Intwine Connected Gateway 200 [ICG-200] 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-200 Router
  - Embedded 4G LTE modem
  - Pre-installed 4G LTE SIM Card
  - 802.11b/g/n/ac and 10/100/1000 Ethernet WAN/LAN
- Two (2) 4G LTE antennas
- Two (2) WiFi antennas
- One (1) 3 foot Ethernet cable
- One (1) 12V 2A power supply
- 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

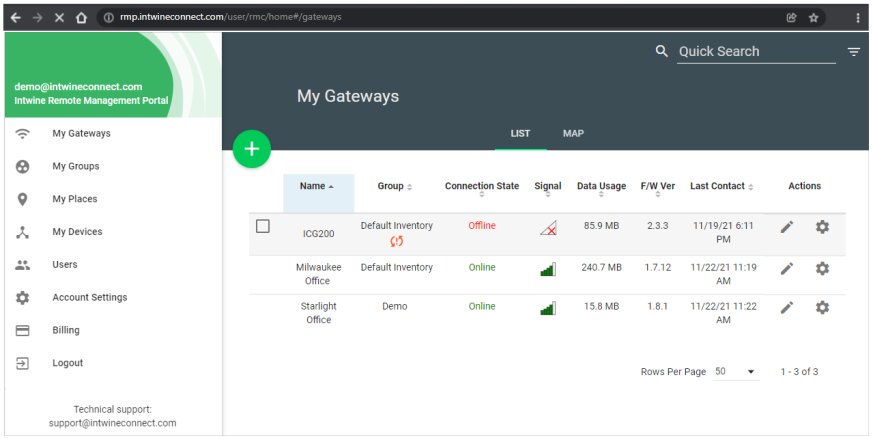
The Intwine Connected Gateway (ICG) is a networking product that provides lower-level, physical layer gateway functionality and upper-level application functionality. The platform was designed with a wide array of physical interfaces and a powerful application processor to enable customers to seamlessly add Machine-to-Machine (M2M) communications to their products and support a wide range of connected applications. The ability to deploy, monitor, control, and automate heterogeneous networks becomes a reality using the ICG.
The features of the ICG separate it from other single purpose networking devices that only provide routing and basic connectivity. A fleet of deployed ICGs can be controlled and monitored using the Intwine Remote Management Portal. This web-based application is a one-stop location that enables users to view device status, monitor the cellular connection, configure alerts, and much more.

Intwine Connect's 4G Router bundled solution includes:

- Intwine Connect 4G LTE Router (ICG-200)
- Cellular activation
- Optional static cellular IP address
- Optional 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 ICG-200 sign up at: rmp.intwineconnect.com

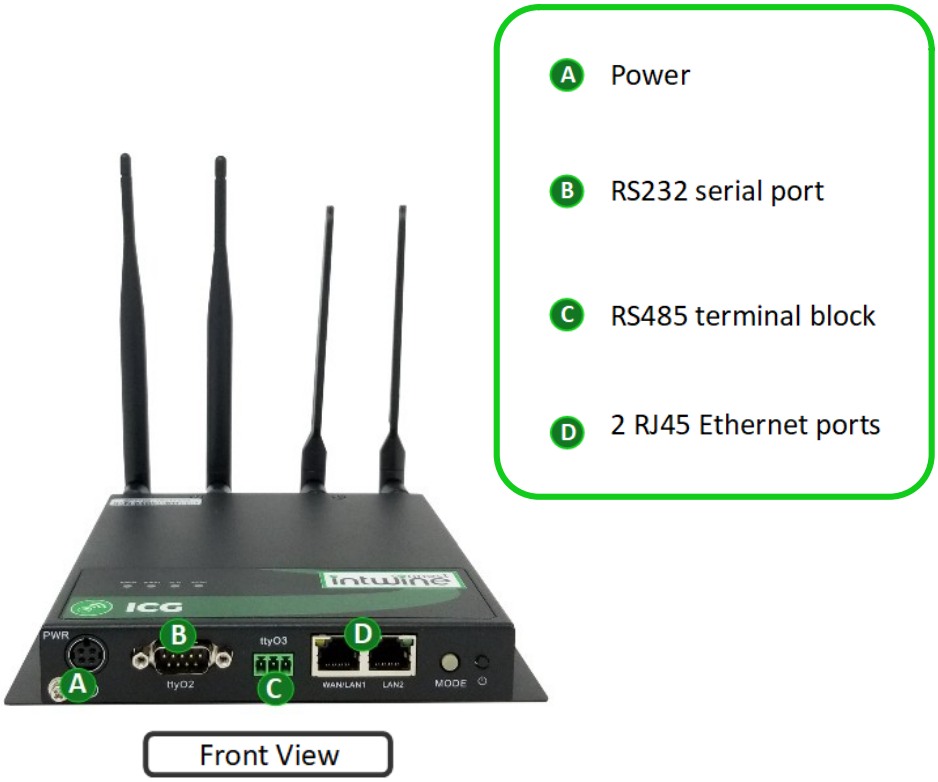
HARDWARE OVERVIEW

The ICG-200 includes all necessary hardware and accessories to deploy cellular connectivity in any home, office, or building with adequate cellular coverage.

ICG-200 features:

- Embedded 4G LTE modem and SIM card
- 802.11b/g/n/ac
- (2) 10/100/1000 Ethernet ports
- Verizon 4G LTE certified
- Verizon Private Network certified
- Rugged sheet metal enclosure with built in mounting tabs
- 12V 2A input power

I/O, LEDs, and Power



Front View

1) The ICG-200 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-200 comes with two 2.4GHz antennas. If WiFi is not being utilized the antennas can be removed, but should be replaced with 50 Ohm terminator.

