Intwine Connected Gateway 150 [ICG-150] User Guide

INTRODUCTION

Intwine's failover broadband services protect small businesses from the loss and disruption of revenue, productivity, and customer experience associated with losing Internet connectivity. Intwine's bundled solution offers customers a fully managed and seamless backup broadband solution that is plug-and-play for failover broadband and parallel networking. The entire solution is developed, configured, billed, and supported by Intwine and also includes a management portal for ongoing maintenance, deployment, and support.

Package Contents

- Intwine Connected Gateway ICG-150 Router
  - Embedded 4G LTE modem
  - Embedded 4G LTE SIM
  - Dual 10/100 Ethernet WAN/LAN
- Two (2) 4G LTE antennas
- One (1) Wi-Fi antenna
- One (1) 5 foot Ethernet cable
- One (1) 12V 1A power supply
- Mounting Brackets
- Quick Start Guide

System Requirements

- Windows 2000/XP/7+, MAC OS X, or Linux computer
- The following web browsers (earliest version in parenthesis): Chrome (43), Internet Explorer (IE11), or Firefox (38)

Overview

The Intwine Connected Gateway (ICG) is an industrial networking device with routing and basic connectivity that provides lower-level, physical layer gateway functionality.
The integrated 802.11bgn solution allows the gateway to serve as a Wi-Fi access point (AP) or as a client to an existing Wi-Fi infrastructure, and the 4G LTE WAN can be configured as the primary WAN or as a network backup to an existing infrastructure. A fleet of deployed ICGs can be controlled and monitored using the Intwine Remote Management Portal, with the ability to monitor, control, and automate heterogeneous networks.

Intwine Connect's 4G Router bundled solution includes:

- Intwine Connected Gateway (ICG-150)
- Cellular activation
- Optional static cellular IP address
- Private cellular network access
- One-year hardware warranty
- Tier 1 technical and installation support
- Bundled data packages
- Remote Management Portal account

Remote Management Portal

Intwine's Remote Management Portal (RMP) enables users to centrally manage a network of connected gateway routers and IoT devices in real time and from anywhere in the world.
With the RMP, users can quickly deploy and manage networks of distributed hardware in order to increase productivity and reduce costs related to IT and customer support.

The RMP is a cloud-based network management application that provides instant scalability and increased visibility into your network including:

- Cellular online/offline status
- Data usage monitoring
- Network health indicators
- Advanced troubleshooting tools
- Remote firmware upgrades

To create an account and register your 4GR sign up at: rmp.intwineconnect.com

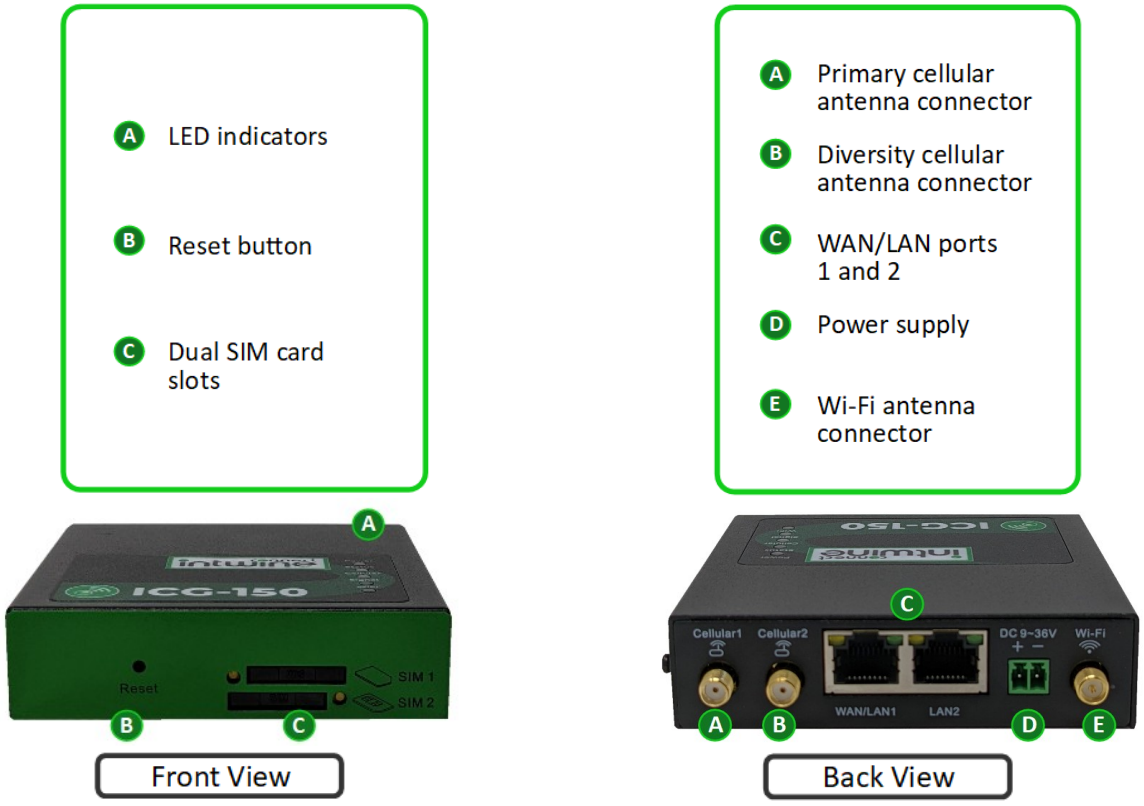
HARDWARE OVERVIEW

The ICG-150 includes all necessary hardware and accessories to deploy cellular connectivity in any home, office, or building with adequate cellular coverage.

ICG-150 features:

- Embedded 4G LTE modem and SIM card
- 802.11b/g/n
- Dual 10/100 Ethernet ports
- Verizon 4G LTE certified
- Verizon Private Network certified
- Plastic or rugged sheet metal enclosure
- 12V 1A input power

I/O, LEDs, and Power



1) The ICG-150 includes two high gain cellular antennas that are easy to attach and adjust for maximum reception. **Warning:** *Antennas are only to be replaced by certified professionals. DO NOT use any external antennas that were not provided by Intwine Connect, LLC, and installed by a certified professional.*
2) The ICG-150 comes with one 2.4GHz antenna. If Wi-Fi is not being utilized the antenna can be removed, but should be replaced with 50 Ohm terminator.

