ProSoft TECHNOLOGY

Where Automation Connects.

ICX35-HWC

Industrial Cellular Gateway

3G/4G LTE

January 10, 2024

User Manual

Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about our products, documentation, or support, please write or call us.

ProSoft Technology, Inc.
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
www.prosoft-technology.com
support@prosoft-technology.com

ICX35-HWC User Manual
For Public Use.

January 10, 2024

ProSoft Technology®, is a registered copyright of ProSoft Technology, Inc. All other brand or product names are or may be trademarks of, and are used to identify products and services of, their respective owners.

In an effort to conserve paper, ProSoft Technology no longer includes printed manuals with our product shipments. User Manuals, Datasheets, Sample Ladder Files, and Configuration Files are provided at our website: www.prosoft-technology.com

Content Disclaimer

This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither ProSoft Technology nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. Information in this document including illustrations, specifications and dimensions may contain technical inaccuracies or typographical errors. ProSoft Technology makes no warranty or representation as to its accuracy and assumes no liability for and reserves the right to correct such inaccuracies or errors at any time without notice. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of ProSoft Technology. All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components. When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use ProSoft Technology software or approved software with our hardware products may result in injury, harm, or improper operating results. Failure to observe this information can result in injury or equipment damage.

© 2024 ProSoft Technology. All Rights Reserved.

Printed documentation is available for purchase. Contact ProSoft Technology for pricing and availability.

For professional users in the European Union

If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.

Warning – Cancer and Reproductive Harm – www.P65Warnings.ca.gov

Installation Instructions:

THIS EQUIPMENT IS AN OPEN-TYPE DEVICE AND IS MEANT TO BE INSTALLED IN AN ENCLOSURE SUITABLE FOR THE ENVIRONMENT SUCH THAT THE EQUIPMENT IS ONLY ACCESSIBLE WITH THE USE OF A TOOL.

SUITABLE FOR USE IN CLASS I, DIVISION 2, GROUPS A, B, C AND D HAZARDOUS LOCATIONS, OR NONHAZARDOUS LOCATIONS ONLY.

WARNING – EXPLOSION HAZARD – DO NOT DISCONNECT EQUIPMENT WHILE THE CIRCUIT IS LIVE OR UNLESS THE AREA IS KNOWN TO BE FREE OF IGNITABLE CONCENTRATIONS.

WARNING – EXPLOSION HAZARD – SUBSTITUTION OF ANY COMPONENT MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2.

INSTRUCTIONS D'INSTALLATION:

CET APPAREIL EST UN DISPOSITIF DE TYPE OUVERT ET EST DESTINÉ A ETRE INSTALLÉ DANS UN ENVIRONNEMENT ADAPTÉ AFIN QUE L'ÉQUIPEMENT SOIT ACCESSIBLE UNIQUEMENT AVEC L'UTILISATION D'UN OUTIL.

ADAPTÉ POUR UNE UTILISATION EN CLASSE I, DIVISION 2, GROUPES A, B, C ET ZONES DANGEREUSES OU NON.

AVERTISSEMENT - RISQUE D'EXPLOSION - NE PAS DÉCONNECTER L'ÉQUIPEMENT LORSQUE LE CIRCUIT EST EN FONCTIONNEMENT A MOINS QUE LA ZONE SOIT DÉPOURVUE D'ÉLÉMENTS INFLAMMABLES.

AVERTISSEMENT - RISQUE D'EXPLOSION – LA SUBSTITUTION DE TOUT COMPOSANT PEUT NUIRE A LA CONFORMITÉ DE LA CLASSE I, DIVISION 2.

Do not operate the ProSoft Technology Wireless products in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the ProSoft Technology Wireless products MUST BE POWERED OFF. The ProSoft Technology Wireless products can transmit signals that could interfere with this equipment.

Do not operate the ProSoft Technology Wireless products in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the ProSoft Technology Wireless products MUST BE POWERED OFF. When operating, the ProSoft Technology Wireless products can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. The ICX35-HWC may be used at this time.

The driver or operator of any vehicle should not operate the ProSoft Technology Wireless products while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offense.

Agency Approvals and Certifications

Please visit our website: www.prosoft-technology.com

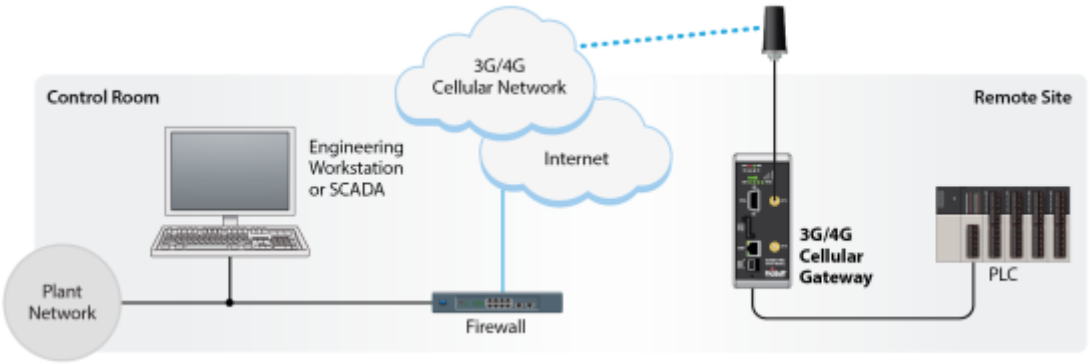
Contents

1 Start Here

1.1 About the ICX35-HWC Industrial Cellular Gateway

The ICX35-HWC Industrial Cellular Gateway provides secure wireless Ethernet and serial connectivity to remote devices over 4G LTE cellular services with fallback to 3G. These devices include PAC/PLCs, RTUs, DCS systems, instruments, electronic billboards and communication towers.

The ICX35-HWC is ideal for programming and maintenance of remote equipment, remote data collection, SCADA, and machine-to-machine (M2M) applications. It operates on LTE/GSM and CDMA networks with a single device



The ICX35-HWC supports:

- 4G LTE with GSM and CDMA cellular technologies
- Cellular networks worldwide
- Secure VPN connections over internet and cellular links for remote site access to corporate networks (VPN Client Mode)
- Simultaneous Ethernet and serial data port (Modbus & DF1 encapsulation) communications providing SCADA migration path to cellular for serial and Ethernet devices.
- Built-in web server for local/remote configuration, monitoring, and wireless network diagnostics.

1.1.1 Specifications

Cellular Modem

Specification	Description
Cellular Technology	LTE, GSM, UMTS/HSPA+, GPRS, EDGE, CDMA
Frequency/Bands	**ICX35-HWC-A:** Frequency: 700 / 800 / 850 / 900 / 1700 / 1800 / 1900 / 2100 MHz HSPA and HSPA+ Bands: 1,2,4,5,8 LTE Bands: 2,4,5,13,17,25 Quad-band EDGE/GPRS/GSM CDMA/EVDO Bands: BC0, BC1, BC10 **ICX35-HWC-E:** Frequency: 800 / 850 / 900 / 1800 / 1900 / 2100 / 2600 MHz HSPA and HSPA+ Bands: 1,2,5,8 LTE Bands: 1,3,7,8,20 Quad-band EDGE/GPRS/GSM
Verizon Certified	ICX35-HWC-A
AT&T Certified	ICX35-HWC-A
PCTRB	ICX35-HWC-A and ICX35-HWC-E
Max Downlink Speeds	Up to 100 Mbps maximum (network, surrounding equipment, environment, carrier and location dependent)
Max Uplink Speeds	Up to 50 Mbps maximum (network, surrounding equipment, environment, carrier and location dependent)
Activation	SIM Slot
Security	OpenVPN client, IPSec client, IP Address Filtering

Physical

Specification	Description
Enclosure	Extruded aluminum with DIN clip
Dimensions (H x W x D)	5.52 x 2.06 x 4.37 in, 14.01 x 5.24 x 11.09 cm
Shock	IEC 60068-2-27; 20G @ 11ms (Operational) IEC 60068-2-27; 30G @ 11ms (Non-Operational)
Vibration	IEC 60068-2-6; 10G, 10 to 150 Hz
Ethernet Port	(1) 10/100 Base-T, RJ45 connector
Serial Port	(1) DB9 female (serial tunneling & encapsulation)
Antenna Ports	(2) Female RP-SMA connector. **Antennas sold separately**
Weight	14.5 oz (411 g)
Enclosure	Extruded aluminum with DIN clip

Environmental

Specification	Description
Operating Temperature	IEC 60068 -40°F to +158°F (-40°C to +70°C)
Humidity	IEC 60068-30 5% to 95%, with no condensation
External Power	10 to 30 VDC
Peak Power Consumption	< 6W

1.2 Package Contents

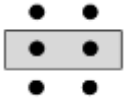
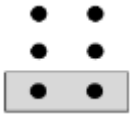
The following components are included with the ICX35-HWC and are required for installation and configuration.

Important: Before beginning the installation, please verify all the following items are present.

Qty.	Part Name	Part Number	Part Description
1	ICX35-HWC Cellular Gateway	ICX35-HWC	3G/4G LTE
1	2-pin Power Connector	002-0116	Power Connector
1	Connector Lever	357-0061	Wire installation tool
1	Jumper for rear pins	357-1517	Two-pin jumper

1.3 Jumpers

The three jumpers on the back of the unit are described from top to bottom:

Jumper Position	Description
	(Not visible) Factory Use Only
	Temporarily sets the LAN IP address to 192.168.0.250. The jumper should be kept on until the unit boots and becomes accessible. It remains at this address as long as the jumper is in place, regardless of the LAN IP address configured on the web server. The ICX35-HWC reverts to the configured server address once the jumper is removed.
	Resets the ICX35-HWC to factory defaults. The jumper should be kept until all the LEDs start to slowly blink. At this point, the jumper should be removed and the unit should be power cycled. After doing so, the front panel LEDs blink continuously, but the unit will not operate any further. Remove this jumper and power cycle the device to restore normal operations with factory defaults. The custom username/password will also be reset to the defaults values.

1.4 Reset (Power Cycle) Button

The reset button is located at the bottom of the front panel of the ICX35-HWC.

1.5 Power Requirements

The ICX35-HWC accepts voltages between 10 and 30 VDC, with an average power draw of 3 watts or less.

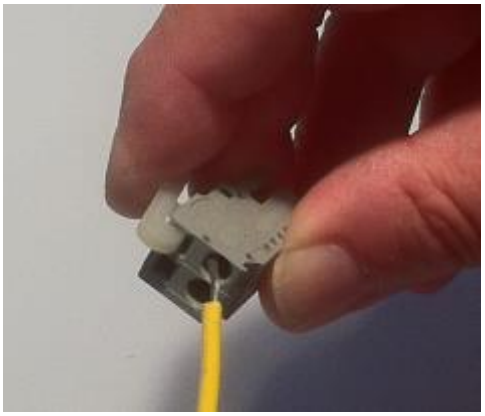
A detachable power connector comes with the radio, as shown below. The connector terminals are labeled + (positive DC connection) and - (DC ground connection).

Important: When wiring the power connector supplied with the radio, be sure to observe the proper polarity markings on the power connector. Wiring the connector incorrectly can cause serious damage to the radio which will not be covered under the ProSoft warranty.

The Power Connector (ProSoft part number 002-0116) is shown on the left. Note the + and – polarity markings. The connector lever (ProSoft part number 357-0061) shown on the right is helpful for installing wires into the spring-loaded contacts inside power connector.

Note: The onsite chassis/earth connection derived from the AC side of the main system power supply should not be connected to either negative or any other power terminal of ICX35-HWC.

To use the connector lever, insert it into the connector as shown:



Press down on the installation tool to use it as a lever to open the connector's contacts to insert a wire. A properly-wired power connector is shown:

2 Connecting to the ICX35-HWC

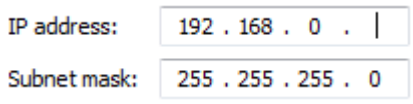
The configuration webpage is used to configure and manage the ICX35-HWC. First-time setup must be performed over a wired network, where provider-specific cellular configuration details are configured. Once initially set up, you can access the webserver over the LAN and cellular networks (unless LAN access is disabled).

Key benefits of the web-based configurator include:

- Login and device parameter configuration
- Network setting adjustments
- Security setting maintenance
- Event reporting update
- Firmware installs

2.1 Configuration Webpage Setup

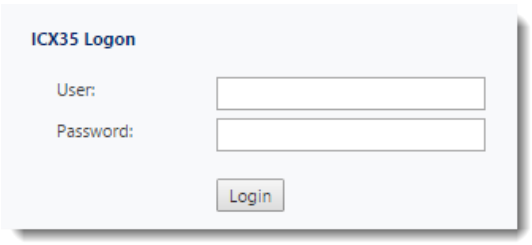
1. Insert the SIM card (size 2FF, Mini-SIM) on the front of the module.
2. Ensure that the module is connected to the network.
3. Apply power to the module.
4. Log into the ICX35-HWC configuration webpage. The default IP address of the ICX35-HWC is 192.168.0.250. If your PC is on a different subnet, temporarily set the IP address of your PC to 192.168.0.xxx with a subnet of 255.255.255.0.



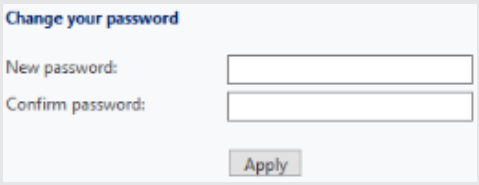
5. Open a web browser and enter the ICX35-HWC default address of: **http://192.168.0.250**.

> **Note:** ProSoft Discovery Service can also be used set a temporary IP address. PDS is a free software utility used to allow your PC to find a ProSoft Technology Ethernet-based product on a local network. It allows you to change its default IP address without being on the same subnet. It can be downloaded from: www.prosoft-technology.com.

6. Once the ICX35-HWC homepage opens, enter the username and password to log in. The default username is '**admin**' and the default password is '**password**'.



Note: For the initial or default ICX35-HWC login, after the default username and password are used, the user will be prompted to change the password.

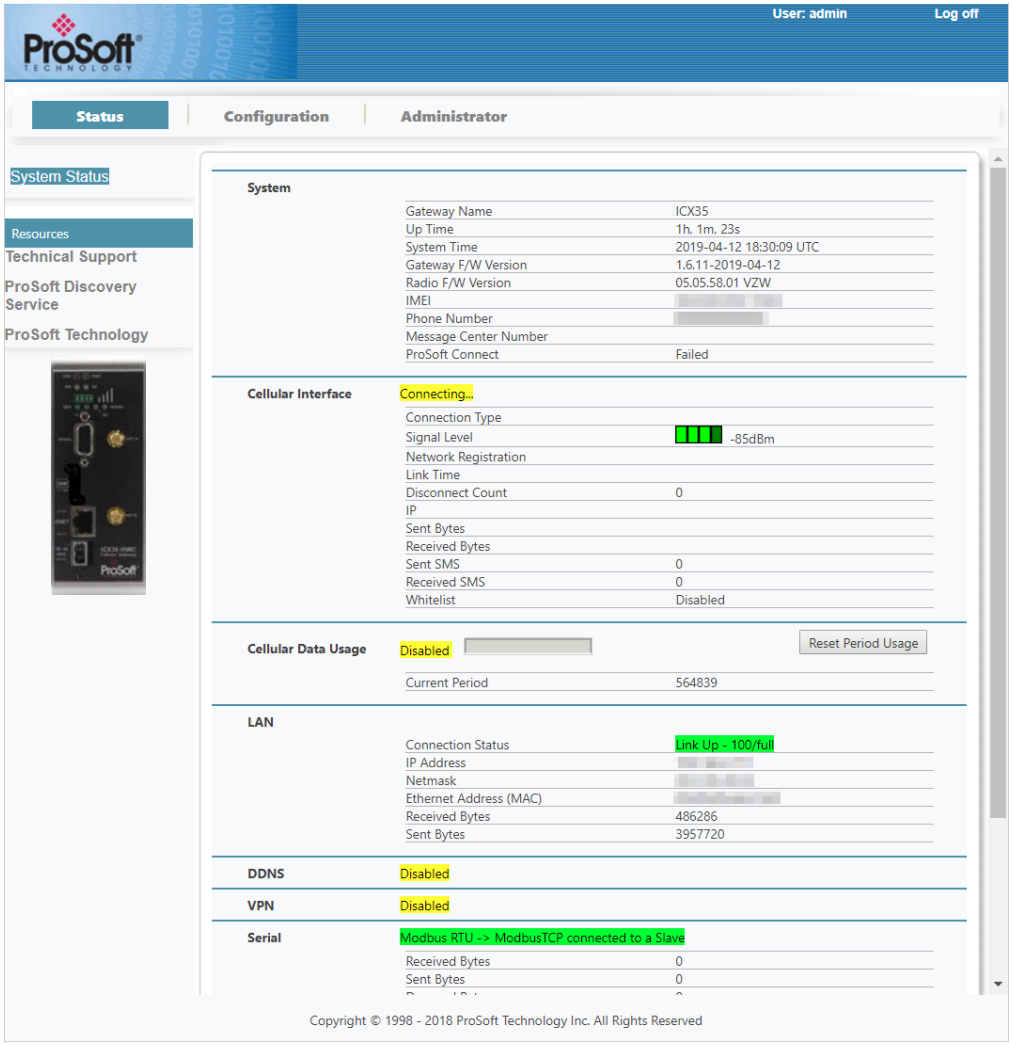


The new password must comply with the following rules:

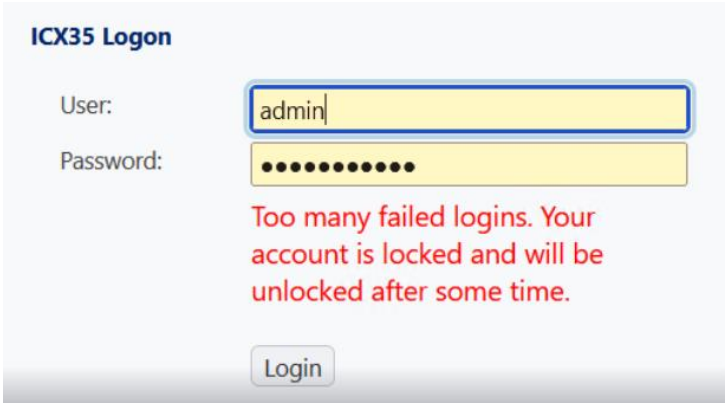
1. Password field must have between 8-40 characters.
2. Password must contain characters from three of the following four categories:
   * Uppercase characters
   * Lowercase characters
   * Base 10 digits (0 through 9)
   * Non-alphanumeric characters: .~`!@#$%^*()-+={}:?_

After successful login with the new password, further password changes can only be done from the Administrator > Access Control webpage.

7 After successful login, the homepage displays data from the *Status* tab.

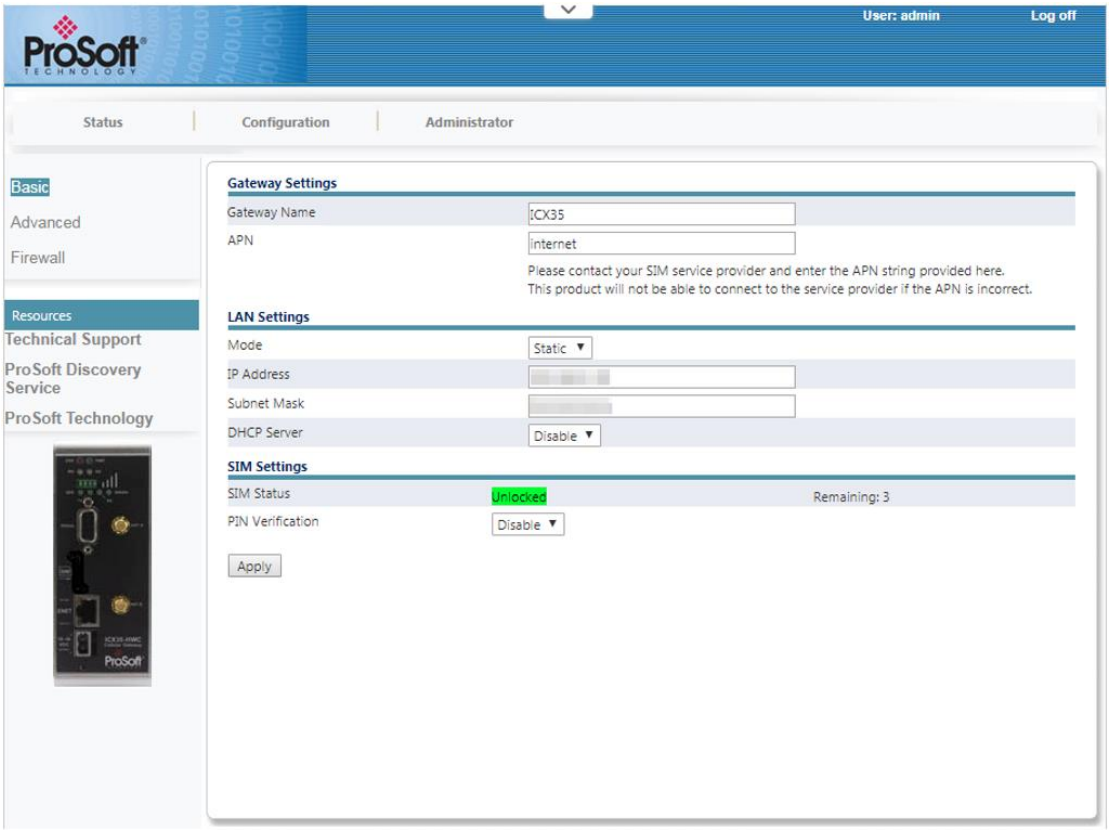


8 After 5 consecutive failed login attempts, you will not be allowed to login for next 10 minutes. The details and status are logged in *syslog* and */psft/loginRecords.txt*. The last 100 login attempts are logged.



2.2 Assigning a LAN IP Address

1 Select the *Configuration* tab and select the *Basic* option.



2 Enter a name for the module in the *Module Name* field.

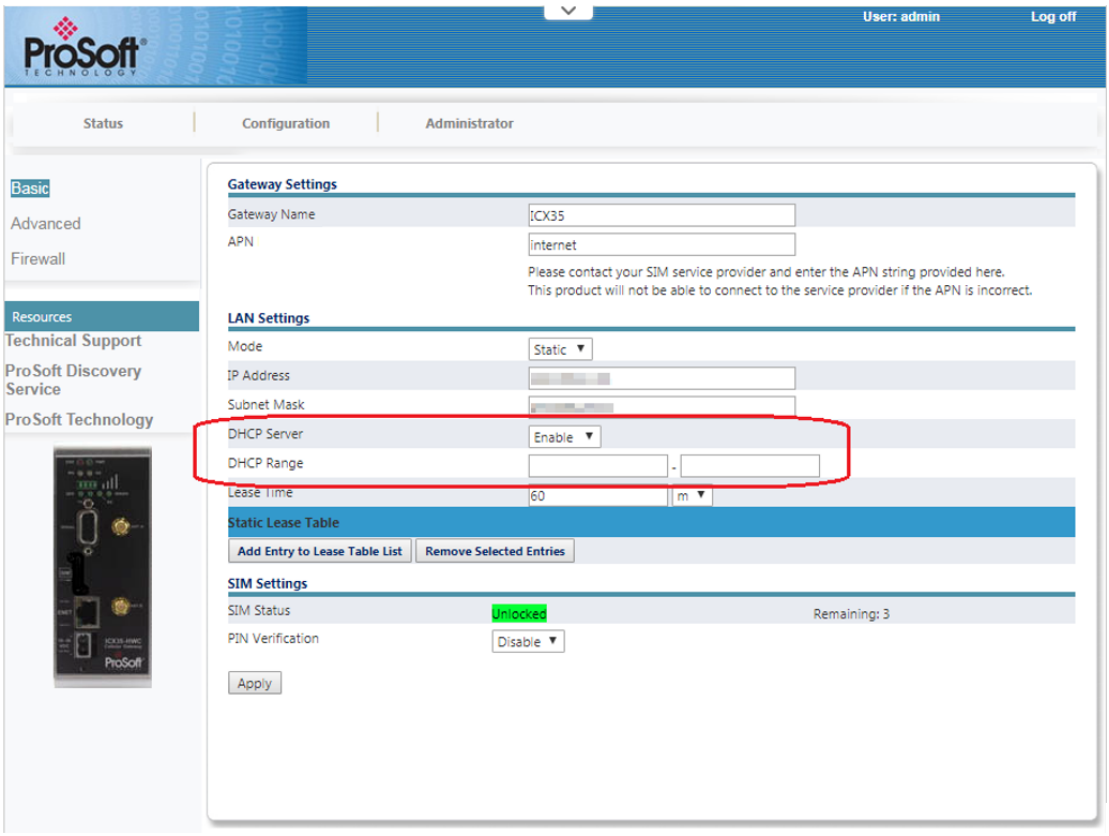
3 Enter the *APN* (Access Point Name). This information is provided by your cellular provider.

4 *Internet Access* via LAN is also possible. Enable this parameter and then click **APPLY**. You will be asked to enter a gateway and 2 DNS servers.

5 Enter the *IP Address* and *Subnet Mask* of the ICX35-HWC.

6 Choose whether or not to use DHCP (Dynamic Host Configuration Protocol) for end devices.

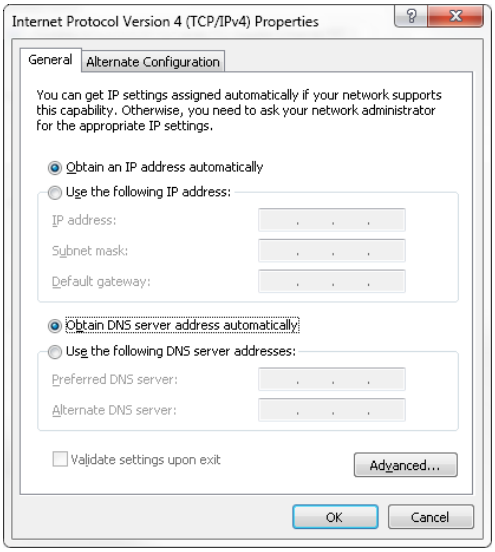
a) If YES, enable the *DHCP SERVER* option and select a *DHCP Range* of IP addresses applicable to multiple end devices.



• **DHCP Range** – A range of IP addresses that can be assigned by the ICX35-HWC DHCP Server application on the LAN side. For example, the ICX35-HWC can assign an IP address to any device that connects to its dedicated LAN network within the specified Range (**192.168.3.0** to **24**). A maximum of 25 Devices will be able to receive an IP address.

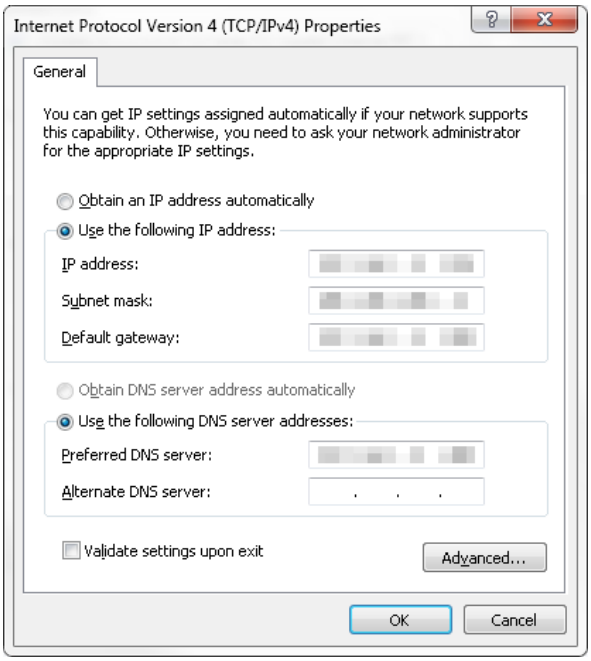
• **Lease Time** – Enter the desired lease time using seconds, minutes, or hours.

b) For each End Device, set the laptop's TCP/IPv4 properties (Found at **Control Panel** > **Network and Internet** > **Network Connections**) as follows:



c) If NO, disable the *DHCP Server* option.

d) On the laptop, set the *TCP/IPv4* properties. Non-PC devices, such PLC's, do not require the *Preferred DNS Server* entry.



7 In the ICX35-HWC configuration webpage, click **APPLY**. The page automatically redirects to the new IP address if the IP address is changed.

8 Reset your PC back to its original IP address. This IP address should be on the same subnet as the ICX35-HWC.

9 Close your browser and open a new session. Enter the new IP address of the ICX35-HWC to access the configuration webpage (192.168.0.250).

2.3 Connecting to Your Cellular Provider

The ICX35-HWC supports 3G GSM/GPRS and 4G LTE (where applicable) networks. It uses your cellular provider as an ISP (Internet Service Provider) to connect to the Internet. All cellular service connections require a Subscriber Identity Module (SIM) to be installed in the ICX35-HWC. This includes connections to CDMA based services like Verizon (previously did not require a SIM). Contact your service provider to obtain a SIM.

2.3.1 Connection Using GSM/GPRS

The Subscriber Identity Module (SIM) in the ICX35-HWC is a smartcard that securely stores the key identifying a cellular subscriber. Generally, you will only need to install a SIM once in the life of the cellular gateway - and it may be pre-installed by your ProSoft Technology Representative.

Important: You must specify the exact APN given by your cellular network provider for your SIM card contract. Otherwise, functionality or billing will be affected.

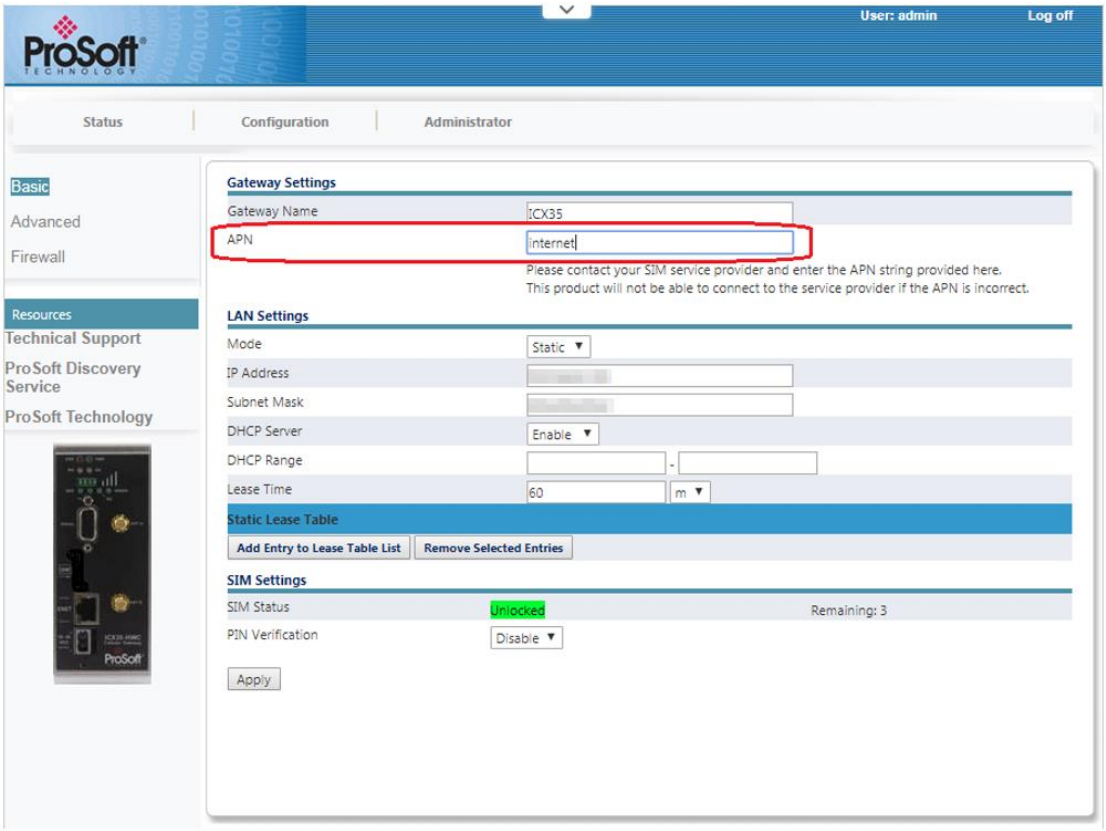
AT&T Users: For SMS texting functionality, you must power up the ICX35-HWC with the SIM installed within 72 hours after AT&T activates the SIM card.

The SIM card slot is located on the front of the cellular gateway.

1. Remove the SIM Card Slot cover by removing the two screws holding it into place.
2. Insert the SIM card (size 2FF, Mini-SIM) into the ICX35-HWC and cycle power. The SIM card is read by the ICX35-HWC upon boot up.

3 Re-attach the SIM Card Slot cover.

4 Enter the *APN* (Access Point Name) in the **Configuration > Basic** section of the UI. The APN is provided by your cellular provider.



5 After the ICX35-HWC reboots, it establishes a link to your cellular provider network, also called registering on the network, and then receives an IP address.

6 When the ICX35-HWC receives its IP address from the cellular provider, a connection to the Internet or the cellular network is also available for computers or other devices to connect directly to the ICX35-HWC.

7 The GSM network information is now displayed on the *Status* webpage.

2.3.2 Connection Using CDMA

1 When the ICX35-HWC is powered on, it automatically searches for cellular service using CDMA-based cellular technology.

2 The ICX35-HWC establishes a PPP (Point-to-Point Protocol or "dial" up connection) link to the cellular network, also called registering on the network, and receives an IP address.

3 When the ICX35-HWC has received its IP address from the cellular provider, a connection to the Internet or the cellular network is also available for computers or other devices to connect directly to the ICX35-HWC.

4 The CDMA network information is now displayed on the *Status* webpage.

2.3.3 SIM Card Security

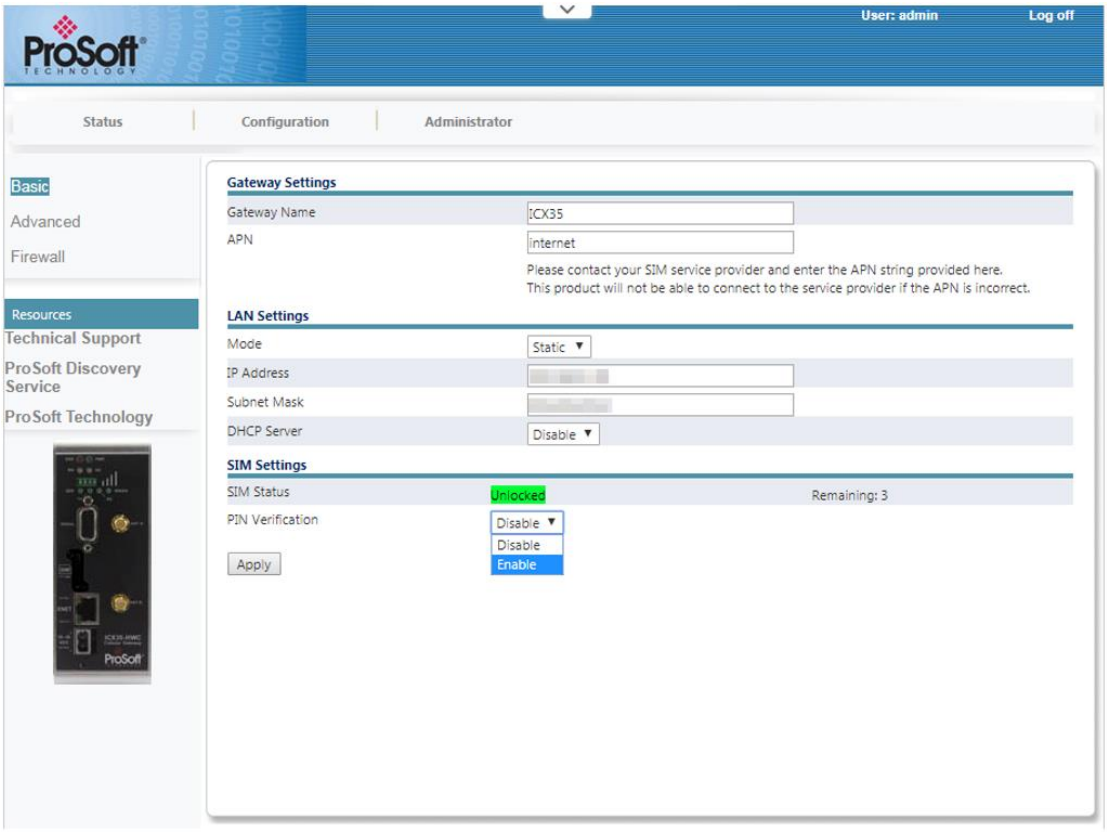
To protect a SIM card from others using it for phone calls or cellular data, a SIM PIN can be used. When a SIM PIN is used, the SIM card will automatically lock upon an ICX35-HWC reboot. The PIN protection enablement, PIN (Personal identification number), and PUK (PIN unlock key) codes are saved on the SIM card. Replacing the SIM card requires a reconfiguration of the SIM settings.

Most mobile devices offer SIM PIN protection. At startup, if the PIN security function is active, the user must enter a 4 to 8 digit PIN to enable the ICX35-HWC's non-emergency functions. You can save the PIN code in the configuration in an encrypted format.

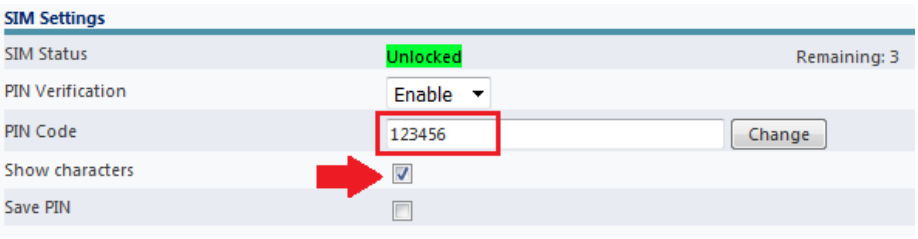
2.3.4 SIM Card PIN Verification

The SIM Card PIN Verification enables the ICX35-HWC's non-emergency functions. By default, this feature is not enabled. The following steps show how to enable (and disable) this feature:

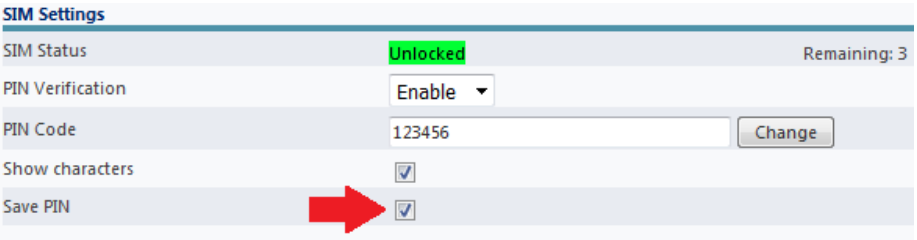
1. On the ICX35-HWC webpage, navigate to the **Configuration > Basic** webpage.
2. Under SIM Settings, click on the PIN Verification setting and select **ENABLE**.



3 Enter a 4 to 8 digit PIN Code. You can display the digits by clicking the *Show Characters* box.

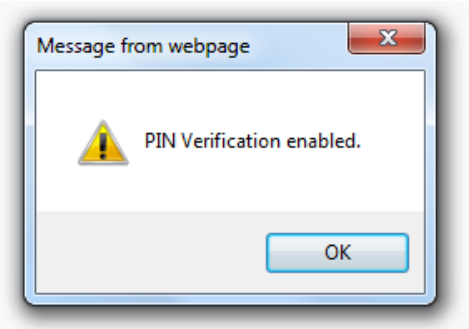


4 You can save the PIN code in the configuration in an encrypted format by clicking the *Save PIN* box.



5 When ready, click the **APPLY** button to apply the changes.

6 When successful, the following message displays:

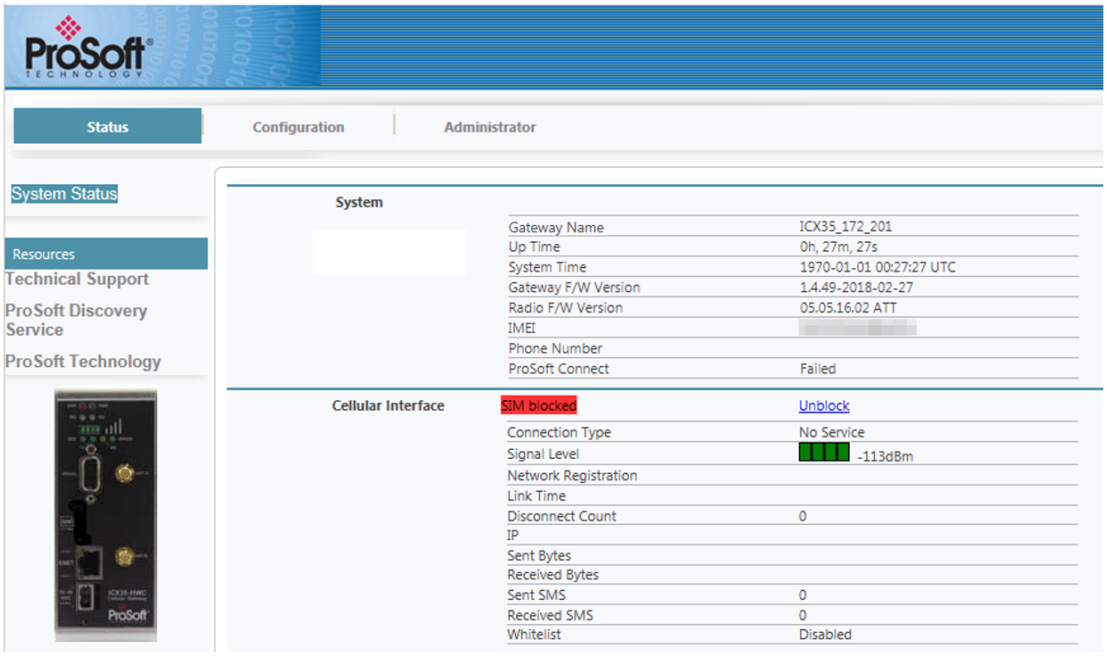


7 To disable this feature, select **DISABLE** from step 2 above and continue through the steps.

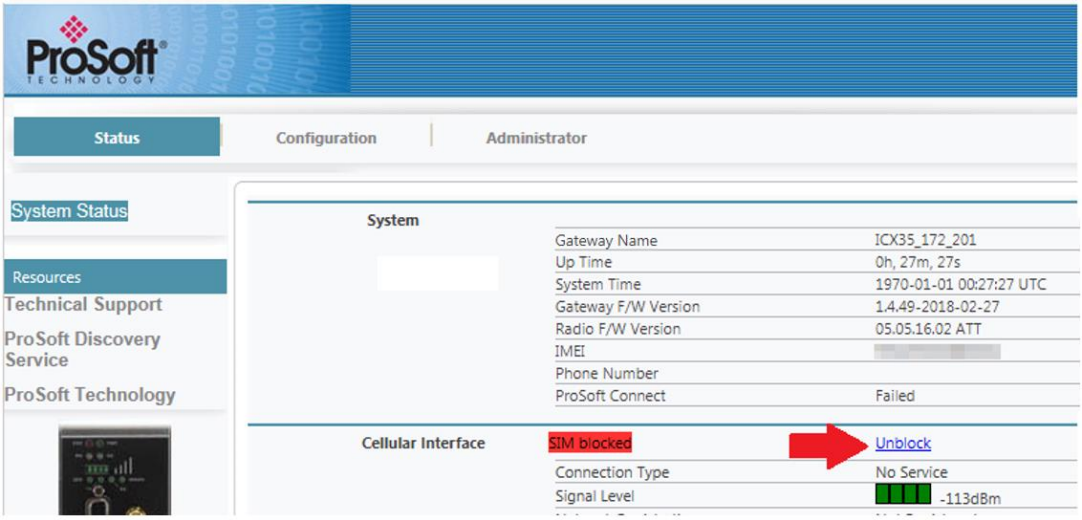
Important: If the wrong PIN Code is entered and submitted more than three times, the SIM card becomes blocked. (Notice the number of Remaining tries in the top right corner of the SIM Settings area). The SIM card can be unblocked by entering a PUK code, provided by the service provider (Example: AT&T). The next section discusses the unblocking process.
When the SIM card is blocked, you will not be able to access the ICX35-HWC configuration webpage via the WAN connection. You can connect via the LAN (Ethernet) port until the SIM card is unblocked.