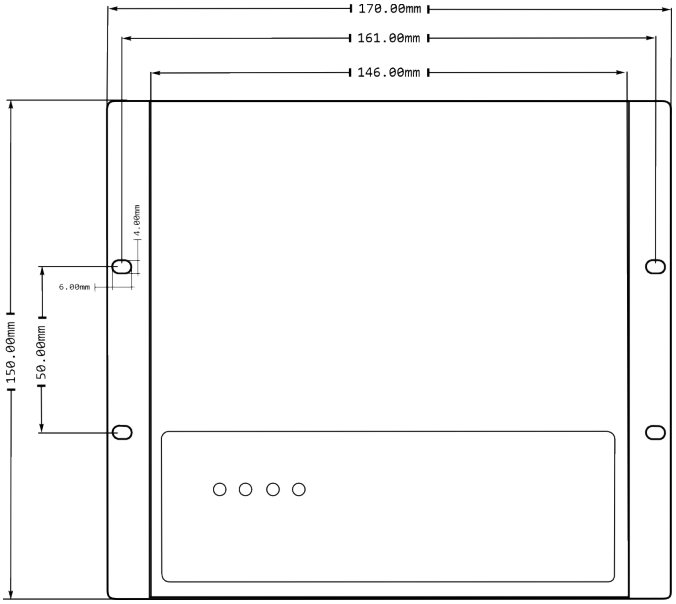
Back View

- A 2 cellular antenna connectors
- B 2 WiFi antenna connectors
- C 2 Standard/Mini/2FF SIM card slots
- D 1 HDMI port
- E 3 USB ports

GETTING STARTED

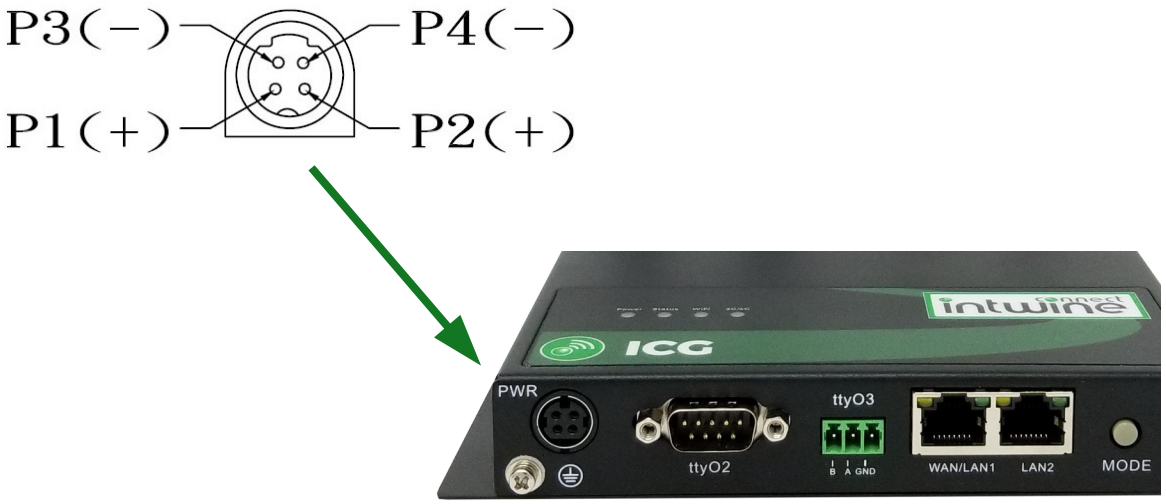
Wall Hanging Installation

The ICG-200 has built in mounting tabs that can be used for wall/panel mount installations. The hole dimensions and locations are shown below.



Power Installation

Plug the 4 pin mini-DIN connector into the port on the front of the system. The mini-DIN pinout is shown below.

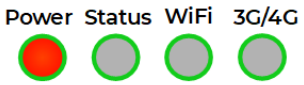


Ground Installation (Optional)

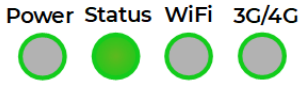
1) Unscrew the ground nut
2) Put the grounding ring of the cabinet ground wire into the ground stud
3) Tighten the ground nut

LED Indicator Guide

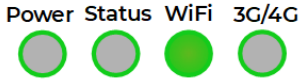
The LED indicators on the top panel of the ICG-200 are used to visually communicate the status of the router. The below chart can be used to determine it's state and cellular connection.



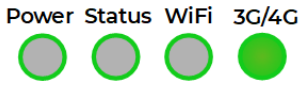
Power: Steady RED when power is ON



Status: Blinks green every 1 second

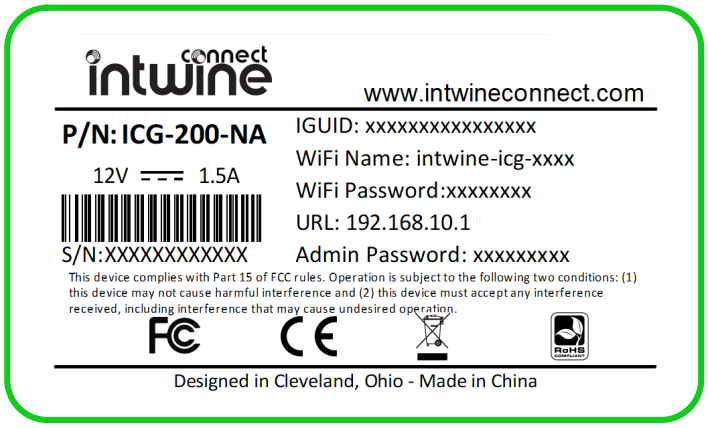


WiFi: Off when WiFi is disabled, steady green when WiFi is enabled



3G/4G: Blinks green when connecting, and steady green when connected to cellular network. Off when not configured

The Label



A variant of the above pictured label ships on every production ICG-200 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, UL number, MAC address, serial numbers, etc. The three most important pieces of information for configuring the ICG-200 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) **WiFi Name/WiFi Password:** The default WiFi Name is the wireless network name that will be broadcast by the ICG-200. The default WiFi Name is will always begin with **intwine-icg-** and the last four digits will be the last four of the IGUID. Since the default WiFi 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 WiFi Name and password can both be changed in the configuration pages, overriding these defaults, so **be sure to keep close track of any changes!**
3) **URL/Admin 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!**