Rail Mount Installation

Bracket is not included in standard package, and can be ordered by contacting Intwine sales representatives at sales@intwineconnect.com

1) Select the installation location of the device and make sure there is enough space.
2) Tilt the equipment to the right 45°, so that the upper part of the DIN rail seat is stuck on the DIN rail, holding the lower end of the equipment, up slightly to rotate the equipment, the DIN rail seat can be stuck on the DIN rail.
3) Verify that the equipment is fixed on DIN rail

Rail Mount Removal

1) Hold the bottom end of the equipment with one hand and the top end of the DIN rail
2) With the other hand, push lower end of the device to leave the DIN rail
3) Turn the equipment clockwise and lift the equipment, removed the equipment from the DIN rail

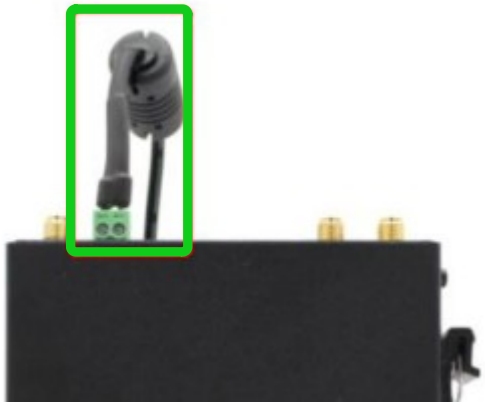
Wall Hanging Installation

Hardware is included in standard package

1) Fix the hanging ear to both sides of the device with the provided screws
2) Fix the hanging ear to the wall with screws selected based on the wall type (not provided)

Power Installation

1) Remove power terminal from router
2) Unscrew the locking screw on the power terminal
3) Insert the power cable into the terminal and lock the screws

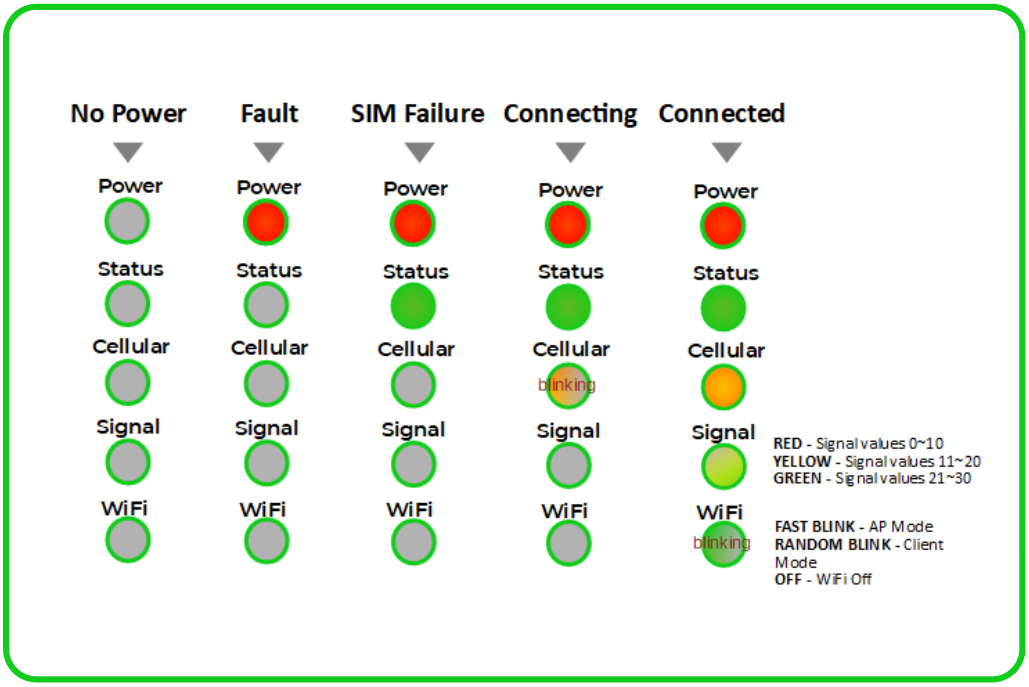


Ground Installation

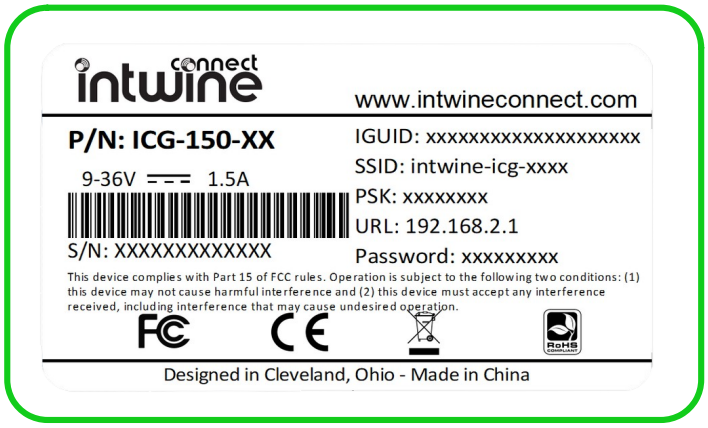
1) Unscrew the ground nut
2) Put the grounding ring of the cabinet ground wire into the ground stud
3) Tighten the ground nut

LED Indicator Guide

The LED indicators on the top panel of the ICG-150 are used to visually communicate the status of the router. The below chart can be used to determine it's state and cellular connection.