2.3.5 Unblocking a SIM Card

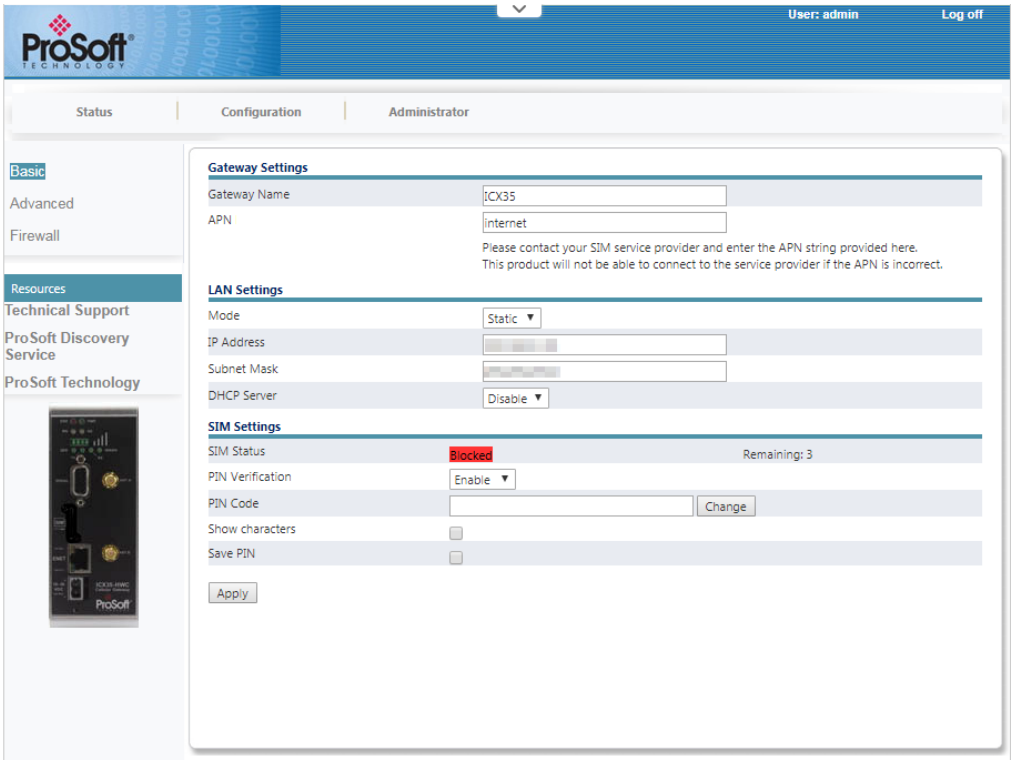
If the wrong PIN Code is entered more than three times, the SIM card becomes blocked. During this time, ICX35-HWC WAN (cellular) connectivity is disabled. The SIM PIN status shows "**SIM Blocked**" on the **Status > System Status** webpage (*WAN* section). You can unblock it by entering the PUK code assigned to the SIM card by your service operator.



1 To unblock the SIM card, click the **Unblock** link from the **Status > System Status** webpage (*WAN* section).



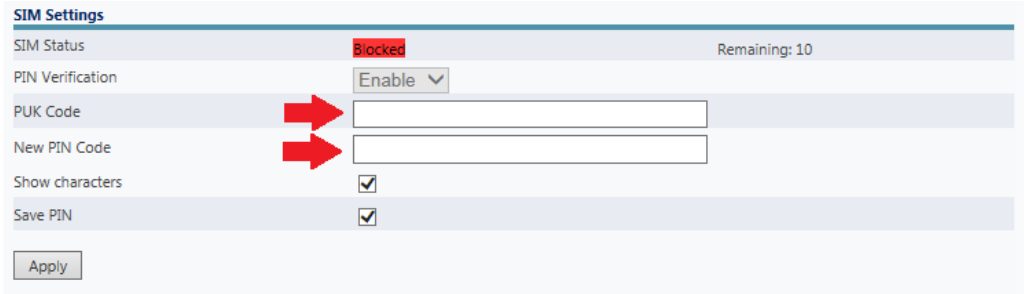
2 The link takes you to the **Configuration > Basic** webpage (*SIM Settings* section).



3 Contact your service provider to provide you with the PUK code. You will need the phone number that is assigned to the SIM card.

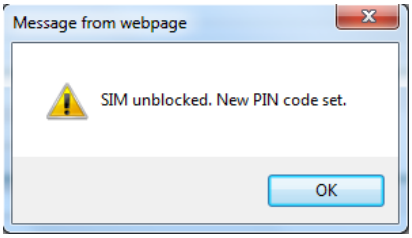
Important: It is recommended to keep the PUK written down in a safe place from the device. Entering an incorrect PUK code ten times in a row will permanently lock the SIM card, requiring a new one.

4 Once you obtain the PUK code, enter the *PUK Code* and a *New PIN Code*.

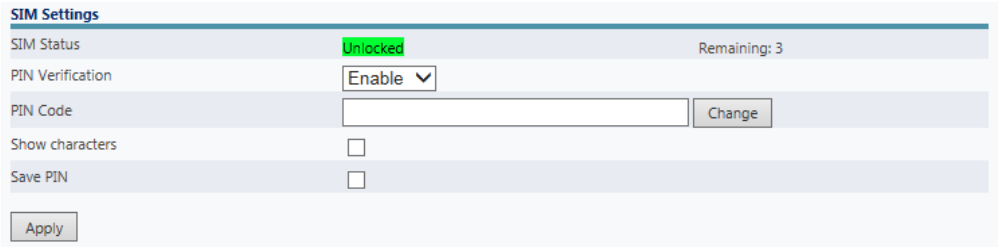


5 Click **APPLY**.

6 Upon success, the following message is displayed:



7 The *SIM Status* is now **Unlocked**. PIN Verification can be enabled, as needed.

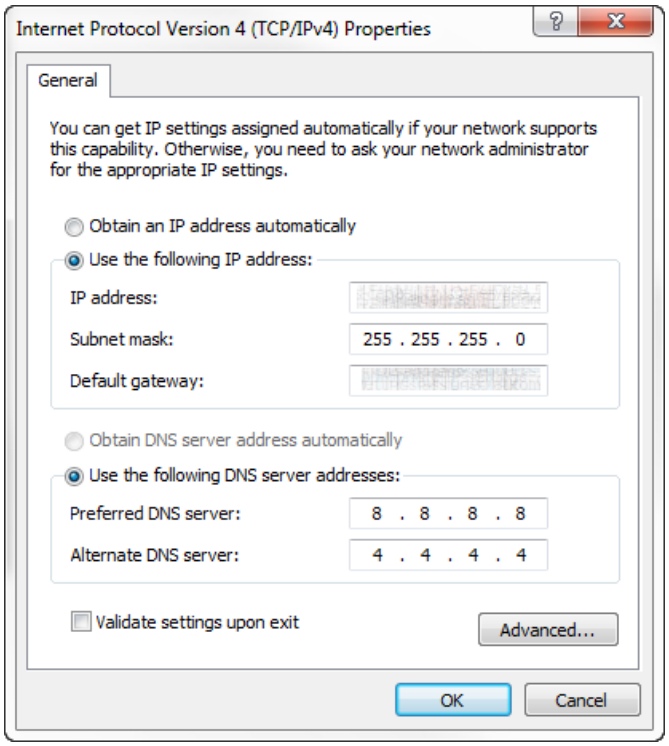


2.4 Connecting to the Internet Using the ICX35-HWC

Internet connectivity through the ICX35-HWC is achieved using the following steps:

1 Connect the laptop LAN port to the Ethernet port on the ICX35-HWC.

2 On the laptop, set the *TCP/IPv4* properties:



Where:

- *IP address* = The assigned IP address of your laptop.
- *Default gateway* = The assigned IP address of the ICX35-HWC IP.
- *Preferred DNS Server* = 8.8.8.8 (Google)
- *Alternate DNS Server* = 8.8.4.4 (Google alternate)

3 Click **OK**.

4 Open your web browser on your laptop to connect to the internet.

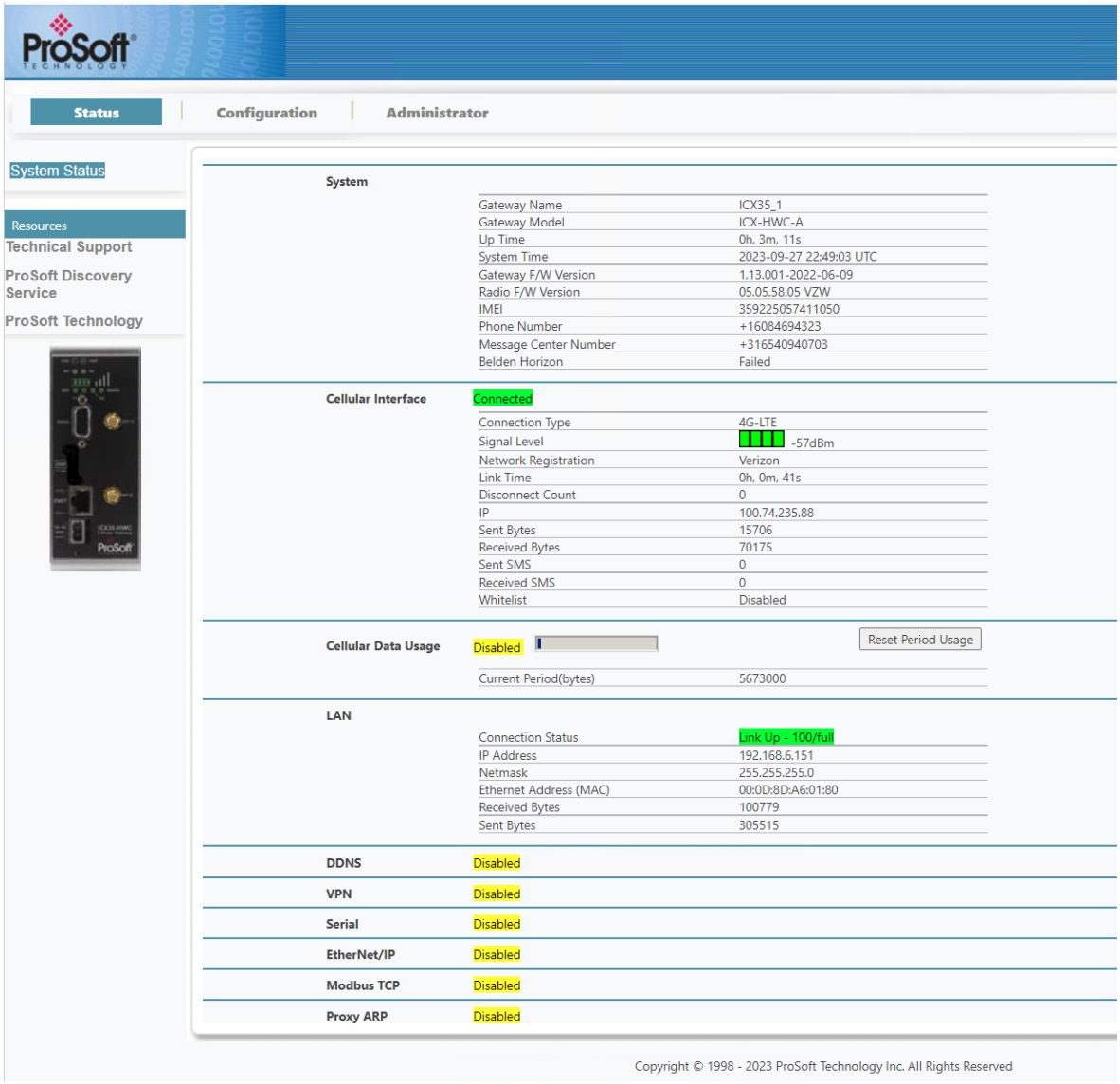
3 ICX35-HWC Webpage

There are three main tabs of the ICX35-HWC webpages:

- Status
- Configuration
- Administrator

3.1 Status Tab

The Status tab displays the current settings of the cellular gateway including up time, IP address, and cellular data usage.

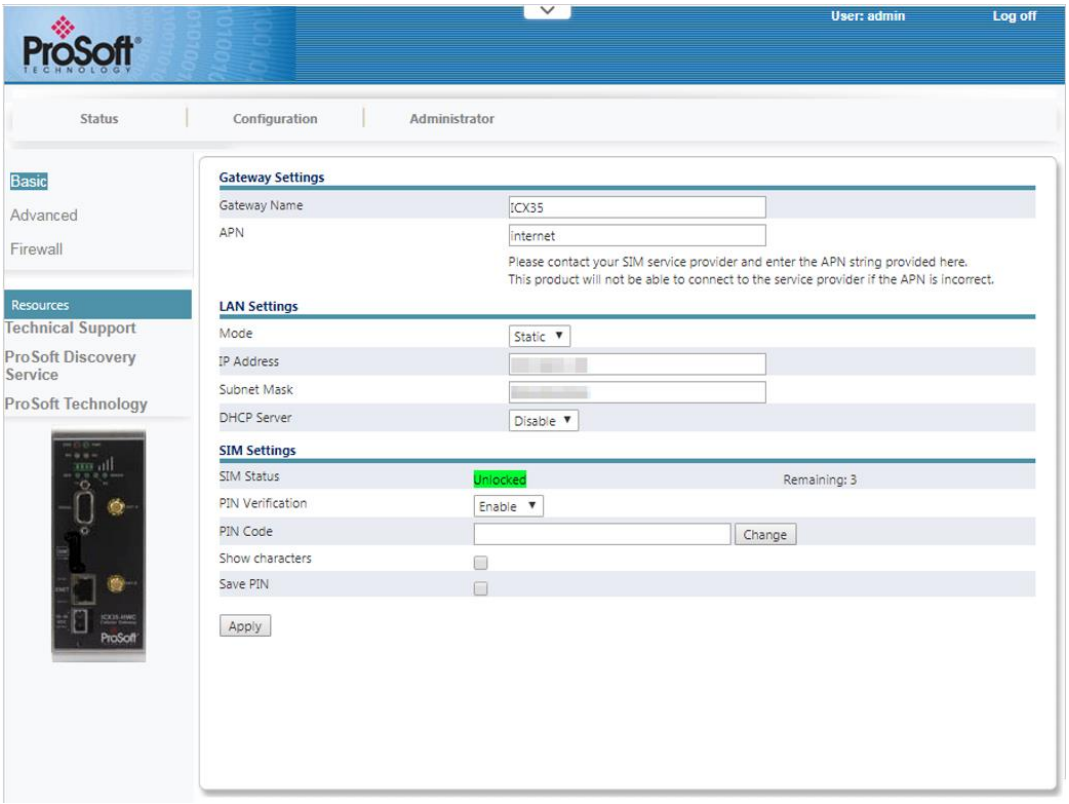


System	Description
Gateway Name	Name of ICX35-HWC on network
Up Time	Amount of time since last power cycle or reset
System Time	Current date and time of the ICX35-HWC
Gateway F/W Version	Firmware version of the cellular hardware
Radio F/W Version	Firmware version of the radio hardware
IMEI	International Mobile Station Equipment Identity number
Phone Number	Phone number assigned by the SIM card
Message Center Number	Message Center Number configured on the SIM card. This number is used to send SMS messages.
Belden Horizon™	Status of Belden Horizon utility
Cellular Interface	
Connection Type	Type of cellular connection. Example: GSM
Signal Level	Signal Level of cellular network (dBm)
Network Registration	Registered local cellular network. If a carrier does not support this request, it will display “Not Available”.
Link Time	The number of days, hours, minutes, seconds connected to the WAN
Disconnect Count	The time the unit has lost communication to a cell tower and has/is attempting to reconnect back to the cellular service. It counts each time the service has disconnected from the cellular service while the unit is running.
IP	IP address of the ICX35-HWC on the WAN
Sent Bytes	Number of sent bytes on the WAN port for this connection
Received Bytes	Number of received bytes on the WAN port for this connection
Sent SMS	Number of sent SMS text messages since power on
Received SMS	Number of received SMS text messages since power on
Whitelist	Indicates if whitelisting is enabled or disabled
Cellular Data Usage	
Current Period	Shows the total number of bytes (sent and received) on an ongoing basis, in bytes. This number is reset on the *Plan Start Day* unless changed by clicking on the **Reset Period Usage** button.
LAN	
Connection Status	Displays the Link status
IP Address	IP address of the ICX35-HWC on the LAN
Netmask	Subnet Mask
Ethernet Address (MAC)	MAC address of the ICX35-HWC
Received Bytes	Total number of bytes received on the Ethernet port
Sent Bytes	Total number of bytes send on the Ethernet port
DDNS	Dynamic DNS (Set in **Configuration > Advanced**)
VPN	Virtual Private Network (Set in **Configuration > Advanced**)
EtherNet/IP	EtherNet/IP status (Set in **Configuration > Advanced**)
Modbus TCP	Modbus TCP/IP status (Set in **Configuration > Advanced**)
Proxy ARP	Proxy ARP status (Set in **Configuration > Advanced**)

3.2 Configuration Tab

3.2.1 Basic

The **Configuration > Basic** tab allows you to configure the *Module* and *LAN* settings.



Gateway Settings

Parameter	Description
Module Name	Name of ICX35-HWC on network
APN	Access Point Name of the network path for cellular connectivity. This name is assigned by your cellular network provider.

LAN Settings

Parameter	Description
Mode	Select Static or DHCP
IP Address	IP address of the ICX35-HWC Ethernet port
Subnet Mask	Subnet mask of the ICX35-HWC Ethernet port
DHCP Server	Enables/Disables DHCP functionality
DHCP Range	Used when *DHCP Server* is enabled. DHCP range of end devices
Lease Time	Used when *DHCP Server* is enabled. Enter the lease time using seconds, minutes, or hours. This setting depends on your cellular plan.
Static Lease Table	Used when a list of specific clients, identified by their MAC addresses, need to be reserved specific IP addresses. Add one static lease per client.

SIM Settings

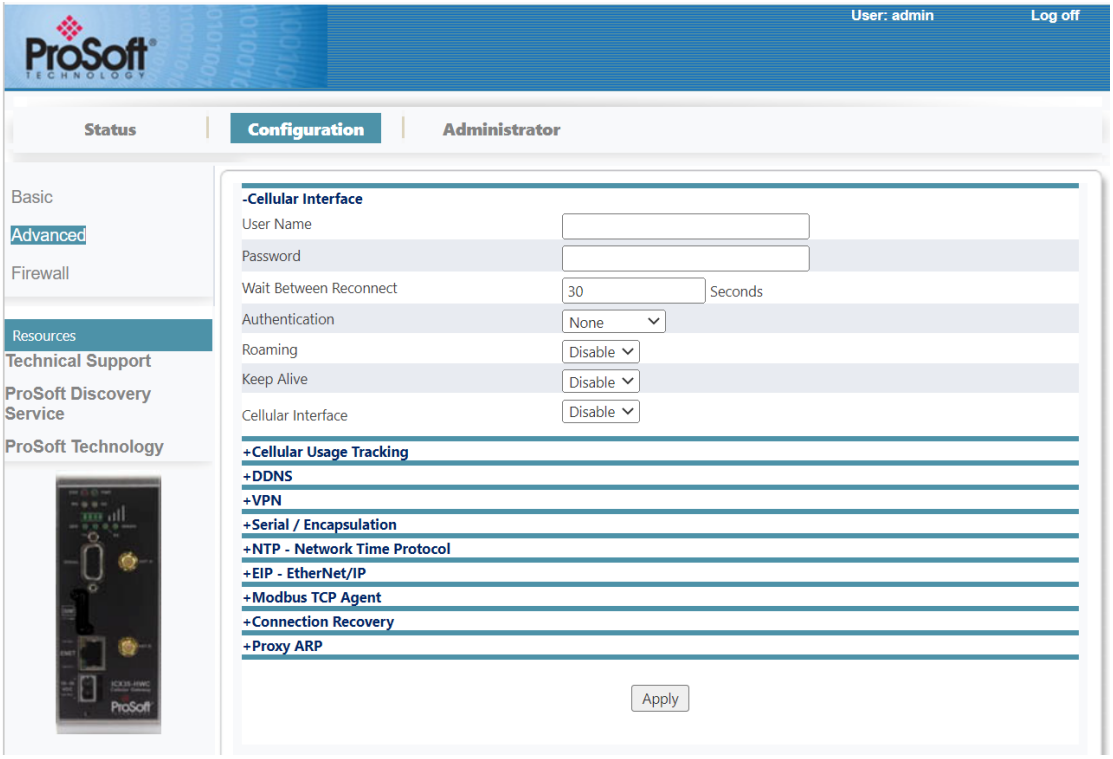
Parameter	Description
SIM Status	Current state of SIM card. For more information, see *SIM Card PIN Verification*. **Unlocked** – The ICX35-HWC's non-emergency functions are enabled. **Locked** – The non-emergency cellular functions are disabled and you must enter the *PIN Verification* to enable them.
PIN Verification	A 4-to-8-digit PIN used to unlock the non-emergency cellular functions of the SIM card.

3.2.2 Advanced

The **Configuration > Advanced** tab allows you to configure the following:

- Cellular Interface
- Cellular Usage Tracking
- DDNS
- VPN
- Serial / Encapsulation
- NTP – Network Time Protocol
- EIP – EtherNet/IP
- Modbus TCP Agent
- Connection Recovery
- Proxy ARP

Cellular Interface

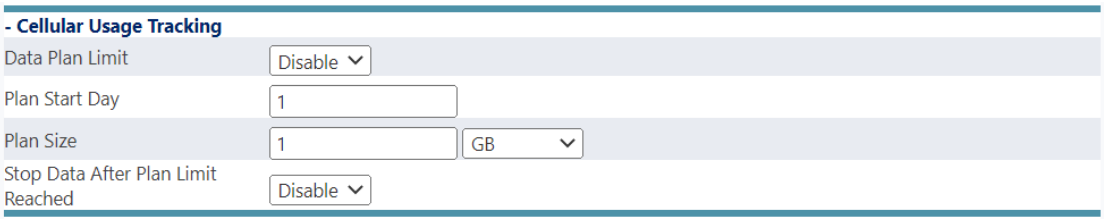


Parameter	Description
User Name	(Optional) User name for the connection
Password	(Optional) Password for connection
Wait Between Reconnect	The number of seconds to wait before trying to establish a reconnect. If this is set to '0', the auto connection is disabled.
Authentication	**CHAP** - Challenge Handshake Authentication Protocol **PAP** - Password Authentication Protocol **PAP & CHAP** - A mix of both methods
Roaming	This setting prevents the device from connecting to a non-native network, helping to prevent additional charges.
Keep Alive	If enabled (0 denoting Disabled), this parameter sets the keep alive ping period time in seconds. When Enabled, the two fields listed below appear.
Keep Alive Ping Address	Time to keep a connected address connection alive
Keep Alive Ping Period	Number of seconds to ping to ping address in order to keep a connection between a cell tower and a module alive
Cellular Interface	Disabling this parameter allows the ICX35-HWC to access the internet, including Belden Horizon through the LAN interface. This would disable the ICX35-HWC WAN interface. SMS will still be available. **Note:** Disabling Cellular Internet Access will enable internet access through the LAN interface. The following features will be disabled: *LAN DHCP ServerOpenVPN *IPsec *Pass Through (End Device Address parameter is cleared) *Port Forwarding (All existing rules are cleared)

Note: Excluding the *Keep Alive* parameter, the ICX35-HWC reboots when updating other WAN parameters (by clicking **Apply**).

Cellular Usage Tracking

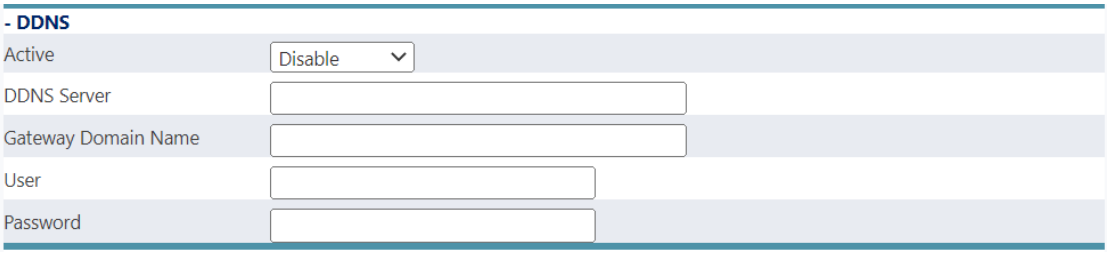
Note: The *Cellular Usage Tracking* feature is not an official value of the usage a carrier reports. Due to possible differences in these values, cellular usage tracking should be used as an aid for gauging how much data the system is using over a period rather than as a reliable method to determine billing costs.



Parameter	Description
Data Plan Limit	Specifies whether or not the cellular data storage usage tracking feature is enabled.
Plan Start Day	Specifies the day of the month (1 to 28) that the data plan begins. For example, AT&T service in the USA is billed from the 19th of the month through the 18th of the following month. This is the day that the Usage Value Counter resets on.
Plan Size	Maximum number of megabytes (MB) or gigabytes (GB) of WAN data usage before 3G communications are shut down until the next plan start day. You can also choose *Unlimited*. It provides a visual status of how much data is being used.
Stop Data After Plan Limit Reached	Specifies whether or not the ICX35-HWC will voluntarily deactivate cellular data if it reaches its data plan limit. You can select *Disabled* or *Enabled*. If you select *Disabled*, the ICX35-HWC will attempt to transfer data even if the Plan Size is exceeded, but the cellular data service provider may halt data, reduce the data rate, or charge additional fees. A 10% buffer is automatically used to help prevent data overages because the gateway usage number isn't instantaneously updated and it may be possible that some amount of byte count loss occurs due to a device reset. If you select *Enabled*, the ICX35-HWC stops transferring data after the Plan (size) limit is reached.

DDNS

Dynamic DNS (DDNS) is a method of mapping WAN IP addresses that are assigned to a domain name.



Parameter	Description
Active	This parameter specifies if dynamic DNS is disabled or to which provider it will update information. (Disabled, DynDNS.org, No-IP.com)

Important: For providers like DynDNS.org, the Time to Live (TTL) value may affect how long it takes an ICX35-HWC to see a change in IP address (for example, the IP address changes because of a reboot). It may take the ICX35-HWC upwards of 30 minutes to see the new address.

DDNS Server	System name for DDNS service.
ICX35 Domain Name	Specifies the domain that is updated with this gateway's current IP address.
User	If the dynamic DNS provider requires a username, this parameter specifies what name is sent to authorize the dynamic DNS transaction.
Password	If the dynamic DNS provider requires a password, this parameter specifies the password that is sent to authorize the dynamic DNS transaction.

VPN

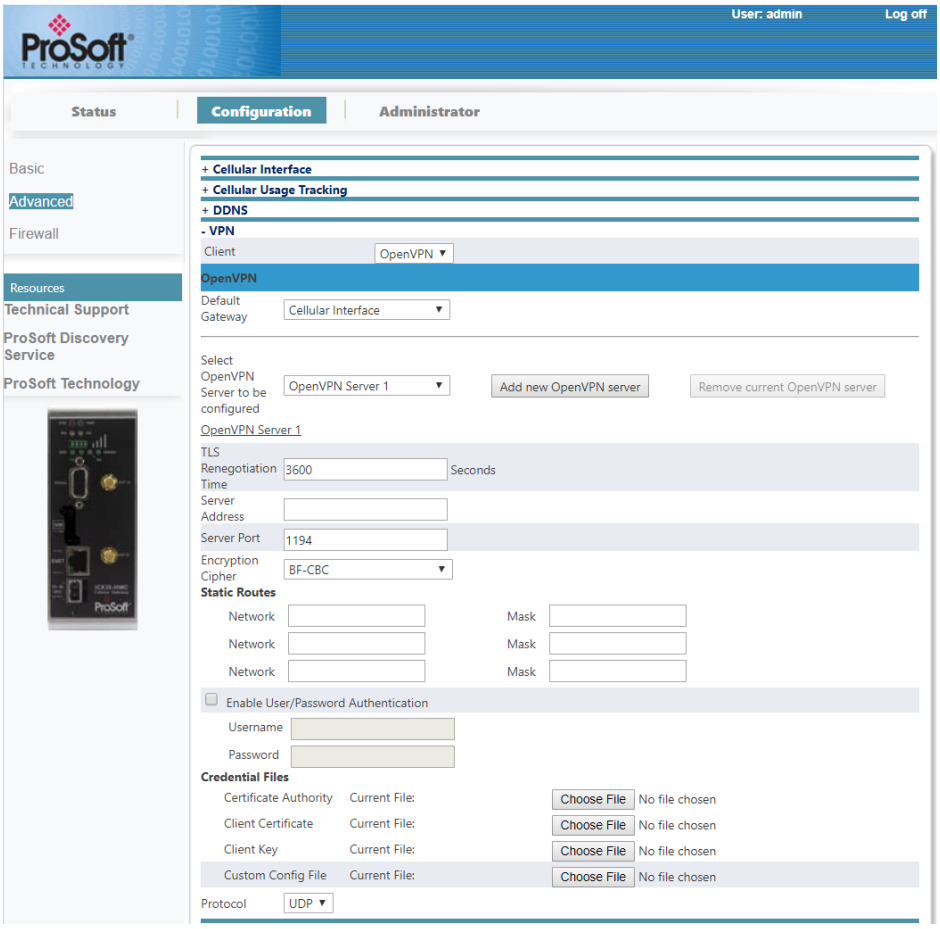
The Client drop-down list includes the following options:

- Disable
- OpenVPN
- IPSec

OpenVPN

The Virtual Private Network (VPN) Tunnel allows you to access a private local network through the ICX35-HWC.

If you select **OpenVPN** from the *Client* drop-down list, the following additional parameters appear:



OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

This document assumes you have access to a running OpenVPN server to generate the required certificates and to authenticate through. Chapter 9 provides details on using OpenVPN.

Note: When applying new configuration parameters, adding or removing a server configuration, all the existing connections will be recreated.

Parameter	Description
Default Gateway	Interface to be used as a default gateway. By default, it is set to **Cellular interface**. It can also be set to pass the traffic through one of the configured tunnels - **OpenVPN Server 1**.
Select the OpenVPN Server to be configured	The OpenVPN Server instance that is being configured.
TLS Renegotiation Time	Transport layer Security renegotiation time in seconds. This controls how often the underlying SSL/TLS session renegotiates. This provides additional security by frequently rekeying the session keys. Default value: 3600.
Server Address	IP address or hostname of the VPN server. This is the IP Address that you are creating the tunnel to. In the previous example, this is the public IP Address of the ICX35-HWC in pass through mode that is being used as the default connection to the Linux server.
Server Port	Service port number on the VPN server. The default port is **1194**. This is the port number for the OpenVPN. Port 1194 is the default port designated for OpenVPN. This is the port number used for the previous example.
Encryption Cypher	Cipher used to encrypt data channel packets. The default value is **BF-CBC**. Some of the ciphers that are supported by OpenVPN are not available in this list because they are considered insecure. However, these can still be used by using a custom configuration file.
Static Routes	Static routes to remote networks to be specifically accessed through the configured OpenVPN connection. A maximum of 3 static routes are supported per tunnel.
Enable User / Password Authentication	Alternative authentication method based on username and password. Enter a *Username* and *Password*.
Credential Files	**Certificate Authority** - VPN authentication that issues certificates for VPN, Secure Internal Communication (SIC), and users. **Client Certificate** - Issued by a certificate authority as proof of identity. **Client Key** - Password to the corresponding client certificate. Click the **Choose File** button to locate these files. Internally, they are renamed (Example: file_OpenVPN_CA.crt), and stored in the appropriate *Current File* area. **Note:** These Credential files are mandatory in order to enable OpenVPN. They can either be uploaded individually or have their content added inline, within the custom configuration file. If by mistake you uploaded them and also have them inline in the configuration file, the files uploaded individually will take precedence.
Custom Config File	Click the **Choose File** button to locate and upload a custom OpenVPN configuration file, which overrides any credential files previously loaded. If you have not previously uploaded any credential files, the Custom Configuration File should include them.
Protocol	The protocol to use when connecting with the remote: **TCP** or **UDP** (default).

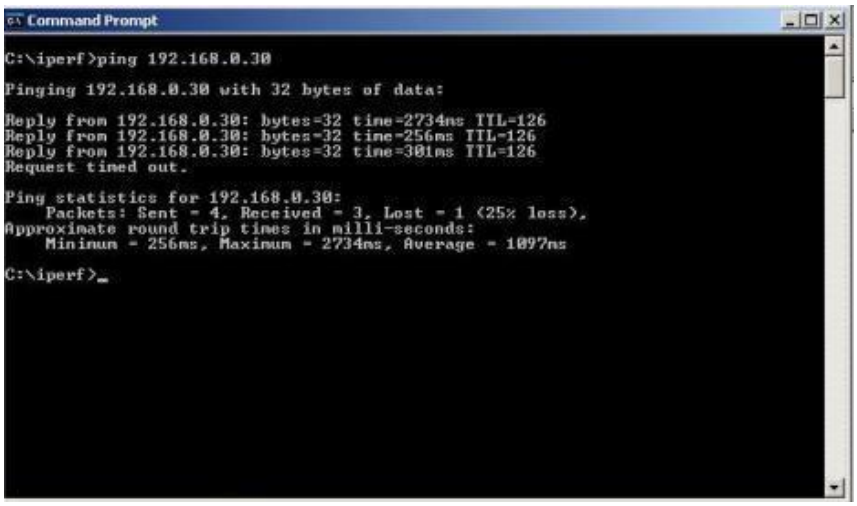
The following table lists the OpenVPN default values:

Parameter	Default Value
Server/Client	Client
Interface	Tun
Protocol	UDP
Authorization	None
Encryption Cipher	Undefined (Should be defined by the server). Default: **BF-CBC**
TLS Renegotiation Time	3600 seconds
LZO Compression	Adaptive
Port	User-configurable. Default: **1194**
Server address	User-configurable

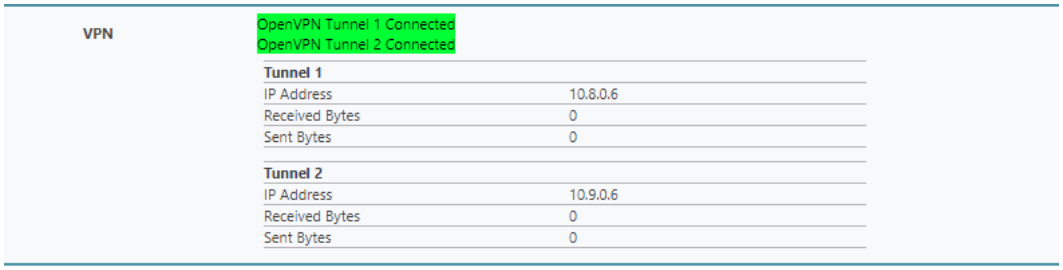
Verification

Once the client and server are configured, the client creates a VPN tunnel through the server to the LAN where the server resides. The Status webpage will indicate that an OpenVPN connection is established.

You can now pass secured data between the two LAN devices. Verify this with a simple ping from one LAN device to the other.

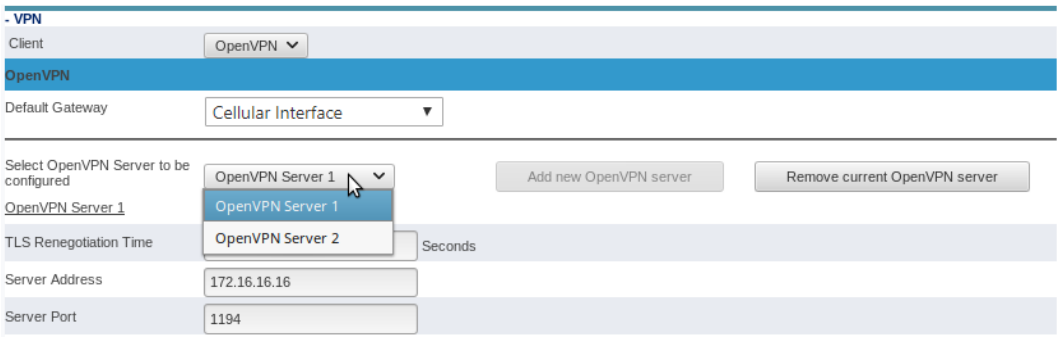


With two tunnels connected, the following information is shown at **Status > System Status**.



Adding a Second OpenVPN Server

To add a second OpenVPN connection, use the **ADD NEW OPENVPN SERVER** button. This creates an additional server configuration section that can be accessed through the drop-down as seen in the image below:

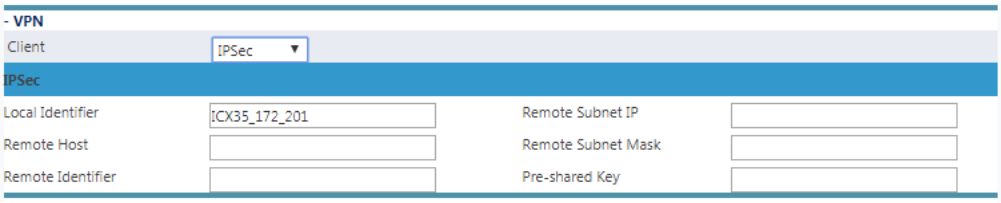


IPSec

The VPN Tunnel Internet Protocol Security (IPsec) feature consists of protocols used for authentication and encryption.

Important: IPSec tunnel does not work with Public Dynamic IP's and DDNS names.

The *IPSec* option from the *Client* drop-down list displays the following parameters:



Parameter	Description
Local Identifier	Specifies the identifier to be used for the local side of the IPsec connection. This is used during authentication of the tunnel. It is a free-form string, although typically it is a Fully Qualified Domain Name, or an IP address. Max length is 28. **Note:** Use the "@" prefix when the IPSec tunnel is established between two ICX35-HWC's. Example: @ICX35_local (This may be the local Module Name. If you are establishing an IPSec tunnel with a network router that supports IPSec, no "@" prefix is needed).
Remote Host	Specifies the IPsec remote IP address.
Remote Identifier	Specifies the identifier to be used for the remote site of the IPsec connection. This is used during authentication of the tunnel. It is a free-form string, although typically, it is a FQDN name, or an IP address. Max length is 28. **Note:** Use the "@" prefix when the IPSec tunnel is established between two ICX35-HWC's. Example: @ICX35_remote (This may be the remote Module Name. If you are establishing an IPSec tunnel with a network router that supports IPSec, no "@" prefix is needed).
Remote Subnet IP	Specifies the subnet address block on the LAN side of the remote peer. This parameter must be specified in the CIDR notation (i.e., a number from 1 to 32).
Remote Subnet Mask	Specifies the subnet mask on the LAN side of the remote peer.
Pre-shared Key	Specifies the pre-shared key that must match between both ends of the VPN tunnel.

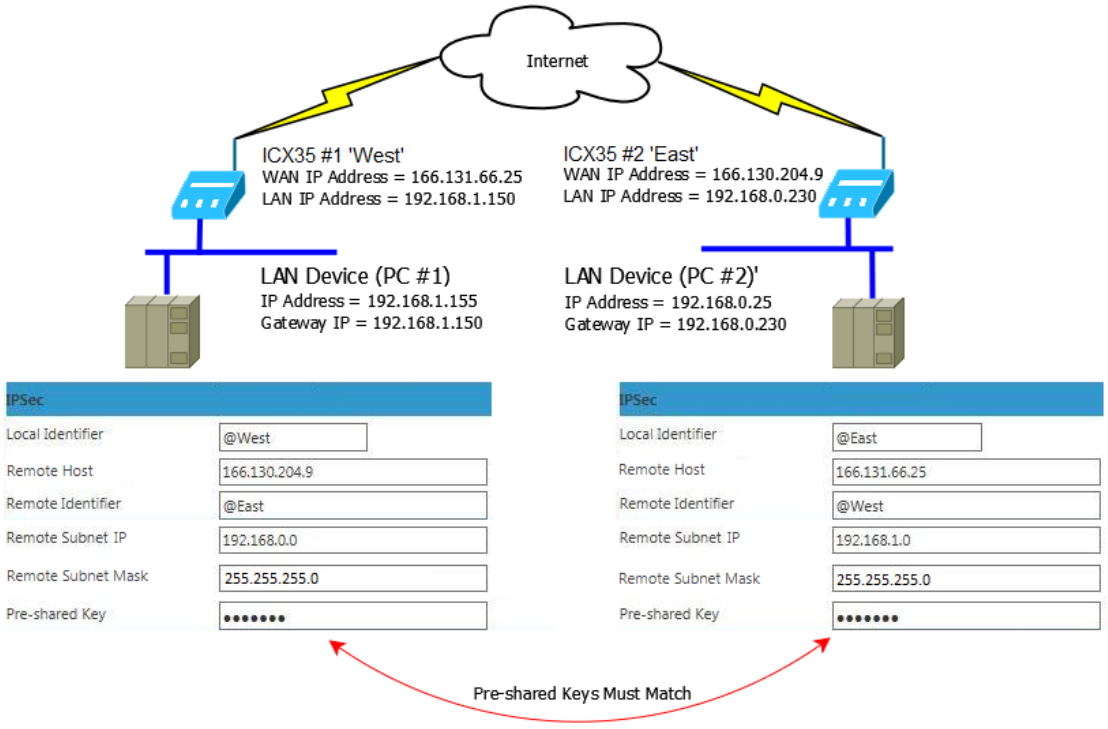
IPSec authenticates and encrypts each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. This is an end-to-end security scheme operating in the internet layer of the Internet Protocol Suite.

The following table lists the IPSec default values:

Parameter	Default Value
Type	Tunnel
Aggressive Mode	Undefined (Default: No)
Phase 1/2 Algorithms	Undefined (Default opportunistic - use remote proposal)

Example

This example connects two devices on different subnets. The devices can be any LAN-based devices that allow you to set the IP Address and Gateway IP address.