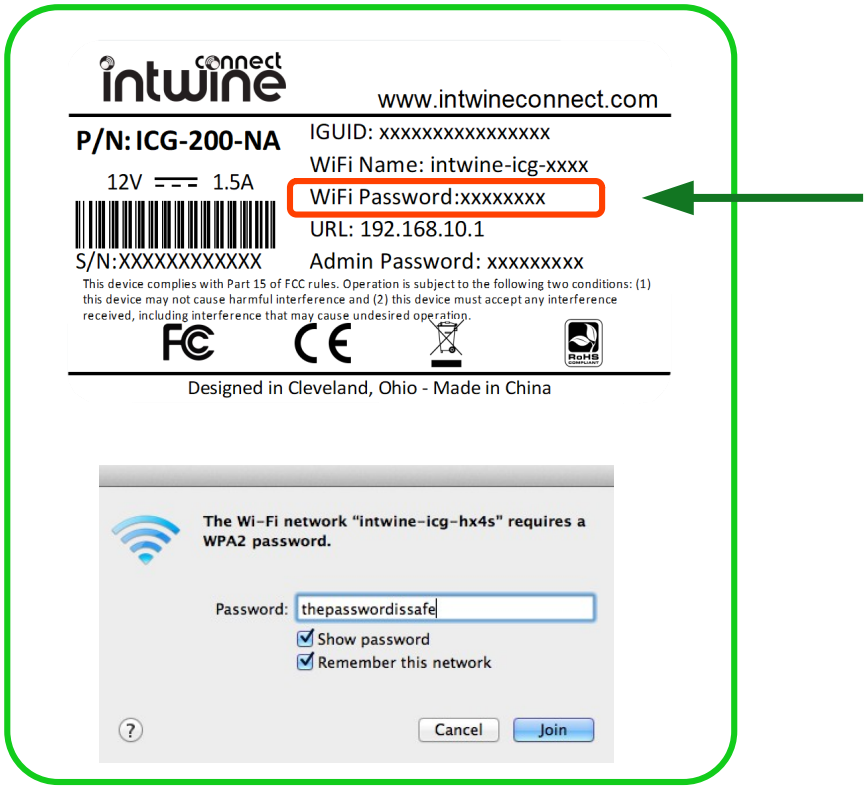
LOCAL CONFIGURATION APP

The ICG-200 local configuration app is a web tool that allows users to customize the network configuration settings on their ICG-200. The tool is useful for kitting, initial installation, and ongoing diagnostics/maintenance.

Logging in

To access the app and configure your ICG-200 simply connect to the ICG-200's WiFi SSID or Ethernet port from any Internet enabled device (e.g. phone, tablet, or PC).

1) **Locate the network:** Using a WiFi enabled device, open the window that shows available Wi-Fi networks. The ICG-200 WiFi network will appear on the list. Select the network (SSID) shown on the label.
2) **Connect to WiFi:** After selecting the ICG-200 WiFi network, you will need to input the default WiFi password shown on the label.

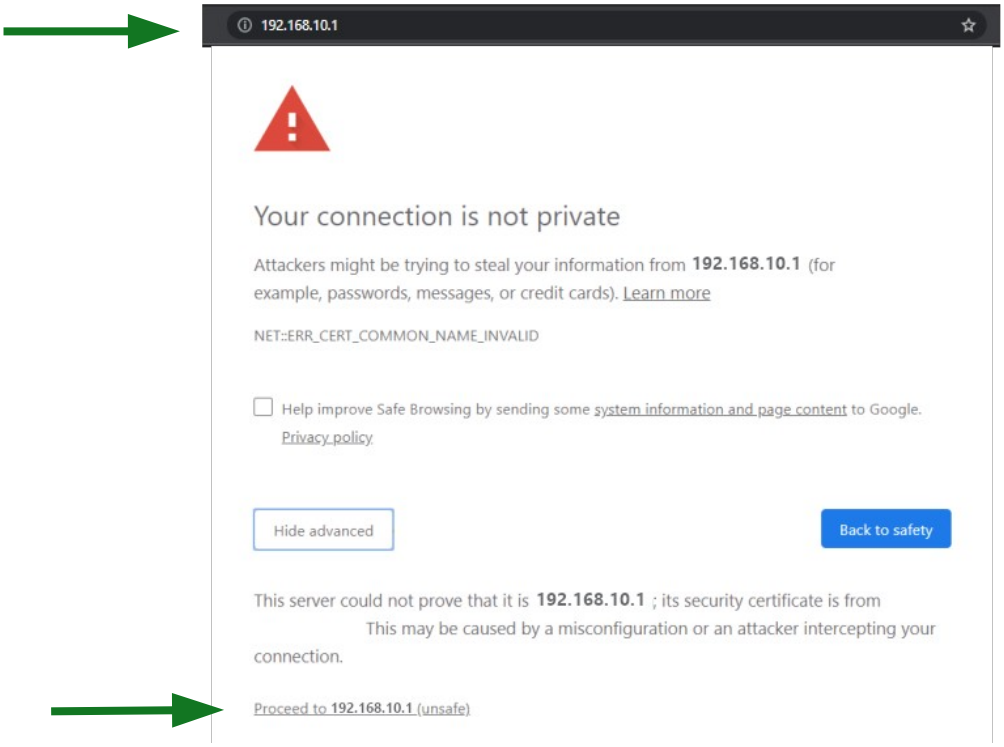


Accessing the Configuration Pages

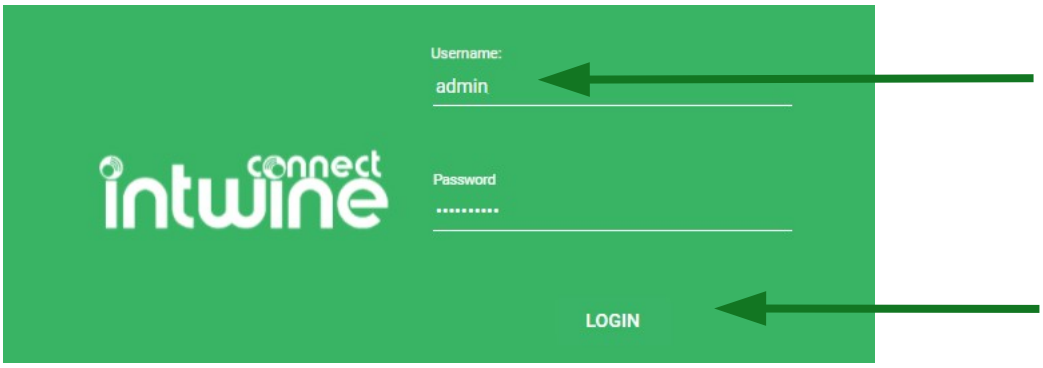
For most users, the ICG-200 can be used directly out of the box as a WiFi/Ethernet to 4G LTE router and does not require any advanced configuration changes.
For those that require custom changes, such as changing passwords, changing WAN/LAN settings, or accessing advanced networking features, you will need to log into the configuration pages.