The Label



A variant of the above pictured label ships on every production ICG-150 with both standard information and information that is specific to each individual Gateway. The label is full of pertinent information including the router's FCC ID, MAC address, serial numbers, etc. The three most important pieces of information for configuring the ICG-150 are labeled above and described below:

1) **IGUID:** The IGUID stands for Intwine Globally Unique Identifier. The IGUID will allow you to register your Gateway to the Remote Management Portal and is the easiest and most assured way of identifying and tracking an individual Gateway.
2) **Admin URL/Password:** The admin URL (the same on each Gateway) is the local address at which users can access the local configuration pages (explained in **Logging In** section). The default username is **admin** and the default password is the unique string of characters that is printed on the label. The admin username and password can both be changed in the configuration pages, overriding these defaults, so **be sure to keep close track of any changes!**
3) **Default SSID/Password:** The default SSID is the wireless network name that will be broadcast by the 4GR. The default SSID is will always begin with **intwine-icg-** and the last four digits will be the last four of the IGUID. Since the default Wi-Fi access point is secured with WPA2 PSK encryption, the default password (pre-shared key) is the randomly generated string of characters printed on the label. The SSID and password can both be changed in the configuration pages, overriding these defaults, so **be sure to keep close track of any changes!**

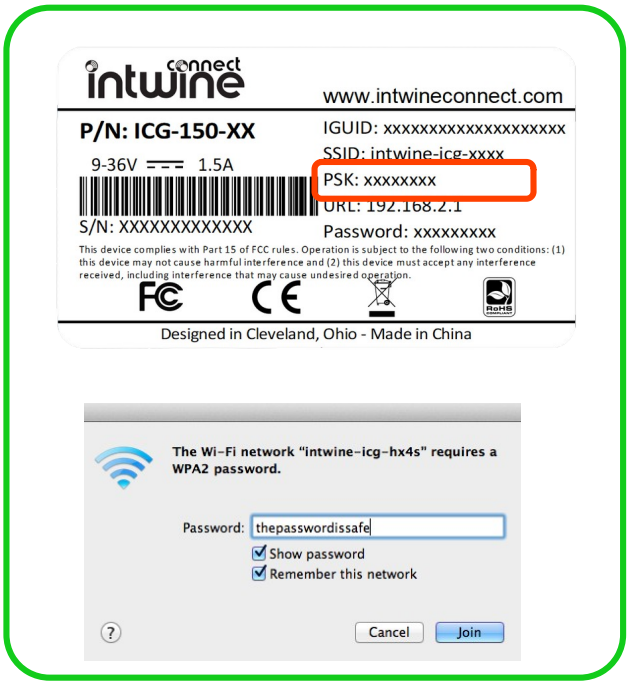
LOCAL CONFIGURATION APP

The ICG-150 local configuration app is a web tool that allows users to customize the network configuration settings on their ICG-150. The tool is useful for kitting, initial installation, and ongoing diagnostics/maintenance.

Logging in

To access the app and configure your ICG-150 simply connect to the ICG-150's Wi-Fi SSID or Ethernet LAN2 port from any Internet enabled device (e.g. phone, tablet, or PC).

1) **Access local config over Ethernet:**
    1) Plug an Ethernet cable into LAN2 port and into your PC/laptop. The ICG-150 will automatically assign a DHCP lease in the 192.168.2.x subnet to your computer.
2) **Access local config over Wi-Fi:**
    1) **Locate the network:** Using a Wi-Fi enabled device, open the window that shows available Wi-Fi networks. The ICG-150 Wi-Fi network will appear on the list. Select the network (SSID) shown on the label.
    2) **Connect to Wi-Fi:** After selecting the ICG-150 Wi-Fi network, you will need to input the default password shown on the label. The password is the PSK value provided on the bottom sticker.



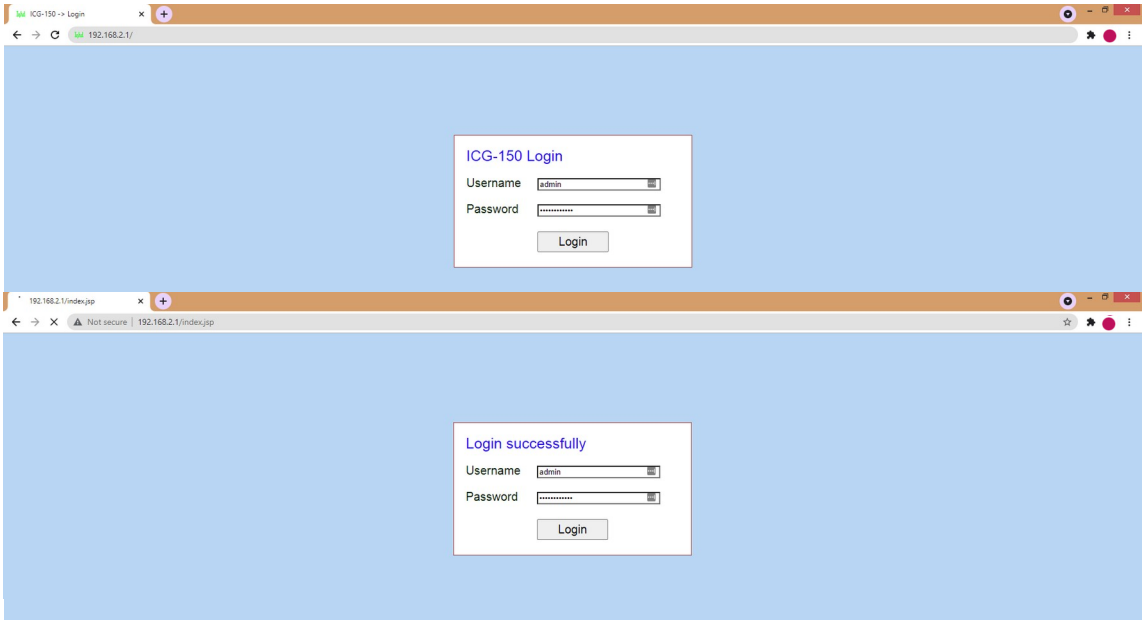
Accessing the Configuration Pages

For most users, the ICG-150 can be used directly out of the box as a Wi-Fi/Ethernet to 4G LTE router and does not require any advanced configuration changes.
For those that require custom changes, such as changing passwords, changing WAN/LAN settings, or accessing advanced networking features, you will need to log into the configuration pages.