Two ICX35-HWC radios and two PCs are used. Once the IPSec tunnel is created, communications can occur between the two PCs. IPSec uses the concept of Local ID and RemoteID to identify each device.

ICX35 #1 "West"

Parameter	Description
Name	ICX35-HWC #1 West
WAN IP	WAN IP Address of ICX35-HWC #1
LAN IP	192.168.1.150
Local Identifier	@West
Remote Host	WAN IP Address of ICX35-HWC #2
Remote Identifier	@East
Remote Subnet IP	192.168.0.0
Remote Subnet Mask	255.255.255.0
Preshared Key	presharedkey (this can be any string)

LAN Device #1 (Connected to ICX35 #1)

Parameter	Description
IP Address	192.168.1.155 (ICX35-HWC #1 end device IP address)
Gateway	192.168.1.150 (ICX35-HWC #1 LAN IP address)
Preferred DNS (if applicable)	192.168.1.150 (ICX35-HWC #1 LAN IP address)

ICX35 #2 "East"

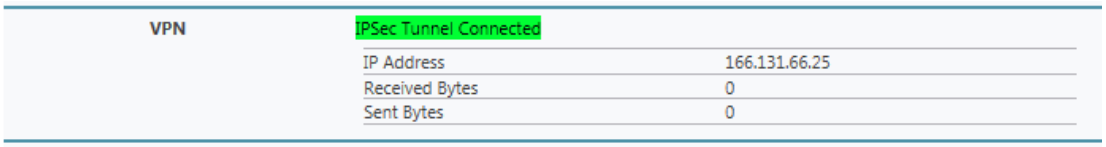
Parameter	Description
Name	ICX35 #2 East
WAN IP	WAN IP address of ICX35-HWC #2
LAN IP	192.160.0.230
Local Identifier	@East
Remote Host	WAN IP address of ICX35-HWC #1
Remote Identifier	@West
Remote Subnet IP	192.168.1.0
Remote Subnet Mask	255.255.255.0
Preshared Key	presharedkey (this can be any string)

LAN Device #2 (Connected to ICX35 #2)

Parameter	Description
IP Address	192.168.0.30 (ICX35-HWC #2's end device IP address)
Gateway	192.168.0.230 (ICX35-HWC #2's LAN IP address)

Verification

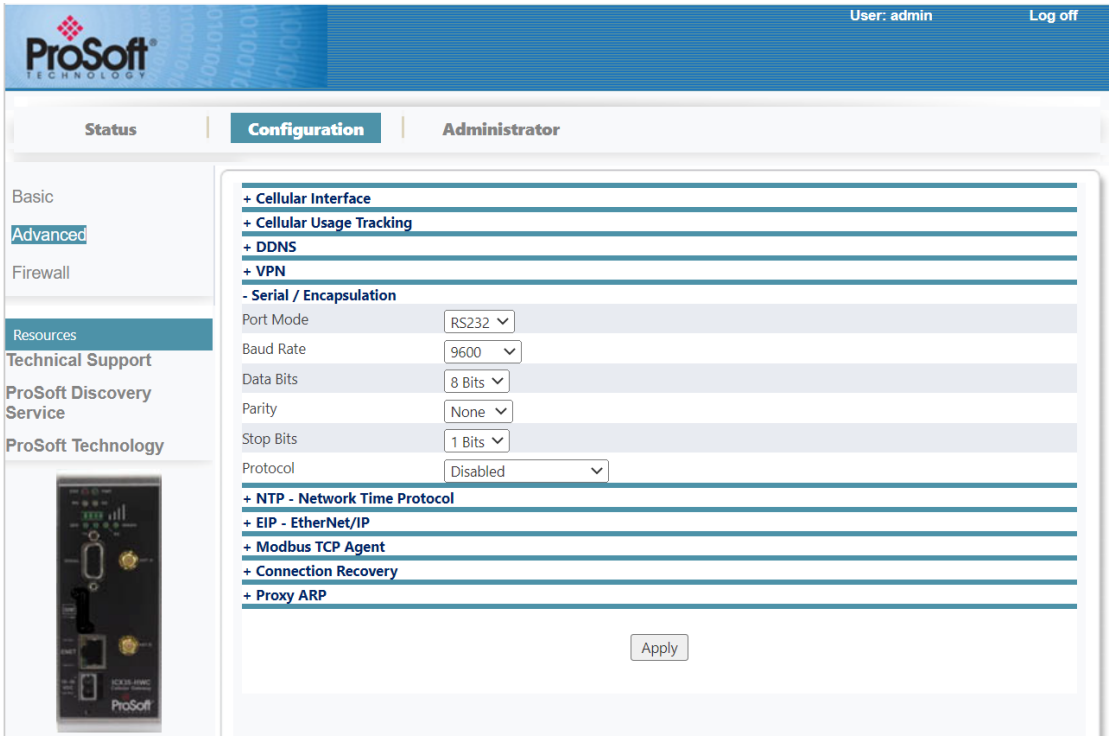
Once all four devices are configured, the status webpage in both of the ICX35-HWC's will indicate that an IPSec VPN connection is made.



You can also ping from one LAN device to the other to verify that the connection is made.

Serial / Encapsulation

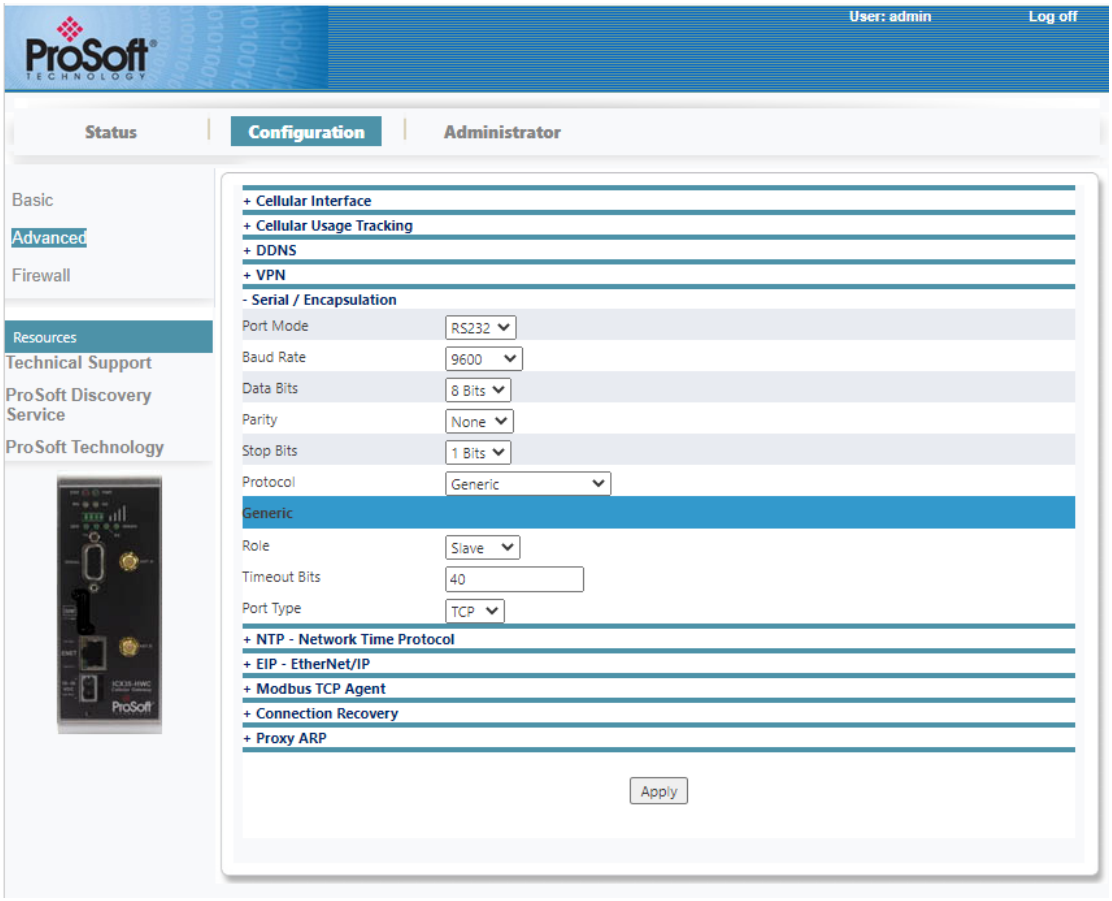
The maximum file size to be transmitted or received at once on the serial port is 4096 bytes. The *Serial/Encapsulation* feature uses IP port 30722 for both TCP and UDP configurations. This port number is not user-configurable.



Parameter	Description
Port Mode	This parameter sets the scheme for the serial port (RS-232 only). **Note:** For RS-422/485 network connectivity, an RS-232 to RS-422/485 converter is recommended.
Baud Rate	Baud rate used on the ICX35-HWC serial port
Data Bits	Number of data bits per character for the serial port
Parity	Parity type used on the serial port. None, Odd, Even, Mark, Space
Stop Bits	Number of stop bits per character for the serial port
Protocol	This parameter sets the serial encapsulation mode for the gateway: o **Disabled** o **Generic** o **Modbus RTU** o **Modbus ASCII** o **Modbus RTU to TCP** o **Modbus ASCII to TCP** o **DF1 Half-Duplex** o **DF1 Full-Duplex** o **DF1 Radio Modem**

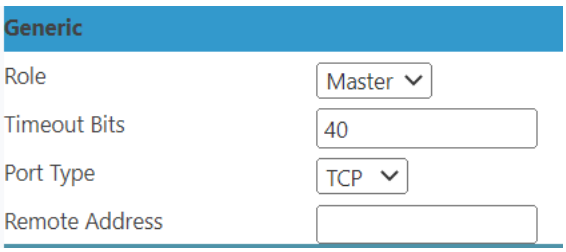
Generic

The *Generic* option sends all serial data to a single destination.



Parameter	Description
Role	Network role for the encapsulation process (Master, Slave, Master/Slave)
Timeout Bits	Length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data. (0 to 65535)
Port Type	Type of IP connection (TCP or UDP) for the encapsulated data.

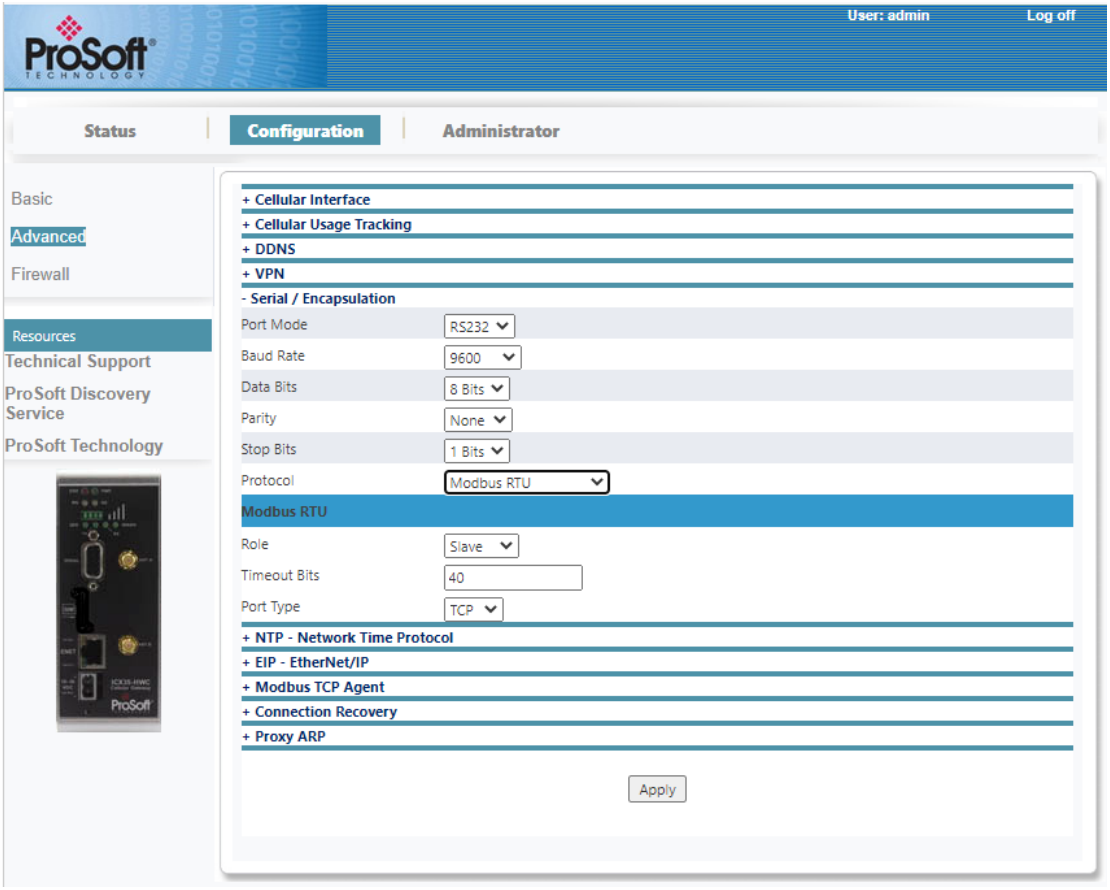
The **Master** role contains an additional parameter:



Parameter	Description
Remote IP	IP address of the Remote connection to which the encapsulated data will be sent.

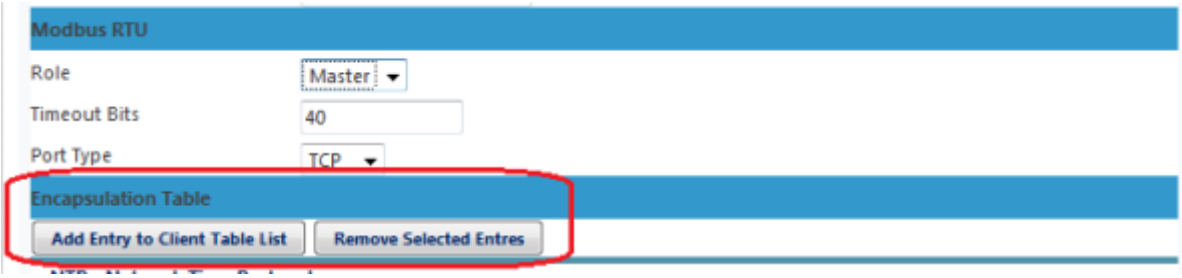
Modbus RTU

The *Modbus RTU* option displays the following additional parameters:



Parameter	Description
Role	Network role for the encapsulation process (Master, Slave, Master/Slave).
Timeout Bits	Sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Type of IP connection (TCP or UDP) for the encapsulated data.

The **Master** role contains additional parameters:



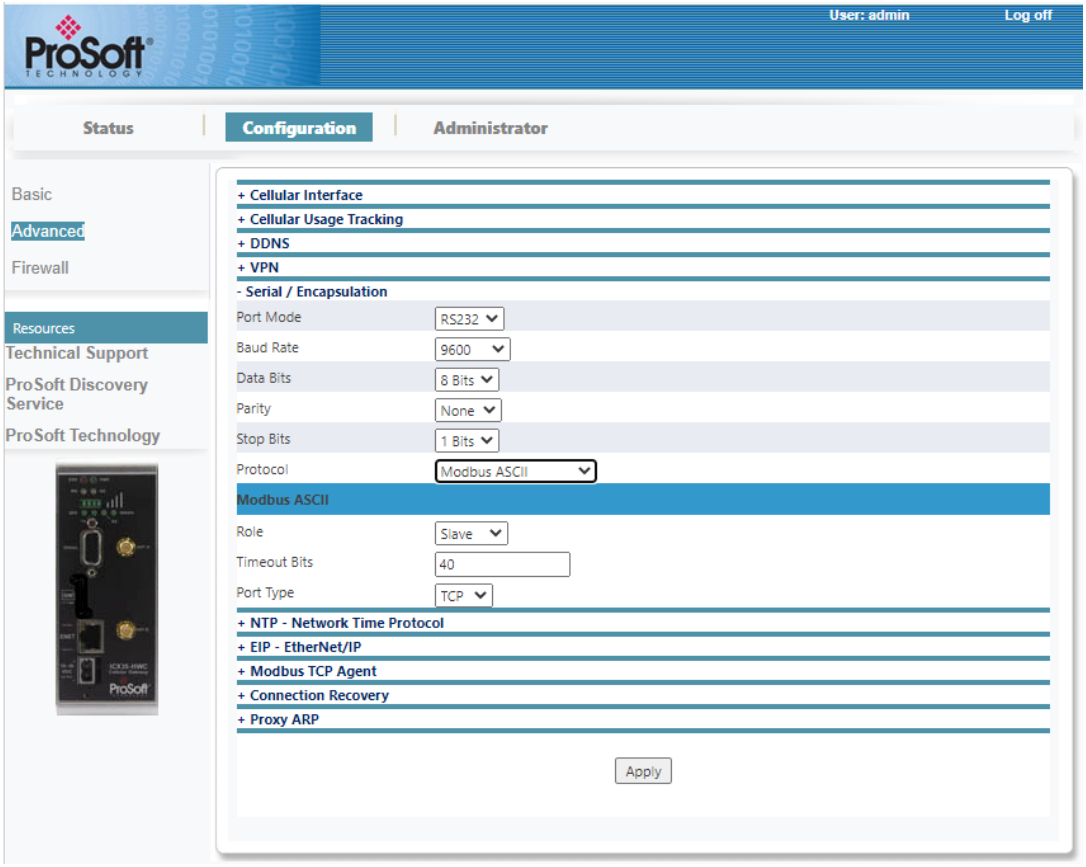
- Add Entry To Client Table List
- Remove Selected Entries

If **Slave** is selected, the *Encapsulation* table is not visible. You can add an entry to the *Client Table* list. Click on the **ADD ENTRY TO CLIENT TABLE LIST** button.

The **REMOVE SELECTED ENTRIES** button selects and removes entries from this list.

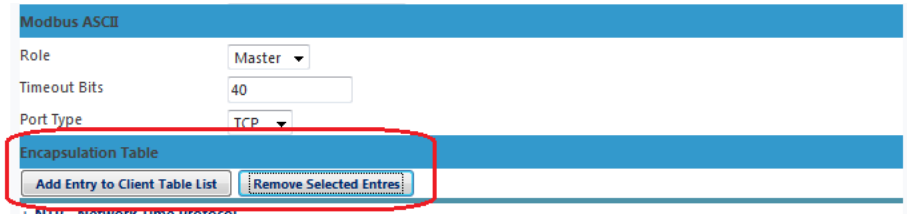
Modbus ASCII

The *Modbus ASCII* option displays the following additional parameters:



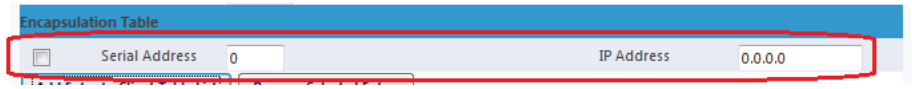
Parameter	Description
Role	Network role for the encapsulation process (Master, Slave, Master/Slave).
Timeout Bits	Sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Type of IP connection (TCP or UDP) for the encapsulated data.

The **Master** role contains additional parameters:



- Add Entry To Client Table List
- Remove Selected Entries

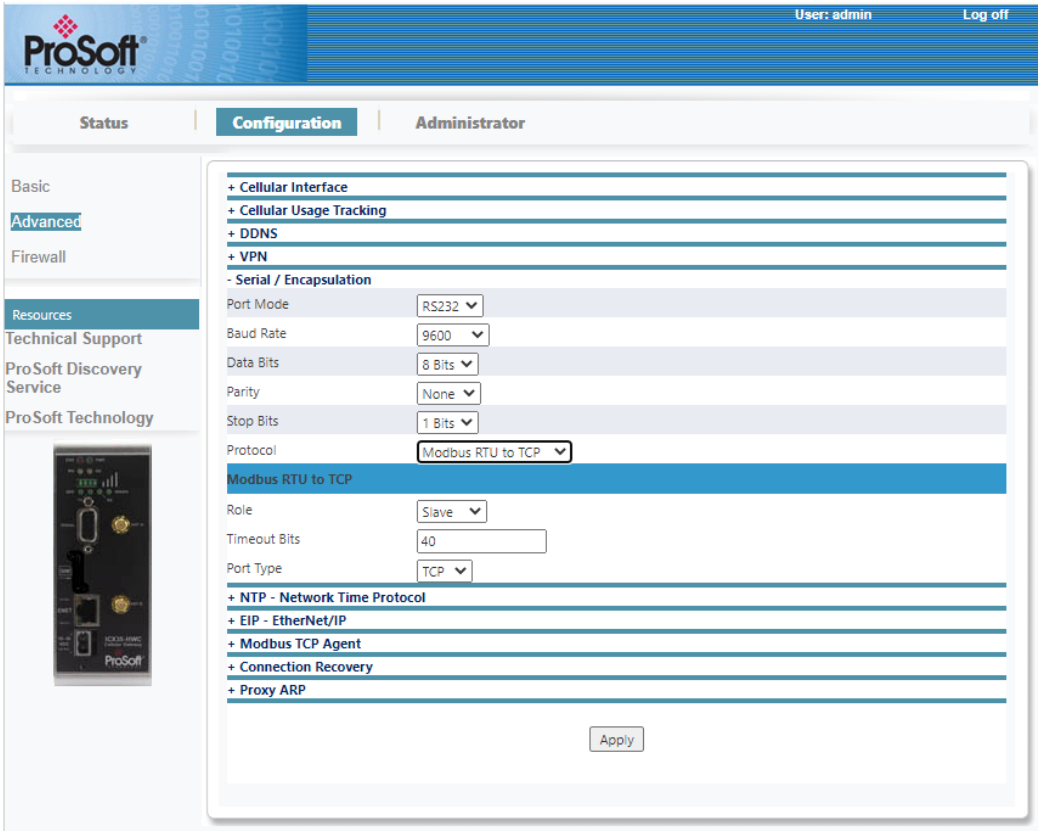
If **Slave** is selected, the *Encapsulation* table is not visible. You can add an entry to the *Client Table* list. Click on the **ADD ENTRY TO CLIENT TABLE LIST** button.



The **REMOVE SELECTED ENTRIES** button selects and removes entries from this list.

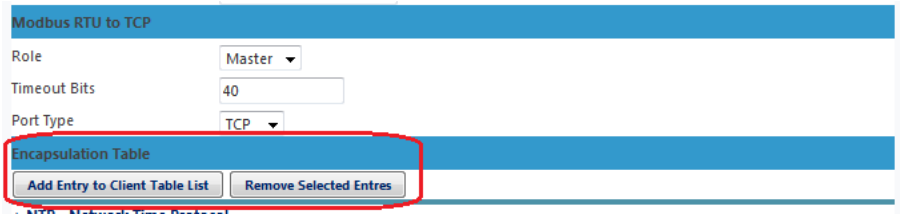
Modbus RTU to TCP

The *Modbus RTU to TCP* option displays the following additional parameters.



Parameter	Description
Role	Specifies the network role for the encapsulation process (Master, Slave).
Timeout Bits	This parameter sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	This parameter specifies the type of IP connection (TCP only) for the encapsulated data.

The **Master** role contains additional parameters:



- Add Entry To Client Table List
- Remove Selected Entries

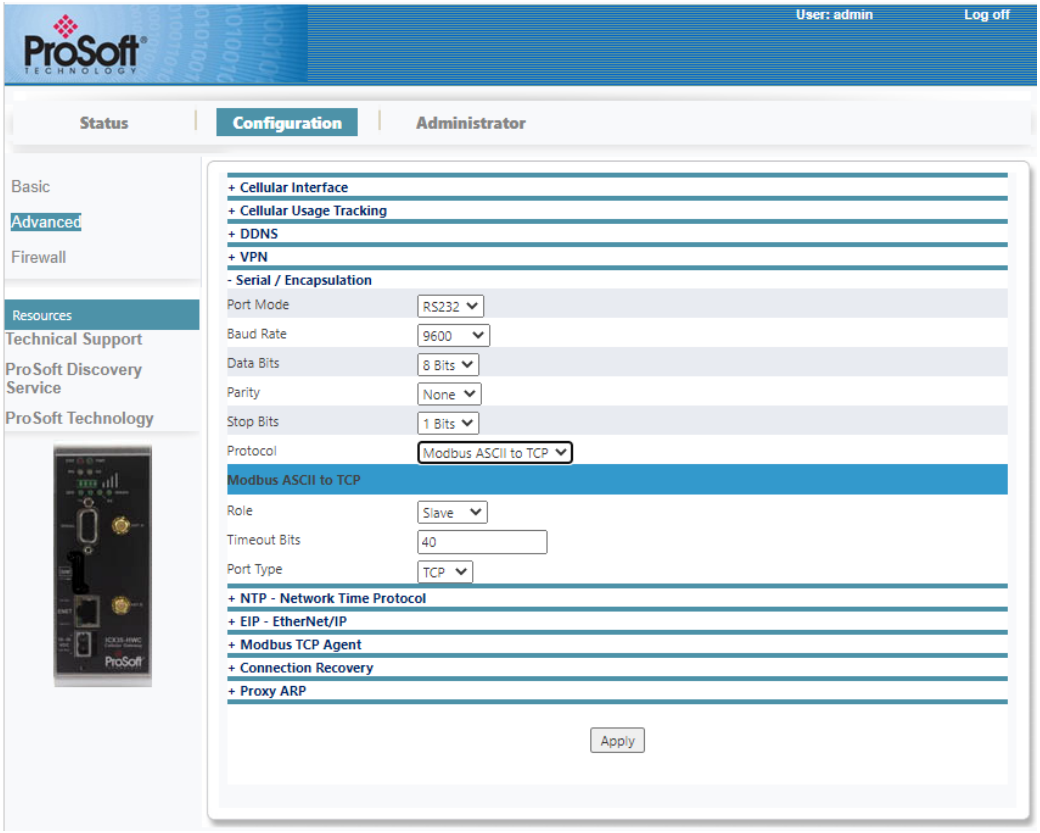
If **Slave** is selected, the *Encapsulation* table is not visible.

You can add an entry to the *Client Table* list. Click on the **ADD ENTRY TO CLIENT TABLE LIST** button.

The **REMOVE SELECTED ENTRIES** button selects and removes entries from this list.

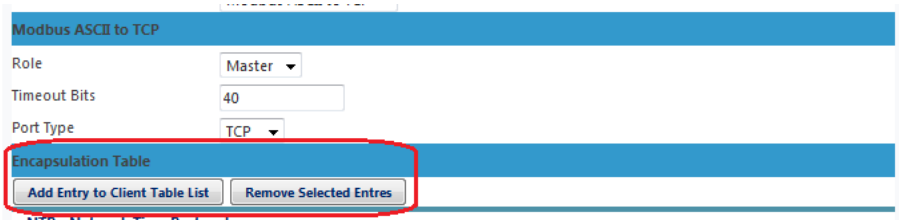
Modbus ASCII to TCP

The *Modbus ASCII to TCP* option displays the following additional parameters.



Parameter	Description
Role	Specifies the network role for the encapsulation process (Master, Slave).
Timeout Bits	This parameter sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	This parameter specifies the type of IP connection (TCP only) for the encapsulated data.

The **Master** role contains additional parameters:



- Add Entry To Client Table List
- Remove Selected Entries

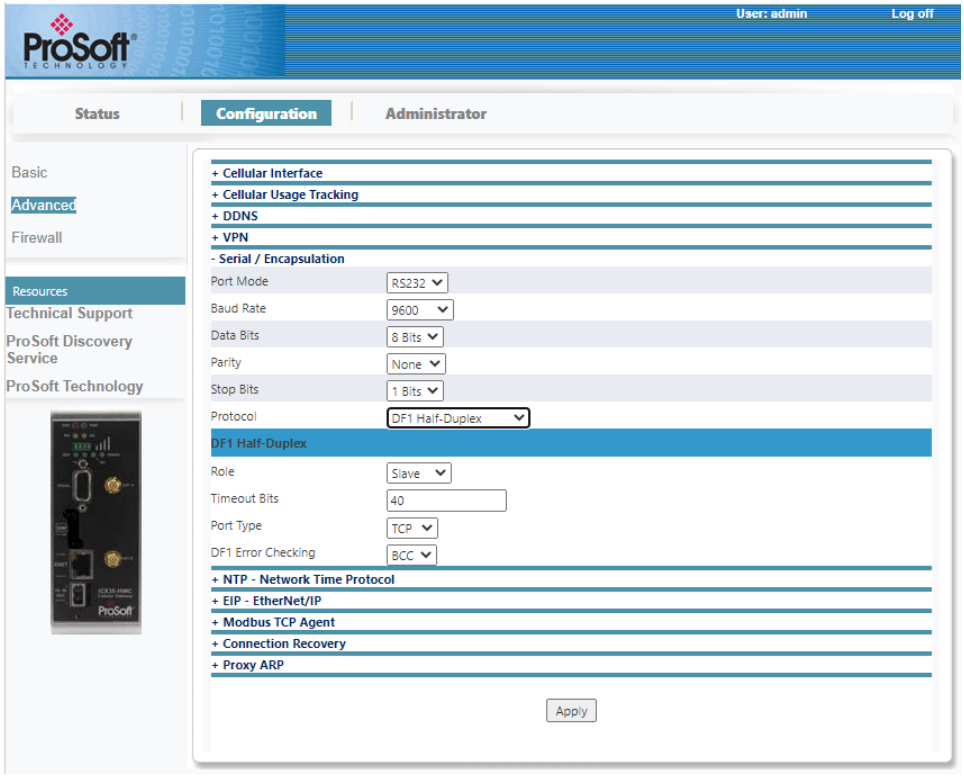
If **Slave** is selected, the *Encapsulation* table is not visible.

You can add an entry to the *Client Table* list. Click on the **ADD ENTRY TO CLIENT TABLE LIST** button.

The **REMOVE SELECTED ENTRIES** button selects and removes entries from this list.

DF1 Half-Duplex

The *DF1 Half-Duplex* option displays the following parameters.



Parameter	Description
Role	Specifies the network role for the encapsulation process (Master, Slave).
Timeout Bits	Sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Only TCP connections are supported for this protocol selection.
DF1 Error Checking	Specifies which type of error checking is used for DF1 data messages (BCC or CRC).

The Master role contains the following additional fields:

- Add Entry To Client Table List
- Remove Selected Entries

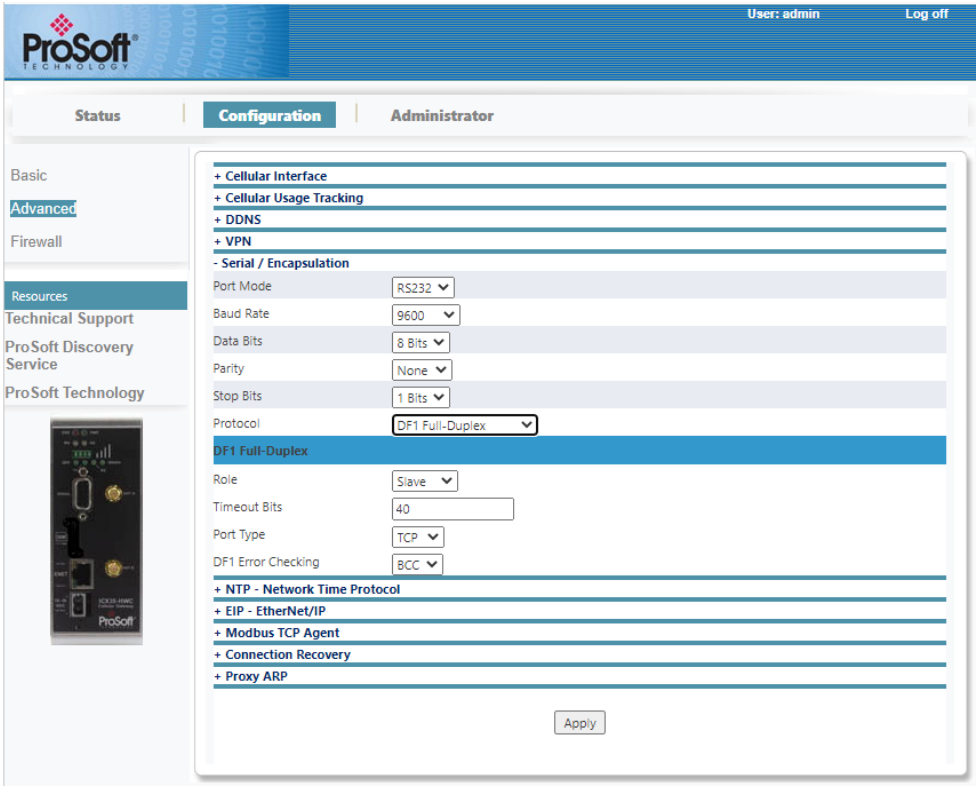
If **Slave** is selected, the *Encapsulation* table is not visible.

You can add an entry to the *Client Table* list. Click on the **ADD ENTRY TO CLIENT TABLE LIST** button.

The **REMOVE SELECTED ENTRIES** button selects and removes entries from this list.

DF1 Full-Duplex

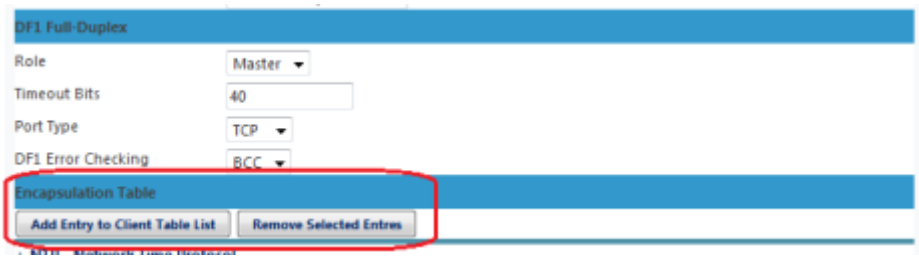
The *DF1 Full-Duplex* option displays the following additional parameters.



Parameter	Description
Role	Specifies the network role for the encapsulation process (Master, Slave).
Timeout Bits	Sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Only TCP connections are supported for this protocol selection.
DF1 Error Checking	Specifies which type of error checking is used for DF1 data messages (BCC or CRC).

The **Master** role contains the following additional fields:

- **Add Entry To Client Table List**
- **Remove Selected Entries**



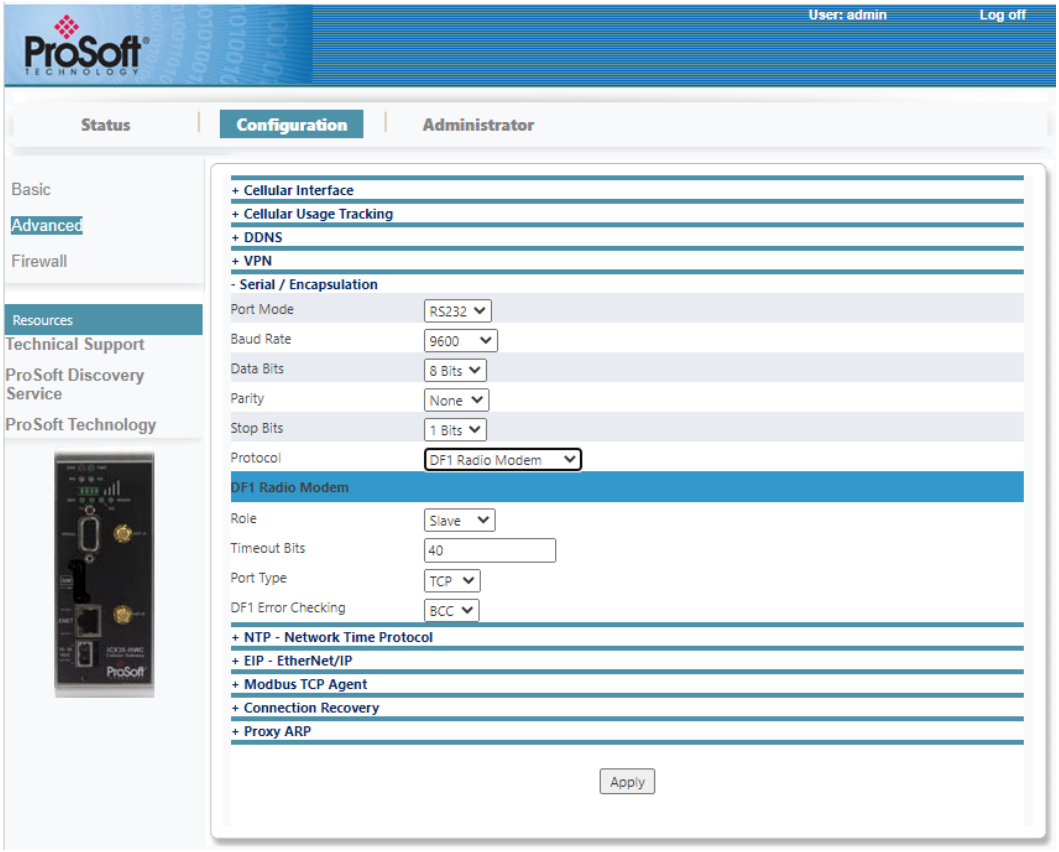
If **Slave** is selected, the *Encapsulation* table is not visible.

You can add an entry to the *Client Table* list. Click on the **ADD ENTRY TO CLIENT TABLE LIST** button.

The **REMOVE SELECTED ENTRIES** button selects and removes entries from this list.

DF1 Radio Modem

The *DF1 Radio Modem* option displays the following additional parameters:



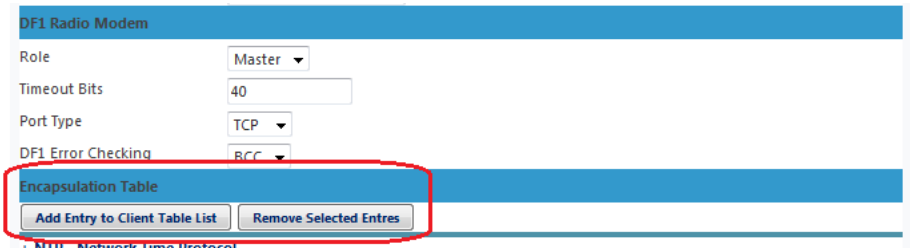
Parameter	Description
Role	Specifies the network role for the encapsulation process (Master, Slave).
Timeout Bits	Amount of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Only TCP connections are supported for this protocol selection.
DF1 Error Checking	This parameter specifies which type of error checking is used for DF1 data messages (BCC or CRC).

The **Master** role contains the following additional fields:

- **Add Entry To Client Table List**
- **Remove Selected Entries**

If **Slave** is selected, the *Encapsulation* table is not visible.

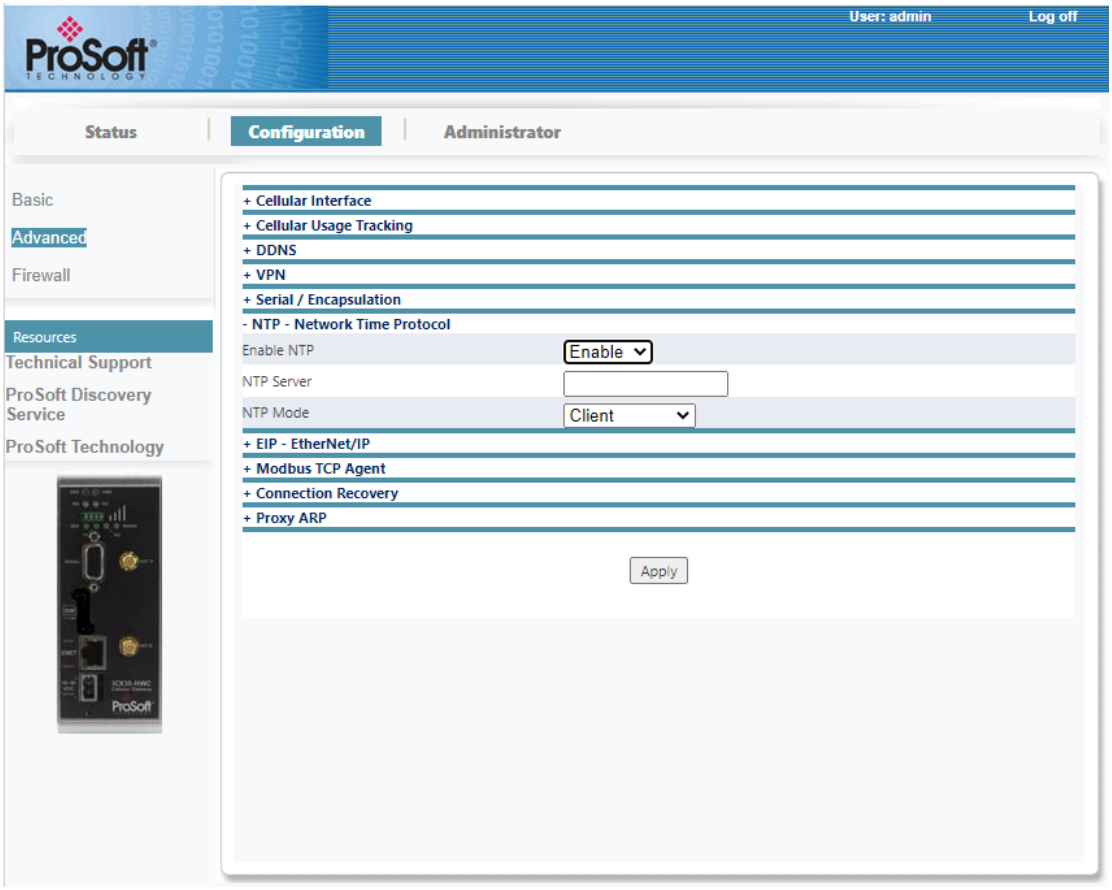
You can add an entry to the *Client Table* list. Click on the **ADD ENTRY TO CLIENT TABLE LIST** button.



The **REMOVE SELECTED ENTRIES** button selects and removes entries from this list.