- To access the router's configuration page, open up any standard web browser and browse to http://192.168.10.1

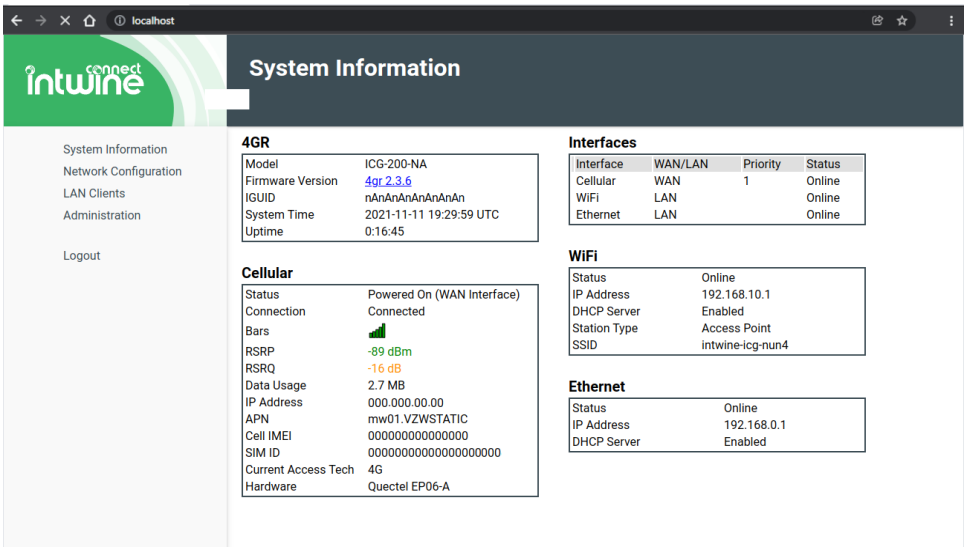
If you receive a security warning, dismiss it and proceed.



2) Enter **admin** as the username and the default password found on the label, then click the **LOGIN** button. It may take up to 30 seconds to login.



3) You are now able to configure your ICG-200! You should now be on the **System Information** screen seen below. This screen shows pertinent ICG-200 settings, allows users to browse to advanced configuration settings, and shows real time data usage.



General Information:

- **Modem Status**: Power on/off
- **Connection State**: Connected/ Disconnected (online/offline)
- **4G LTE Signal Strength**: Signal strength indicator, 1 (poor) through 5 (excellent)
- **4G LTE Data Usage**: XX MB
- **4G LTE WAN IP Address**: x.x.x.x
- **Interfaces**: Cellular/WiFi/Ethernet – WAN/LAN – Online/Offline

Default Settings

Out of the box, the ICG-200 is configured as a WiFi/Ethernet LAN to 4G LTE WAN router. All default usernames and passwords are printed on the label that can be seen on the bottom of the ICG-200. Devices can be connected to the router to access the Internet using these Wi-Fi credentials or by plugging in via Ethernet.

Changing Passwords

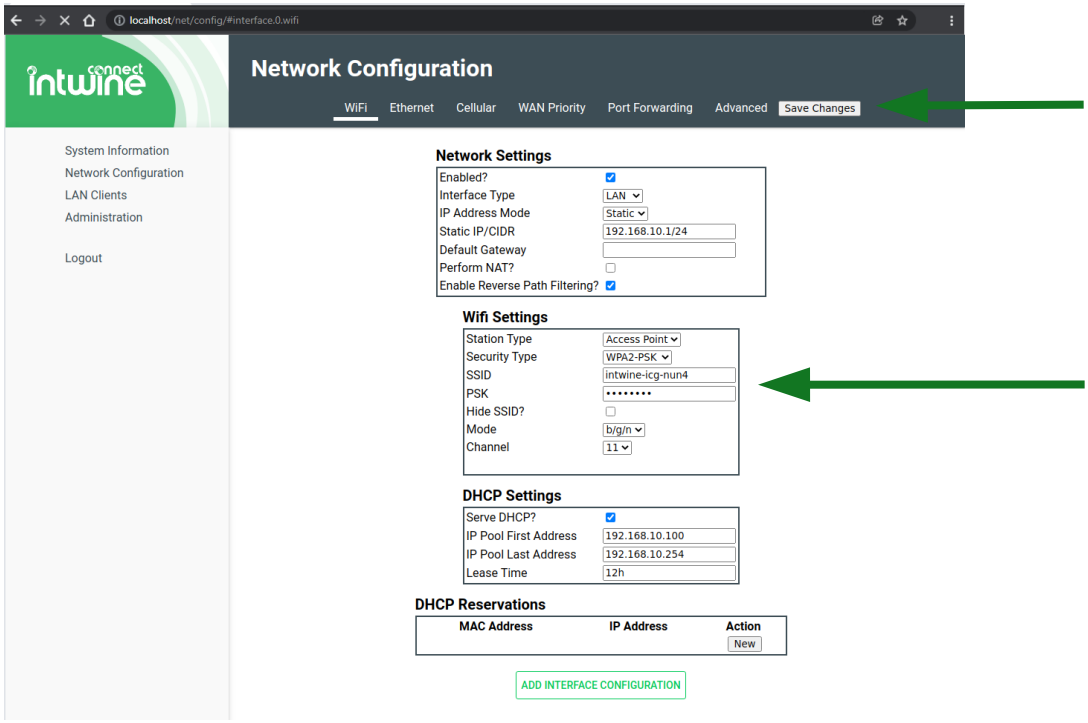
To change existing passwords and/or usernames, follow the steps above to log into the configuration pages, and then follow the below instructions.

NOTE: Changing usernames/passwords will replace the information on the label. Be sure to **WRITE IT DOWN and store in a SECURE LOCATION.**

1) From the system information page, click on **Network Configuration** on the left hand of your browser and then **select the WiFi** tab.
2) To change your SSID and/or WiFi password, edit the text in the current box and press **SAVE**.

> **NOTE**:
> Changes to the SSID and WPA2 key will kick you off of the network upon saving.