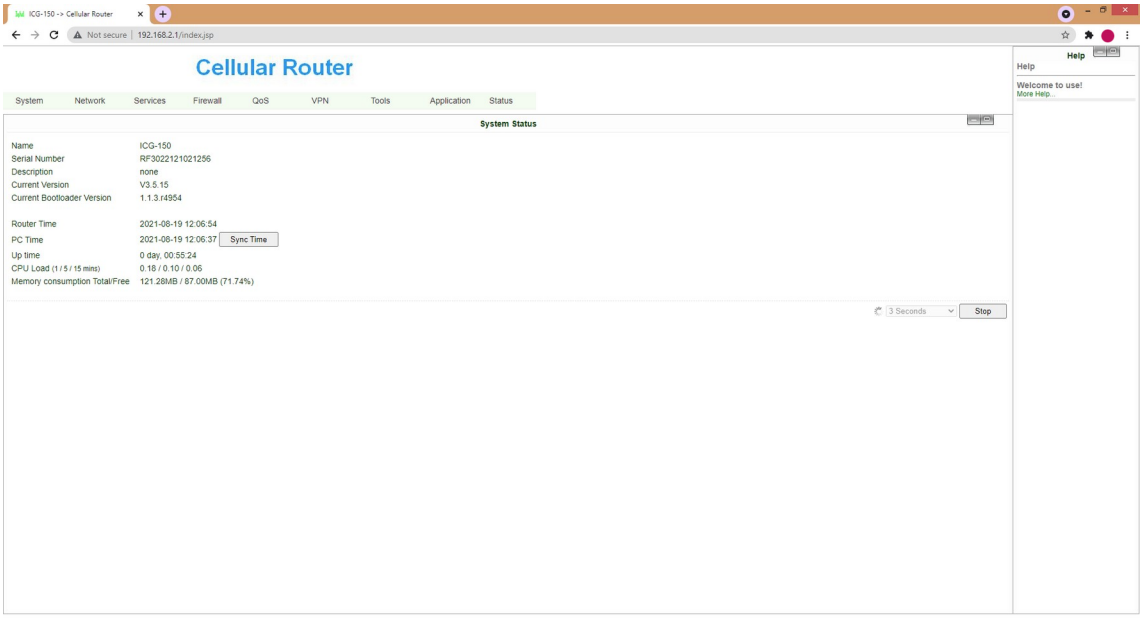
1) To access the router's configuration page, open up any standard web browser and browse to **http://192.168.2.1**

If you receive a security warning, dismiss it and proceed.

2) Enter **admin** as the username and the default password found on the label, then click the **LOGIN** button. The password is the **Password** printed on the bottom sticker.



3) You are now able to configure your ICG-150! You should now be on the System Status screen seen below.

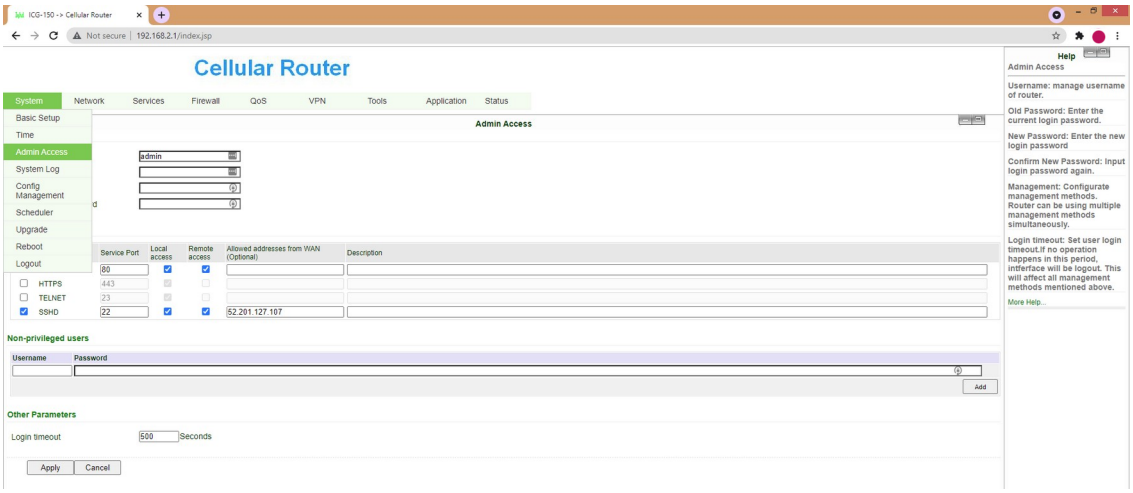


Default Settings

Out of the box, the ICG-150 is configured as a Wi-Fi/Ethernet LAN to Ethernet WAN/4G LTE failover router.
All default usernames and passwords are printed on the label that can be seen on the bottom of the ICG-150. Devices can be connected to the router to access the Internet using these Wi-Fi credentials or by plugging in via Ethernet LAN2. If you have an existing ISP or primary Internet connection please connect that via Ethernet to the WAN/LAN1 port. The ICG-150 will then attempt to obtain a DHCP lease from the connected service.
When the ICG-150 detects that lack of an active Internet connection on the WAN/LAN1 Ethernet port it will automatically switch to using cellular as the Internet connection. This may result in a short (<30 second) interruption in service.

Changing Passwords

To change the administrator password hover over System and select Admin Access

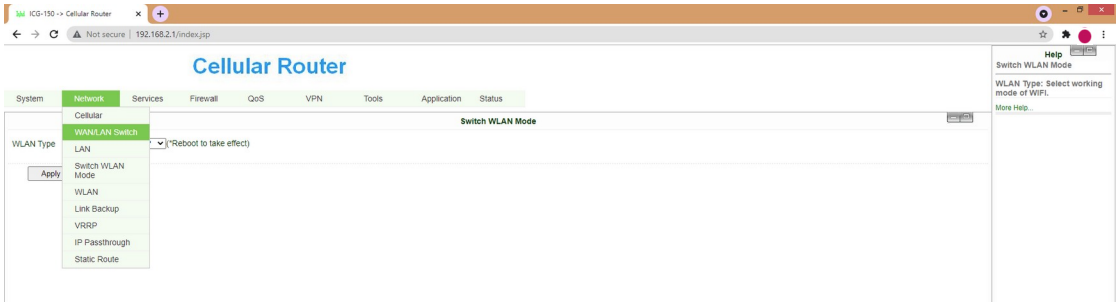


To change the administrator password enter the old password and the new password twice, then press the Apply button at the bottom of the page.