NTP – Network Time Protocol

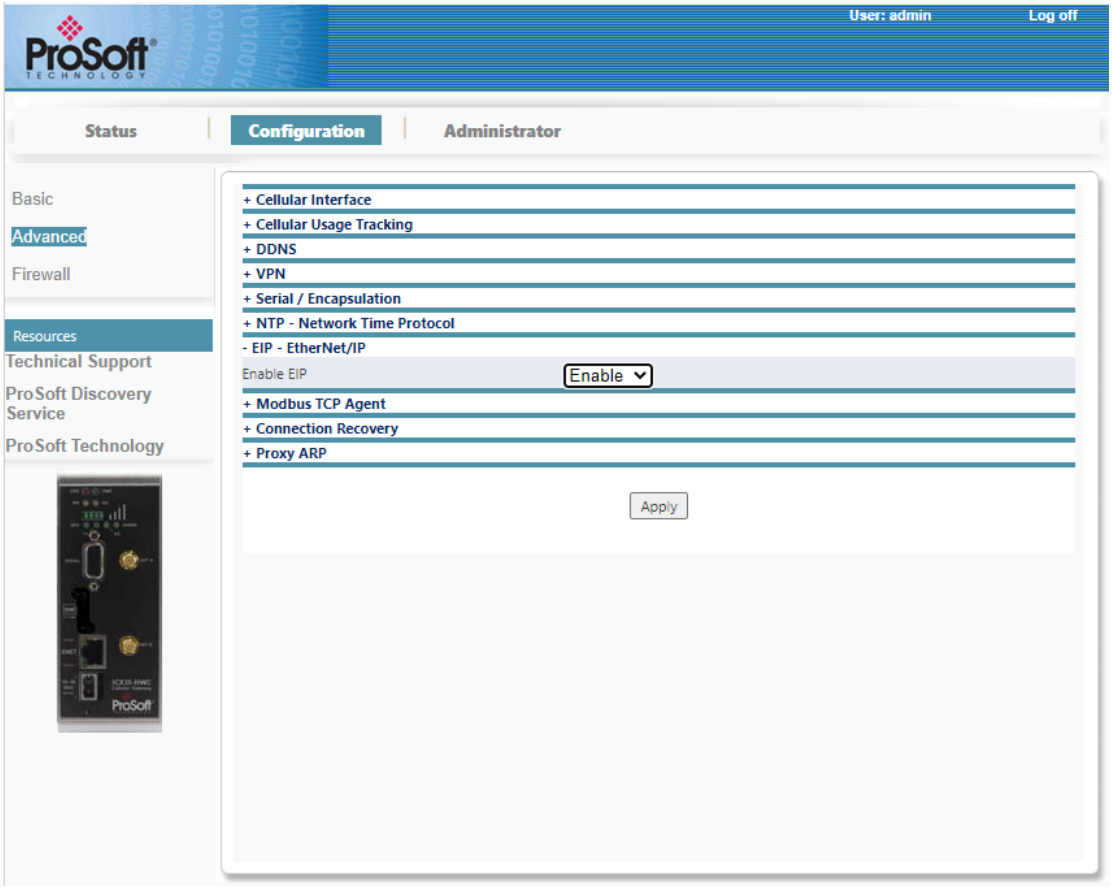
This feature enables the Network Time Protocol to synchronize the clocks of data networks and the ICX35-HWC.



Parameter	Description
Enable NTP	Enables the NTP feature.
NTP Server	Server time updates for the ICX35-HWC. **Example:** pool.ntp.org
NTP Mode	**Client** - NTP process will query NTP server and update ICX35-HWC system time. **Client/Serve**r - NTP process will query NTP server and update ICX35-HWC system time and resolve NTP requests from the LAN clients.

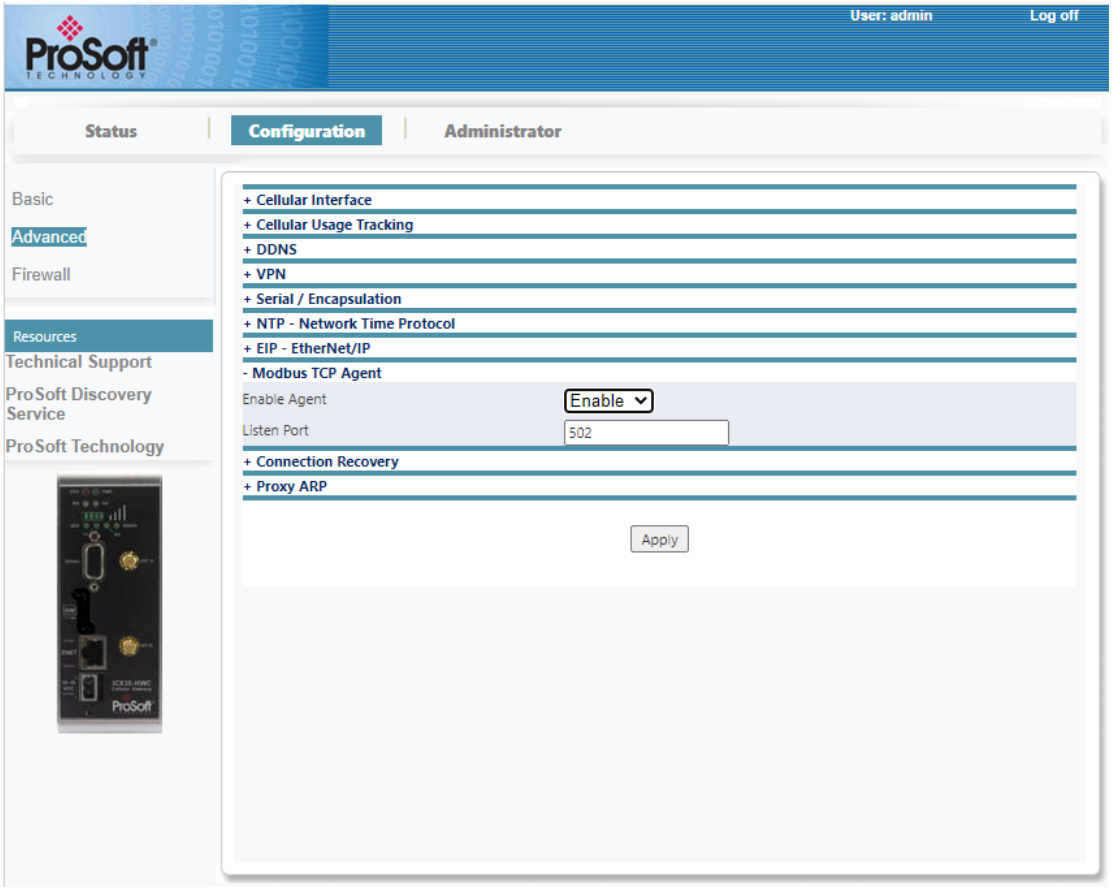
EIP – EtherNet/IP

The ICX35-HWC can run as an explicit message server and will respond to requests received on the LAN. An SMS message can be sent to user(s) upon alarm.



Modbus TCP Agent

The ICX35-HWC can run as a Modbus TCP/IP server to remote Modbus TCP/IP device(s). Enabling the *Modbus TCP Agent* is a prerequisite for Diagnostics & SMS features. See *Modbus TCP/IP Communications* for more information.



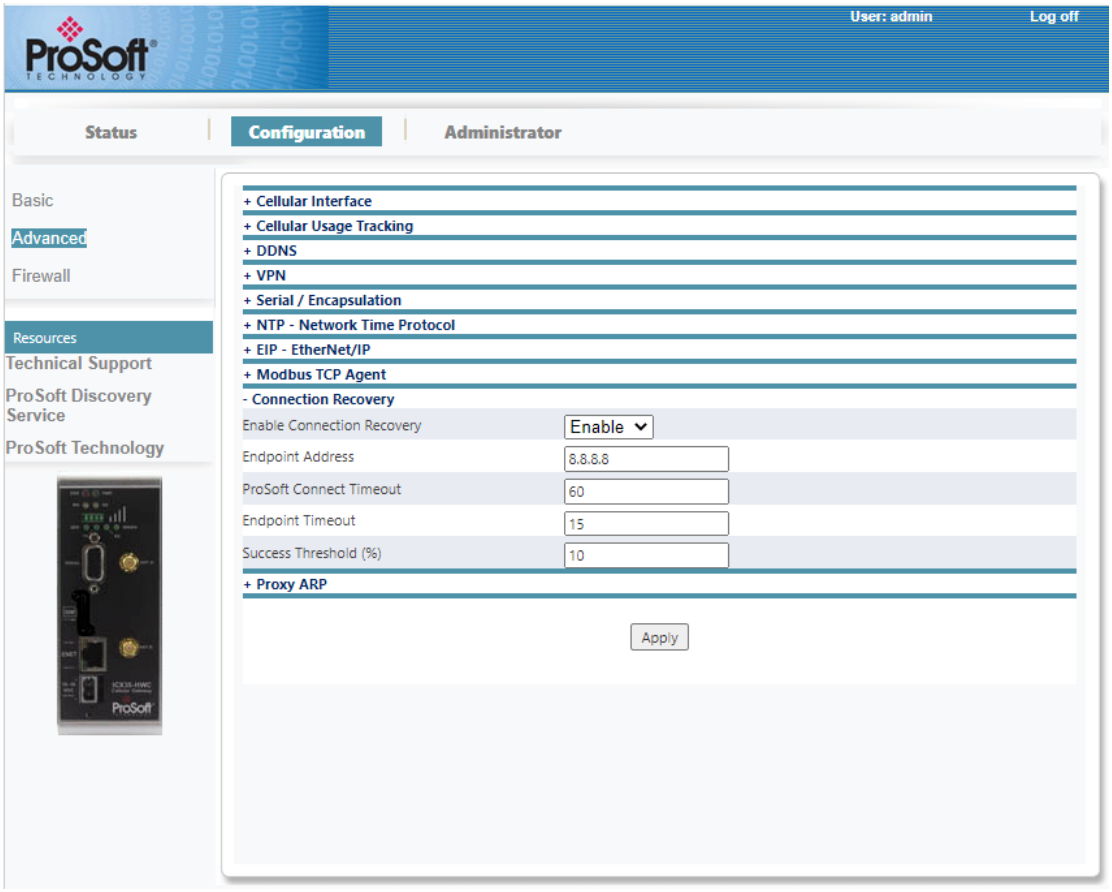
Parameter	Description
Enable Agent	Enables the *Modbus TCP Agent* feature
Listen Port	The Modbus TCP/IP service port number

Note: When using both *Serial Encapsulation* and *Modbus TCP Agent*, the default *Listen Port* configured for the *Modbus TCP Agent* needs to be changed to another value than 502.

Connection Recovery

The Connection Recovery is used to trigger a reboot of the ICX35-HWC when there is a loss of connectivity or if the ICX35-HWC stops communicating. The reboot trigger conditions are:

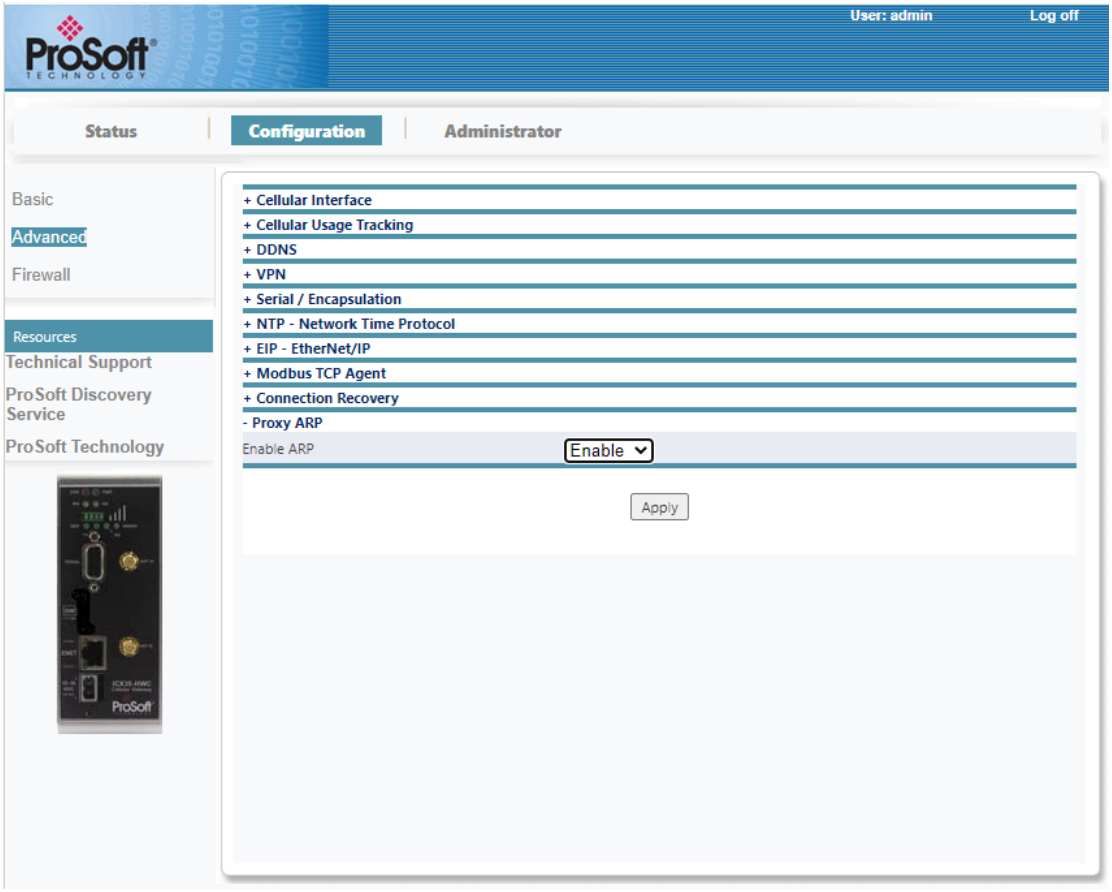
- Loss of communications to a known endpoint WAN IP
- Loss of communications to Belden Horizon



Parameter	Description
Enable Connection Recovery	Enables the Connection Recovery feature.
Endpoint Address	Configure a known WAN IP address (Default 8.8.8.8, a known Google DNS address). If the ICX35-HWC is not able to reach this WAN IP and the *Endpoint Timeout* parameter is true, then the ICX35-HWC will reboot.
Belden Horizon Timeout	The time interval (in minutes) after which the ICX35-HWC will reboot if there is no connectivity with Belden Horizon. Maximum value: 1439 (23 hours, 59 minutes).
Endpoint Timeout	The time interval (in minutes) after which the ICX35-HWC will reboot if the *Endpoint Address* is not reachable.
Success Threshold (%)	Percentage of successful attempts to reach the endpoint/ Belden Horizon, for which the ICX35-HWC does not reboot.

Proxy ARP

Proxy ARP is a technique in which a proxy server on a given network answers the Address Resolution Protocol (ARP) queries for an IP address that is not on that network. For more information, please see *Proxy ARP* on page 139.

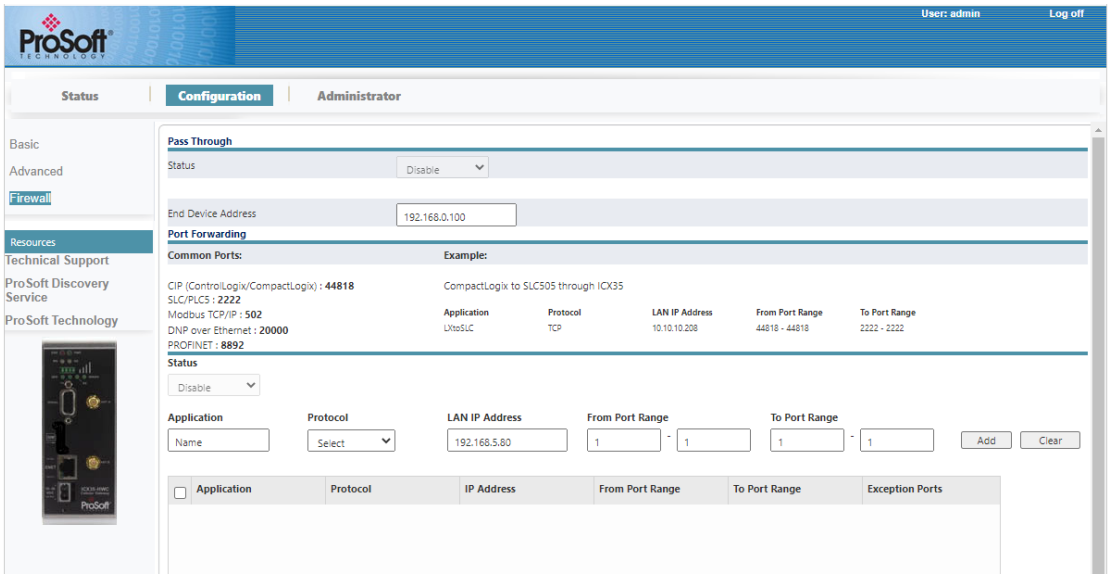


3.2.3 Firewall

The **Configuration > Firewall** tab displays the following fields for *Pass Through* and *Port Forwarding*.

Pass Through allows all traffic from a remote client device to be forwarded to the configured end device (*End Device Address* parameter) connected to the ICX35-HWC LAN.

Port Forwarding allows a remote client device to access multiples server devices connected to the ICX35-HWC port number. Up to 10 mappings can be created.

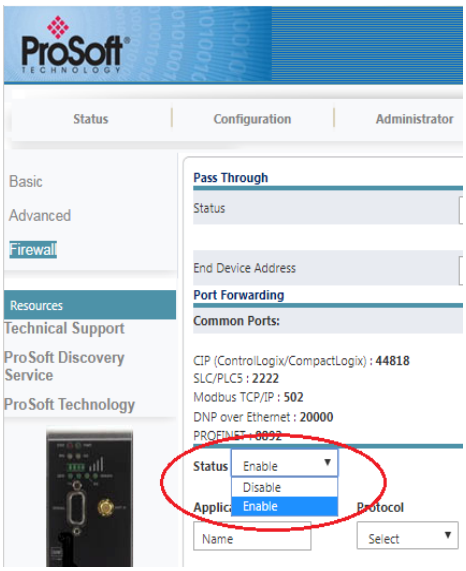


Pass Through

Parameter	Description
Status	Enable or disable pass through status
End Device Address	Used when DHCP is disabled. IP address of end device.

Port Forwarding

Enable this feature by selecting *Enable* in the dropdown menu.

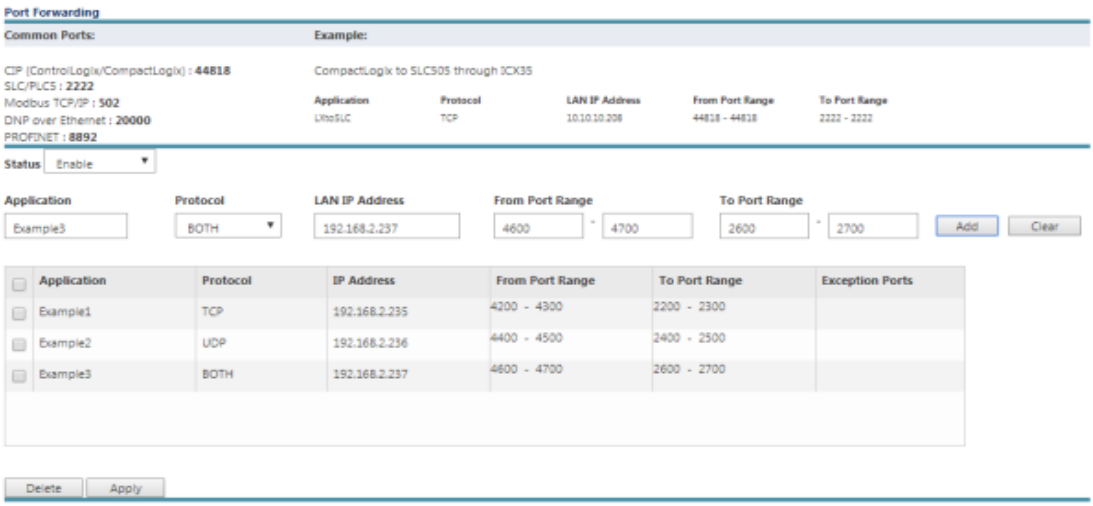


Parameter	Description
Application	Name of particular mapping
Protocol	Packet delivery method (TCP, UDP, both)
IP Address	IP address of the destination LAN device
From Port Range	WAN port range through which data will be forwarded to each device
To Port Range	LAN device port range listening for forwarded traffic
Exception Ports	Lists the ports included in the *From Port Range* interval that are already in use by services running on the ICX35-HWC, and will not be forwarded to the end device connected to the LAN port.

When the fields above are complete, click the **ADD** button to load the parameters into the table. To remove an existing mapping in the table, highlight it and click **DELETE**.

When complete, click **APPLY**.

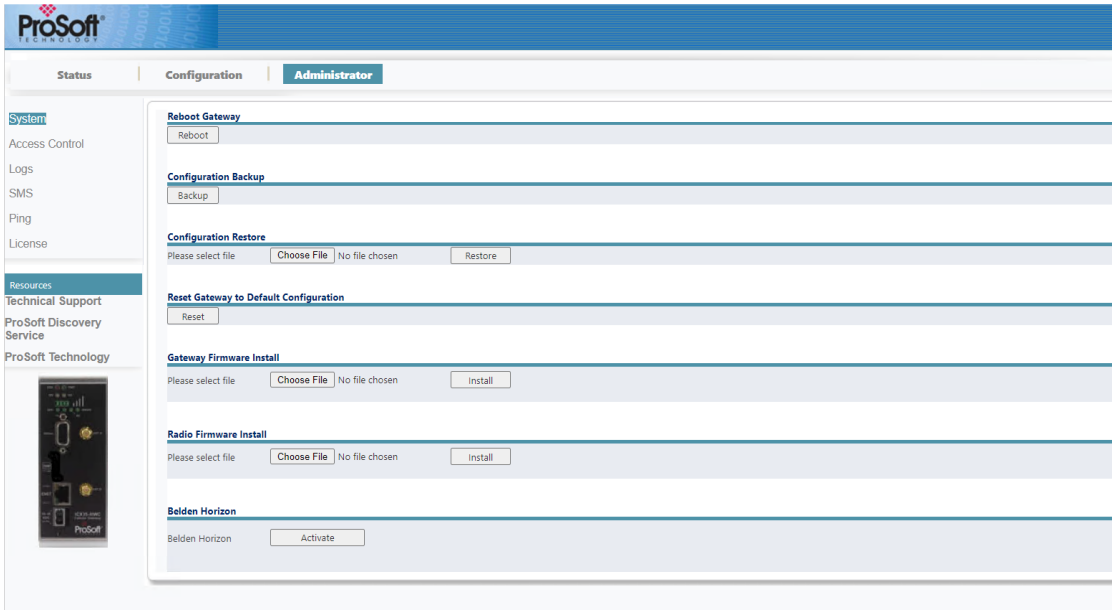
Example:



3.3 Administrator Tab

The *Administrator* tab allows you to configure the password, back up the configuration, record logs, install firmware, etc.

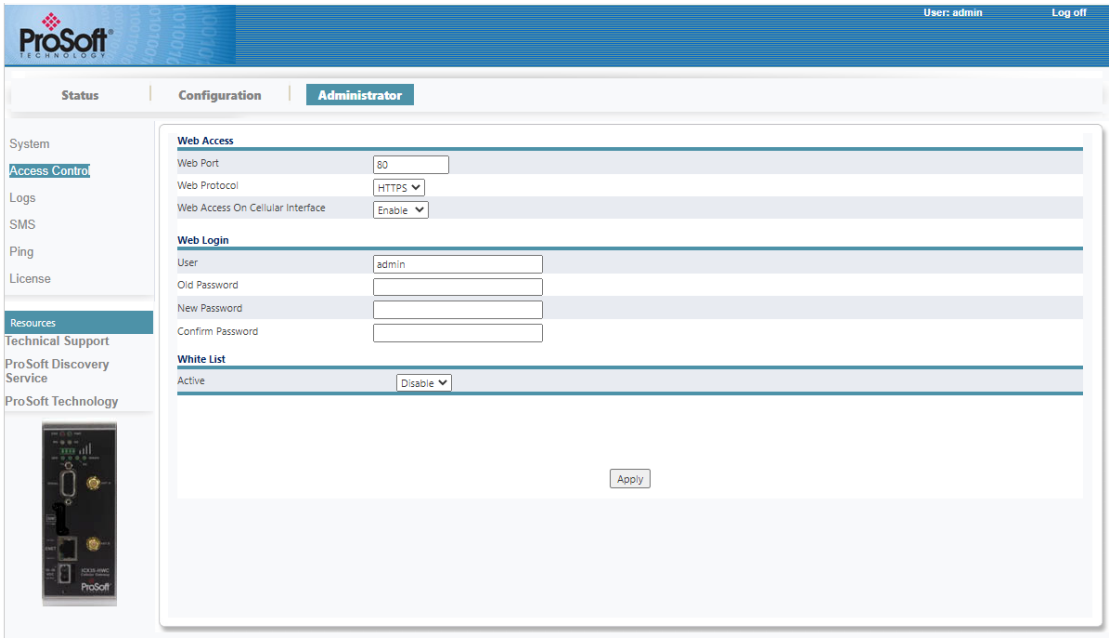
3.3.1 System



Parameter	Description
Reboot Gateway	Reboots the ICX35-HWC.
Configuration Backup *	Saves the configuration to a file.
Configuration Restore *	Loads the configuration to the module. The **Choose File** button allows you to locate and select the configuration file to be restored. The **Restore** button restores the file.
Reset Gateway to Default Configuration	Restores the ICX35-HWC to factory defaults – the previous configuration is lost. A countdown timer is used during the reset. When the countdown is complete, the webpage will be redirected to the factory default webpage address **192.18.0.250**.
Gateway Firmware Install	Performs a firmware install (*.img file).
Radio Firmware Install	Performs an internal radio software install (*.spk file).
Belden Horizon Server	Secure webpage interface to activate, setup VPN clients, invite team members, and manage multiple ProSoft Technolgoy cellular radios on the network.
Belden Horizon	**Activate** or **Deactivate** Belden Horizon.

(*) The *Username* and *Password* are not backed up. When importing a configuration, the current password remains unchanged.

3.3.2 Access Control



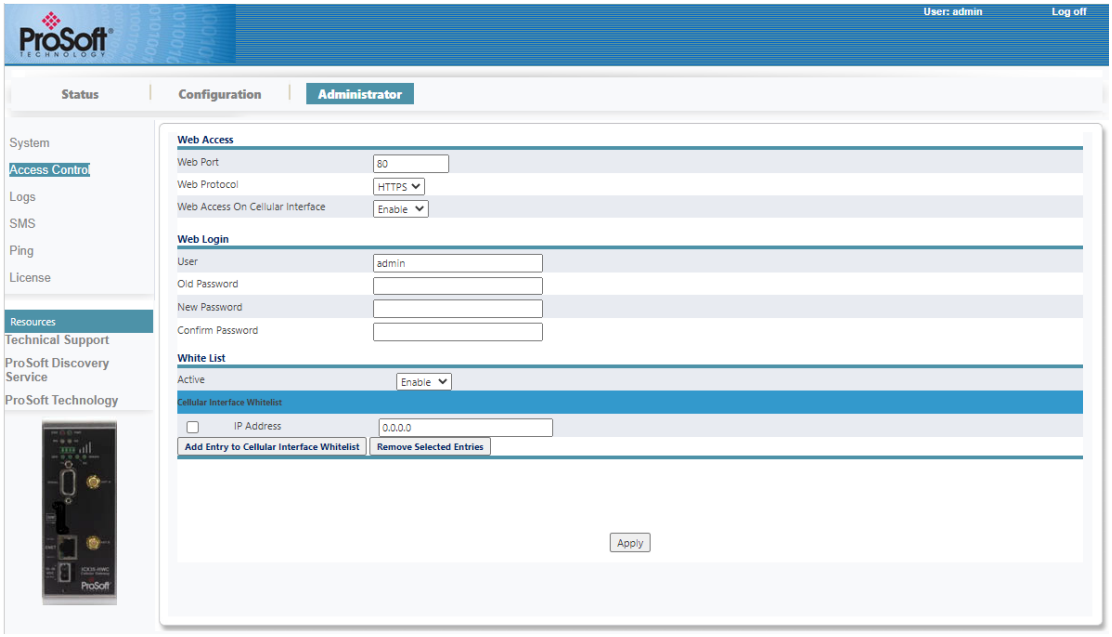
Parameter	Description
Web Access	
Web Port	Web access port number
Web Protocol	HTTP or HTTPS
Web Access on WAN	Allows or blocks webpage access from the WAN.

Warning: Belden Horizon currently uses port 443 to tunnel. Selecting port 443 will prevent Belden Horizon from functioning properly. HTTPS can function properly using port 8080 or other ports.

User	
User Name	New login user name
Old Password	Old login password
New Password	New login password
Confirm Password	Confirm new password
White List	
Active	Select **Enable** or **Disable**. If you select **Enable**, the unit displays the **Add Entry to WAN Whitelist** button.

Adding Entries to the Whitelist

Click on the **ADD ENTRY TO CELLULAR INTERFACE WHITELIST** button. This displays a line entry in which you can enter an IP address.



Whitelist entries can either be single IP addresses (e.g., 50.40.20.15) or IP addresses followed by a CIDR netmask (e.g., 50.40.20.0/8) allowing subnets to be whitelisted via a single whitelist entry. Whitelists only apply to the cellular (WAN) interface. No whitelist filtering is possible on the LAN interface.

Since all VPN traffic is presumably between trusted hosts, whitelist entries are ignored (but not deleted) when an OpenVPN or IPsec tunnel is configured.

To remove whitelist entries, click the checkbox of the entry and click on the **REMOVE SELECTED ENTRIES** button. Click **APPLY** when done.

HTTPS Warning Message

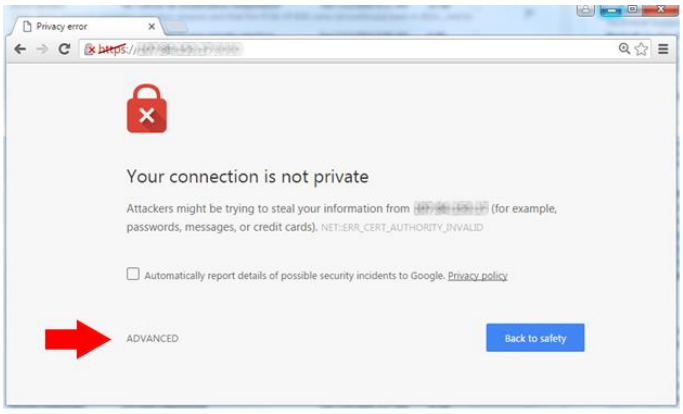
When HTTPS is enabled, you must enter the WAN or LAN IP address into your web browser in the following format: https://xxx.xxx.xxx.xxx:8080

Depending on your browser, you may encounter a warning message. It warns that the page was not securely loaded due to the unknown verification of a ProSoft site certificate.

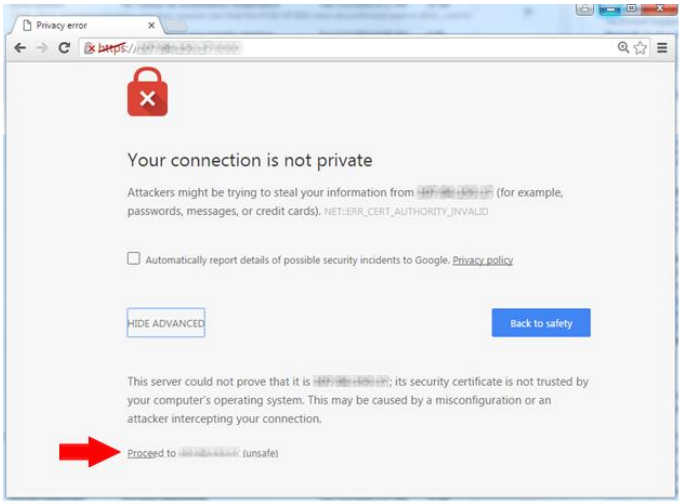
You may need to add an exception in your browser to proceed to the ICX35-HWC webpage.

Google Chrome

1 Click on the **ADVANCED** link.

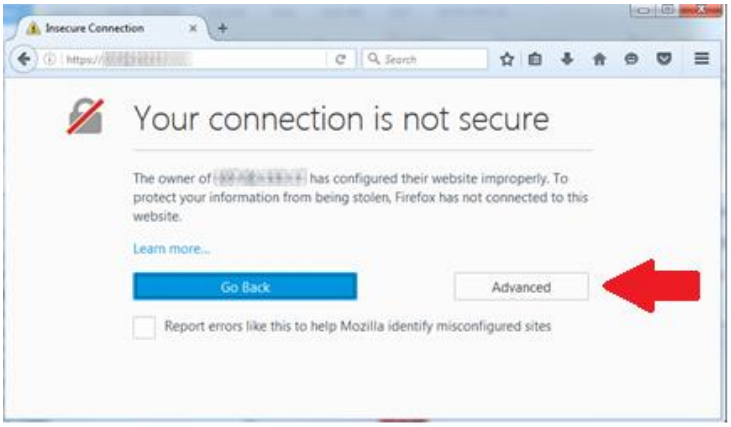


2 Click on the **PROCEED TO XXX.XXX.XXX.XXX** link.

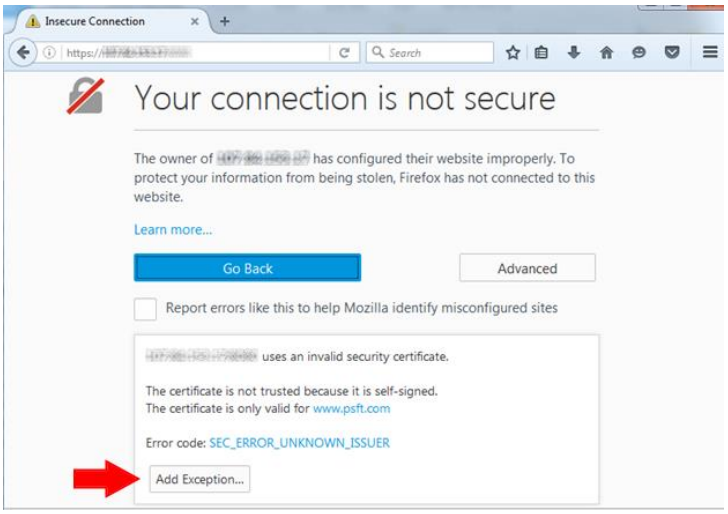


Firefox

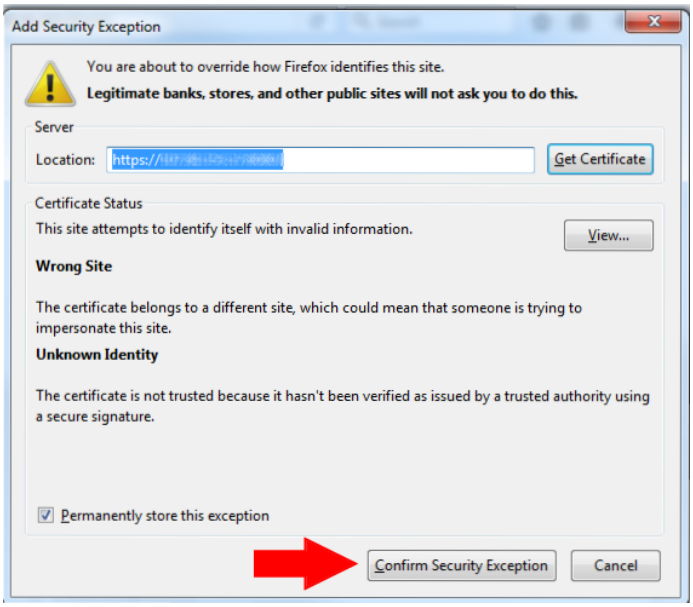
1 Click on the **ADVANCED** link.



2 Click on the **ADD EXCEPTION…** link.

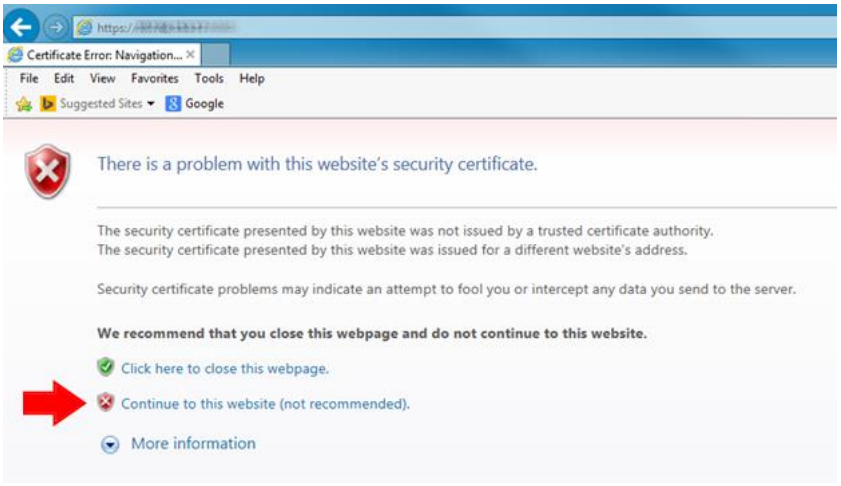


3 In the *Add Security Exception* window, click on the **CONFIRM SECURITY EXCEPTION** button.



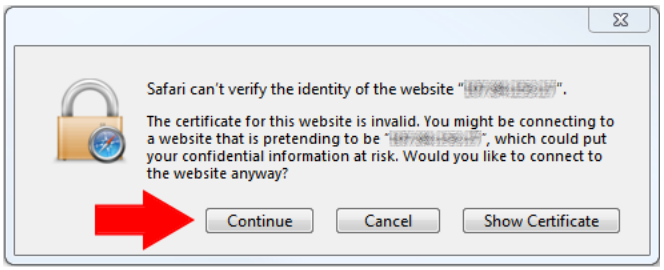
Internet Explorer

1 Click on the **CONTINUE TO THIS WEBSITE** link.

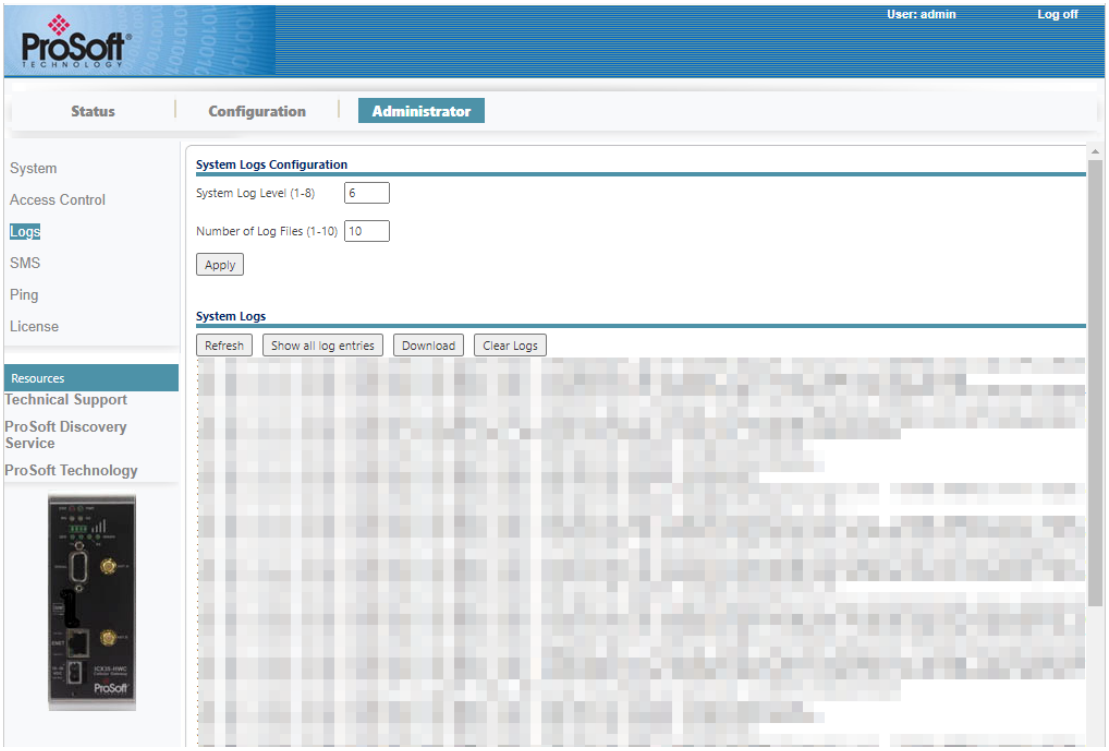


Safari

1 Click on the **CONTINUE** button.



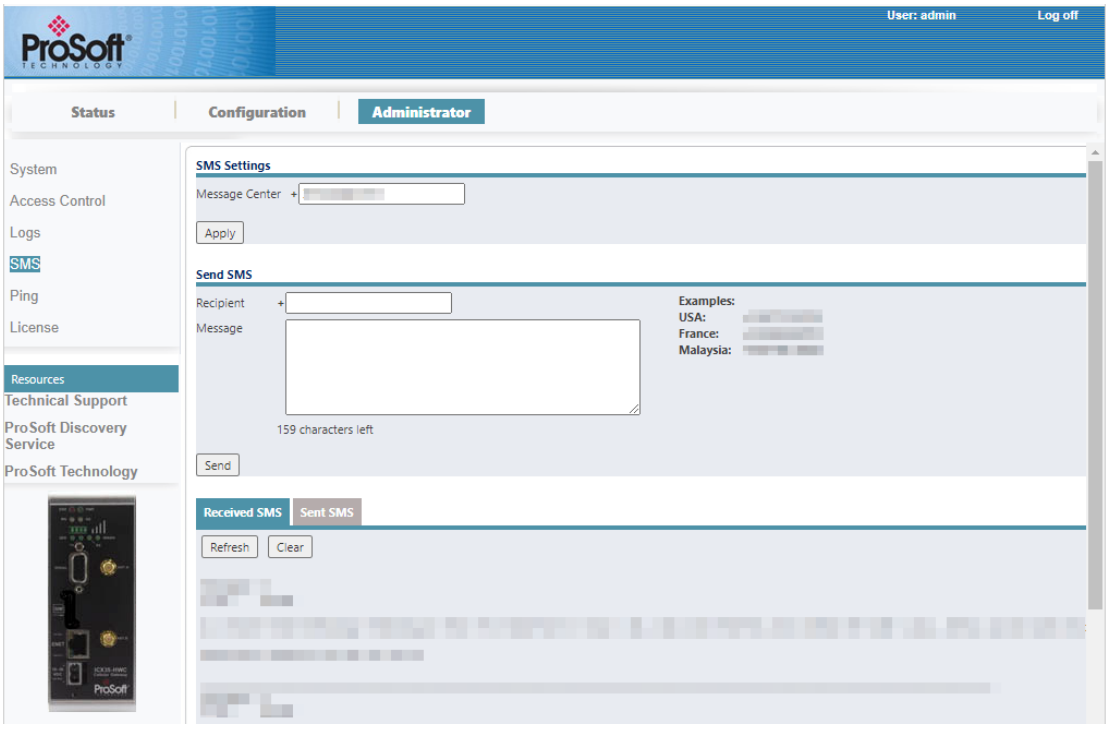
3.3.3 Logs



Parameter	Description
System Log Level (1 to 8)	Specifies how much information is saved to the log file. Lower numbers limit the log entries to more critical information, while higher numbers include information useful for troubleshooting. Higher numbers include all entries associated with lower-level numbers. This value can typically be left alone until instructed by a Technical Support representative.
Number of Log Files(1 to 10)	Specifies the number of log files to be recorded internally.
Refresh	Performs a refresh of the log results
Show all Log Entries	Refreshes and displays all log entries
Download	Allows you to download and save the log to a file
Clear Logs	Clears the recorded logs

3.3.4 SMS

The SMS text message contents of the ICX35-HWC buffer can be viewed using this feature. You can also send an SMS text message to a valid SMS recipient.



SMS Settings

Parameter	Description
Message Center	This is used to configure the Message Center Number used to send SMS. The phone number is in international format (including prefixes and country code). It can be entered in the following formats: ▪ With or without preceding '+' sign ▪ With or without spaces ▪ With or without dashes '-' ▪ With or without periods '.' **Warning:** The new SMS Message Center Number will be written to the SIM card. Please note the current number before continuing.