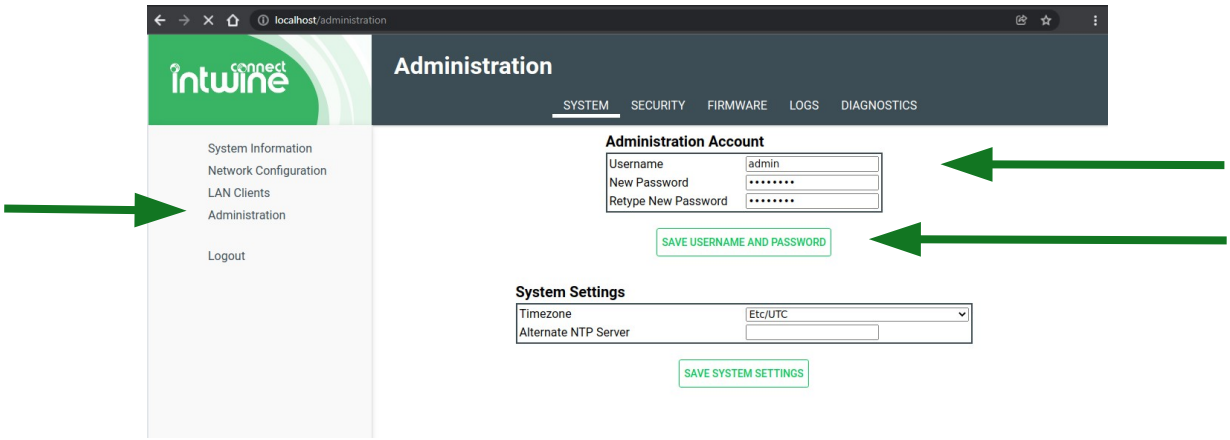
To log back in, repeat the **Logging In** steps above with your new information. Any changes that are saved are permanent until changed again and will **REPLACE** the information printed on the label.



3) To change the administration username and password, click on the **Administration** tab on the left hand side of your browser. Change the username and password using the text boxes provided.

> **NOTE:**
> Changes to the admin username and password will keep you logged in, but will change upon logging out.

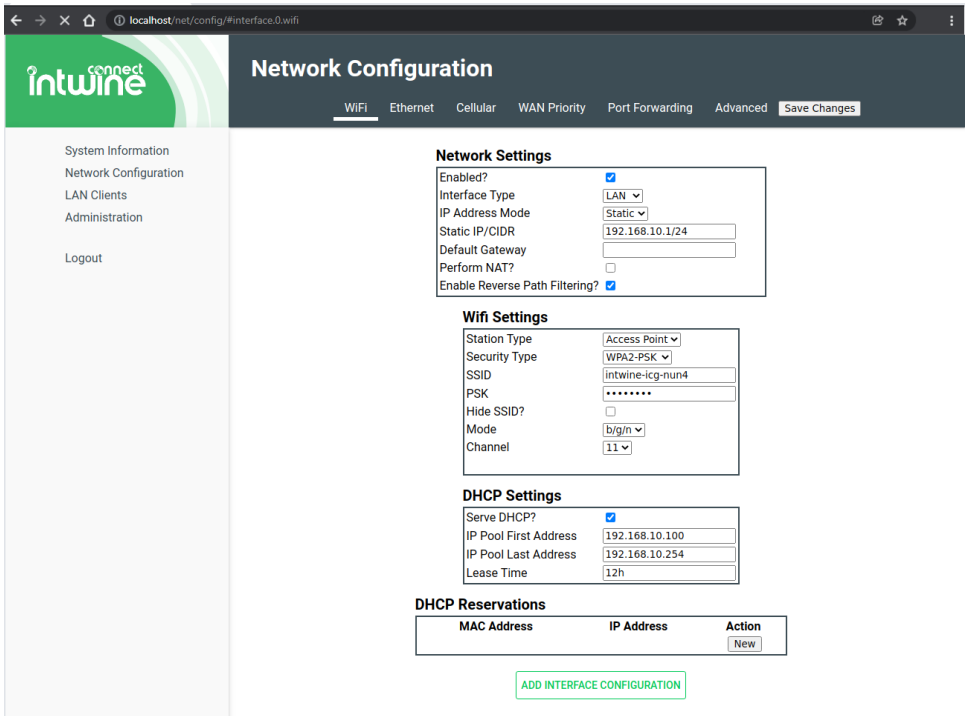
To log back in, repeat the **Logging In** steps with your new information. Any changes that are saved are permanent until changed again and will **REPLACE** the information printed on the label.



Network Configuration

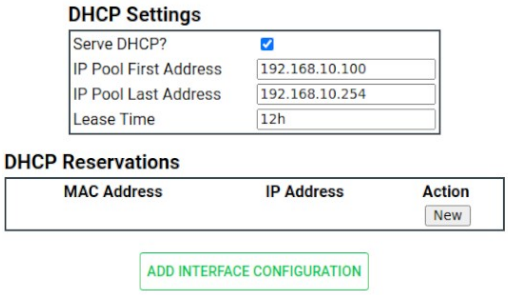
For those users that require more complex configurations, the below sections show the advanced settings of the ICG-200 and best practices to ensure appropriate configuration. All headings refer to a specific tab in the **Network Configuration** page and explain its function in detail.

WiFi



General WiFi Information:

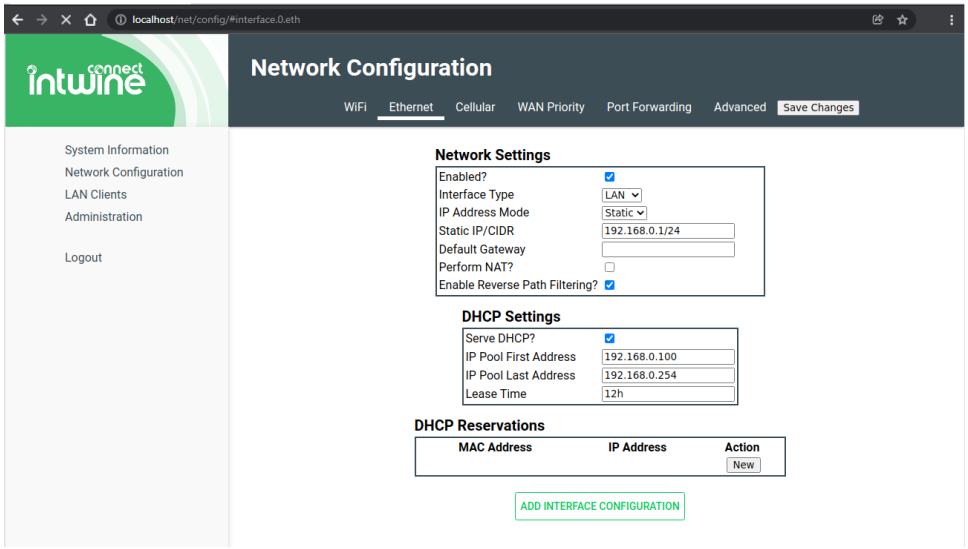
- **SSID**: Customizable network identifier.
- **Wireless Mode**: b/g or b/g/n/ac
- **WiFi Radio Channel**: Auto or 1-11
- **Security**: WPA2-PSK or UNSECURED
- **Password**: WPA2 Key
- **IP Address Mode** Static or DHCP