NETWORK CONFIGURATION

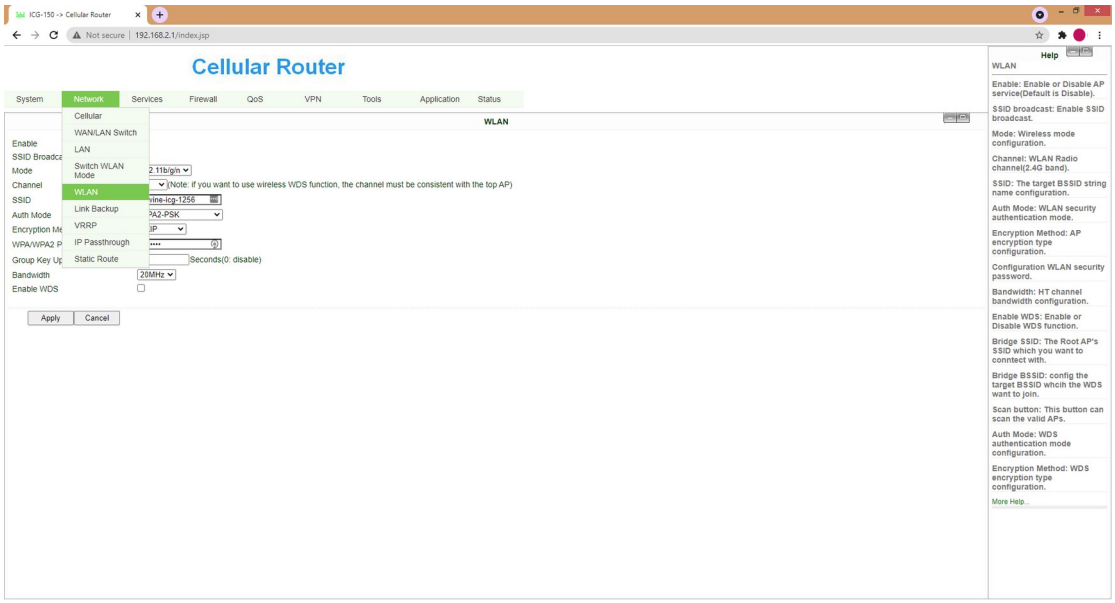
Wi-Fi

By default the Wi-Fi is configured as an Access Point (AP). To change to a client (also called station or STA), hover over Network then select Switch WLAN Mode.

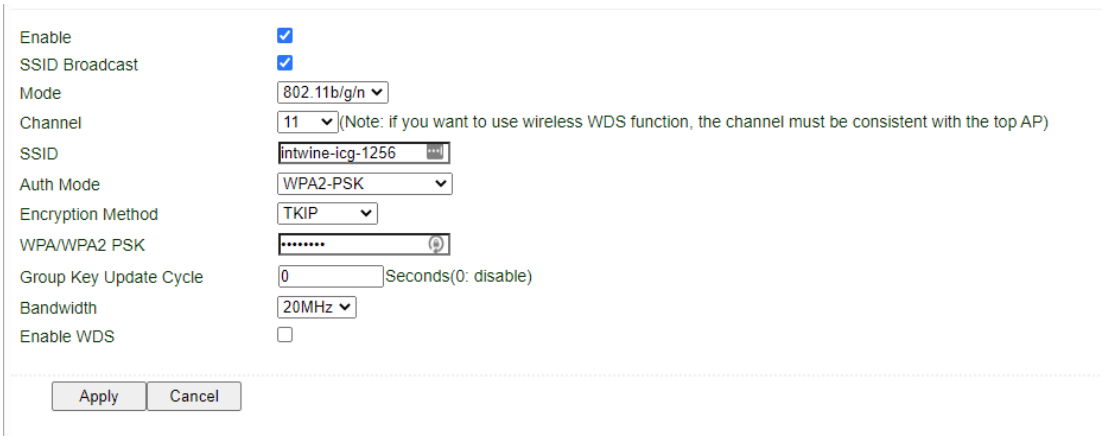


You can change the type of Wi-Fi network by selecting the desired value from the drop-down list. The press Apply and reboot the ICG-150 in order for the change to take effect.

To modify the Wi-Fi settings hover over Network then select WLAN.



This page will allow you to configure the Wi-Fi interface. Note that these settings will be different based on the type of interface you are configured as (AP versus client/station).



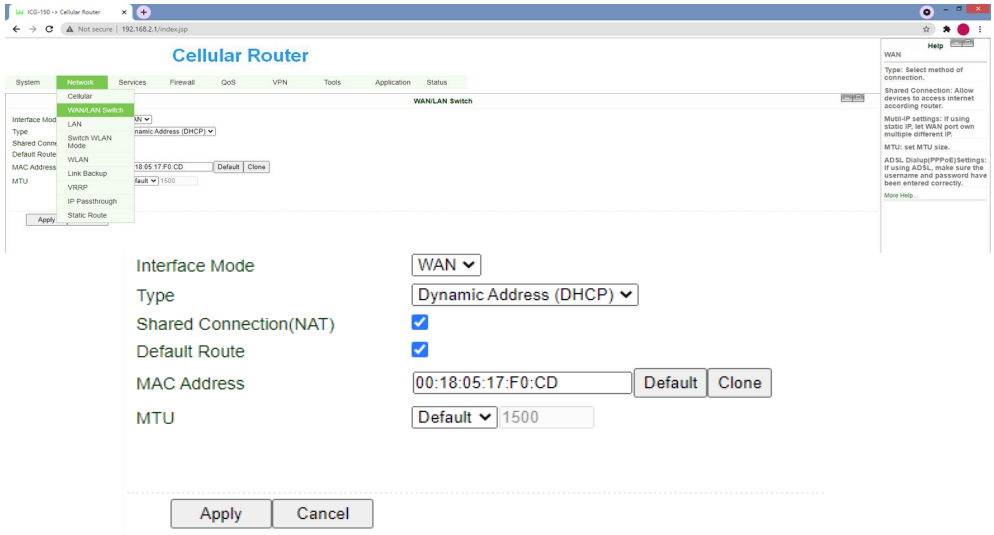
Change any desired settings, then press Apply to save.