Send SMS

Parameter	Description
Recipient	Recipient's phone number in international format (including prefixes and country code). It can be entered in the following formats: ▪ With or without preceding '+' sign ▪ With or without spaces ▪ With or without dashes '-' ▪ With or without periods '.' **Warning:** The new SMS Message Center Number will be written to the SIM card. Please note the current number before continuing.
Message	SMS text message to be sent, up to 160 characters. It supports the GSM Basic Character Set.

Note: Messages stored in the ICX35-HWC are retrieved using the FIFO rule: The first message received is the first to be retrieved, and so on.

Received SMS

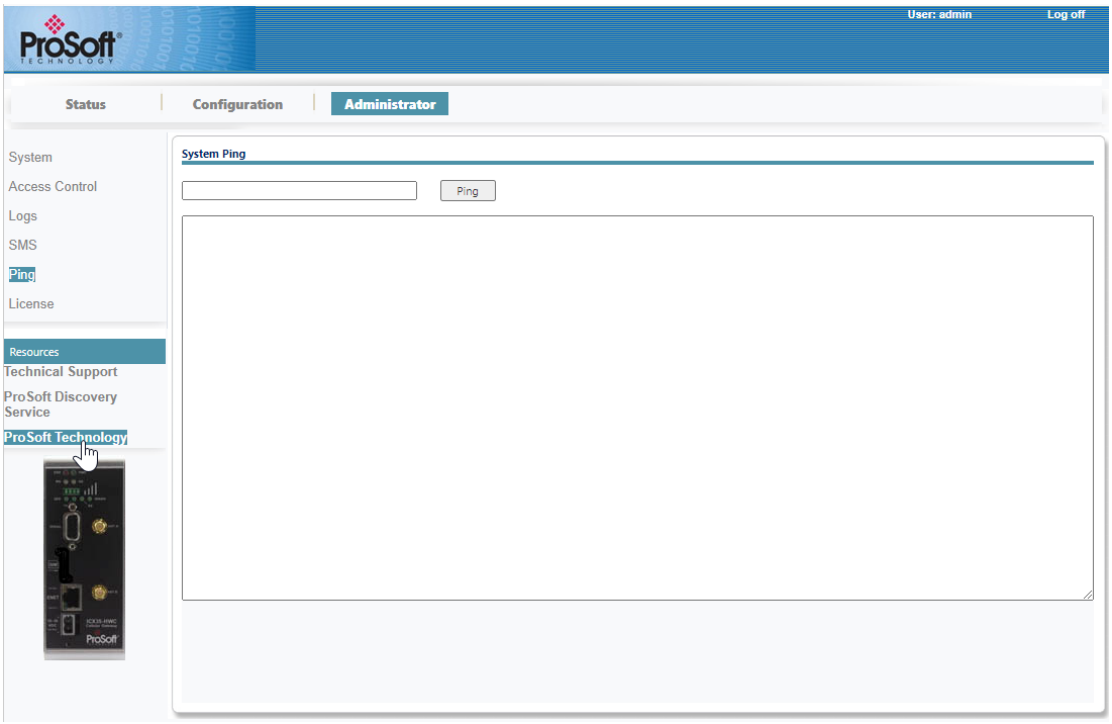
You can **Refresh** or **Clear** the messages that have been received by the ICX35-HWC.

Sent SMS

You can **Refresh** or **Clear** the messages that have been sent by the ICX35-HWC.

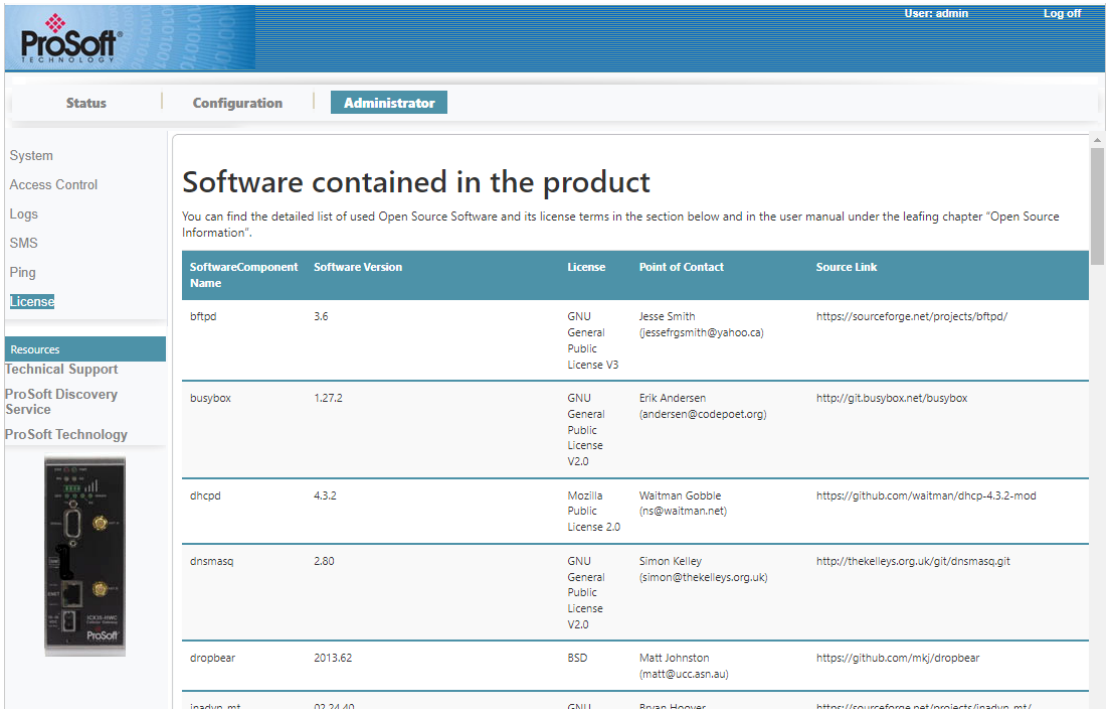
3.3.5 Ping

You can ping a remote device to determine whether you can connect to it. Enter the WAN IP address or hostname to be pinged and click the **PING** button.



3.3.6 License

This section contains a list of the software contained in the ICX35-HWC. It includes the Open Source Software and its license terms.



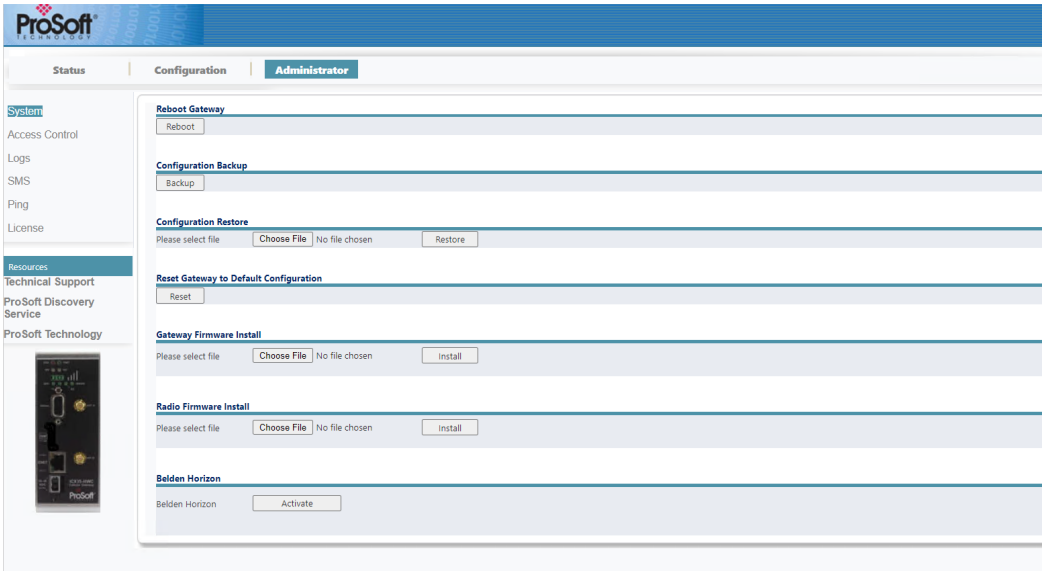
4 Belden Horizon

Belden Horizon is a secure webpage interface to activate, setup VPN clients, invite team members, and manage multiple ProSoft Technology cellular radios on the network.

4.1 Activation

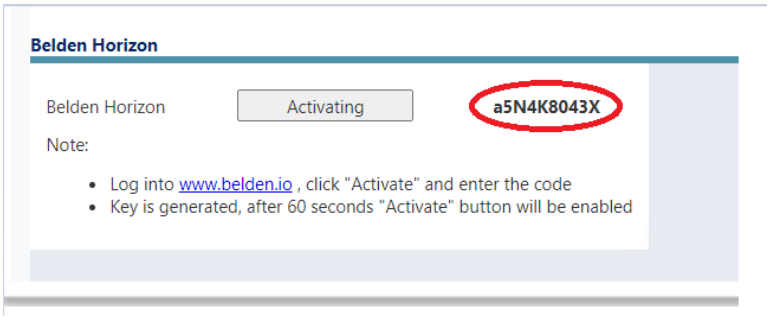
Belden Horizon requires you to activate the ICX35-HWC upon initial use.

1. On the Configuration webpage, click on **Administrator > System**.
2. Under the *Belden Horizon* section, click on the **ACTIVATE** button.



Note: During the activation process, the **ACTIVATE** button will be greyed out for 60 seconds.

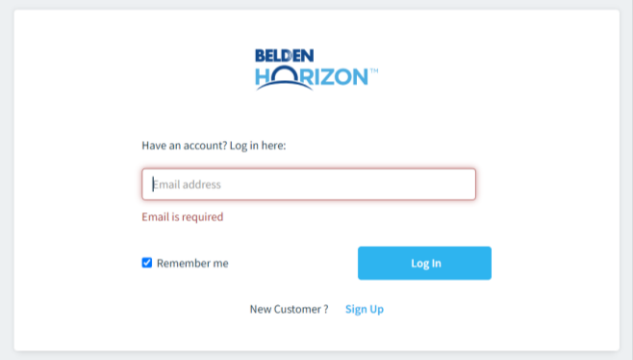
3. An alphanumeric Activation Key is generated. Record this key for later use.



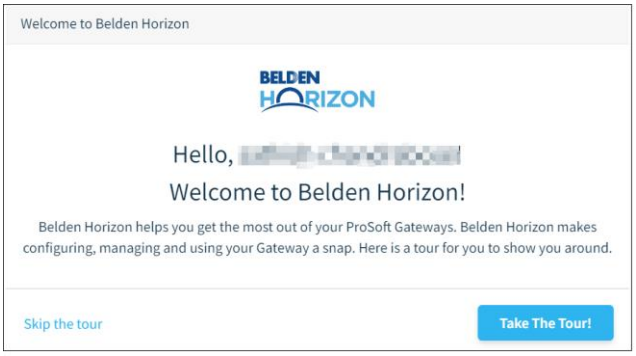
Note: If the browser is disconnected from the Internet or the cellular interface is disabled, the Activation Key will not be displayed. Upon clearing the browser cache/history, a warning message to check connectivity will appear.

4. Click on the www.belden.io link. Or open a new tab in your web browser, enter "**www.belden.io**", then press **ENTER**.

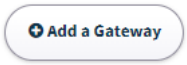
5 Enter or create an account in the Belden Horizon log-in screen.



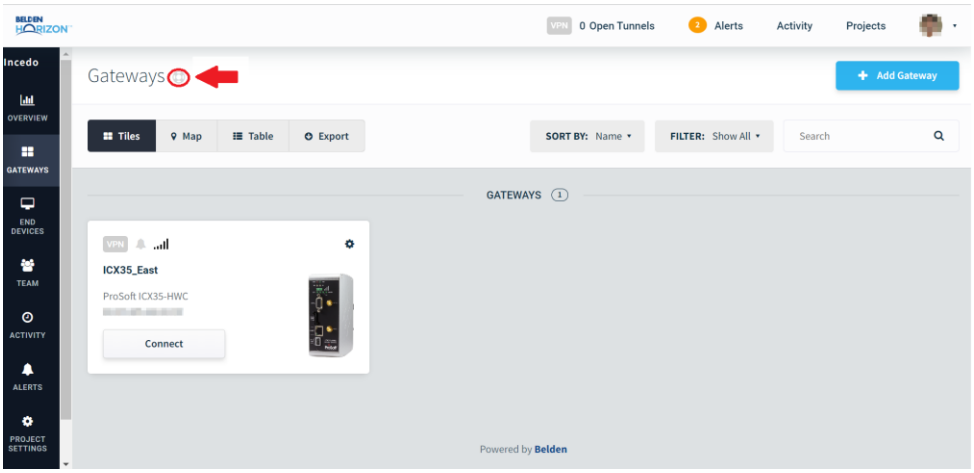
6 Once logged in, you can take a tour of the features of the Belden Horizon utility.



7 When ready, activate the ICX35-HWC within the tour, or you can click on the **ADD A GATEWAY** button at the top of the screen. It will prompt you for the Activation Key.



8 Once the ICX35-HWC is activated, you can navigate to each tab on the left-hand side of the page. Each tab contains a 'lifesaver' icon for a tutorial of the feature.



5 Hardware Installation

The ICX35-HWC should be mounted in a position that allows easy access for the cables so they are not bent, constricted, in close proximity to high amperage, or exposed to extreme temperatures. The LEDs on the front panel should be visible for ease of operational verification. Ensure that there is adequate airflow around the device but kept free from direct exposure to the elements, such as sun, rain, dust, etc.

Caution: The ICX35-HWC has a hardened enclosure and is designed for use in industrial and extreme environments. Unless you are using cables expressly designed for such environments, they can fail if exposed to the same conditions the ICX35-HWC can withstand.

5.1 Antenna Installation

Antennas selected should not exceed a maximum gain of 5 dBi under standard installation configuration. In more complex installations (such as those requiring long lengths of cable, and/or multiple connections), it is imperative that the installer follow maximum dBi gain guidelines in accordance with the radio communications regulations of the Federal Communications Commission (FCC), Industry Canada, or your country's regulatory body (if used outside the US).

The ICX35-HWC will work with most quad-band GSM/CDMA cellular antennas with an RP-SMA connector. Connect the primary antenna or primary RF cable directly to the 'ANT A' antenna connector on the front of the ICX35-HWC.

A secondary antenna port labeled 'ANT B' is provided to attach an additional antenna. Use of a secondary antenna is not required, but will often increase cellular reliability and throughput performance.

This device is not intended for use within close proximity of the human body. Antenna installation should have at least 20 cm separation from the operator.

Tip: When using a cable to an antenna placed away from the modem, minimize the length of your cable. All gain from a more advantageous antenna placement can be lost with a long cable to the modem.

5.2 Connecting the Radio to a Network Device

The application ports are located on the front of the radio.

- The Ethernet port uses a standard RJ45 connector
- The serial port uses a standard DB9 connector for serial connectivity

5.2.1 Ethernet Cable Specifications

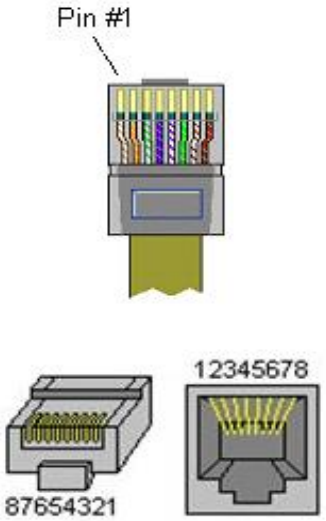
The recommended Ethernet cable is category 5 or better. A category 5 cable has four twisted pairs of wire that are color-coded and cannot be swapped. The module only uses two of the four pairs when running at 10 MBit or 100 MBit speeds.

The Ethernet port on the module is Auto-Sensing. Use either a standard Ethernet straight-through cable or a crossover cable when connecting the module to an Ethernet hub, a 10/100/1000 Base-T Ethernet switch, or directly to a PC. The module will detect the cable type and use the appropriate pins to send and receive Ethernet signals.

Ethernet cabling is like U.S. telephone cables but have eight conductors. Some hubs have one input that can accept either a straight-through or crossover cable, depending on switch position. In this case, ensure that the switch position and cable type agree.

Ethernet Cable Configuration

Note: The standard connector view shown is color-coded for a straight-through cable.

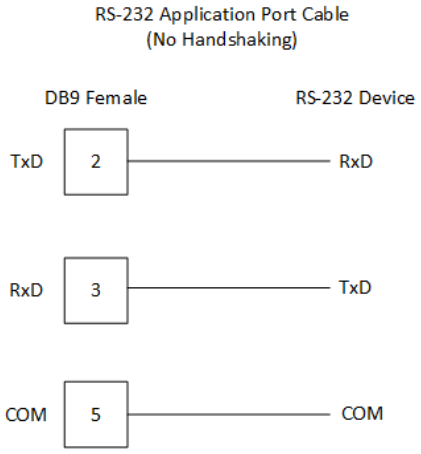


Crossover Cable		Straight-through Cable	
RJ45 Pin (Connector 1)	**RJ45 Pin (Connector 2)**	**RJ45 Pin (Connector 1)**	**RJ45 Pin (Connector 2)**
1 Rx +	3 Tx +	1 Rx +	1 Tx +
2 Rx -	6 Tx -	2 Rx -	2 Tx -
3 Tx +	1 Rx +	3 Tx +	3 Rx +
6 Tx -	2 Rx -	6 Tx -	6 Rx -

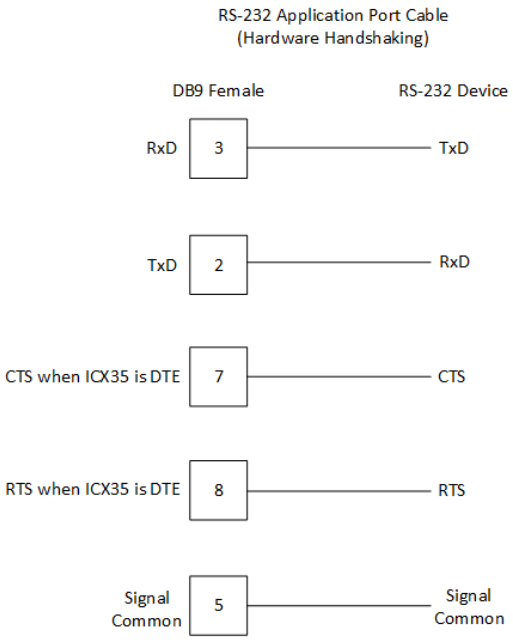
5.2.2 Serial Port Basics

RS-232

The use of hardware handshaking (control and monitoring of signal lines) depends on the requirements of the networked device. If no hardware handshaking will be used, the cable to connect to the port is as shown below:



If hardware handshaking is required, the cable to connect to the port is as shown below:



5.3 LED Indicators

LED	State	Description
PWR	Off	Power is not connected to the power terminals or source is insufficient to properly power the device.
	Solid Green	Power is connected to the power terminals
ERR	Off	Normal operation
	Solid Red	A critical error has occurred. Program executable has failed or has been user-terminated and is no longer running. Press the Reset button or cycle power to clear the error.
MS* (Module Status)	Off	ICX35-HWC is powered off
	Solid Green	Initialization complete / OK
	Blinking Green	ICX35-HWC is in the process of configuring
	Solid Red	Unrecoverable error
	Blinking Red	Reading configuration / minor error / No SIM
NS* (Network Status)	Off	ICX35-HWC is powered off
	Solid Green	ICX35-HWC has a connection to cellular tower
	Blinking Green	ICX35-HWC is attempting to connect to cellular tower
	Solid Red	Duplicate IP (EtherNet/IP) / Non-recoverable network fault
	Blinking Red	Established connection timeout (EtherNet/IP) / Minor network fault

(*) The MS and NS LED's are only enabled if the Ethernet/IP parameter is enabled in the Configuration tab of the webpage.

Serial Port LEDs

LED	State	Description
SER	Flashing	Indicates that data is moving from the serial port to the WAN port
TX	Off	No activity on the port
	Flashing Amber	Port is actively transmitting data
RX	Off	No activity on the port
	Flashing Green	Port is actively receiving data

Ethernet Port LEDs

LED	State	Description
100 Mbit	Off	No activity on the port
	Flashing Amber	The Ethernet port is actively transmitting or receiving data.
LNK/ACT	Off	No physical connection is detected. No Ethernet communication is possible. Check wiring and cables.
	Solid Green	Physical network connection detected. This LED must be ON (solid) for Ethernet communication to be possible.

WWAN LED

LED	State	Description
Off	Off	ICX35-HWC is powered off.
Solid Green	On	ICX35-HWC is powered and connected, but is not transmitting or receiving.
Slow Blink	Flashes at a steady, slow rate: 0.2 Hz (5 sec)	ICX35-HWC is powered and searching for a connection.
Faster Blink	Flashes at a steady, fast rate: About 3 Hz (333 ms)	ICX35-HWC is transmitting or receiving data.

Note: The WWAN LED indicates a physical connection state between the ICX35-HWC and the cell tower. It is not an indicator of a logical connection state. There may be a situation when you may see a "Disconnect, will retry" indicator on the ICX35-HWC webpage, even when the WWAN LED light is on (solid green). This indicates that the module was able to make a physical connection to the tower, but the logical connection was not made between the ICX35-HWC and the cellular provider.

6 EtherNet/IP and SMS Text Messaging

The ICX35-HWC provides connectivity via the EtherNet/IP communications protocol as a Class 3 client. With this connectivity, PLC and SCADA software can monitor the diagnostics of the ICX35-HWC.

The ICX35-HWC Add-On Instruction (AOI) file for RSLogix 5000 supports the following features:

- ICX35-HWC diagnostic data retrieval
- ICX35-HWC diagnostic counter reset
- Receiving SMS text message from the ICX35-HWC
- Sending SMS text message to the ICX35-HWC

Example application: The ICX35-HWC can be installed in a remote location with its LAN directly connected to a PLC. The PLC code can monitor the values and if/when a value is out of range, and SMS message is sent to a user via the ICX35-HWC. The user can then send a SMS back to the PLC to clear the notification.

Note: This chapter uses examples in a ControlLogix environment. It also applies to a CompactLogix environment, with notes indicating the differences.

6.1 Creating a New RSLogix 5000 Project

1 Open the *File* menu and select New.

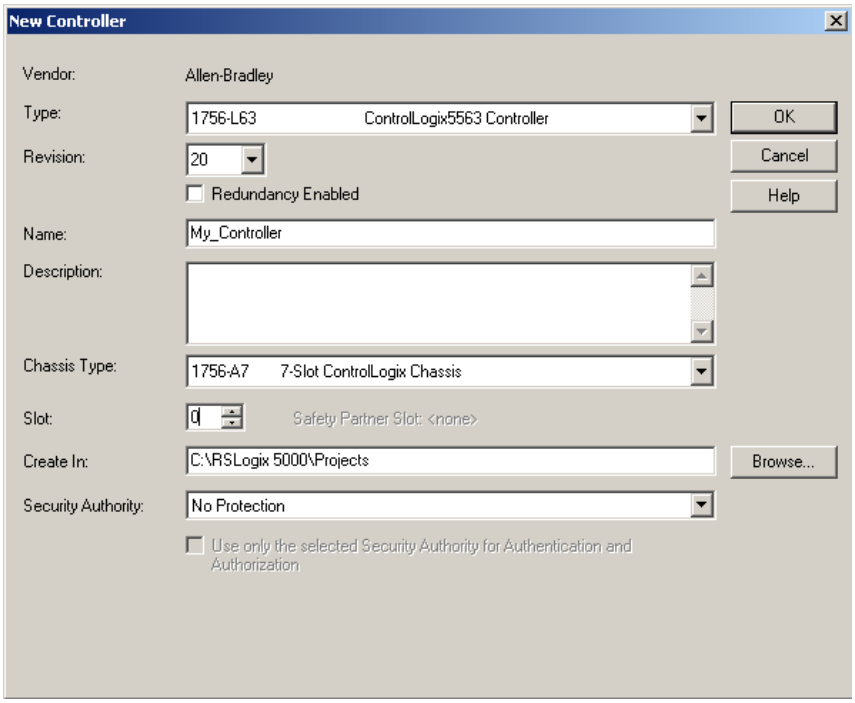
2 Select your controller *Type*.

3 Select the *Revision* of your controller. (Revision 16 or newer only)

4 Enter a *Name* for your controller, such as "**My_Controller**".

5 Select your *Chassis Type*.

6 Select *Slot x* indicating the slot location of your controller.



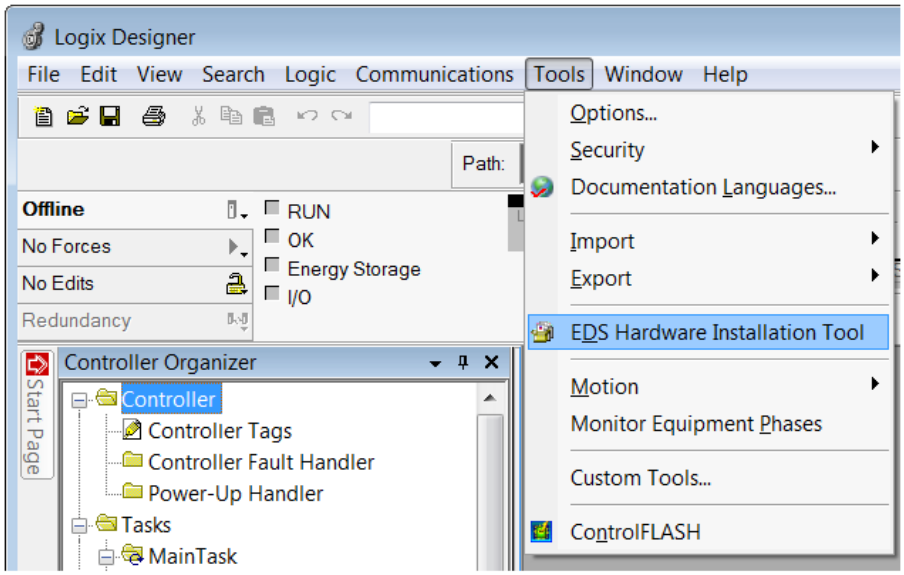
7 Click **OK**.

6.1.1 EDS Installation

The ICX35-HWC can be integrated with Allen-Bradley Logix family of controllers. Integration with the Logix family in Studio 5000 makes use of the EDS Add-On-Profile (AOP).

Using RSLinx, the EDS file can be uploaded from the ICX35-HWC. When complete, the *EDS Hardware Installation Tool* is invoked to complete the registration.

Alternatively, the EDS file can be downloaded from the product web page at www.prosoft-technology.com and registered manually using the *EDS Hardware Installation Tool* shortcut in the Studio 5000 *Tools* menu.

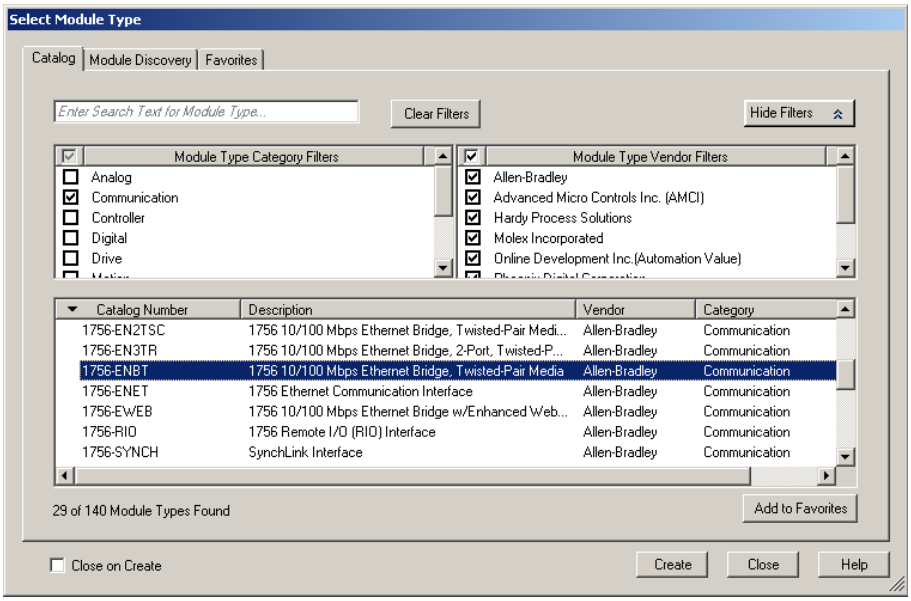


6.1.2 Adding Ethernet Connectivity to the Project

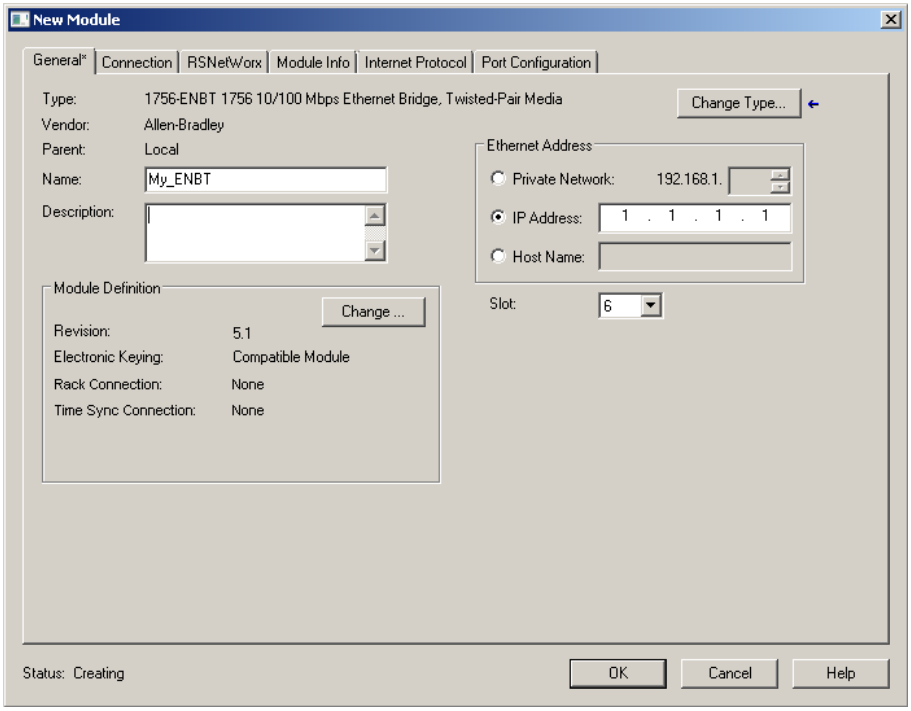
Note: This section can be skipped if you have a CompactLogix processor with a built-in Ethernet port.

1 You will need to add a 1756-ENBT Ethernet Bridge module to the project. In the *Controller Organizer* window, select the Controller that was imported and click the right mouse button to open a shortcut menu. On the shortcut menu, select **New Module...**.

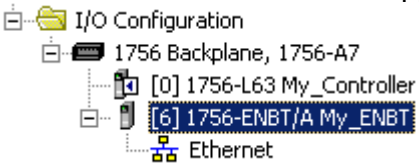
2 This action opens the *Select Module Type* dialog box. Select the **1756-ENBT** under the *Communicatio*n Module Type Category and click the **CREATE** button.



3 Enter the *Name*, *Slot*, *Revision*, and *IP Address* of the 1756-ENBT module and click **OK**.



4 The 1756-ENBT module now appears in the *Controller Organizer* window.

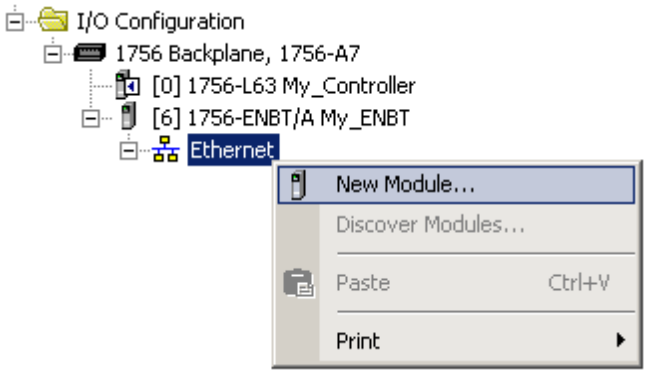


5 Save the RSLogix 5000 project.

6.1.3 Ethernet Bridge Network Setup

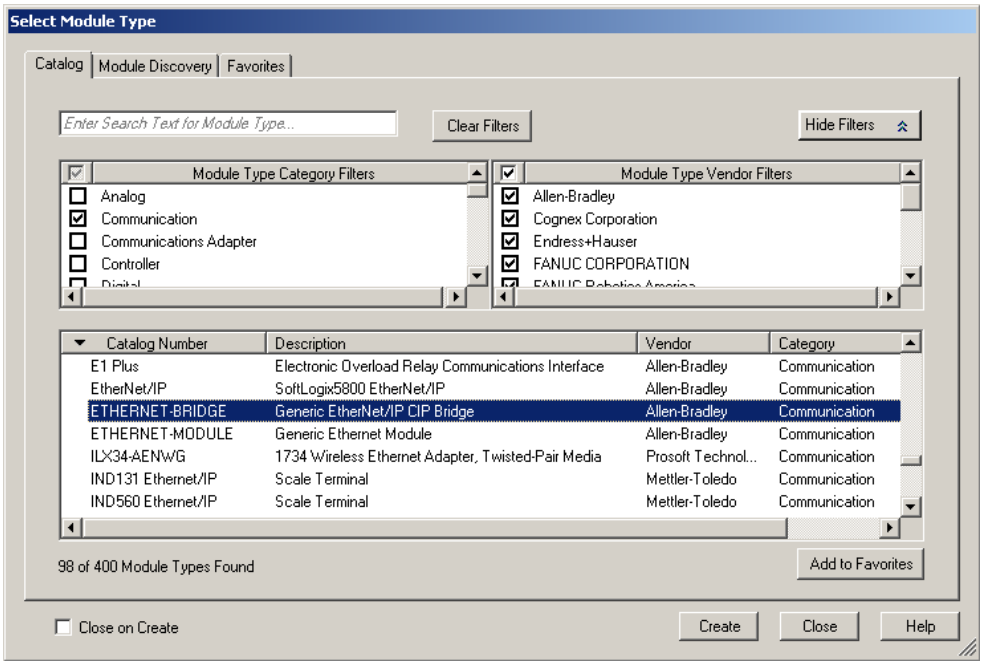
An Ethernet Bridge needs to be added to the 1756-ENBT module. For CompactLogix, connect the Ethernet Bridge to the Ethernet port on the controller.

1. In the *Controller Organizer* window, click the right mouse button on the **ETHERNET** icon to open a shortcut menu. On the shortcut menu, choose **NEW MODULE…**



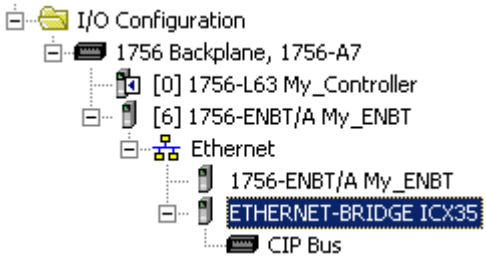
Note: For both ControlLogix and CompactLogix controllers, the *Ethernet* icon is located under the controller icon.

2. This opens the *Select Module Type* dialog box. Select the **ETHERNET-BRIDGE** module under the *Communication* directory and click the **CREATE** button.

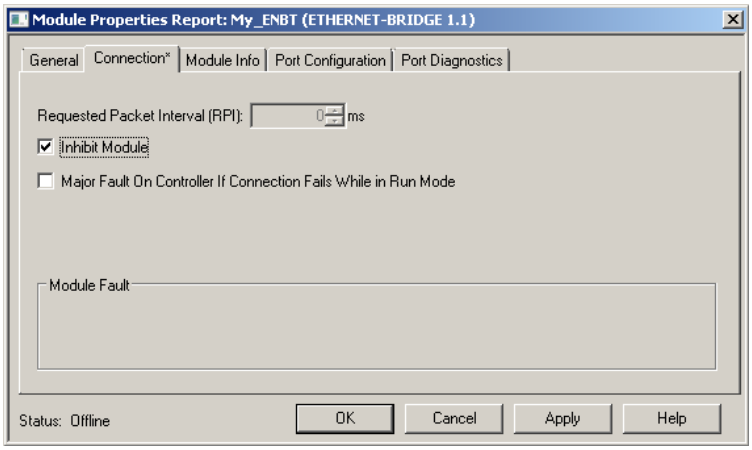


3. This opens the *New Module* dialog box. Enter '**ICX35**' as the *Name.*
4. Enter the LAN IP address of the ICX35-HWC. This is the connection to the outside world for the 1756-ENBT.
5. Click **OK**.

6 The **ETHERNET-BRIDGE** now appears in the *Controller Organizer* window under the 1756-ENBT module.



7 Double click the **ETHERNET-BRIDGE** icon in the *Controller Organizer* window to open the *Module Properties* window. Click on the *Connection* tab and check the *Inhibit Module* box. Click **OK**.

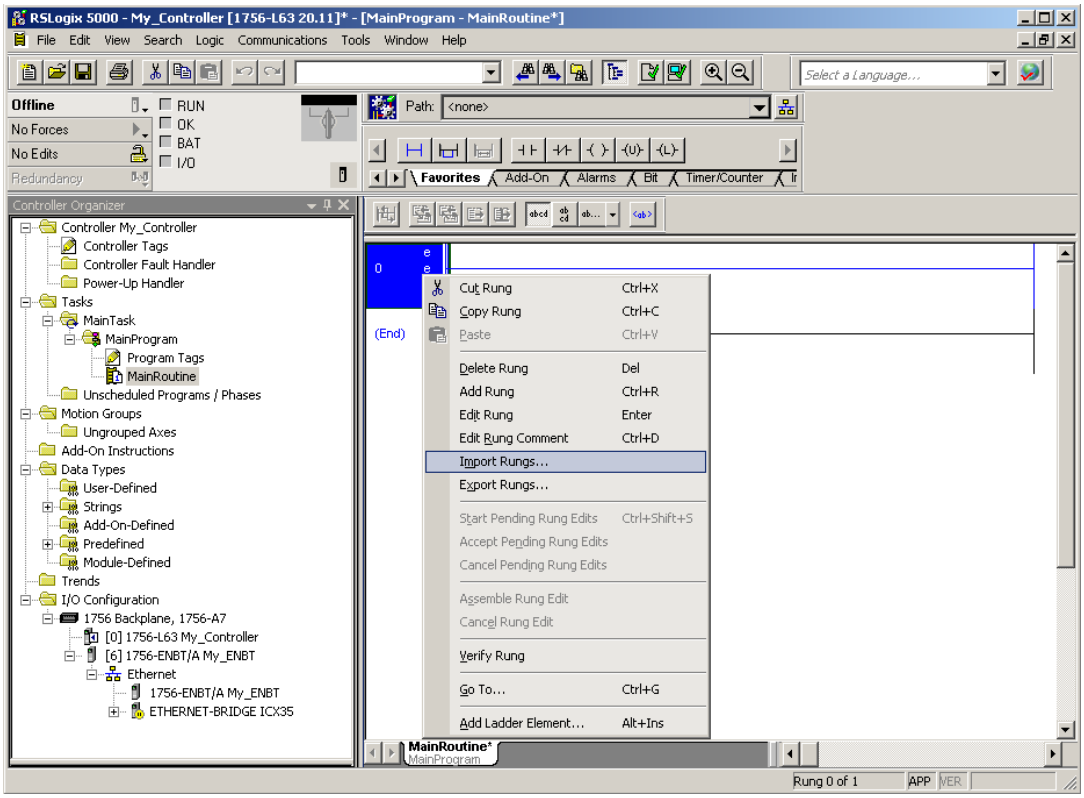


8 Save the file.

6.2 Importing the AOI

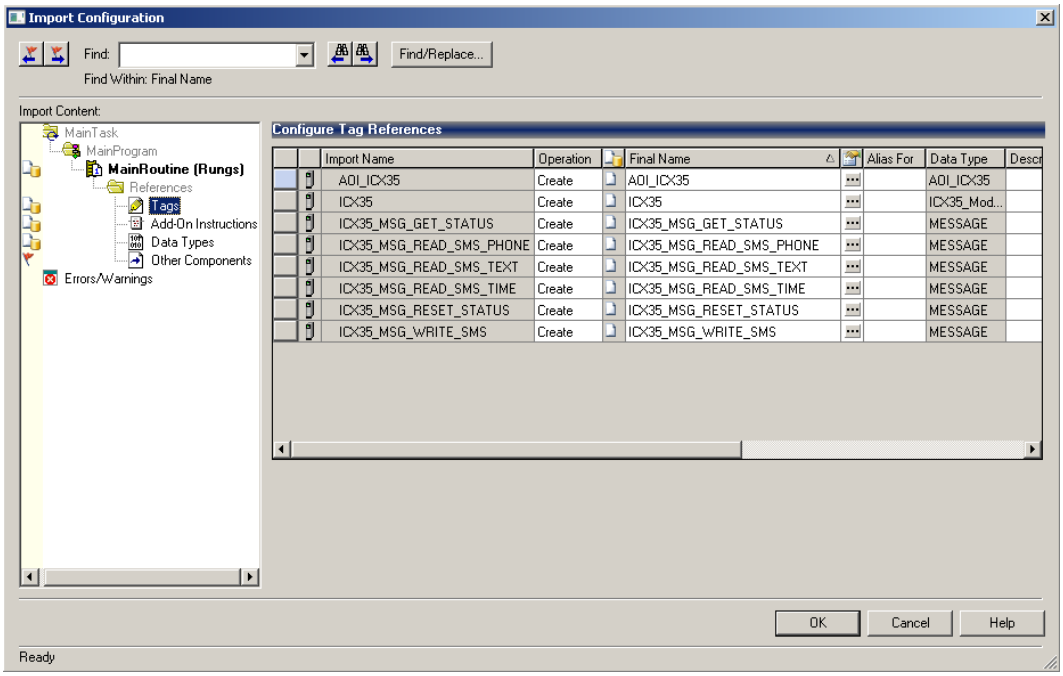
Note: When importing an ICX35-HWC AOI file into a new project, use the ICX35-HWC AOI v1.6 file from www.prosoft-technology.com. Also, the ICX35-HWC firmware version must be v1.2.2 or later.

1. In the *Controller Organizer* window, expand the *Tasks* folder and subfolders until you reach the *MainProgram* folder.
2. In the *MainProgram* folder, double-click to open the **MainRoutine** ladder.
3. Select an empty rung in the routine, and click the right mouse button to open a shortcut menu. On the shortcut menu, choose **IMPORT RUNGS...**

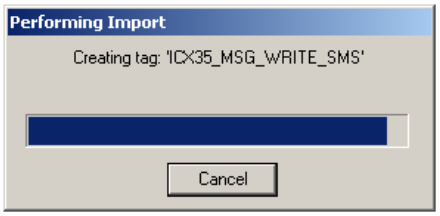


4 Navigate to the location on your PC where you saved the Add-On Instruction (for example, Desktop). Select the .L5X file and click the **IMPORT…** button.