To enable DHCP reservations:

1) Click **Enable DHCP Reservations** (check mark should be showing).
2) Click on New
3) Enter the MAC address of the device to which you would like to assign a specific IP address.
4) Enter the IP address that you would like to assign to the device (within the correct pool address range).
5) Click **Save Changes** at the top of the page**.**

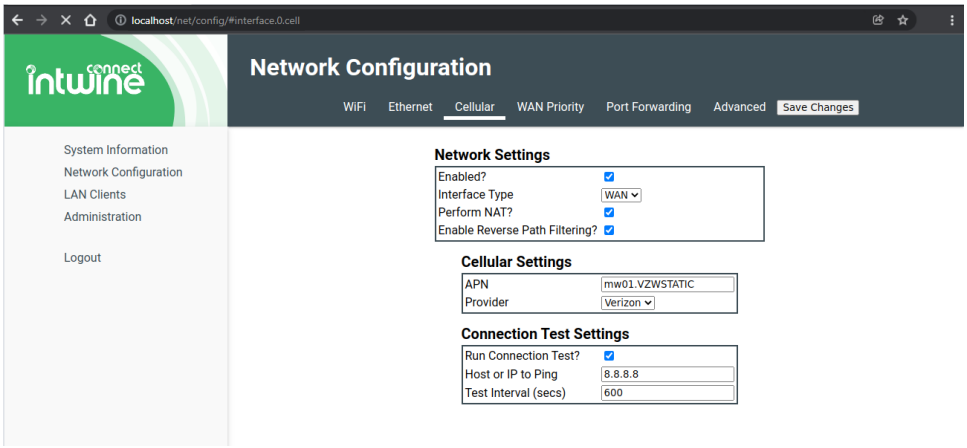
Ethernet



General Ethernet Information:

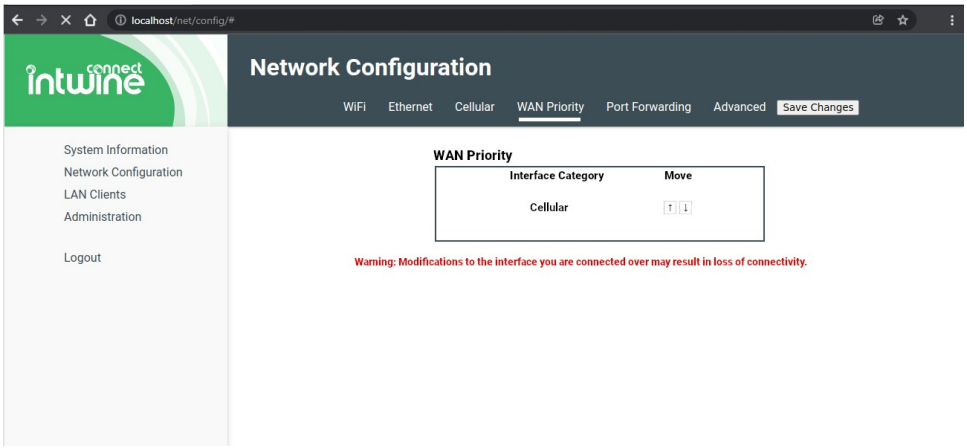
- **Interface Type**: LAN or WAN
- **IP Address Mode:** Static or DHCP
- **Static IP/CIDR**: Local IP address/CIDR
- **Reverse Path Filtering**: Yes or No
- **Serve DHCP**: Yes or No
- **Lease Time**: Configurable by hour (default = 12 hours)
- New DHCP Reservations can be added or removed.
- **Changes will be applied once the Save Changes button is pressed. Use care when changing these settings.**

Cellular



The **Cellular** tab allows users to configure which interfaces are configured as **WAN/LAN**. The **APN and the Provider** can be changed.

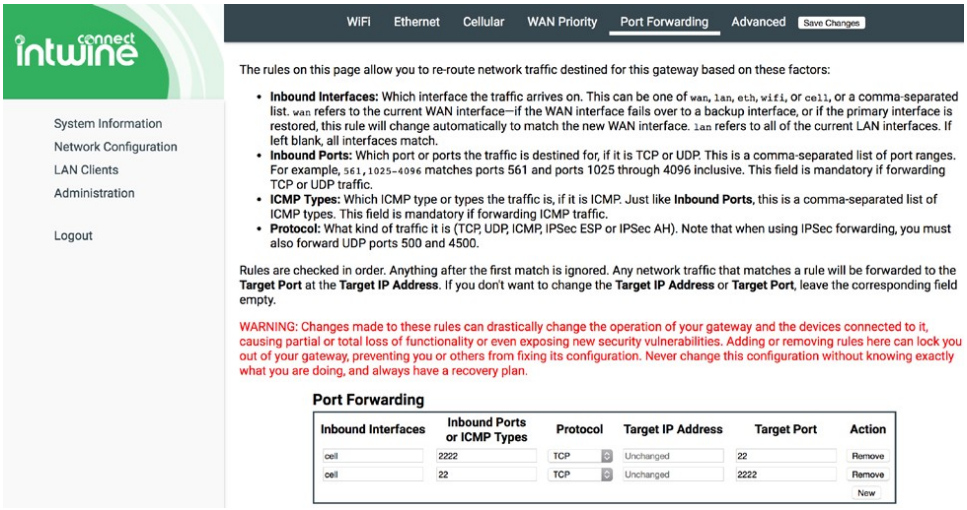
WAN Priority



Allows users to choose primary and secondary WAN connections. For example, in a typical cellular backup scenario, a user will want to configure Ethernet as the Primary WAN (priority 1) and Cellular as the backup WAN (priority 2), in case of a network outage.

Port Forwarding

Rules set under the **Port Forwarding** tab allow traffic from the Internet to reach a computer on the inside of your network. For example, a port-forwarding rule might be used to provide outside access to a local file server. Exercise caution when adding new rules, as they impact the security of your network.