Ethernet

The ICG-150 has two Ethernet ports on the rear of the system, one is labeled WAN/LAN1 and the other is labeled LAN2. By default the WAN/LAN1 port is configured as the primary WAN and the LAN2 port is LAN with an IP address of 192.168.2.1.

To use both Ethernet ports as a bridged LAN (basically a 2 port hub):

Hover over Network and select WAN/LAN Switch:



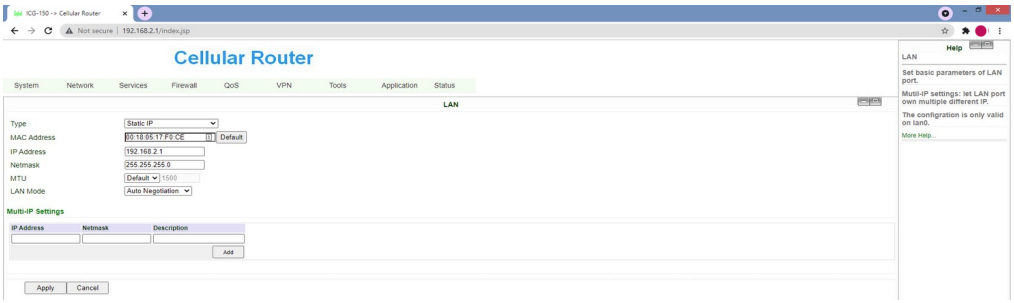
To change the WAN/LAN1 port to LAN, simply change the Interface Mode from WAN to LAN and press the Apply button.

To change the WAN port from DHCP to a Static IP:

Hover over Network and select WAN/LAN Switch. Verify that Interface Mode is WAN. Change the Type dropdown from Dynamic Address (DHCP) to Static IP. Then completely enter the values in the IP Address, Netmask, and Gateway fields to match those desired.

To configure the LAN IP address

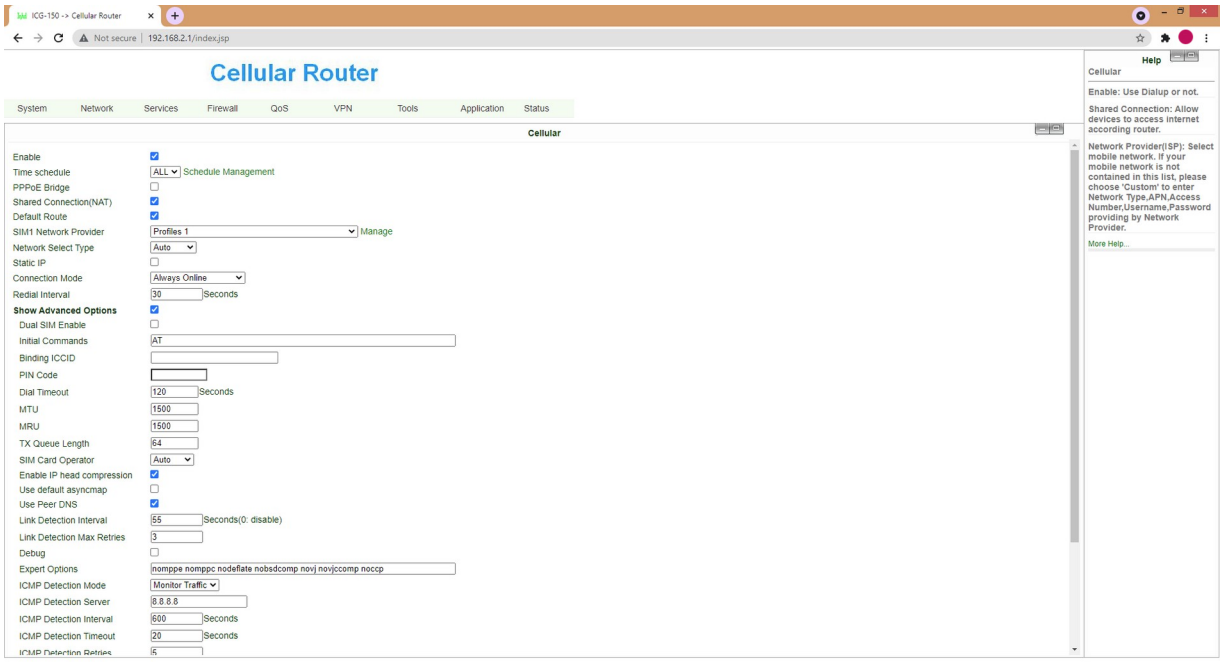
All LAN interfaces on the ICG-150 are bridged. This means that the Wi-Fi Access Point and any configured LAN Ethernet ports will all be on the same network. The default is a static IP of **192.168.2.1** with a netmask of **255.255.255.0**. These values can be changed by hovering over Network and selecting LAN.



Here you can change to either DHCP or change the specific static IP settings. Note that it is critical to remember these settings as they will be required to connect to the system after changes are made.

Cellular

To access the Cellular interface settings hover over Network then select Cellular.

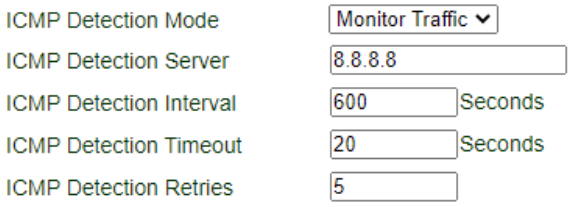


NOTE: The majority of the following settings should NOT be changed!