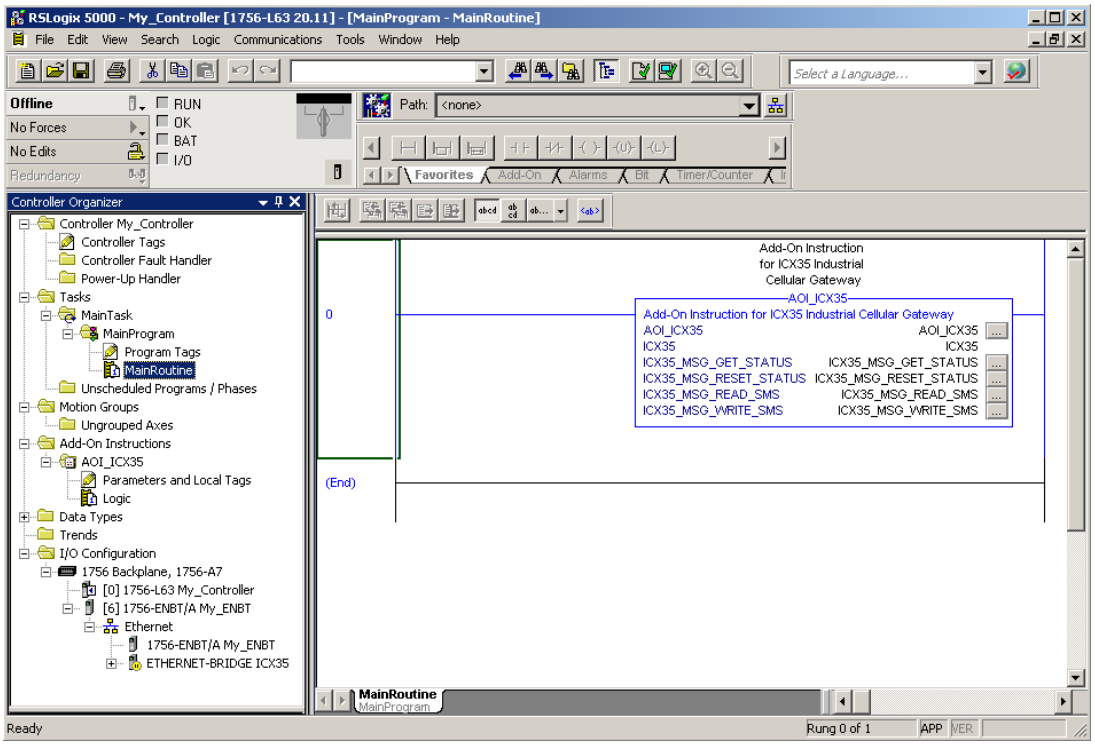
5 This action opens the *Import Configuration* dialog box, showing the controller tags that will be created.



6 Click **OK** to confirm the import. RSLogix will indicate that the import is in progress:



7 When the import is complete, the new rung with the Add-On Instruction will be visible as shown in the following illustration.



8 The procedure has also imported new User Defined Data Types, Controller Tags, and the Add-On instruction for your project.

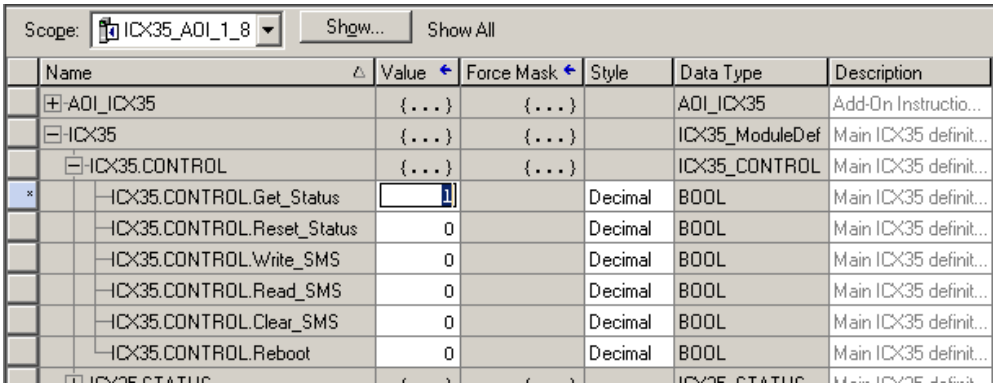
9 Save the project. When ready, download the project to the processor.

6.3 EtherNet/IP and SMS Text Message Features

6.3.1 ICX35-HWC Diagnostic Data Retrieval

The ICX35-HWC AOI can retrieve the ICX35-HWC status from the radio and display it in RSLogix 5000.

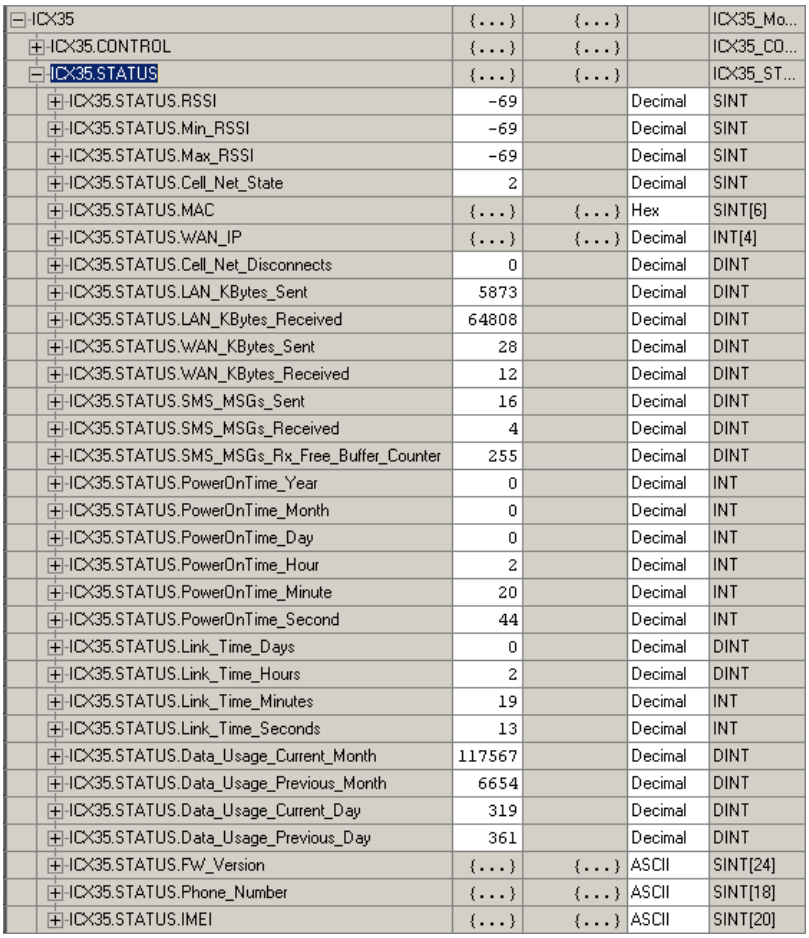
1 Enter '**1**' in the *ICX35.CONTROL.Get_Status* controller tag and press **ENTER**.



Scope: ICX35_AOI_1_8 | Show... | Show All

Name	Value	Force Mask	Style	Data Type	Description
AOI_ICX35	{...}	{...}		AOI_ICX35	Add-On Instructio...
ICX35	{...}	{...}		ICX35_ModuleDef	Main ICX35 definit...
ICX35.CONTROL	{...}	{...}		ICX35_CONTROL	Main ICX35 definit...
ICX35.CONTROL.Get_Status	1		Decimal	BOOL	Main ICX35 definit...
ICX35.CONTROL.Reset_Status	0		Decimal	BOOL	Main ICX35 definit...
ICX35.CONTROL.Write_SMS	0		Decimal	BOOL	Main ICX35 definit...
ICX35.CONTROL.Read_SMS	0		Decimal	BOOL	Main ICX35 definit...
ICX35.CONTROL.Clear_SMS	0		Decimal	BOOL	Main ICX35 definit...
ICX35.CONTROL.Reboot	0		Decimal	BOOL	Main ICX35 definit...

2 The *ICX35.STATUS* array populates with the ICX35-HWC status.



ICX35	{...}	{...}		ICX35_Mo...
ICX35.CONTROL	{...}	{...}		ICX35_CO...
ICX35.STATUS	{...}	{...}		ICX35_ST...
ICX35.STATUS.RSSI	-69		Decimal	SINT
ICX35.STATUS.Min_RSSI	-69		Decimal	SINT
ICX35.STATUS.Max_RSSI	-69		Decimal	SINT
ICX35.STATUS.Cell_Net_State	2		Decimal	SINT
ICX35.STATUS.MAC	{...}	{...}	Hex	SINT[6]
ICX35.STATUS.WAN_IP	{...}	{...}	Decimal	INT[4]
ICX35.STATUS.Cell_Net_Disconnects	0		Decimal	DINT
ICX35.STATUS.LAN_KBytes_Sent	5873		Decimal	DINT
ICX35.STATUS.LAN_KBytes_Received	64808		Decimal	DINT
ICX35.STATUS.WAN_KBytes_Sent	28		Decimal	DINT
ICX35.STATUS.WAN_KBytes_Received	12		Decimal	DINT
ICX35.STATUS.SMS_MSGs_Sent	16		Decimal	DINT
ICX35.STATUS.SMS_MSGs_Received	4		Decimal	DINT
ICX35.STATUS.SMS_MSGs_Rx_Free_Buffer_Counter	255		Decimal	DINT
ICX35.STATUS.PowerOnTime_Year	0		Decimal	INT
ICX35.STATUS.PowerOnTime_Month	0		Decimal	INT
ICX35.STATUS.PowerOnTime_Day	0		Decimal	INT
ICX35.STATUS.PowerOnTime_Hour	2		Decimal	INT
ICX35.STATUS.PowerOnTime_Minute	20		Decimal	INT
ICX35.STATUS.PowerOnTime_Second	44		Decimal	INT
ICX35.STATUS.Link_Time_Days	0		Decimal	DINT
ICX35.STATUS.Link_Time_Hours	2		Decimal	DINT
ICX35.STATUS.Link_Time_Minutes	19		Decimal	INT
ICX35.STATUS.Link_Time_Seconds	13		Decimal	INT
ICX35.STATUS.Data_Usage_Current_Month	117567		Decimal	DINT
ICX35.STATUS.Data_Usage_Previous_Month	6654		Decimal	DINT
ICX35.STATUS.Data_Usage_Current_Day	319		Decimal	DINT
ICX35.STATUS.Data_Usage_Previous_Day	361		Decimal	DINT
ICX35.STATUS.FW_Version	{...}	{...}	ASCII	SINT[24]
ICX35.STATUS.Phone_Number	{...}	{...}	ASCII	SINT[18]
ICX35.STATUS.IMEI	{...}	{...}	ASCII	SINT[20]

3 The ICX35-HWC status controller tags are defined below:
EtherNet/IP Class ID: 0xA1 (161)
Number of Instances: 1

ICX35.STATUS.	Data Type	Description
RSSI	SINT	Current Signal Strength. Range -50 to -125 dBm Value[1] = -128
Min_RSSI *	SINT	Minimum Signal Strength. Range -50 to -125 dBm Value[1] = 127 (Set during initialization)
Max_RSSI *	SINT	Maximum Signal Strength. Range -50 to -125 dBm Value[1] = -128 (Set during initialization)
Cell_Net_State	SINT	Status of the connection to the cellular network. 0: Disconnect 1: Connecting 2: Connected Value[1] = 0 (Not connected)
MAC	SINT[6]	ICX35-HWC MAC ID. Value[1] = Not available
WAN_IP	DINT	Cellular network IP. Value[1] = 0.0.0.0
Cell_Net_Disconnects *	DINT	Number of times ICX35-HWC is disconnected from the cellular network since power on
LAN_KBytes_Sent *	DINT	Number Kbytes sent on LAN since power on
LAN_KBytes_Received *	DINT	Number of Kbytes received LAN since power on
WAN_KBytes_Sent *	DINT	Number of bytes sent WAN since power on
WAN_KBytes_Received *	DINT	Number of bytes received WAN since power on
SMS_MSGs_Sent *	DINT	Number of SMS messages sent since power on
SMS_MSGs_Received *	DINT	Number of SMS messages received since power on
SMS_MSGs_Rx_Free_Buffer_Counter *	DINT	Number of free slots in the Rx SMS buffer. Max 500 message storage.
PowerOnTime_Year	INT	Power on time year
PowerOnTime_Month	INT	Power on time month
PowerOnTime_Day	INT	Power on time day
PowerOnTime_Hour	INT	Power on time hour
PowerOnTime_Minute	INT	Power on time minute
PowerOnTime_Second	INT	Power on time seconds
Link_Time_Days	DINT	Link Time: Days of cellular connection. Value[1] = 0
Link_Time_Hours	DINT	Link Time: Hours of cellular connection. Value[1] = 0
Link_Time_Minutes	INT	Link Time: Minutes of cellular connection. Value[1] = 0
Link_Time_Seconds	INT	Link Time: Seconds of cellular connection. Value[1] = 0
Data_Usage_Current_Month	DINT	Data usage of current month in KB
Data_Usage_Previous_Month	DINT	Data usage of last month in KB
Data_Usage_Current_Day	DINT	Data usage for today in KB
Data_Usage_Previous_Day	DINT	Data usage of previous day in KB
FW_Version	SINT[24]	ICX35-HWC firmware version
Phone_Number	SINT[18]	ICX35-HWC cellular phone number
IMEI	SINT[20]	ICX35-HWC IMEI number

* These parameters can be reset to 0.

[1] These tags provide a placeholder value when the ICX35-HWC WAN/LAN is disconnected or in a Connecting state.

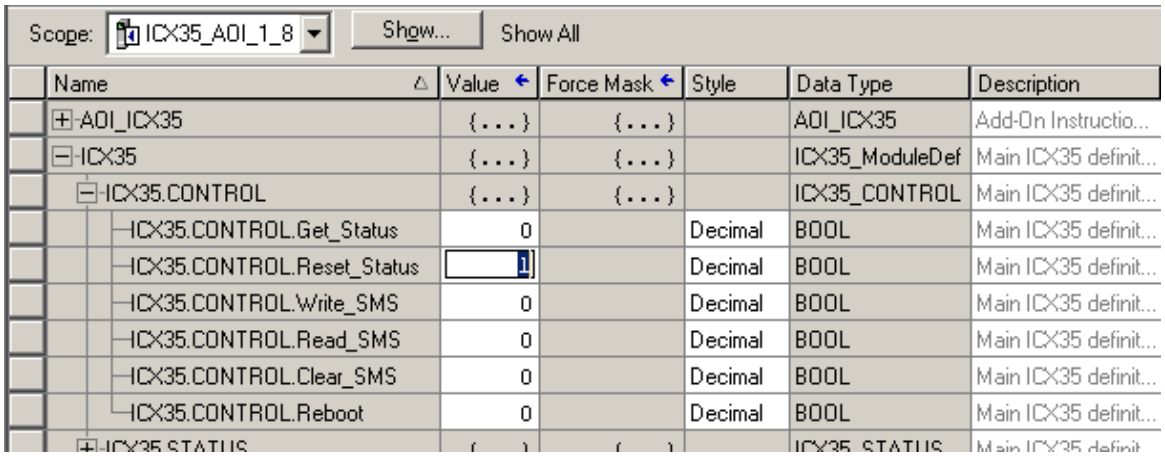
Tip: To check if a new SMS text message is received, monitor the *ICX35.STATUS.SMS_MSGs_Received* controller tag. This tag increments by 1 for every SMS text message received. You must toggle the *ICX35.CONTROL.Get_Status* controller tag for updates.

6.3.2 ICX35-HWC Diagnostic Counter Reset

The following ICX35-HWC status parameters can be reset to 0. They cannot be individually reset.

ICX35.STATUS.Min_RSSI
ICX35.STATUS.Max_RSSI
ICX35.STATUS.Cell_Net_Disconnects
ICX35.STATUS.LAN_KBytes_Sent
ICX35.STATUS.LAN_KBytes_Received
ICX35.STATUS.WAN_KBytes_Sent
ICX35.STATUS.WAN_KBytes_Received
ICX35.STATUS.SMS_MSGs_Sent
ICX35.STATUS.SMS_MSGs_Received
ICX35.STATUS.SMS_MSGs_Rx_Free_Buffer_Counter

Enter '**1**' in the *ICX35.CONTROL.Reset_Status* controller tag and press **ENTER**.

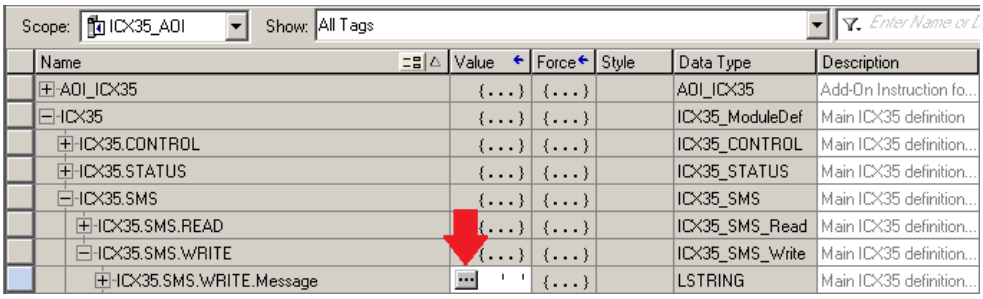


6.3.3 Sending SMS Text Messages from the ICX35-HWC

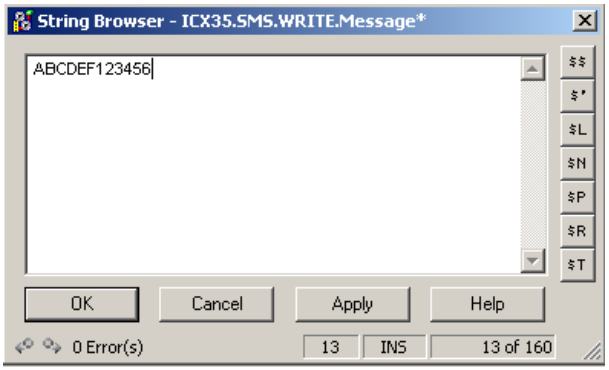
Using the ICX35-HWC AOI, SMS text messages can be sent from the ICX35-HWC to SMS text devices.

AT&T Users: For SMS texting functionality, you must power up the ICX35-HWC with the SIM installed within 72 hours after AT&T activates the SIM card.

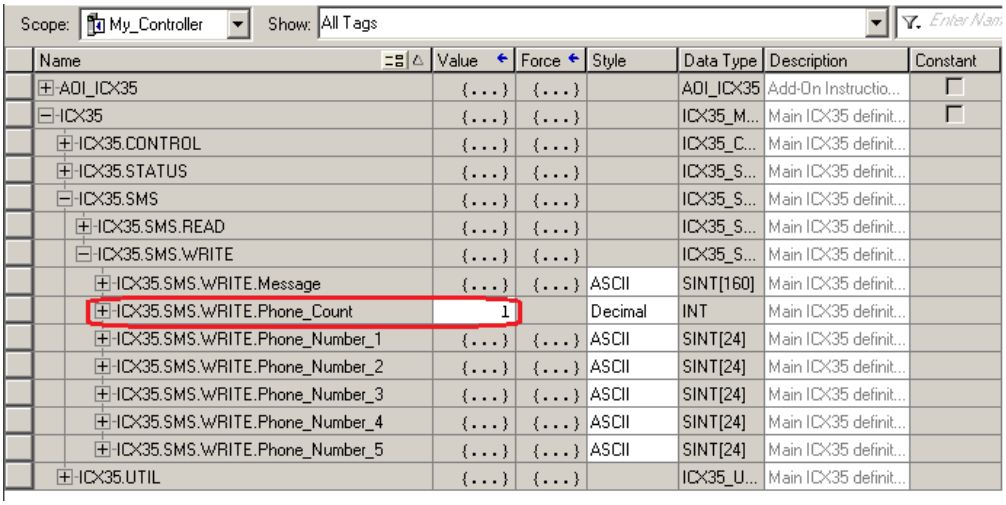
1. The text message contents are entered in the *ICX35.SMS.WRITE.Message* controller tag. Click on the box.



2. Enter the SMS text message characters in the *String Browser* dialog box. Click **OK**.

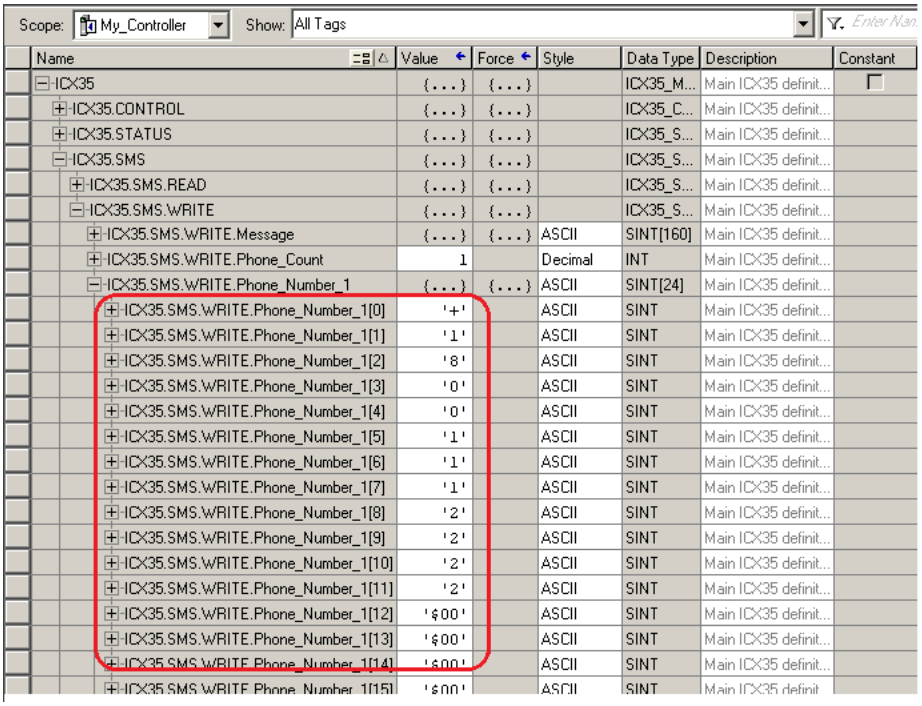


3. Enter the number SMS text recipient devices (up to 5 devices) in the *ICX35.SMS.WRITE.Phone_Count* controller tag.

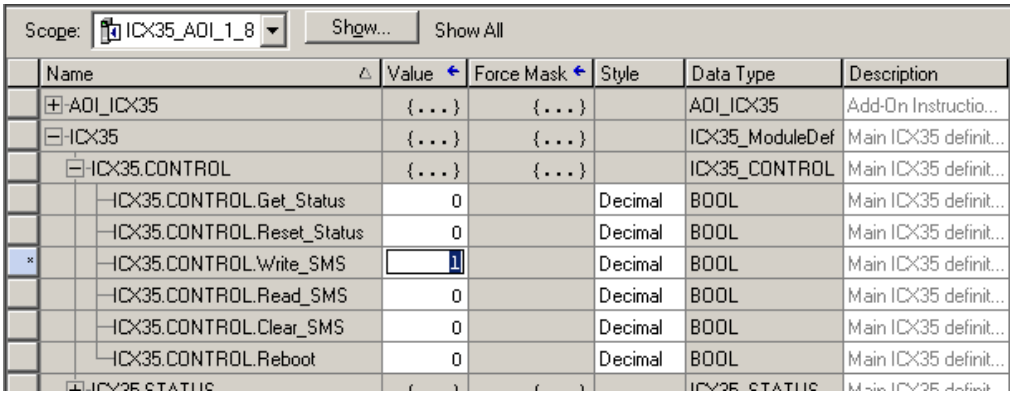


4 Enter the SMS text message recipient/phone number(s) in the *ICX35.SMS.WRITE.Phone_Number_x* controller tag(s).

Example: To send an SMS text message to phone number (800)111-2222, the format should be entered into the *ICX35.SMS.WRITE.Phone_Number_x* controller tag array as follows: +18001112222



5 To trigger the SMS text messages, enter '**1**' in the *ICX35.CONTROL.Write_SMS* controller tag and press **Enter**.



6 To check if the SMS text message was sent, enable the *ICX35.CONTROL.Get_Status* controller tag.
The *ICX35.STATUS.SMS_MSGs_Sent* controller tag increments by 1 when a SMS text message is successfully sent.

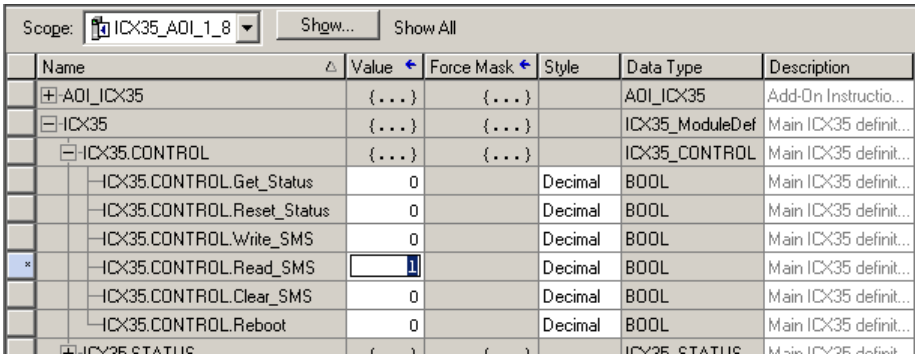
6.3.4 Retrieving SMS Text Messages from the ICX35-HWC

Using the ICX35-HWC AOI, SMS text messages that have been sent to the ICX35-HWC from remote devices can be transferred into RSLogix 5000.

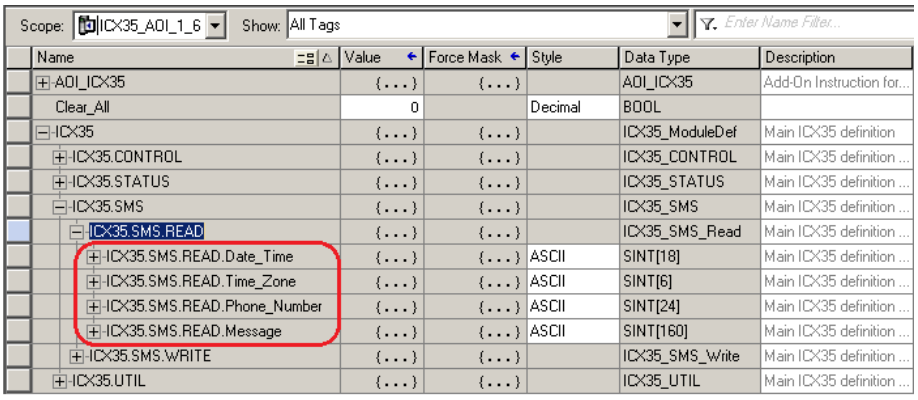
AT&T Users: For SMS texting functionality, you must power up the ICX35-HWC with the SIM installed within 72 hours after AT&T activates the SIM card.

Security Tip: For increased security and to avoid spam, we recommend that you restrict or limit the phone numbers allowed to send messages to the ICX35-HWC. Please note that some cellular providers do not offer this capability.

1 Enter a '**1**' in the *ICX35.CONTROL.Read_SMS* controller tag and press **ENTER**.



2 The *ICX35.SMS.READ* controller tag array populates with the date/time, time zone, phone number, and SMS text information from the ICX35-HWC internal buffer.



3 The *ICX35.SMS.READ* parameters are defined in the following table:

Controller Tag	Description
ICX35.SMS.READ.Date_Time[0] – [1]	Year
ICX35.SMS.READ.Date_Time[2] – [3]	Month
ICX35.SMS.READ.Date_Time[4] – [5]	Day
ICX35.SMS.READ.Date_Time[6] – [7]	Hour
ICX35.SMS.READ.Date_Time[8] – [9]	Minute
ICX35.SMS.READ.Date_Time[10] – [11]	Second
ICX35.SMS.READ.Time_Zone	Time zone of ICX35-HWC present location
ICX35.SMS.READ.Phone_Number[0] – [23]	Phone number of SMS text origination. (Ex. +18001112222)
ICX35.SMS.READ.Message[0] – [159]	Text message contents

Warning: The ICX35-HWC should not receive SMS messages faster than once every 30 seconds; otherwise it may repeatedly disconnect from the cellular network.

Warning: The ICX35-HWC must not buffer more than 500 received SMS messages before transmission to RSLogix 5000; otherwise, new incoming messages will be discarded.

Check the number of free slots in the Rx buffer by continuously monitoring the *SMS_MSGs_Rx_Free_Buffer_Counter* tag (Starting value is 500). The ICX35-HWC may buffer SMS messages in case the messages are received from the cellular network faster than the PLC polling rate. If a receiving PLC is offline during the sending of more than 250 SMS messages, upon reconnection, it will only poll the last 250 received SMS messages.

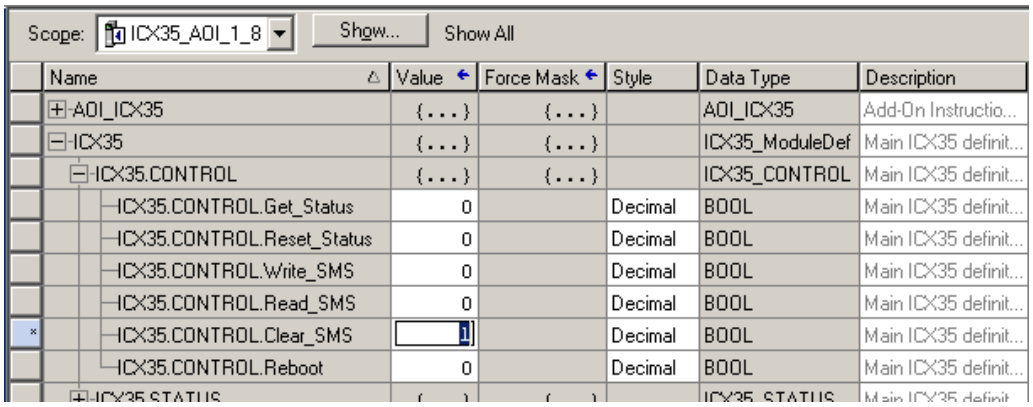
For reliable communications, the number of free slots in the ICX35-HWC receive buffer should be greater than '0'. Otherwise, messages received when the buffer is full are discarded.

6.3.5 Clearing SMS Text Messages from the ICX35-HWC

This controller tag clears all SMS messages within the ICX35-HWC.

Note: This feature requires ICX35-HWC v1.4.78 firmware or later.

Enter '**1**' in the *ICX35.CONTROL.Clear_SMS* controller tag and press **ENTER**.



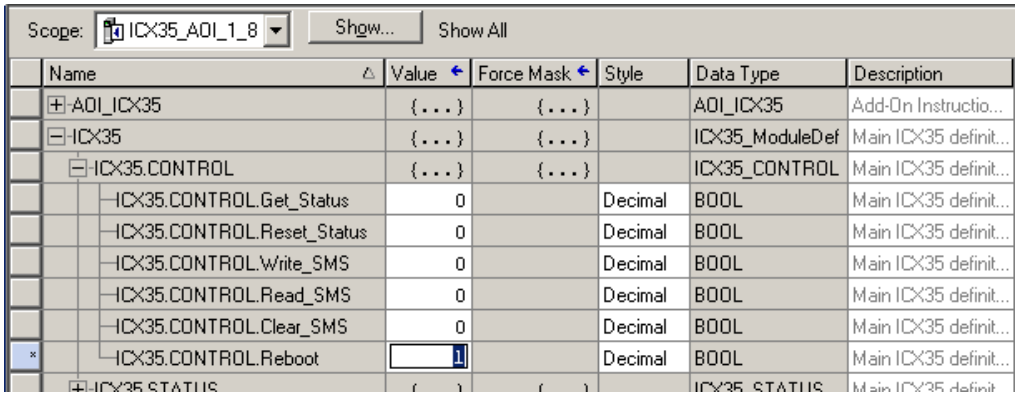
Note: Once triggered, it does not immediately clear the ICX35.SMS.READ.Message array. To do this, you must trigger the ICX35.CONTROL.Read_SMS controller tag after the SMS text messages have been cleared within the ICX35-HWC.

6.3.6 Rebooting the ICX35-HWC

This controller tag reboots the ICX35-HWC.

Note: This feature requires ICX35-HWC v1.4.78 firmware or later.

Enter '**1**' in the *ICX35.CONTROL.Reboot* controller tag and press **ENTER**.



7 Modbus TCP/IP Communications

7.1 ICX35-HWC Diagnostic Data Retrieval

The following table displays the read-only Modbus addresses of the ICX35-HWC diagnostics information. Use Modbus Function Code 4 to read these values.

ICX35_	Modbus Address	Data Type	Description
Diag.RSSI	30001	SINT	Current Signal Strength. Range -50 to -125 dBm
			Value[1] = -128
Diag.Min_RSSI *	30002	SINT	Minimum Signal Strength. Range -50 to -125 dBm
			Value[1] = 127 (Set during initialization)
Diag.Max_RSSI *	30003	SINT	Maximum Signal Strength. Range -50 to -125 dBm
			Value[1] = -128 (Set during initialization)
Diag.Cell_Net_State	30004	SINT	Status of the connection to the cellular network. 0: Disconnect 1: Connecting 2: Connected Value[1] = 0 (Not connected)
Diag.MAC_Address	30005 to 30010	SINT[6]	ICX35-HWC MAC ID. Value[1] = Not available
Diag.WAN_IP	30011 to 30014	SINT[4]	Cellular network IP. Value[1] = 0.0.0.0
Diag.Cell_Net_Disconnects *	30015 to 30016	DINT	Number of times ICX35-HWC is disconnected from the cellular network since power on
Diag.LAN_KBytes_Sent *	30017 to 30018	DINT	Number Kbytes sent on LAN since power on
Diag.LAN_KBytes_Received *	30019 to 30020	DINT	Number of Kbytes received LAN since power on
Diag.WAN_KBytes_Sent *	30021 to 30022	DINT	Number of bytes sent WAN since power on
Diag.WAN_KBytes_Received *	30023 to 30024	DINT	Number of bytes received WAN since power on
Diag.SMS_MSGs_Sent *	30025 to 30026	DINT	Number of SMS messages sent since power on
Diag.SMS_MSGs_Received *	30027 to 30028	DINT	Number of SMS messages received since power on
Diag.SMS_MSGs_Free *	30029 to 30030	DINT	Number of free slots in the Rx SMS buffer. Max 500 message storage.
Diag.Power_Year	30031	INT	Power on time year
Diag.Power_Month	30032	INT	Power on time month
Diag.Power_Day	30033	INT	Power on time day
Diag.Power_Hour	30034	INT	Power on time hour
Diag.Power_Min	30035	INT	Power on time minute
Diag.Power_Sec	30036	INT	Power on time seconds
Diag.Link_Days	30037 to 30038	DINT	Link Time: Days of cellular connection. Value[1] = 0
Diag.Link_Hours	30039 to 30040	DINT	Link Time: Hours of cellular connection. Value[1] = 0
Diag.Link_Min	30041	INT	Link Time: Minutes of cellular connection. Value[1] = 0
Diag.Link_Sec	30042	INT	Link Time: Seconds of cellular connection. Value[1] = 0
Diag.Data_Usage_Current_Month	30043 to 30044	DINT	Data usage of current month in KB
Diag.Data_Usage_Previous_Month	30045 to 30046	DINT	Data usage of last month in KB
Diag.Data_Usage_Current_Day	30047 to 30048	DINT	Data usage for today in KB
Diag.Data_Usage_Previous_Day	30049 to 30050	DINT	Data usage of previous day in KB
Diag.FW_Version	30051 to 30062	REAL	ICX35-HWC firmware version
Diag.Phone_Number	30063 to 30071	SINT[18]	ICX35-HWC cellular phone number
Diag.IMEI	30072 to 30081	SINT[20]	ICX35-HWC IMEI number

* These parameters can be reset to 0.

[1] These tags provide a placeholder value when the ICX35-HWC WAN/LAN is disconnected or in a Connecting state.

7.2 ICX35-HWC Diagnostic Counter Reset

The following ICX35-HWC status parameters can be reset to '0'. They cannot be individually reset.

Diag.Min_RSSI
Diag.Max_RSSI
Diag.Cell_Net_Disconnects
Diag.LAN_KBytes_Sent
Diag.LAN_KBytes_Received
Diag.WAN_KBytes_Sent
Diag.WAN_KBytes_Received
Diag.SMS_MSGs_Sent
Diag.SMS_MSGs_Received
Diag.SMS_MSGs_Rx_Free_Buffer_Counter

Use Modbus Function Code 6 write a value of '**1**' to 40001 in the ICX35-HWC.

7.3 Sending SMS Text Messages to the ICX35-HWC

Using the Modbus Function Codes 6 and 16, a Modbus TCP/IP Client can send SMS text message contents to the ICX35-HWC. In turn, the ICX35-HWC sends the SMS text message to the phone number recipient(s).

Before triggering, you must first load the SMS text message contents, message length, and phone number information. Below is a table of the Modbus addresses required to send an SMS text message.

Parameter	Modbus Address	Data Type	Description
SMS.TX_Send	40003	SINT	Trigger to send SMS text message when Value = 1
SMS.TX_MessageLength	40004	INT	Number of bytes (characters) to send
SMS.TX_NumCount	40005	INT	Number of phone numbers that the SMS will be sent to
SMS.TX_MessageString	40006 to 40085	SINT[160]	SMS text message string to be transmitted
SMS.TX_Ph_Number1	40086 to 40097	SINT[24]	Phone number including prefixes, country, code, etc.
SMS.TX_Ph_Number2	40098 to 40109	SINT[24]	Phone number including prefixes, country, code, etc.
SMS.TX_Ph_Number3	40110 to 40121	SINT[24]	Phone number including prefixes, country, code, etc.
SMS.TX_Ph_Number4	40122 to 40133	SINT[24]	Phone number including prefixes, country, code, etc.
SMS.TX_Ph_Number5	40134 to 40145	SINT[24]	Phone number including prefixes, country, code, etc.

- **SMS text message contents (40006):** The ICX35-HWC can send up to 160 characters (80 16-bit integers) per SMS text message. To load the text message string, use the Modbus Function Code 16 to write to Modbus address starting at 40006 in the ICX35-HWC.
- **SMS text message length (40004):** Use the Modbus Function Code 6 to write the number of characters (up to 160) to send.
- **Amount of phone numbers to send to (40005):** Use the Modbus Function Code 6 to write the amount of phone numbers that will be used.
- **Phone number entry (40086):** Use the Modbus Function Code 16 to write the recipient's phone number including prefixes, country, code, etc. You can enter up to 5 phone numbers, each starting at a different Modbus address (see table above).
- **Trigger the SMS text message (40003):** When you are ready to send the SMS text message, use the Modbus Function Code 6 to write a value of '**1**' to 40003.

7.4 Retrieving SMS Text Messages from the ICX35-HWC

Using the Modbus Function Code 4, a Modbus TCP/IP Client can read the SMS text message contents, date/time, and its phone number origination. To receive the SMS text message, use Modbus Function Code 16 to write a value of '**1**' to 40002.

Below is a table of the ICX35-HWC Modbus addresses used to read the SMS text message information.

Parameter	Modbus Address	Data Type	Description
SMS_Text.Receive	40002	SINT	To receive the SMS text message, use Modbus Function Code 16 to write a value of '**1**' to 40002.
SMS_TEXT.DateTime	30093 to 30108	SINT	Time Stamp for received SMS text. MM/DD/YY HH:MM:SS
SMS_TEXT.Phone_Number	30109 to 30120	SINT	Phone number of SMS text origination. (Ex. +18001112222)
SMS_TEXT.Text_Str	30121 to 30200	SINT	Text message contents

- **SMS text message contents (30121):** Use the Modbus Function Code 4 to read from ICX35-HWC Modbus address **30121**. Each 16-bit Modbus address contains 2 characters (1 byte each) of the SMS text message.
  Example: A 100-character text message occupies 50 Modbus addresses.
- **SMS text phone number (30109):** Use the Modbus Function Code 4 to read from ICX35-HWC Modbus address **30109**. Each (16 bit) Modbus address contains 2 characters (1 byte each) of the phone number.
- **SMS text date/time (30093):** Use the Modbus Function Code 4 to read from ICX35-HWC Modbus address **30093**. Each (16 bit) Modbus address contains 2 characters (1 byte each) of the time stamp.

7.5 Additional Features

Clearing the Received SMS Text Message Buffer

A Modbus TCP/IP Client can clear the received SMS text messages in the ICX35-HWC. Use the Modbus Function Code 6 to write a value of '**1**' to Modbus Address 40146 in the ICX35-HWC.

Rebooting the ICX35-HWC

A Modbus TCP/IP Client can reboot the ICX35-HWC by using a Function Code 6 to write a value of '**1**' to Modbus Address 40147 in the ICX35-HWC.

8 Watchdog

The *Connection Recovery* watchdog mechanism is used to reboot the ICX35-HWC when there is a loss of connectivity or halts for any other reason.