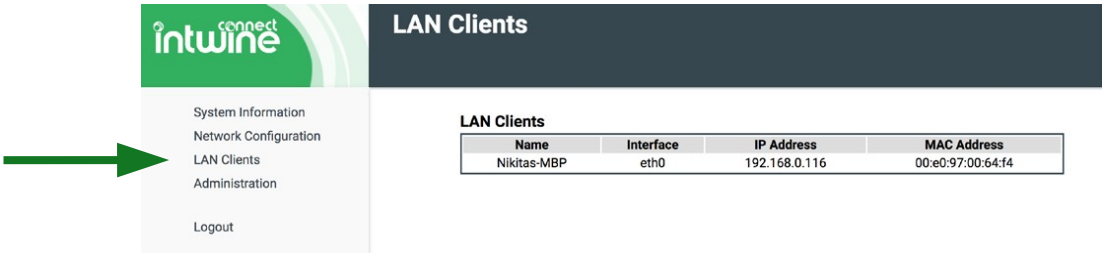
To add a new port-forwarding rule:

1) Type the inbound interface if desired. Possible values are wan, lan, eth, wifi, or cell. Only traffic on the selected interface will be forwarded to the desired destination.
2) Enter the Inbound Port numbers (can be specified as single value, comma separated list, or range).
3) Select the desired protocol (TCP/UDP/ICMP).
4) Enter the target IP address.
5) Enter the target port.
6) When complete, press the **Save Changes** button.

Port Forwarding Example: Your gateway is configured with an Ethernet connection to the Internet, with a 4G failover. You have a device connected to the Internet through the gateway, and have assigned it an IP address of 192.168.10.61 on a permanent basis through the WiFi settings page. Your device serves a web page on ports 80 (for HTTP) and 443 (for HTTPS), and you want to make it accessible to the Internet, on those ports. If you wish to keep your access to the gateway's web interface open, you need three rules. The first two rules open up ports 8080 and 8443 on the gateway, and expose the gateway's web interface on them, and the third rule forwards ports 80 and 443 to your device's web server as shown below:

Inbound Interfaces	Inbound Ports or ICMP Types	Protocol	Target IP Addresses	Target Port
Wan	8080	TCP		80
Wan	8443	TCP		443
Wan	80, 443	TCP	192.168.10.61	

LAN Clients

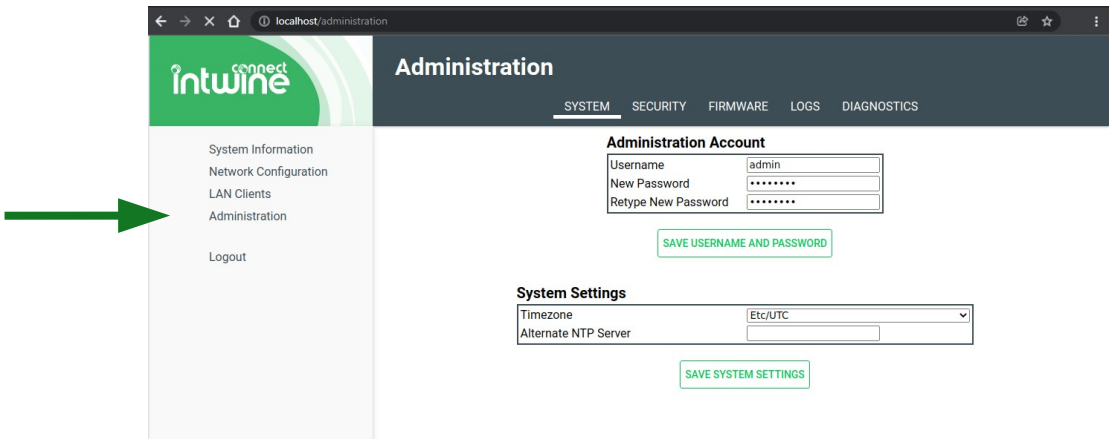


The **LAN Clients** tab shows a complete listing of all WiFi and/or Ethernet devices that are connected to the gateway. Each LAN client will show its **Interface** (WiFi/Ethernet), **IP Address**, **MAC Address**, and for devices that have been assigned a **Name,** that will show as well.

Administration

The **Administration** tab enables users to perform general (non-networking) administrative tasks including setting the time zone, updating firmware, loading and saving network configurations, and reviewing logs.

System

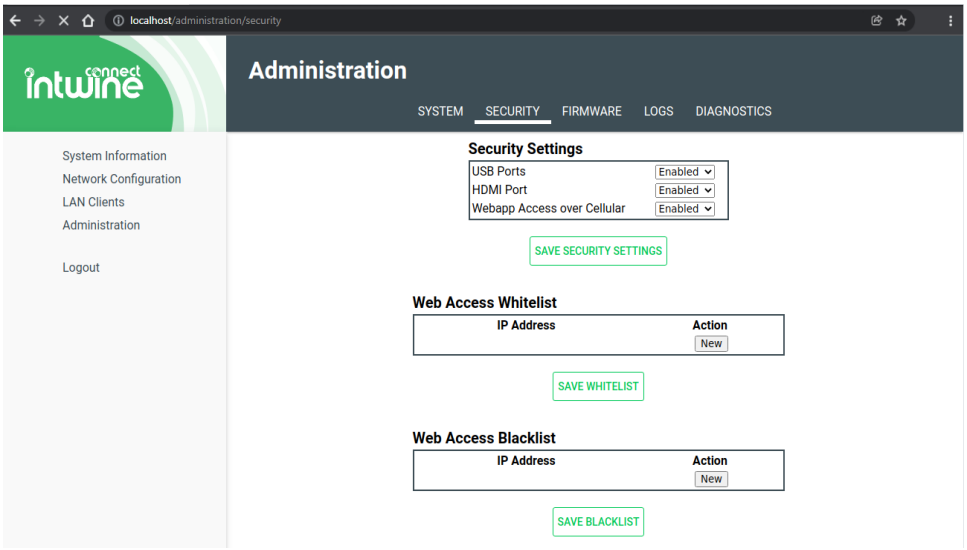


General Information:

- **Administration Account**: Change administrative username and password
- **System Settings**: Change time zone and NTP server.