To change the APN which the SIM is attempting to authenticate to you will need to modify the Profiles section:

Here the APN is set to Verizon's mw01.VZWSTATIC. Simply click on the APN name and the text will change to a text box:

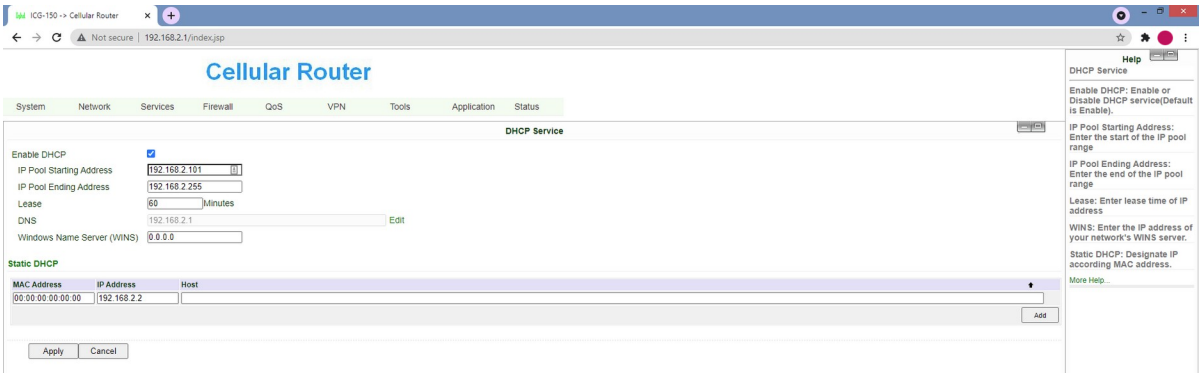
Change the APN to the desired value then press the OK button on the right side of the row. Once done, press the Apply button at the bottom of the page.
The only other settings that a user might change are the Connection status settings. Note that these defaults are set to minimize the amount of cellular data used.



The system will automatically monitor the traffic on the system to determine if the cellular modem is connected to the network. In cases where traffic is low or sporadic, the system will initiate an ICMP ping message to the IP address specified in the "Detection Server" box. This defaults to 8.8.8.8. By default, this ping will occur every 600 seconds with a 20 second timeout. If 5 failures occur the system will reset the connection.

DHCP Configuration

To configure the DHCP server hover over Services and select DHCP Service.

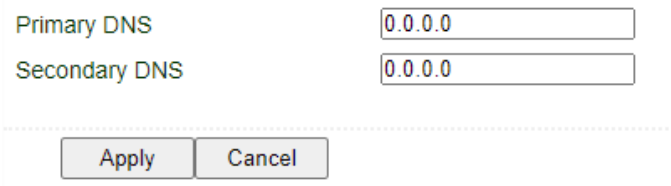


By default, the DHCP range is from 192.168.2.101 to 192.168.2.255. This address range can be changed.

Users can also use the Static DHCP lease table to provide static leases to specific systems that connect to the ICG-150. To add a new static lease, enter the MAC address of the target system, the desired IP address (on the 192.168.2.1/255.255.255.0 subnet unless you have changed those settings). New static leases can be created by pressing the Add button on the right side of the page. When complete, press Apply to save.

DNS Settings

By default, the ICG-150 will get DNS servers via DHCP. However users can specify a primary and secondary DNS server if desired. To do so, hover over Services and select DNS.



Change the values and press Apply to save. These values will overwrite the values provided by DHCP.

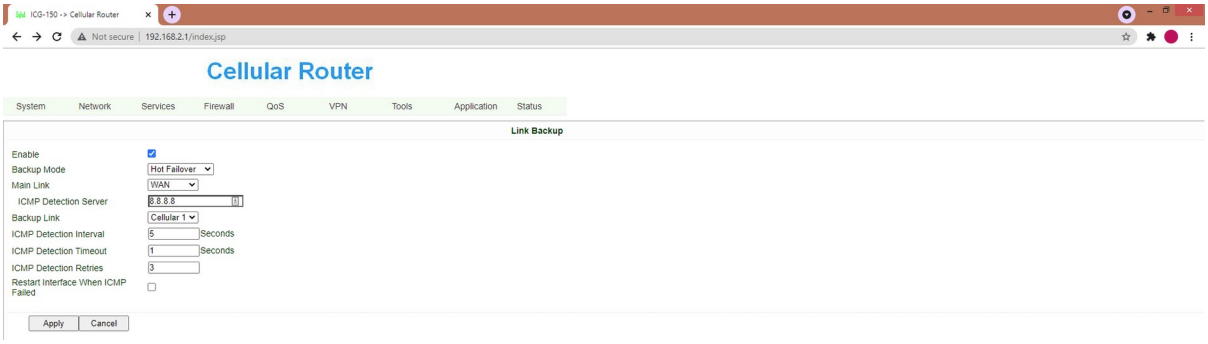
Dynamic DNS

The ICG-150 allows users to configure Dynamic DNS through a number of providers. This option is disabled by default. To enable DDNS hover over Services and select DDNS. The DDNS can be configured independently for each WAN interface. Simply select the desired service provider and fill out fields based on their instructions.

Automatic Cellular Failover

By default, the ICG-150 is configured to use Cellular as the WAN connection anytime the Ethernet WAN port is unable to reach the Internet (specifically 8.8.8.8).

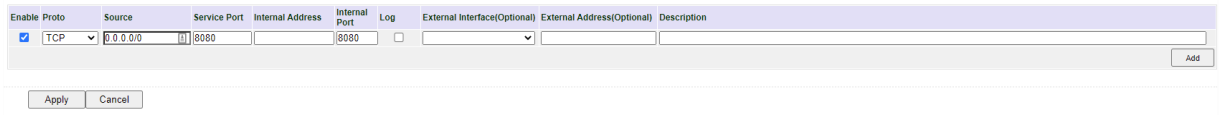
These settings can be changed by hovering over Network and selecting Link Backup.



To disable the backup functionality uncheck the Enable box. The mode is set to Hot Failover by default. This means that the cellular connection is maintained in the "connected" state but data is not routed over it until required. This dramatically increases the speed at which the automatic failover occurs. To determine if the primary WAN is up, the system will ping the ICMP Detection Server (default of 8.8.8.8) periodically (default of 5 seconds).

Port Forwarding

To configure the ICG-150 to forward ports from a WAN to LAN device hover over Firewall and select Port Mapping



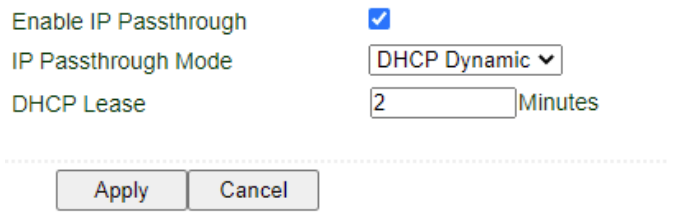
To modify an existing rule simply click on the rule and change the desired fields. To add a new rule press the Add button on the far right of the page.