There are multiple scenarios for the watchdog functionality:

- No Belden Horizon connection due to no data plan left
- No Belden Horizon connection and data plan left
- No Belden Horizon connection
- No Belden Horizon connection and usage monitoring disabled
- No connection to the configured endpoint address
- No Belden Horizon connection while endpoint address is reachable
- The Belden Horizon connection through the agent is compromised (no traffic through the websockets connection, agent hangs)

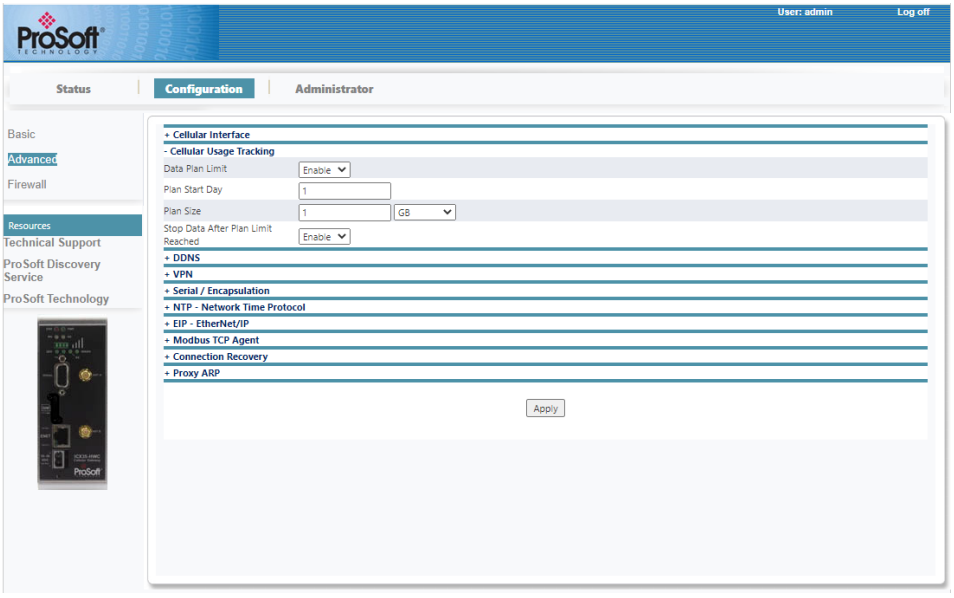
8.1 Watchdog Scenarios

There are several scenarios in which the watchdog is triggered:

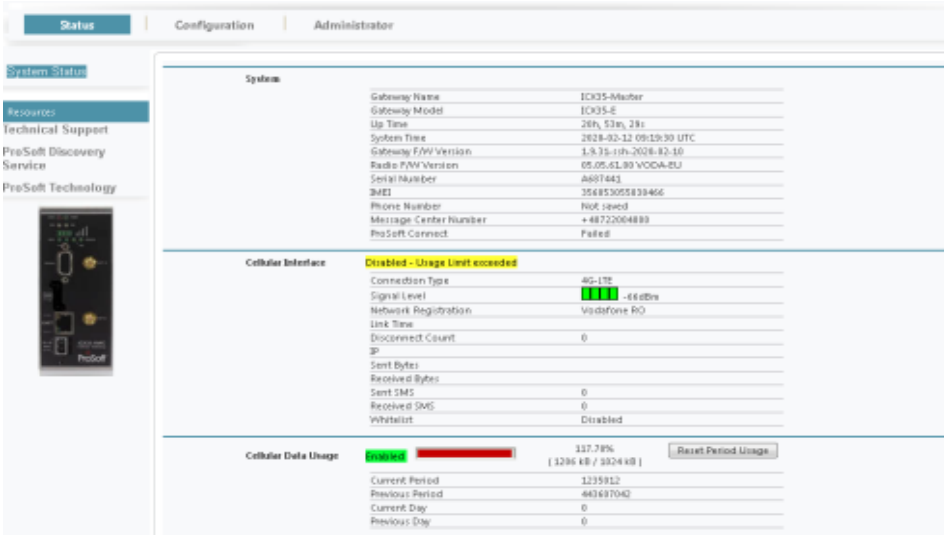
A. No Belden Horizon connection due to no data plan left.

This scenario is activated if:

- The device is active in Belden Horizon;
- The number of attempts to reach Belden Horizon are less than the configured threshold (watchdog/percentatagefail);
- *Data Plan Limit* and *Stop Data After Plan Limit Reached* are enabled;



- There is no data left in the Data Plan.

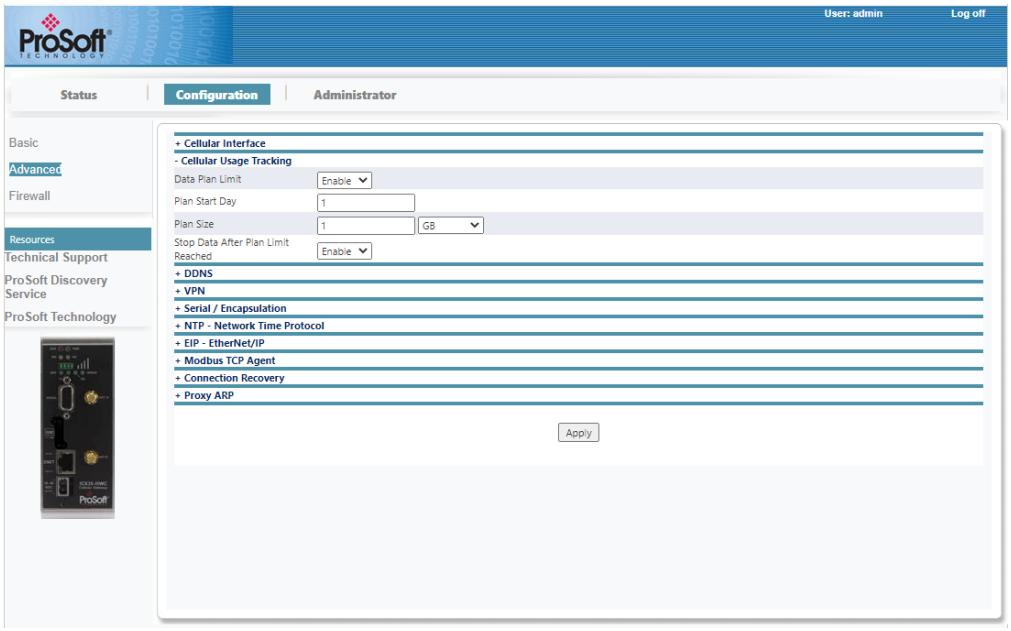


In this scenario, the watchdog mechanism will reboot the device at the time interval specified (minutes) in the configuration file (watchdog/datatimeout=1440). This is the 24 hour scenario. This is not configurable from the local UI.

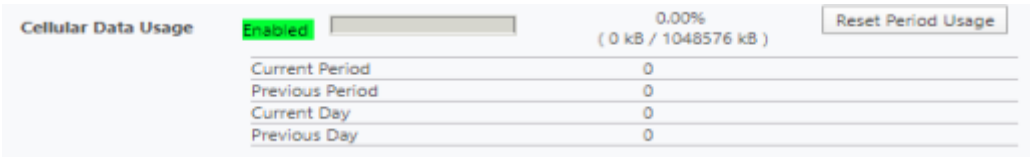
B. No Belden Horizon connection and data plan left.

This scenario is activated if:

- The device is active in Belden Horizon;
- The number of attempts to reach Belden Horizon are less than the configured threshold (watchdog/percentatagefail);
- *Data Plan Limit* and *Stop Data After Plan Limit Reached* are enabled;



- There is data available in the Data Plan.



In this scenario, the watchdog mechanism will reboot the device at the time interval specified (minutes). This is configurable from the local UI via the *Belden Horizon Timeout* parameter.

C. No Belden Horizon connection.

This scenario is activated if:

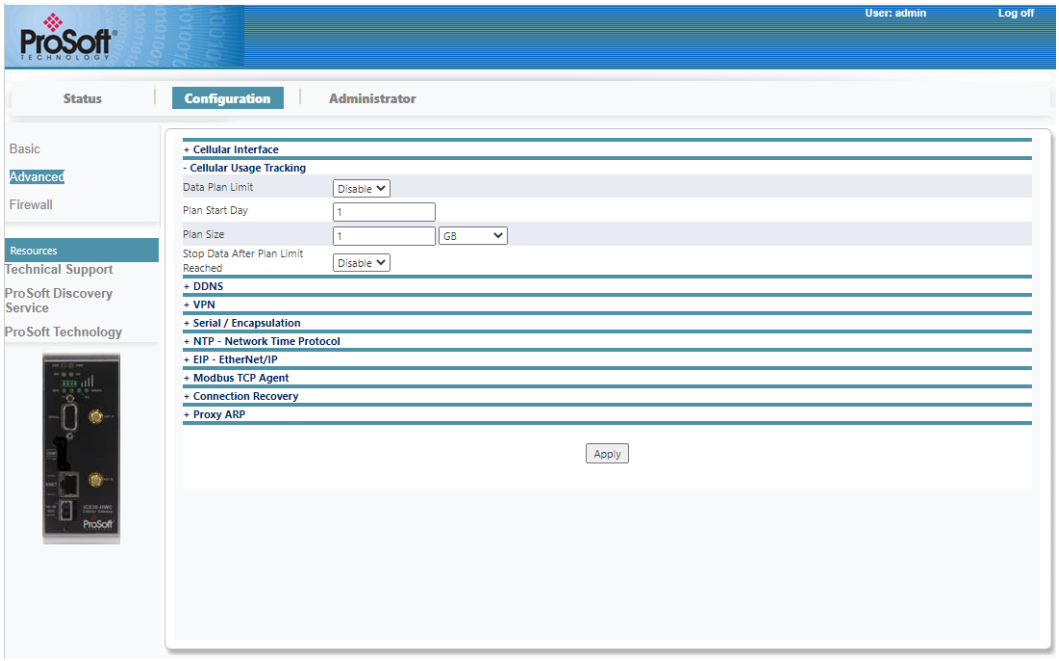
- The device is active in Belden Horizon;
- The number of attempts to reach Belden Horizon are less than the configured threshold (watchdog/percentatagefail);
- *Data Plan Limit* is enabled and *Stop Data After Plan Limit Reached* is disabled;

In this scenario, the watchdog mechanism will reboot the device at the time interval specified (minutes). This is configurable from the local UI via the *Belden Horizon Timeout* parameter.

D. No Belden Horizon connection and usage monitoring disabled.

This scenario is activated if:

- The device is active in Belden Horizon;
- The number of attempts to reach Belden Horizon are less than the configured threshold;
- *Data Plan Limit* is disabled and *Stop Data After Plan Limit Reached* is disabled;



In this scenario, the watchdog mechanism will reboot the device at the time interval specified (minutes). This is configurable from the local UI via the *Belden Horizon Timeout* parameter.

E. No connection to the configured endpoint address.

> **Note:** This case is made for the devices that are not activated in Belden Horizon.

The default endpoint address present in the configuration file is 8.8.8.8 (watchdog/endpointaddr=8.8.8.8).

This scenario is activated if:

- The gateway is not activated in Belden Horizon;
- The connectivity to the desired endpoint (rate of successful pings to the address) is less than the configured threshold (watchdog/percentatagefail).

In this scenario, the watchdog mechanism will reboot the device at the time interval specified (minutes) in the configuration file (watchdog/endpointtimeout=15). This is configurable from the local UI via the *Endpoint Timeout* parameter.

F. No Belden Horizon connection while endpoint address is reachable.

The default endpoint address present in the configuration file is 8.8.8.8 (watchdog/endpointaddr=8.8.8.8).

This scenario is activated if:

- The device is active in Belden Horizon;
- The connectivity to the desired endpoint (rate of successful pings to the address) is good (the internet connection is up);
- The number of attempts to reach Belden Horizon are less than the configured threshold (watchdog/percentatagefail).

In this scenario, the watchdog mechanism will reboot the device at the time interval specified (minutes) in the configuration file (watchdog/endpointtimeout=15). This scenario applies if the device is not active in Belden Horizon. This is configurable from the local UI via the Endpoint Timeout parameter.

G. The Belden Horizon connection through the agent is compromised (no traffic through the websockets connection, agent suspends).

This scenario is activated if:

- The device is active in Belden Horizon;
- The agent process, which is responsible for the connection with Belden Horizon is suspended (Belden Horizon and internet connection are up but there is an internal issue with the agent software).

In this scenario, the watchdog mechanism will reboot the device at the time interval specified (minutes). This is configurable from the local UI via the *Belden Horizon Timeout* parameter.

8.2 Watchdog Configuration From Export File

The watchdog parameters can be manually edited by exporting the configuration file from the ICX35-HWC.

1 Export the configuration file from the ICX35-HWC.

2 In the newly exported configuration file, look for the watchdog parameters. They are pointed out in the example below (marked in **bold**):

config/version=0
ddns/system=
ddns/mode=0
ddns/hostname=
ddns/username=
ddns/password=
ddns/ipcheckperiod=600
.....
watchdog/psctimeout is set to: 60
watchdog/datatimeout is set to: 1440
watchdog/enabled is set to: 1
watchdog/percentagefail is set to: 10
watchdog/endpointtimeout is set to: 15
watchdog/endpointaddr is set to: 8.8.8.8
watchdog/armed is set to: 0
.....
system/ntpport=123
system/eipenable=0
system/mbenable=0
system/mbport=502
ovpnroutes1/1=
ovpnroutes1/2=

3 Below are the 7 parameters with their functional descriptions:

A. **watchdog/psctimeout=60**
This is the time value expressed in minutes for the cases when the watchdog resets itself after 1 hour.

Cases:
- No Belden Horizon connection
- No Belden Horizon connection and data plan left
- No Belden Horizon connection and usage monitoring disabled
- The Belden Horizon connection through the agent is compromised (no traffic through the websockets connection, agent hangs)

B. **watchdog/datatimeout=1440**
This is the time value expressed in minutes for the single case when the watchdog resets itself after 24 hours:

Case:
- No Belden Horizon connection

C. **watchdog/enabled=1**
By default the watchdog mechanism is enabled in the configuration file (1=enabled; 0=disabled).

Note: The watchdog/enabled=1 has no effect if watchdog/armed is set to 0.

D. **watchdog/percentagefail=10**
This parameter shows the percentage of successful attempts to:
- Ping the configured endpoint address (check watchdog/endpointaddr parameter; the default endpoint IP Address is 8.8.8.8)
- Reach https://www.belden.io/device-gateway/status

If out of 100 attempts there are 10 successful and 90 failed, the gateway will not reboot. If the successful attempts are less than 10, the gateway will reboot.

E. **watchdog/endpointtimeout=15**
This is the time value expressed in minutes for the cases when the watchdog resets itself after 15 minutes.

Cases:
- No connection to the configured endpoint address (check watchdog/endpointaddr parameter; by default there is no endpoint configured).
- No Belden Horizon connection while endpoint address is reachable.

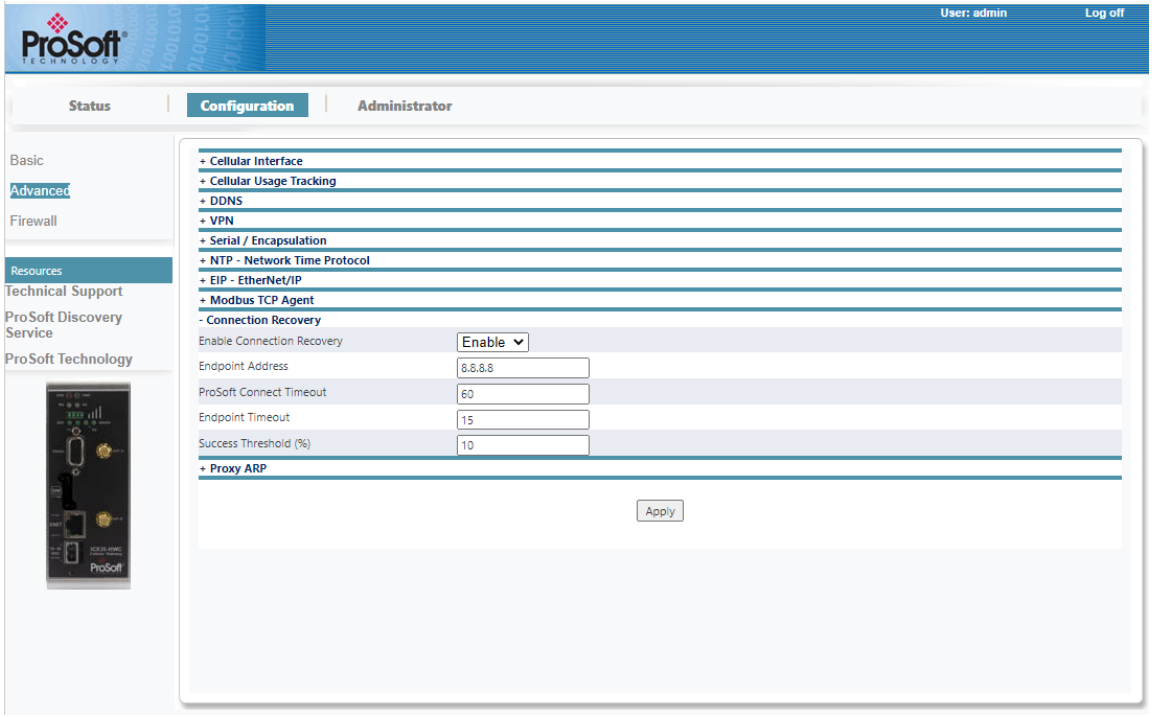
F. **watchdog/endpointaddr is set to: 8.8.8.8**
By default endpoint IP address configured is 8.8.8.8. This is used to perform a health check of the gateway connectivity to the designated IP address 8.8.8.8. This parameter can be configured with any IPv4 address.

G. **watchdog/armed is set to: 0**
For the cases when there is no internet connection available at boot time, the watchdog/armed parameter prevents the unit from resetting itself spontaneously. This parameter is not configurable. The state changes from 0 to 1 when an internet connection is detected. Once this happens, the watchdog mechanism will start. From that point onward this parameter will not go back to 0 unless a factory reset is issued.

4 Once the desired watchdog configuration is set, you can load it back on the gateway from the local UI.

8.3 Watchdog Configuration on ICX35-HWC Webpage

A number of the Watchdog parameters are found on the ICX35-HWC webpage. They can be found at: **Configuration > Advanced > Connection Recovery**.

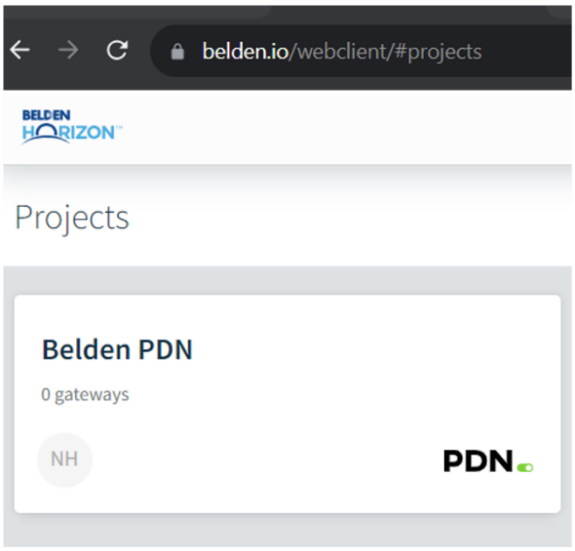


You have the options to:

- Enable/disable the *Connection Recovery* watchdog mechanism
- Configure the desired Endpoint Address (Default value is **8.8.8.8**)
- Configure the timeout that manages the connection to Belden Horizon (applies for cases 2, 3, 4 and 7 described above)
- Configure the endpoint timeout (applies for case 5 described above, where the ICX35-HWC is not activated in Belden Horizon)
- Configure the success threshold (percentage of successful attempts to reach the endpoint/ Belden Horizon, for which the ICX35-HWC does not reboot)

9 Easy Bridge

The ICX35-HWC supports bridge capability to allow access to Logix Controllers using RSLinx. This chapter covers the “Easy Bridging” configuration between a Local System and Remote Devices, using the VPN Tunneling functionality. This feature is only available for PDN Projects on the **Belden.io** page.

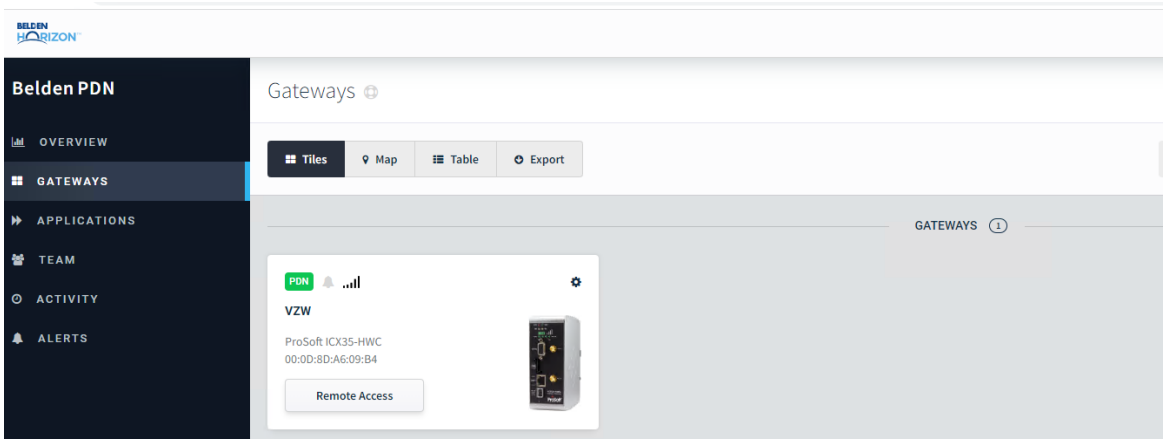


9.1 VPN Tunnel Connection

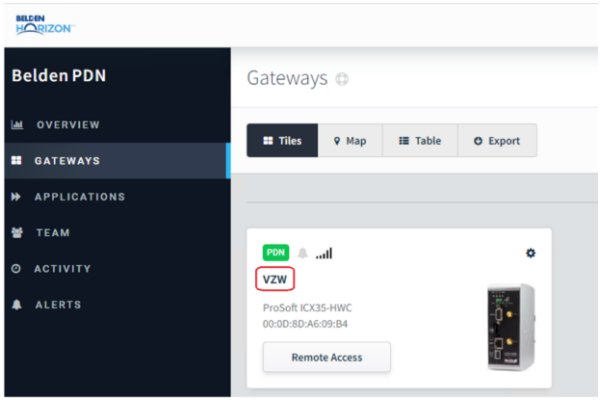
Once a local connection to the ICX35-HWC gateway has been established (see *Assigning a LAN IP Address* on page 14 for more information), ensure the following:

- WAN port has internet access
- Activation is successful through the Belden Horizon UI

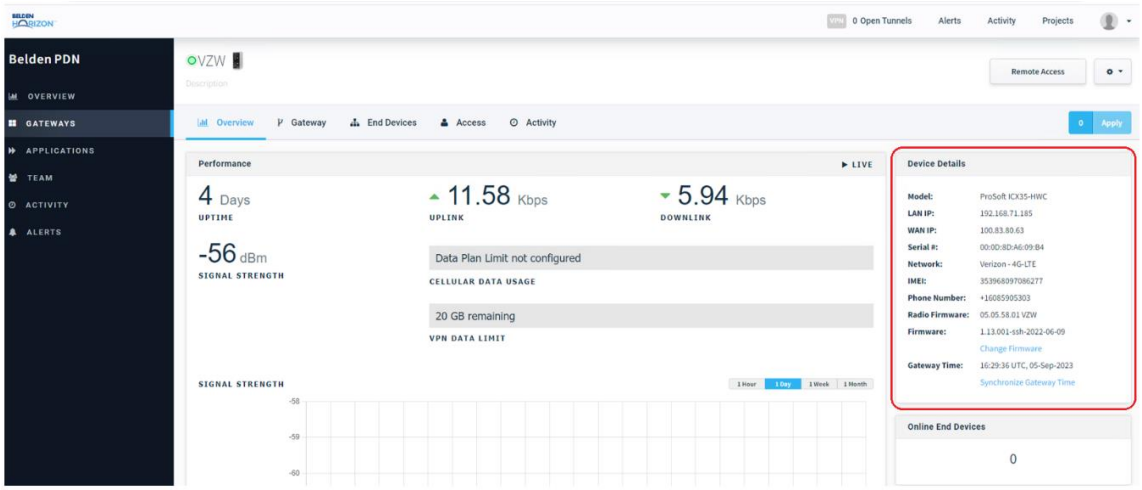
Once the ICX35-HWC is activated, it will be listed in the *Gateways* section of the **Belden.io** page.



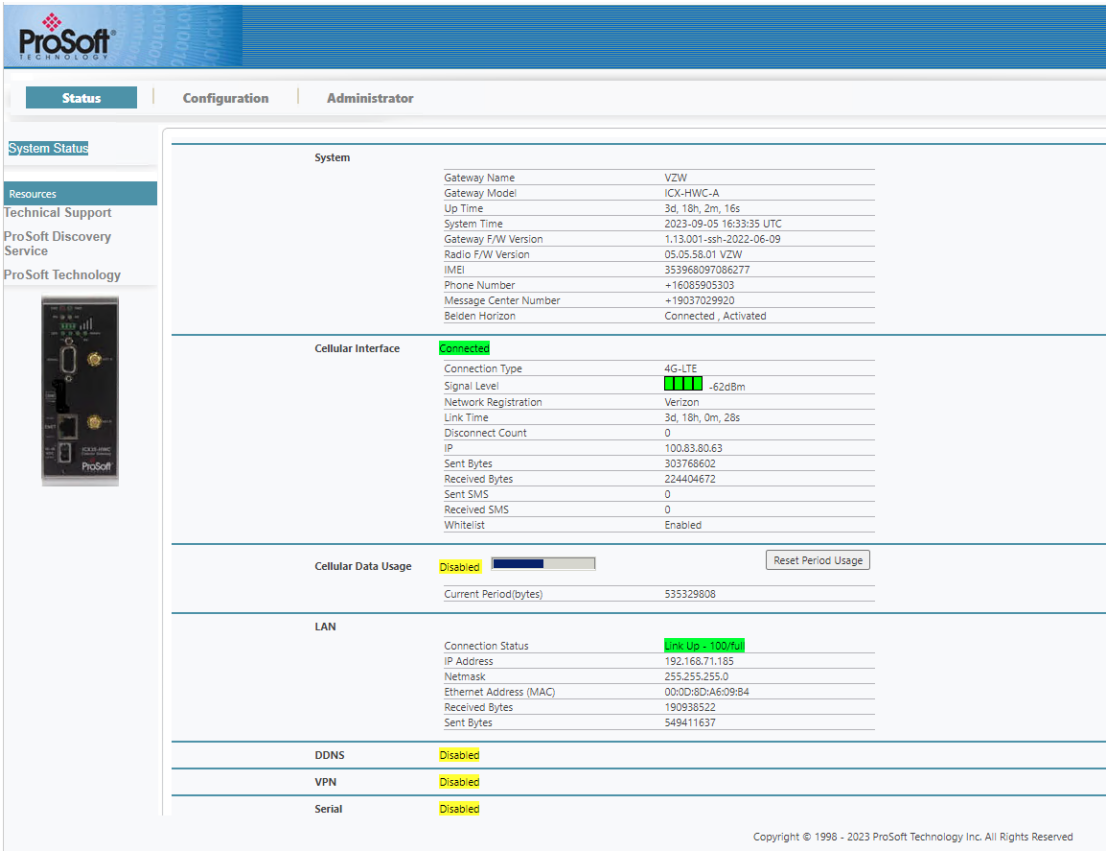
1 Click on the **ICX35-HWC** name within the tile.



2 In the *Overview* tab, ensure the *Device Details* are correct.

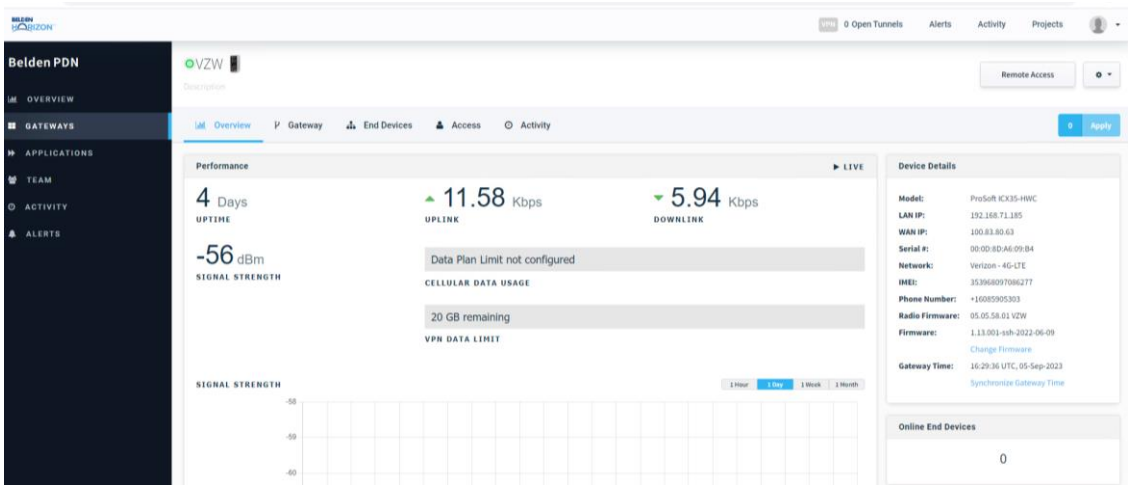


3 The *Device Details* should match the device details on the gateway's webpage (see below). This confirms the Activation and PDN are operating prior to starting the VPN Tunnel.

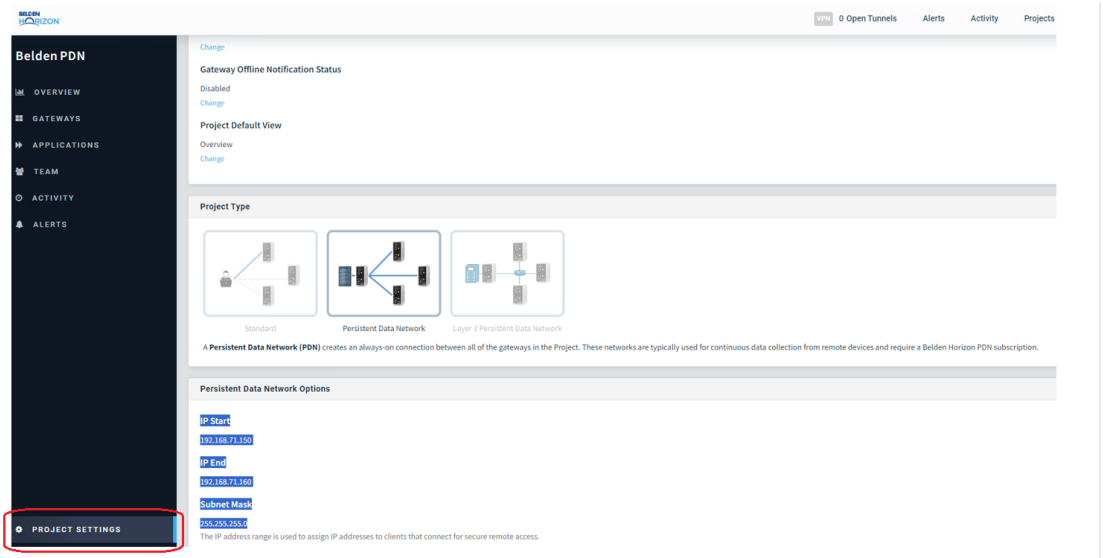


4 Ensure the ICX35-HWC LAN IP address is on the same network as the PLC Controller IP address. For ICX35-HWC LAN IP configuration information, please see *Assigning a LAN IP Address* on page 14

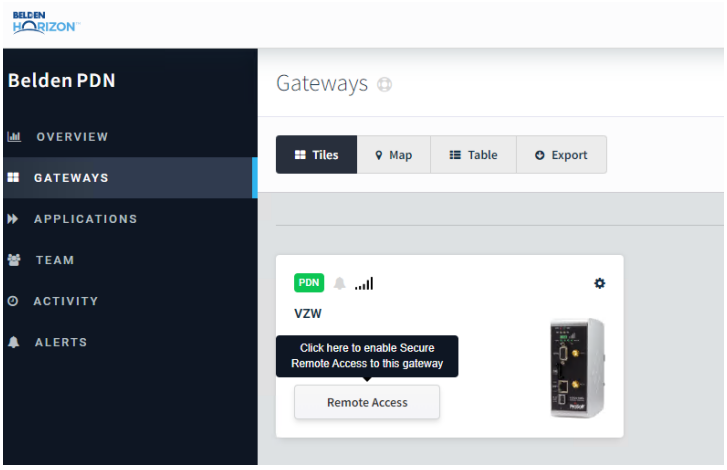
This exercise uses the following IP address examples:
ICX35-HWC LAN IP: **192.168.71.185**
PLC Controller: **192.168.71.215**



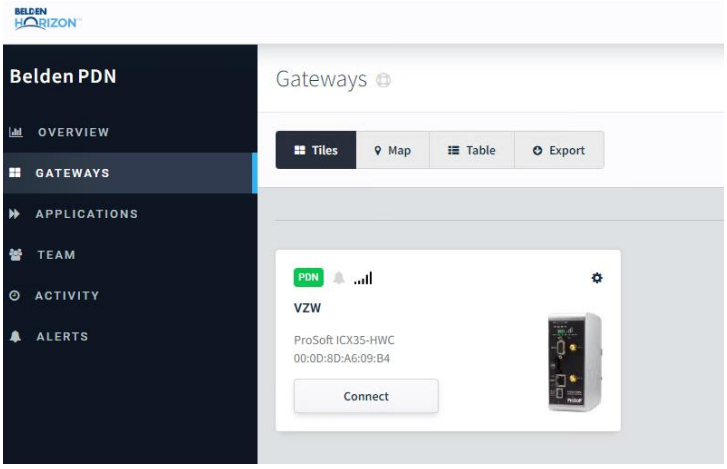
5 On the left tab of the **Belden.io** page, click on the **PROJECT SETTINGS** button. Under the *Persistent Data Network Options* section, verify the ICX35-HWC IP address range is correct.



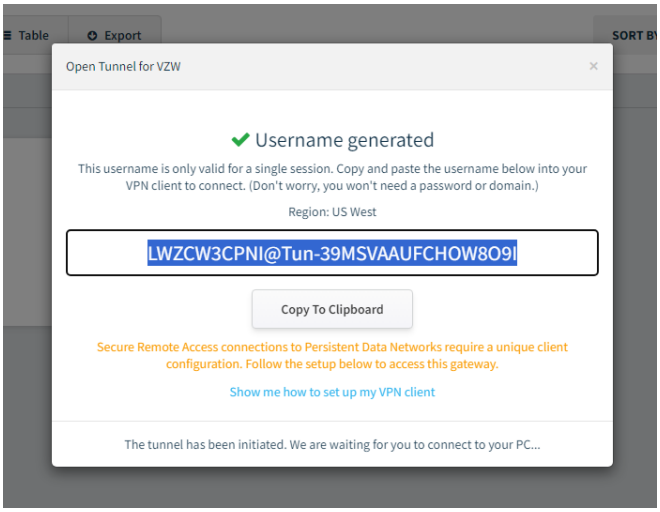
6 In the *Gateways* section, click on the gateway's **REMOTE ACCESS** button to enable a secure, remote access to the ICX35-HWC.



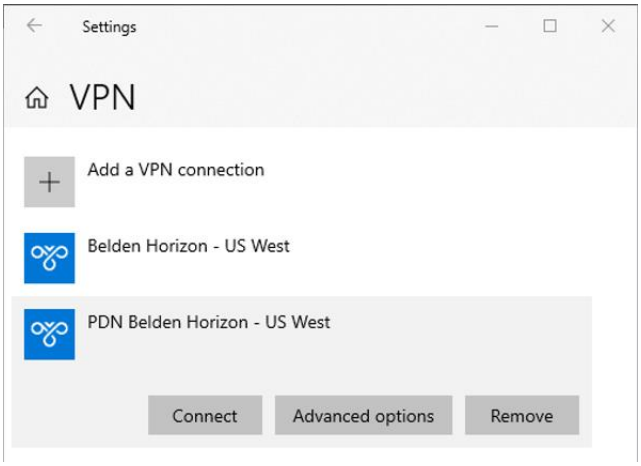
Then click on the **CONNECT** button.



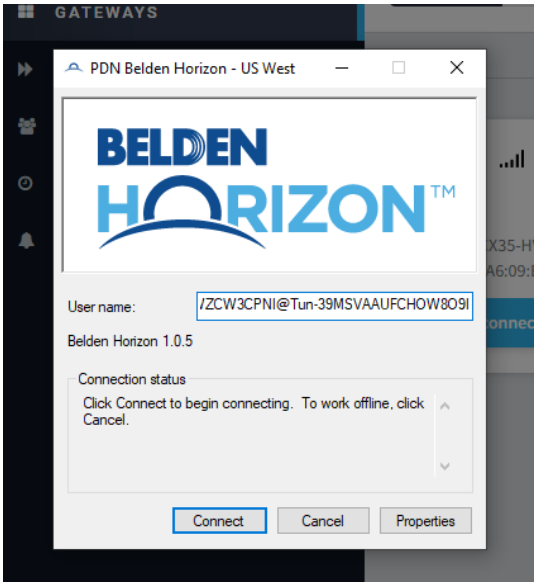
7 In the *Open Tunnel for ICX35-HWC* dialog, a username is automatically generated. Click the **COPY TO CLIPBOARD** button. This is a one-time use username key. This key is needed to connect the VPN Client to the Belden Horizon Tunneling Server.



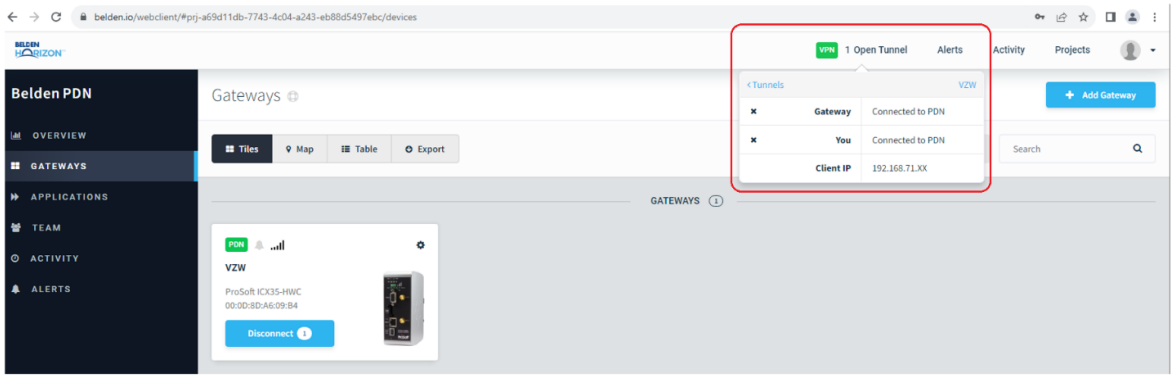
8 Open the **WINDOWS SETTINGS** > **NETWORK & INTERNET** > **VPN** selection. Under the *PDN Belden Horizon – US West* VPN option, click the **CONNECT** button.



9 In the *PDN Belden Horizon* dialog, paste the one-time username key and click the **CONNECT** button.

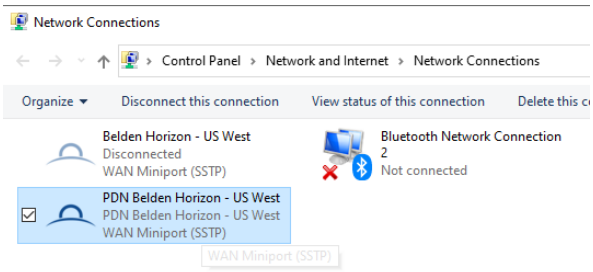


10 Upon successful VPN tunnel connection, the status is shown in the **OPEN TUNNEL** option in the **Belden.io** menu.

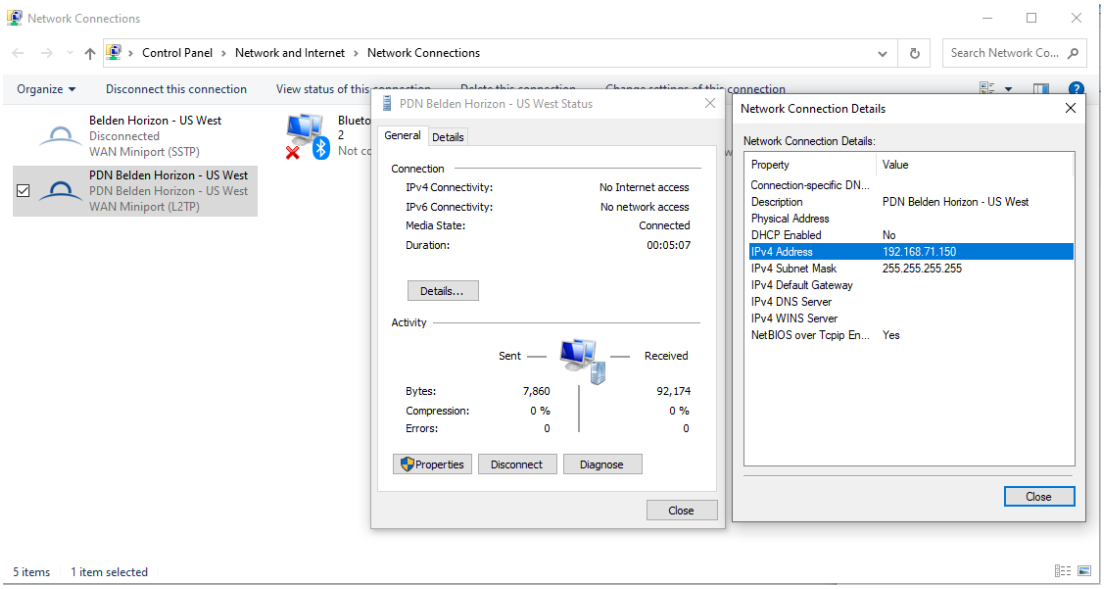


9.1.1 Verifying VPN Tunnel Connection

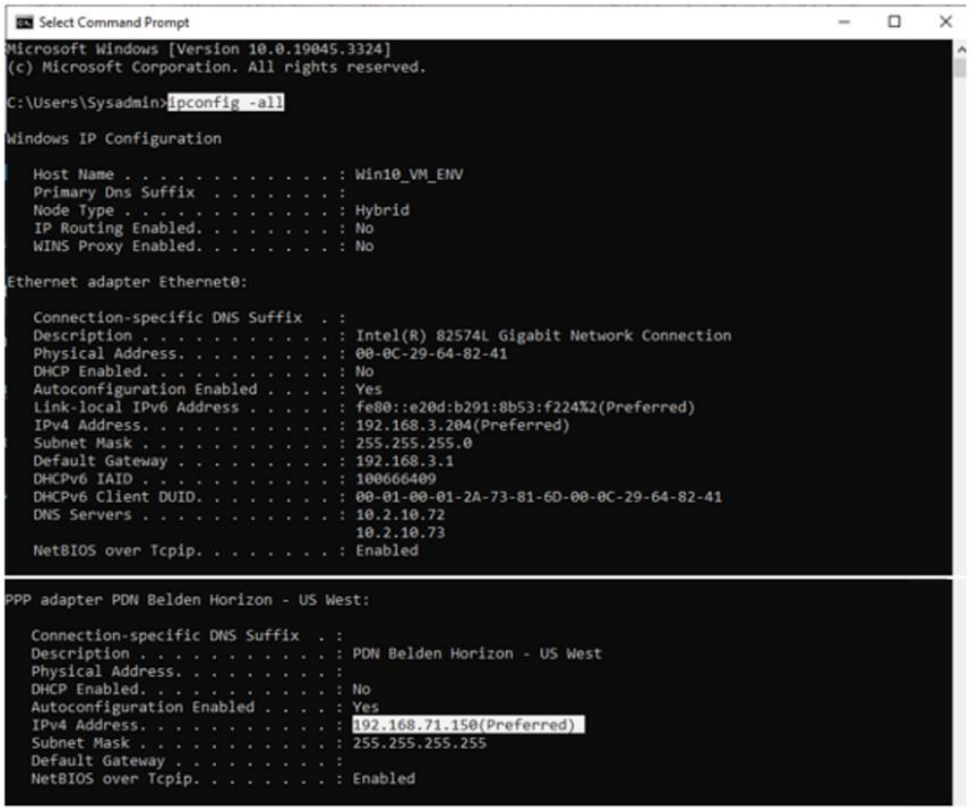
1 To verify the VPN Tunnel connection is active, double-click the Belden Horizon icon in the Windows *Network Connections* dialog.