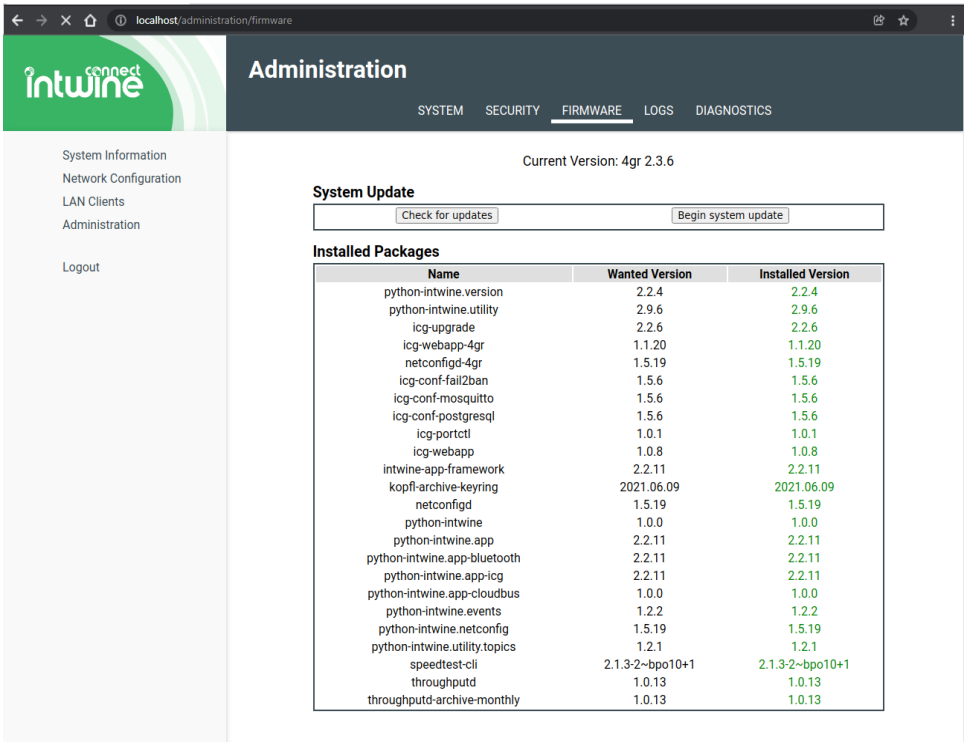
Security

The Security tab allows you to customize additional security options on the ICG-200. You can disable the use of USB ports, the HDMI interface, or prevent the local configuration webapp from being accessed via the cellular network.



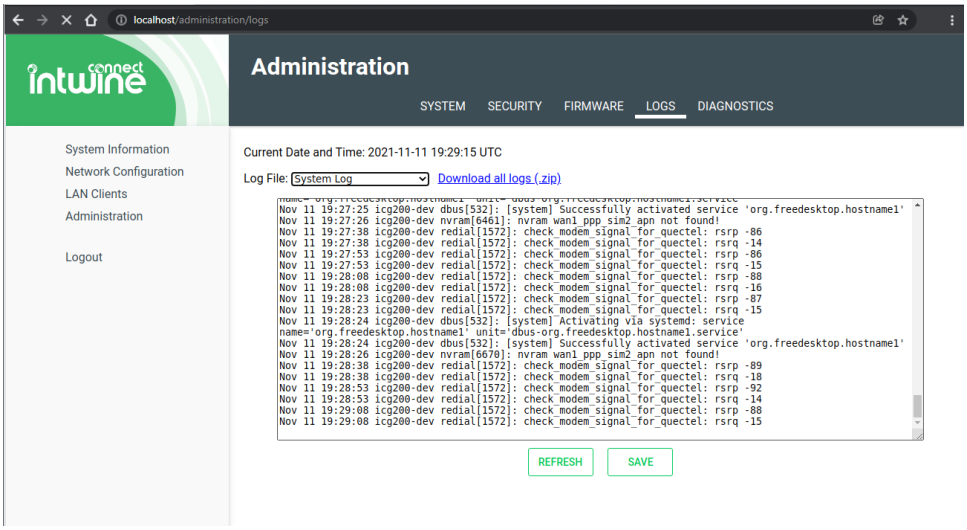
The page also allows you to allow or block specific IP addresses from accessing the local configuration webapp. The ICG-200 will automatically detect remote intrusion attempts and block those devices without any user intervention.

Firmware



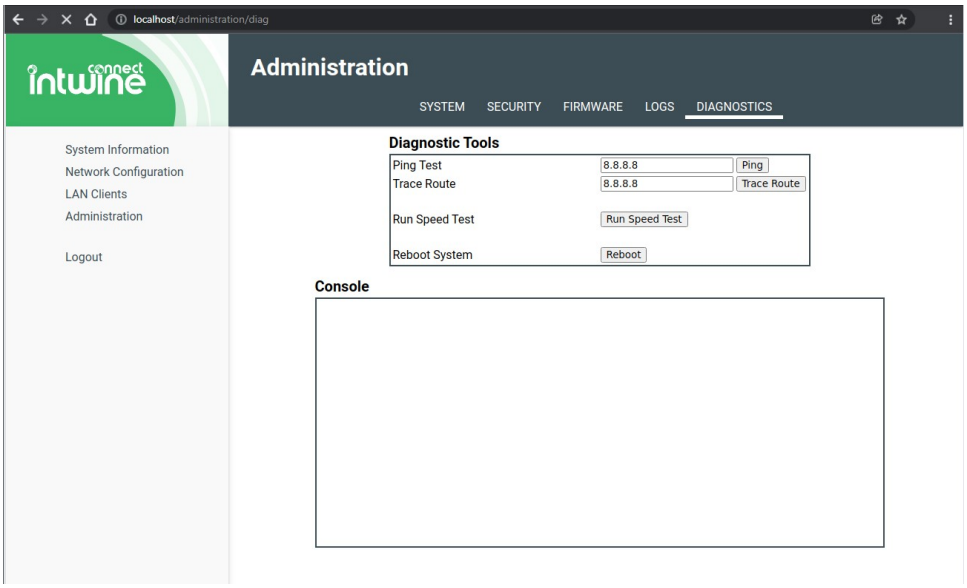
Shows current firmware version and allows the user to check for updates.

Logs



The **Logs** tab allows users to take a look at or download the logs. The available log files are – **System Log, Application Framework, Network Config daemon, ICG Log**.

Diagnostics



The **Diagnostics** tab allows users to conduct tests to help determine that their system is properly working or to isolate and resolve problems. Users can make the ICG-200 ping a specific IP address or URL as well as run a trace route. These tests can allow you to resolve network connectivity problems. Users can also have the system run a speed test and reboot the system.

ADDITIONAL RESOURCES

Contact tech support at (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 ICG-200 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-200 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-200 device MUST BE POWERED OFF AT ALL TIMES (since the device otherwise could transmit signals that might interfere with such equipment).

NOTE – The ICG-200 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-200 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 User 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-200 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-200, please visit www.intwineconnect.com.