The specifics of the individual fields are:

- Enable: this checkbox allows the user to specifiy if the rule is enabled or disabled.
- Proto: the protocol of the packet to forward. Options are TCP, UDP, or TCP and UDP
- Source: this allows users to select the source IP address that will be forwarded. A value of 0.0.0.0/0 means every source IP will be forwarded. If you want to limit the forwarding rule to a specific IP address then you would use something like 30.0.0.1/32
- Service Port: the inbound port number
- Internal Address: the IP address of the system to which the packet is to be forwarded. In general this should be the IP of a device with either a Static IP or a Static DHCP lease.
- Internal Port: the port on the internal system to send the packet to.
- External Interface: this allows users to select a specific WAN interface (either the WAN port or the cellular interface)
- External Address: best left blank
- Description: a human readable description so you remember why you made the rule.

IP Passthrough

In general, Intwine highly recommends that users do not use IP Passthrough, as it makes it extremely difficult to manage the ICG-150. However if you absolutely need to it can be enabled by hovering over Network and selecting IP Passthrough. To enable Passthrough, check the box which will show additional configuration options.



Users can select either DHCP Dynamic mode or Fixed MAC mode. We recommend Fix MAC mode as you can then specify the MAC address of the device that you will provide the Passthrough settings to.

LAN Clients

Go to Status > Device List

Firmware

Firmware upgrades are generally best performed using the Intwine Remote Management Portal. If a local firmware update is required the page can be accessed by hovering over System then clicking Upgrade. Here users can select a firmware file by pressing Browse. When complete, press Upgrade. Contact Intwine support to obtain the necessary firmware file.

Logs

Go to Status > Log

Users can Download the log by pressing the Download Log File.

Diagnostics

The ICG-150 has the capability to run diagnostics via the local configuration webapp. These are located within the Tools menu and include Ping and Traceroute. These tests can help isolate problems within the network.

Security Options

Disable remote access to local configuration webserver:

Go to System > Admin Access: uncheck the Remote Access box next to HTTP. Click the Apply button.

Change the default webserver port:

Go to System > Admin Access: next to HTTP change 80 to a different value then click the Apply button. Note that any future attempts to login will require the user to specify the new port. For example: http://192.168.2.1:8080

ADDITIONAL RESOURCES

Contact tech support at +1(216)314-2922 or support@intwineconnect.com.

CERTIFICATIONS, LICENSES AND WARNINGS

This Section contains safety, handling, disposal, regulatory, trademark, copyright, and software licensing information. Read all safety information below and operating instructions before using the 4GR device to avoid injury.

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT FCC CAUTION: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such 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 provided by Intwine Connect, may cause harmful interference to radio communications. This device must accept any interference received, including interference that may cause undesired operations. 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 using 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 or television technician for help.

Changes or modifications not expressly approved by Intwine Connect, LLC could void the user's authority to operate the product.

RSS-GEN COMPLIANCE: This device complies with RSS-GEN of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Ce dispositif est conforme à la norme CNR-GEN d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

This radio transmitter has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance are strictly prohibited for use with this device.
Le présent émetteur radio a été approuvé par Industrie Canada pour fonctionner avec les types d'anten neénumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

RADIATION EXPOSURE STATEMENT: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.
To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

SAFETY AND HAZARDS - Under no circumstances should the ICG-150 device be used in any areas: (a) where explosives are being used ; (b) where explosive atmospheres may be present; or (c) that are proximate to any equipment which may be susceptible to any form of radio interference where such interference would result in harm of any kind. In such areas, the ICG-150 device MUST BE POWERED OFF AT ALL TIMES (since the device otherwise could transmit signals that might interfere with such equipment).

NOTE – The ICG-150 was not designed for safe in-vehicle use and, as such, it should not be used in any moving vehicle by the operator. In some jurisdictions, use of the ICG-150 device while driving or operating a vehicle constitutes a civil and/or criminal offense.

OPEN SOURCE SOFTWARE - This product contains software distributed under one or more of the following open source licenses: GNU General Public License Version 2, BSD License, and PSF License Agreement for Python 2.7. For more information on this software, including licensing terms and your rights to access source code, contact Intwine at info@intwineconnect.com.

WARRANTY INFORMATION - Intwine warrants this product against defects in materials and workmanship to the original purchaser (or the first purchaser in the case of resale by an authorized distributor) for a period of one (1) year from the date of shipment. This warranty is limited to a repair or replacement of the product, at Intwine's discretion as purchaser's sole and exclusive remedy. Intwine does not warrant that the operation of the device will meet your requirements or be error free. Within thirty (30) days of receipt should the product fail for any reason other than damage due to customer negligence, purchaser may return the product to the point of purchase for a full refund of the purchase price. If the purchaser wishes to upgrade or convert to another Intwine product within the thirty (30) day period, purchaser may return the product and apply the full purchase price toward the purchase of another Intwine product. Any other return will be subject to Intwine's existing return policy.

LIMITATION OF INTWINE LIABILITY - The information contained in this Quick Start Guide is subject to change without notice and does not represent any commitment on the part of Intwine or its affiliates. INTWINE AND ITS AFFILIATES HEREBY SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL: (A) DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION FORLOSS OF PROFITS OR REVENUE OR OF ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE THE DEVICE, EVEN IF INTWINE AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF SUCH DAMAGES ARE FORESEEABLE; OR (B) CLAIMS BY ANY THIRD PARTY. Notwithstanding the foregoing, in no event shall the aggregate liability of Intwine and/or its affiliates arising under or in connection with the device, regardless of the number of events, occurrences, or claims giving rise to liability, exceed the price paid by the original purchaser of the device.

PRIVACY - Intwine collects general data pertaining to the use of Intwine products via the Internet including, by way of example, IP address, device ID, operating system, browser type and version number, etc. For more information, contact Intwine at info@intwineconnect.com.

OTHER BINDING DOCUMENTS, TRADEMARKS, COPYRIGHT - By activating or using your ICG-150 device, you agree to be bound by Intwine's Terms of Use, User License and other Legal Policies. For more information, contact Intwine at info@intwineconnect.com
For a complete list of warnings, warranties, and other useful information about your ICG-150, please visit www.intwineconnect.com.