LAN, 5

Login, 2, 11

Loopback, 14

## M

MAC Filtering, 4

## N

NMEA, 6

NTP, 12

## O

OpenVPN, 8, 9

## P

Password, 11

Port Forwarding, 10

Power, 1

PPP, 3

Preferred Cards, 2

Pre-shared key, 4

Protocol, 8

## R

Reboot, 13

Remote Access, 10

Reset, 13

Restore Defaults, 13

Restore Settings, 13

Routing, 11

RS-232, 6

## S

Save Settings, 13

Security, 3

Settings, 14

Settings Persistence, 14

Specifications, 16

SSID, 3

Static DHCP, 12

Static Route, 11

Status, 14

## T

TCP, 8

Troubleshooting, 17

## U

UDP, 8

Update, 13

## **V**

VPN Server, 9  
VPNClient, 7, 8

## **W**

WAN, 5, 10  
Watchdog, 3  
WEP, 3  
WiFi, 3  
WPA, 3  
WPA/WPA2, 3

## **X**

Xauth, 8

## **PRODUCT LIMITED WARRANTY**

### **LIMITED WARRANTY**

NexusISR LLC (NexusISR?) warrants the hardware Product to which this warranty applies for a period of two (2) years beginning on the date of first power-up. NexusISR warrants that the Product shall conform to and perform in accordance with published technical specifications and the accompanying written materials, and shall be free of defects in materials and workmanship, for the period of time herein indicated, such warranty period commencing upon receipt of the Product by the Customer. This warranty is limited to the repair and/or replacement, at the discretion of NexusISR,, of the defective or non-conforming Product.

The warranty does not cover the product for damages due to improper installation, improper testing, improper operation, abuse, misuse, accident, neglect, alteration, corrosion, force majeure and/or any acts of god.

The warranty does not cover any updates and patches necessary to fix problems that were not discovered during normal testing of the Product by NexusISR or to fix problems peculiar to a Customer's site and situation.

NexusISR shall not be responsible for any software, firmware, information, memory or customer data that is contained in, stored on, or integrated with any products returned to NexusISR pursuant to any warranty claim.

### **LIMITATION OF LIABILITY**

EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEXUSISR MAKES NO WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, WITH RESPECT TO ANY EQUIPMENT, PARTS OR SERVICES PROVIDED PURSUANT TO THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER NEXUSISR OR ITS DISTRIBUTORS AND RESELLERS SHALL BE LIABLE FOR ANY OTHER DAMAGES, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION IN CONTRACT OR TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), SUCH AS, BUT NOT LIMITED TO, LOSS OF ANTICIPATED PROFITS OR BENEFITS RESULTING FROM, OR ARISING OUT OF, OR IN CONNECTION WITH THE USE OF AND/OR FURNISHING OF EQUIPMENT, PARTS OR SERVICES HEREUNDER OR THE PERFORMANCE, USE OR INABILITY TO USE THE SAME, EVEN IF NEXUSISR OR ITS DEALER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL NEXUSISR OR ITS DISTRIBUTORS AND RESELLERS OR ITS DEALERS TOTAL LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT. Where dictated by State Law, some of the above exclusions or limitations may not be applicable in some states. This warranty provides specific legal rights; other rights that vary from state to state may also exist. This warranty shall not be applicable to the extent that any Federal, State or Municipal Law that cannot be preempted prohibits any provision of this warranty.

### **WARRANTY DETAILS**

Upon return of the hardware Product to NexusISR, NexusISR will, at its discretion, either repair or replace Product at no additional charge to Customer, freight prepaid, except as set forth below. Repair parts and replacement Product will be furnished on an exchange basis and will be either reconditioned or new, at the discretion of NexusISR. All replaced Product and parts become the property of NexusISR. If NexusISR determines that the Product is not under warranty or that, for any other reason, the warranty does not apply to a particular problem, NexusISR will, at the Customer's option, repair the Product using current NexusISR standard rates for parts and labor, and return the Product to the Customer via UPS Ground at no charge to the Customer, whether the problem raised by the Customer is determined to be within the coverage afforded by the warranty or outside the coverage afforded by the warranty.

Replacement products provided by NexusISR as warranted herein may be new or reconditioned. Any replaced or repaired product or part will remain under warranty for the remainder of the initial warranty period.

### **HOW TO OBTAIN SERVICE UNDER THIS WARRANTY**

If the hardware Product is found to be defective, the Product must be delivered with a pre-authorized return material authorization (RMA) number.

To Obtain an RMA Number, NexusISR may be contacted using the following methods:

Phone: Customer Care can be contacted during normal business hours (EST) at 585-436-0015.

USPS: A letter request for an RMA can be sent via US Mail addressed to:

NexusISR LLC  
Attn: Customer Care RMA  
207 Tremont St.  
Rochester, NY 14608

**REQUIREMENTS**

To qualify for this limited hardware warranty the customer may be required to provide a valid proof of purchase to NexusISR at the time that a warranty claim is presented.

Customer agrees to insure the Product or assume the risk of loss or damage in transit, to prepay shipping charges to NexusISR, and to use the original shipping container or equivalent.

**Federal Communications Commission**

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**Industry Canada**

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.