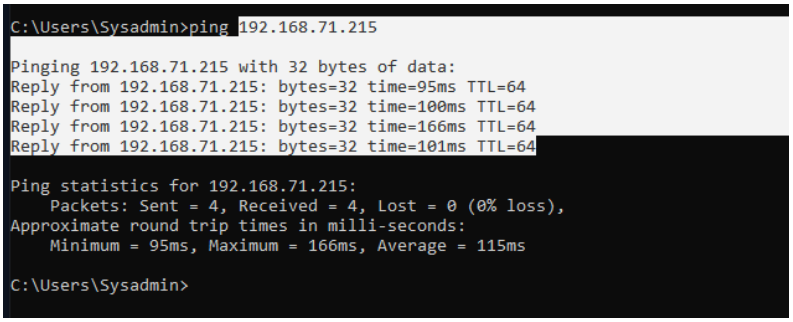
2 In the *Belden Horizon Status* dialog, click on the **DETAILS…** button to open the *Network Connection Details* dialog. The *IPv4 Address* (Alias IP address) is the link through the established VPN Tunnel.



3 The active network connection can also be viewed through a Command Prompt '`ipconfig -all`' command.



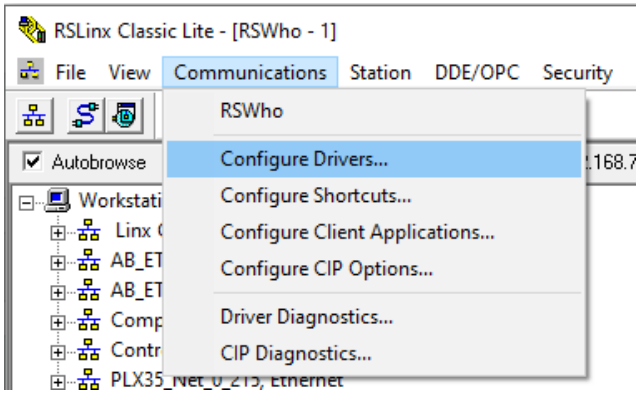
4 The PLC Controller's IP Address (ex. 192.168.71.215) can now be pinged.



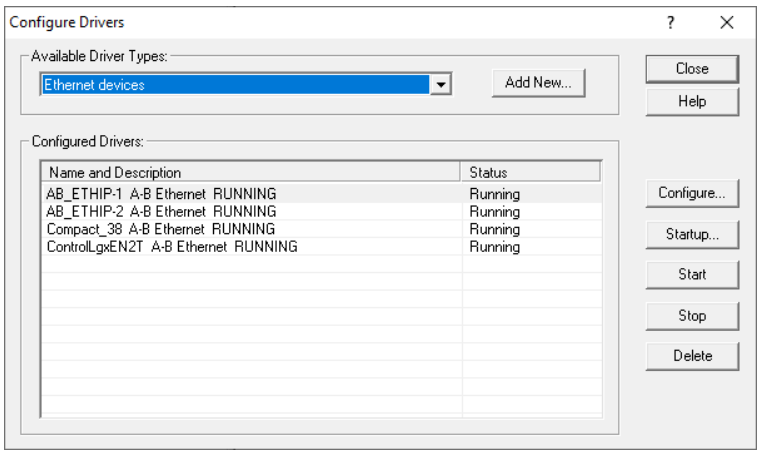
9.2 Configuring a New Driver in RSLinx

1 Open RSLinx to view the available Rockwell Controllers.

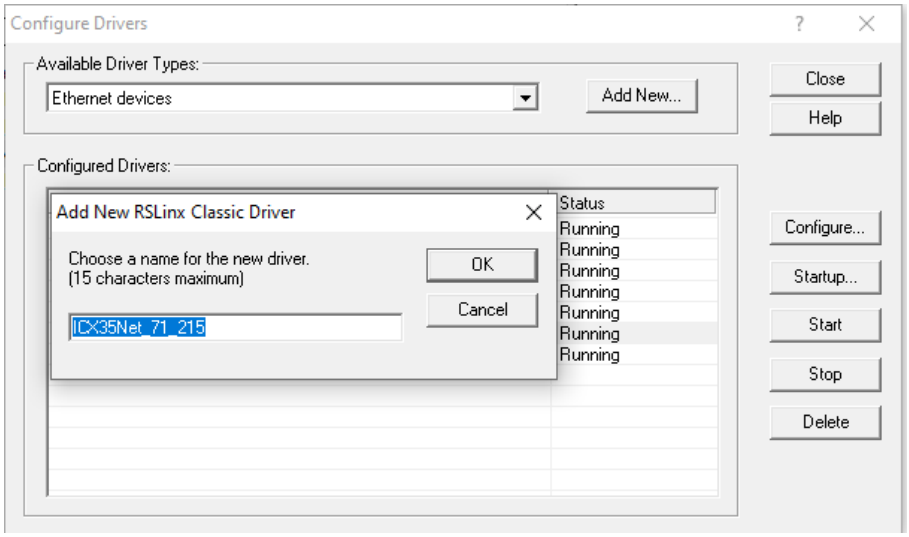
2 Click on the **COMMUNICATIONS** > **CONFIGURE DRIVERS** option to configure a new driver.



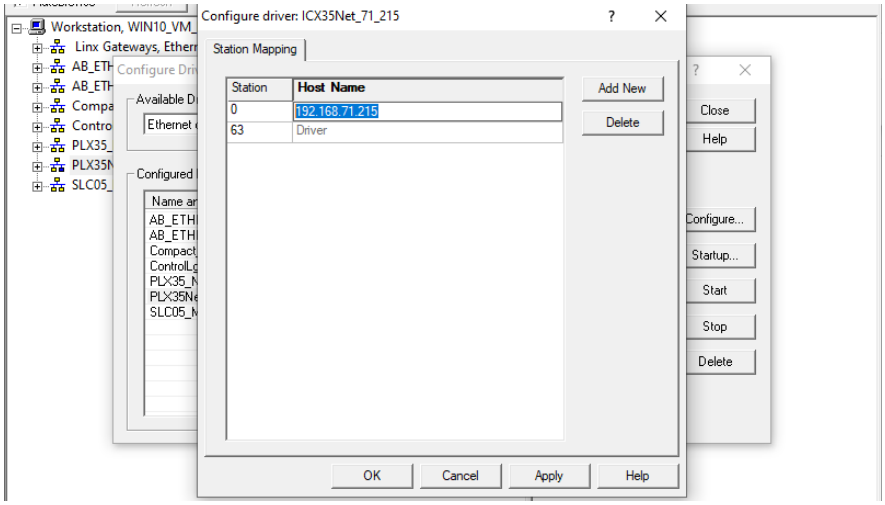
3 Click the **ADD NEW** button and select the **ETHERNET DEVICES** Driver Type.



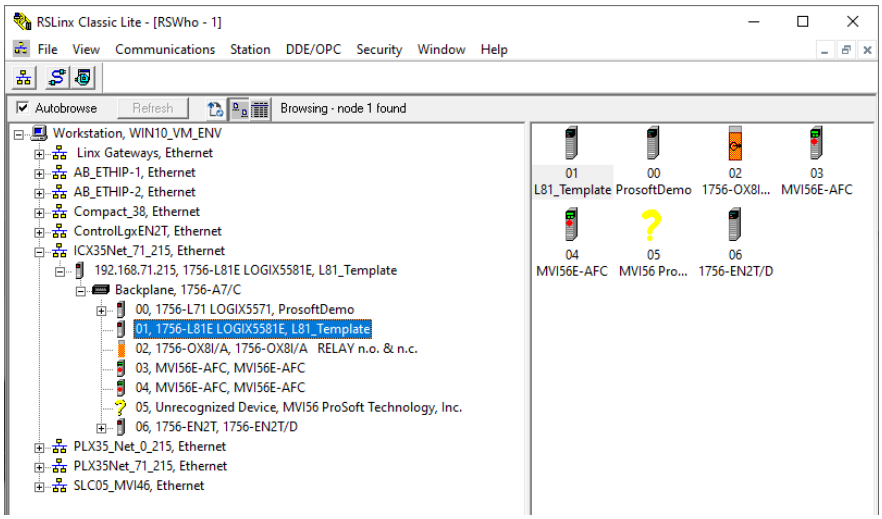
4 In the *Add New RSLinx Driver* dialog, assign a unique name.



5 Add the Controller's IP Address and click the **APPLY** button. Then click the **OK** button.



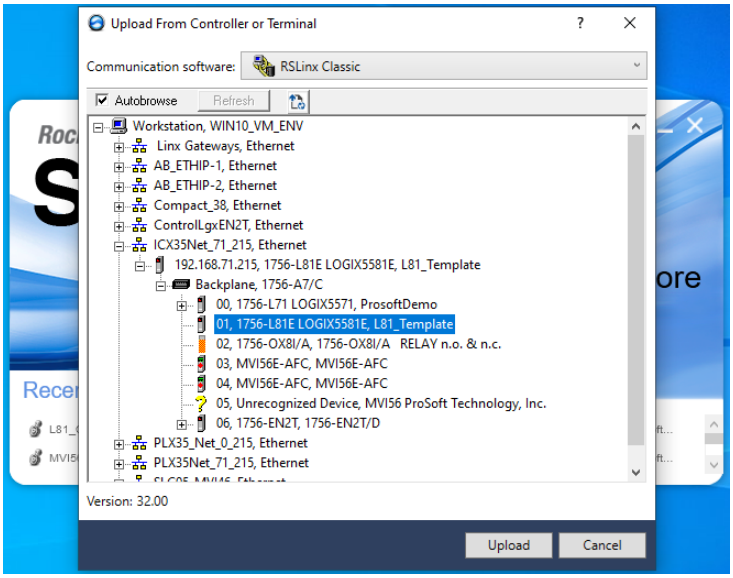
6 To locate the newly created Driver in the RSLinx panel, expand its branches to display the Controller. The Controller is ready to be accessed.



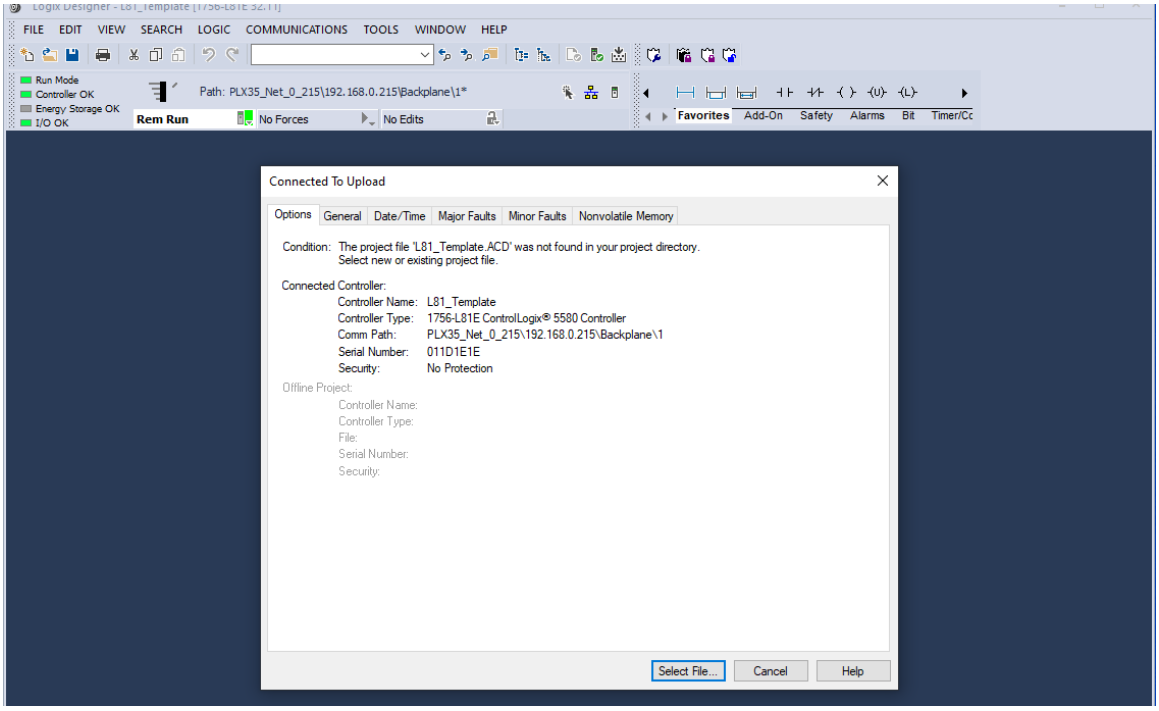
9.3 Uploading .ACD Project File

1 Open Studio/RSLogix 5000 and select the option to open **FROM UPLOAD**.

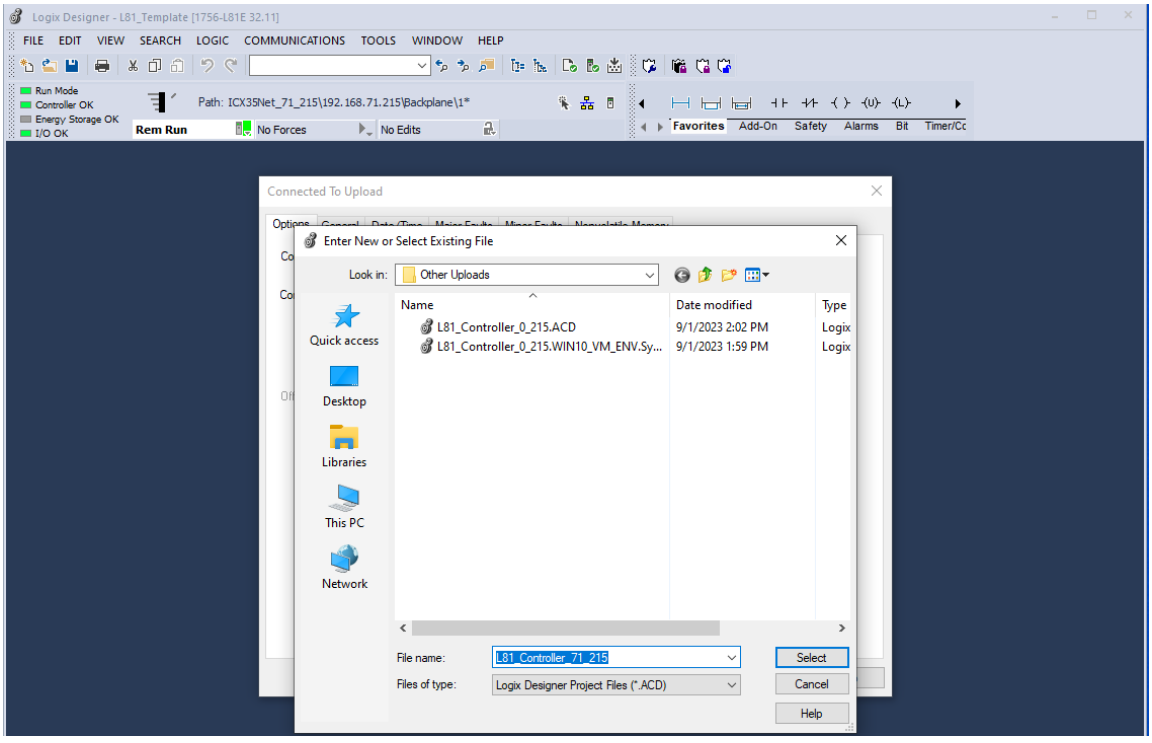
2 In the *Upload From Controller or Terminal* dialog, select the Controller to upload its .ACD project file from. Click the **UPLOAD** button.



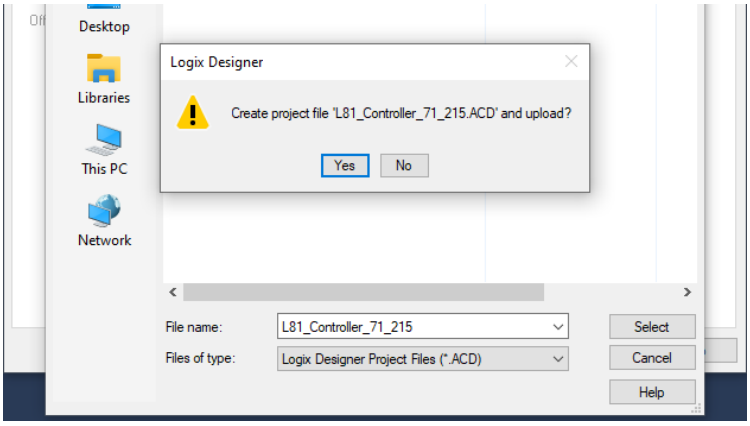
3 In the *Connected to Upload* dialog, click the **SELECT FILE…** button.



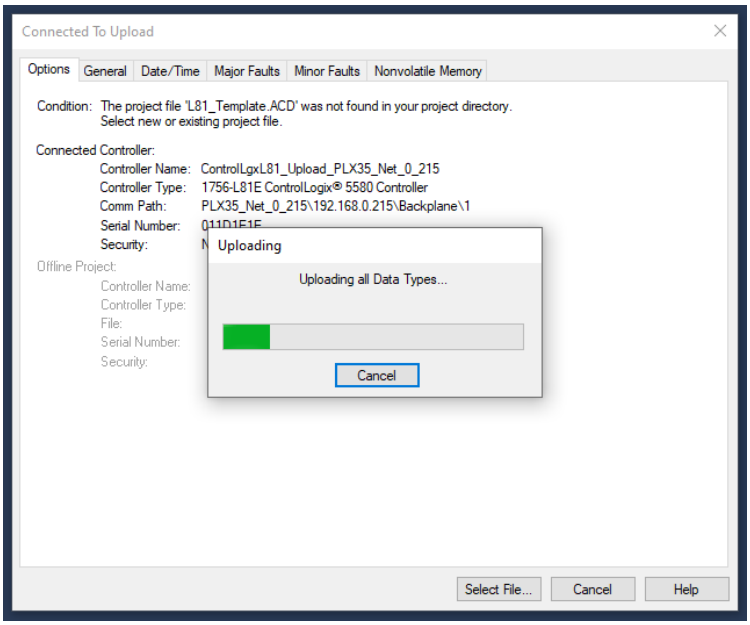
4 This opens the *Enter New or Select Existing File* dialog. Enter a new file name or select an existing .ACD file, then click the **SELECT** button.



5 Click the **YES** button to create and upload the project file.

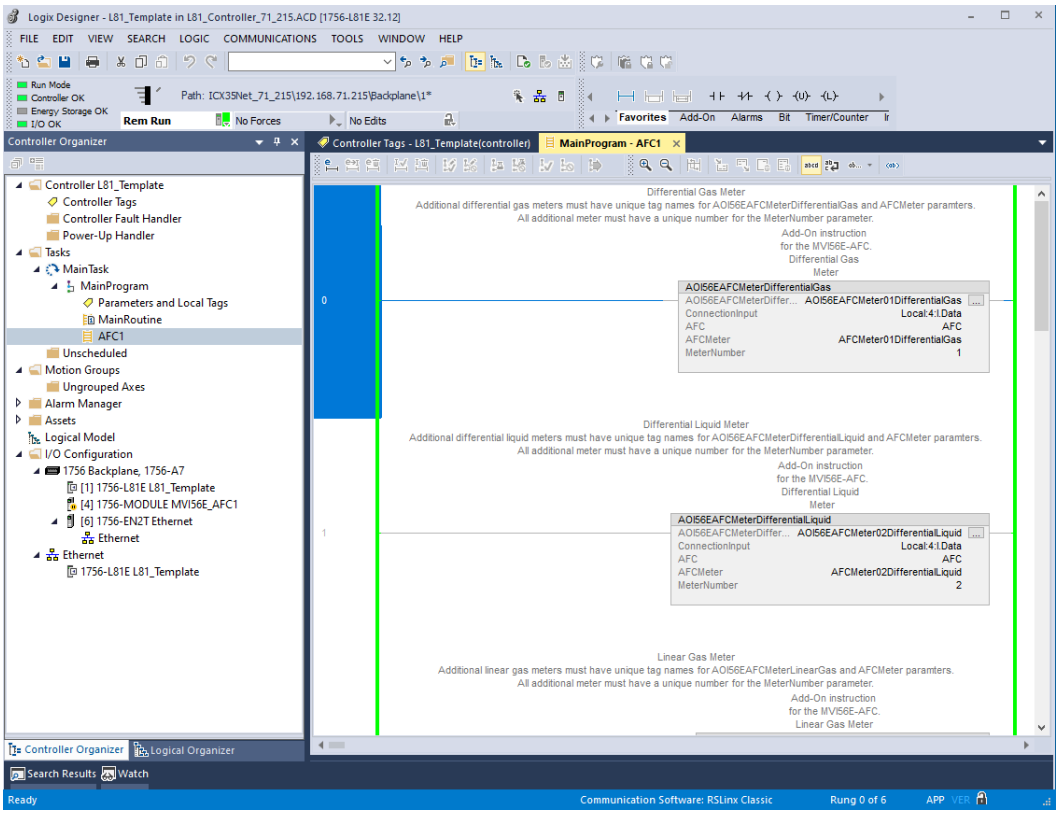


6 The upload process will initiate and complete.

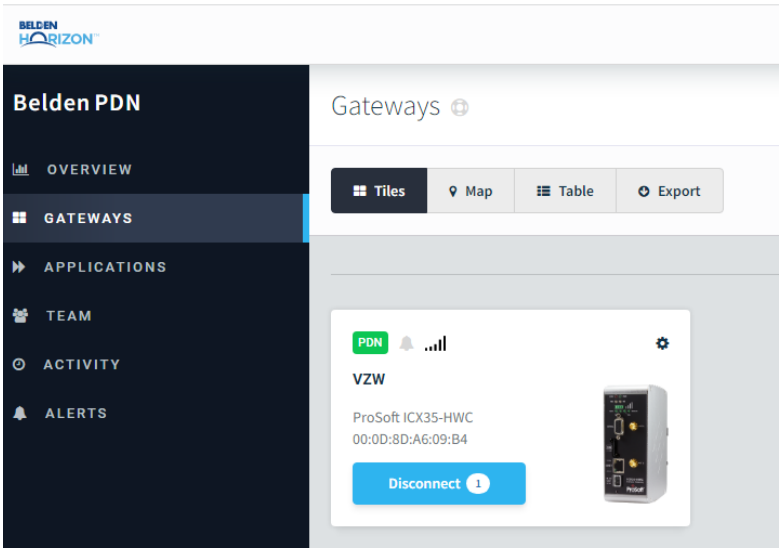


9.4 Ending the Tunnel Connection

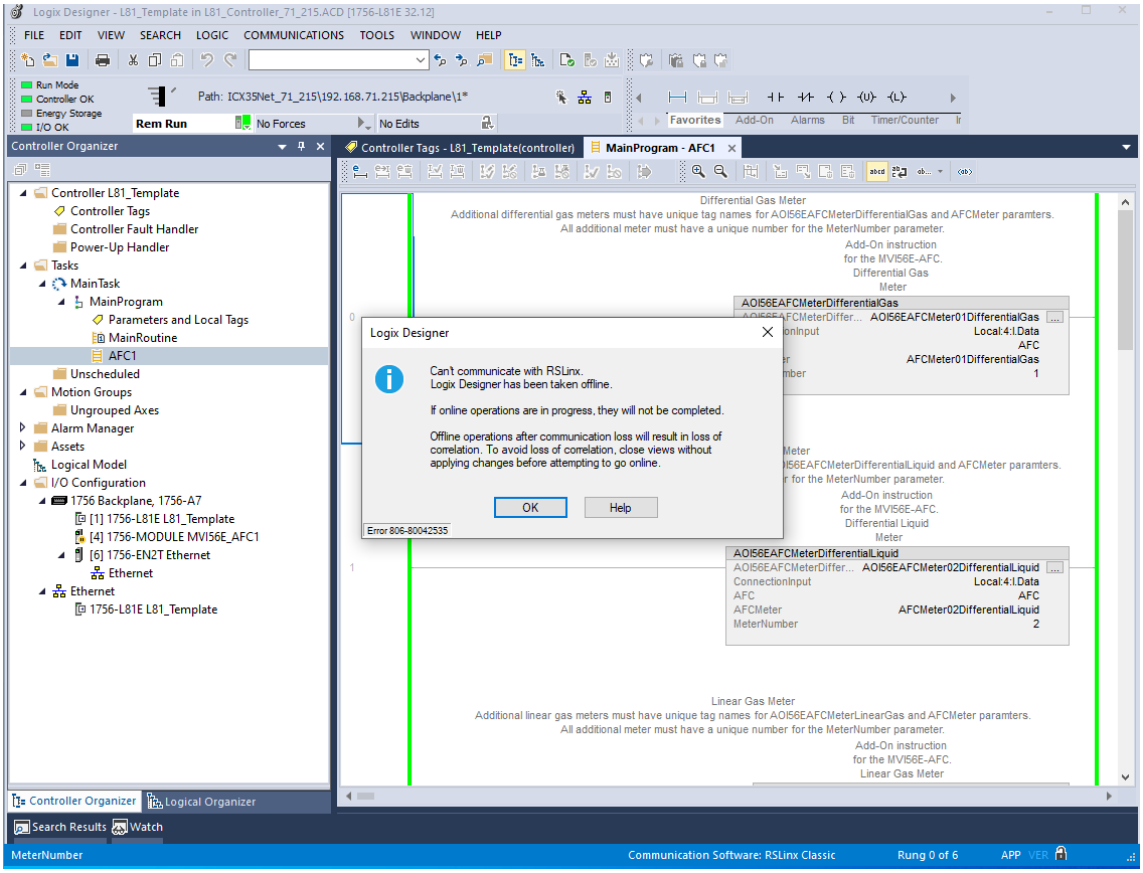
1 In Logix, connect to the Controller and set it to **Remote Run** mode to confirm the VPN Tunnel connectivity.



2 While the Controller is in **Remote Run** mode, the Tunnel Connection can be ended by clicking the **DISCONNECT** button in Belden Horizon.



3 When the Tunnel Connection terminates, the Controller displays a 'lost communications' message.



10 Firmware Procedures

There are two types of ICX35-HWC firmware installations:

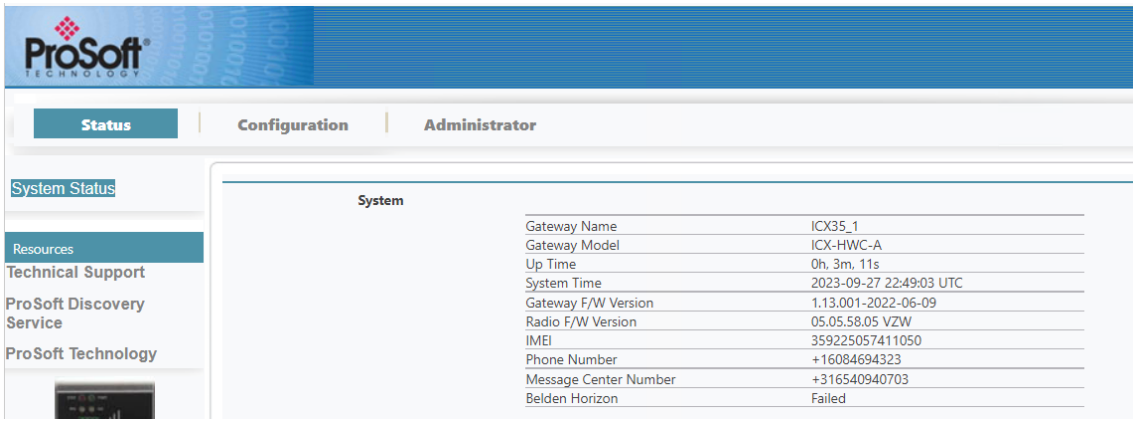
- Gateway Firmware Install
- Radio Firmware Install

The *Gateway Firmware Install* is for motherboard upgrades of the ICX35-HWC. This includes the LED, serial/Ethernet port, and software upgrades.

The *Radio Firmware Install* is for daughterboard changes of the ICX35-HWC. It is for cellular technology upgrades only.

Warning: If you are using an ICX35-HWC with ProSoft Technology's Add-on Instruction for Rockwell Automation Studio 5000 and wish to install the ICX35-HWC firmware to v1.2.2 or later, the **AOI v1.5** will no longer work. After the firmware install, you will also need to update the PLC program with the new **AOI v1.7**.

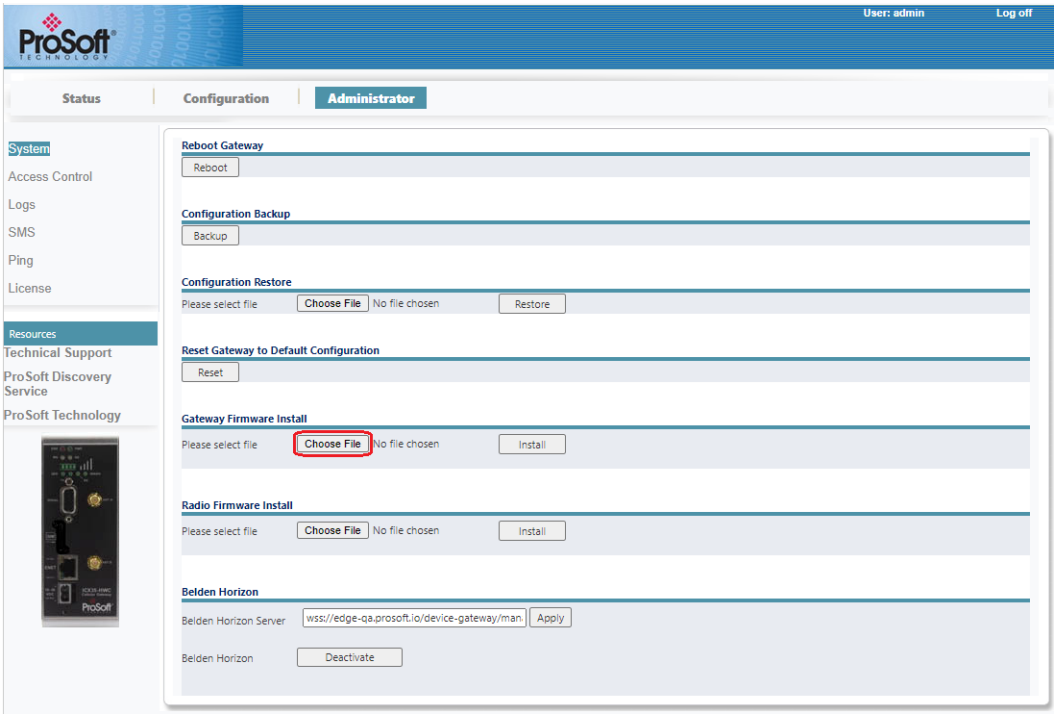
The ICX35-HWC firmware can be found at the *Gateway F/W Version* parameter on the **Status > System Status** webpage.



10.1 Gateway Firmware Install

Important: If the current firmware is older than v1.1 (Example: 766, 1.0, etc.), you will need to upgrade to v1.1 first, then to latest firmware available. Please contact ProSoft Technology technical support for the v1.1 firmware file.

1. On the ICX35-HWC webpage, click on **ADMINISTRATOR > SYSTEM**.
2. Under the *Gateway Firmware Install* section, click the **CHOOSE FILE** button.

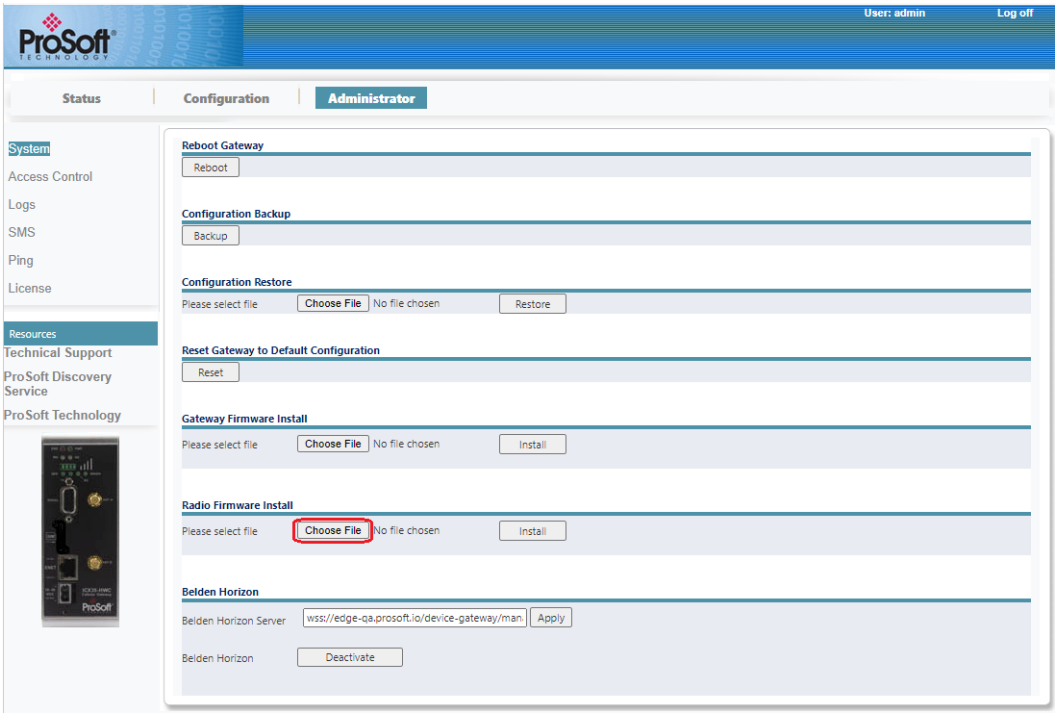


3. Browse to the *.img firmware file location and click **OK**.
4. Click the **INSTALL** button, then click **OK** in confirmation dialog box.
5. The install process takes approximately 10 minutes. It will automatically reboot the ICX35-HWC.
6. Verify the *Gateway F/W Version* on the **STATUS > SYSTEM STATUS** webpage.

10.2 Radio Firmware Install

1 On the ICX35-HWC webpage, click on **ADMINISTRATOR > SYSTEM**.

2 Under the *Radio Firmware Install* section, click the **CHOOSE FILE** button.



3 Browse to the *.spk firmware file location and click **OK**.

4 Click the **INSTALL** button, then click **OK** in confirmation dialog box.

5 The install process takes approximately 10 minutes. It will automatically reboot the ICX35-HWC.

6 Verify the *Radio F/W Version* on the **STATUS > SYSTEM STATUS** webpage.

10.2.1 Verizon Support

Important: This section is for the ICX35-HWC-A only.

By default, the ICX35-HWC-A ships in AT&T (GSM) mode. This procedure is used to convert the ICX35-HWC-A to Verizon (CDMA) mode. You can use the same procedure to convert back to GSM mode (using GSM internal radio software file).

1. Download the CDMA internal radio software file from the ICX35-HWC webpage at www.prosoft-technology.com.
2. To install the internal radio software, follow the steps in the Radio Firmware Install section.

Note: You can select to have ICX35-HWC radios shipped in the Verizon (CDMA) mode by ordering part number **ICX35-VZW** when placing the order for the ICX35-HWC-A.

11 ICX35-HWC Tech Notes

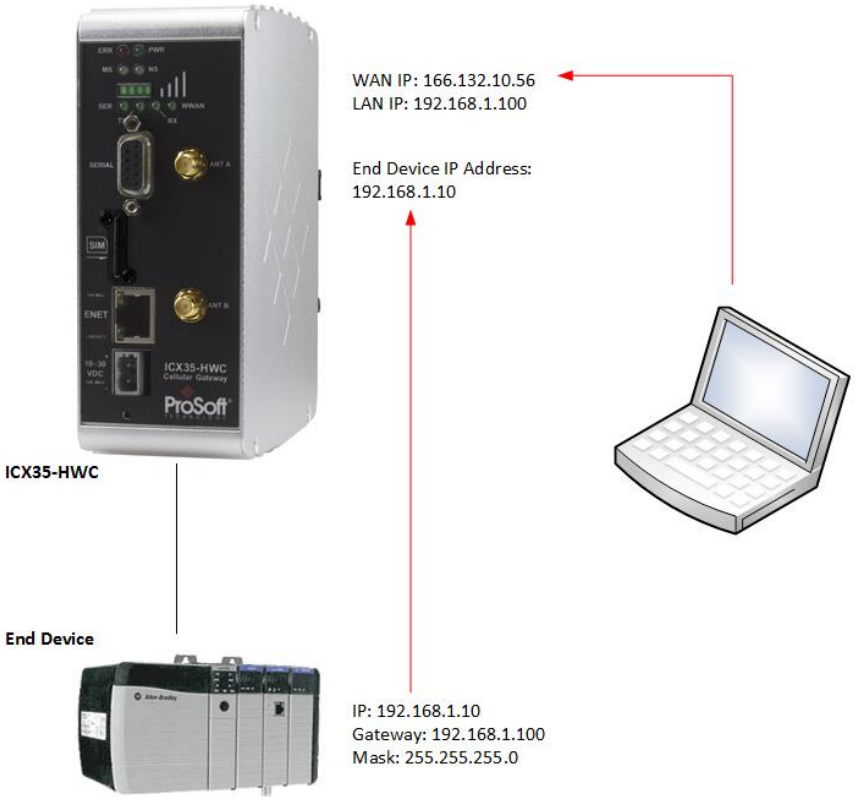
This section describes example configurations of the ICX35-HWC using:

- Pass Through (End Device to End Device) mode
- VPN OpenVPN in End Device to End Device mode
- VPN OpenVPN in DHCP mode

This chapter does not go into End Device configuration procedures since it is assumed the user knows how to configure End Devices. However, examples are provided to show how the End Device is configured along with the ICX35-HWC.

11.1 Pass Through Mode (End Device to End Device) Example

The following diagram illustrates a Pass Through mode configuration example:



In this scenario, the laptop wants to communicate with a ControlLogix rack.

To configure the ICX35-HWC, you must supply:

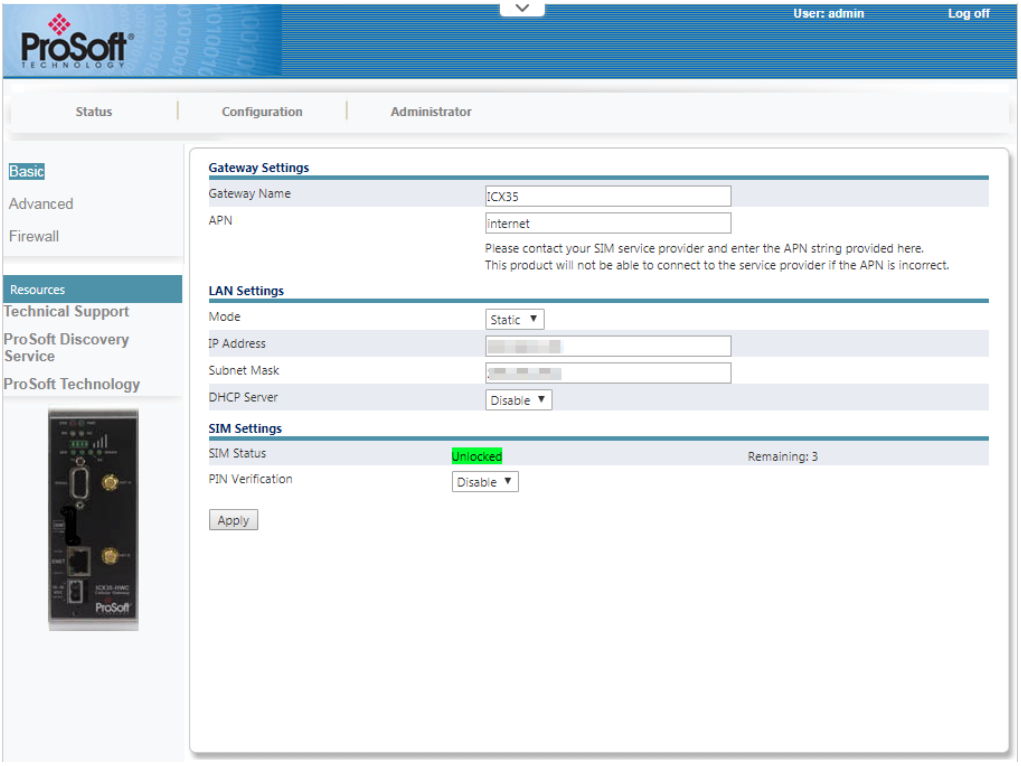
- WAN IP – This number is supplied by the cellular provider.
- Module Name
- APN – This is provided by the cellular provider
- LAN IP
- End Device Address

To configure the end device, you must supply:

- IP Address
- Mask
- Gateway IP Address

11.1.1 ICX35-HWC Configuration Parameters

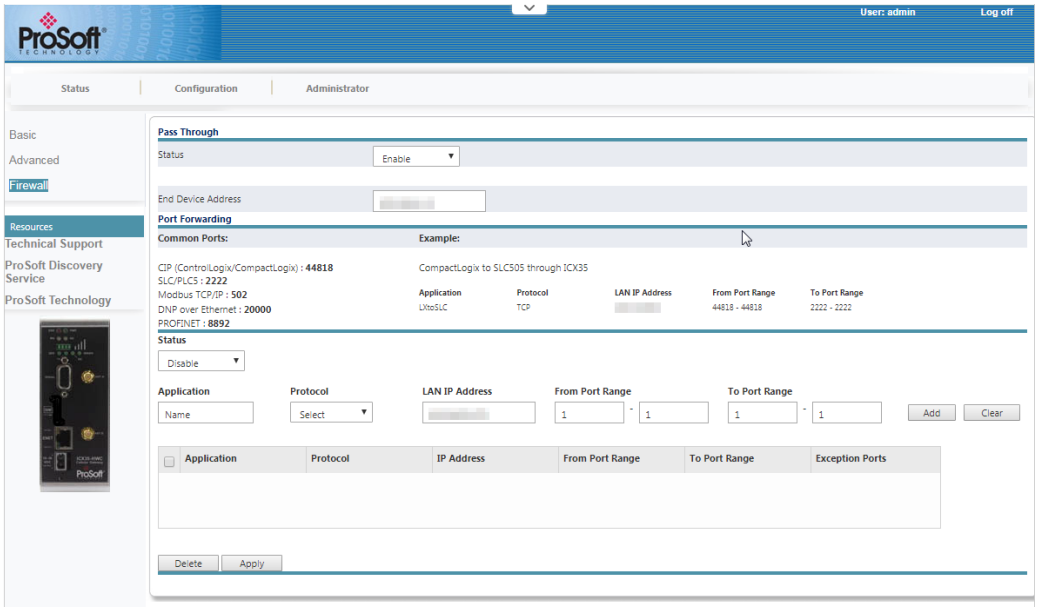
1. Log in to the ICX35-HWC built-in web server.
2. Navigate to **Configuration > Basic**.



3. Enter the *Gateway Name* and APN of your network.
4. Using the previous example, the ICX35-HWC IP Address is **192.168.1.100**. This is configured in the *IP Address* and *Subnet Mask* fields.
5. Click the **APPLY** button.

11.1.2 Enable Pass Through

1. Navigate to **Configuration > Firewall**.
2. Enable the *Status* parameter under the *Pass Through* heading.
3. Enter the IP Address of the device connected to the *ICX35-1* (172.020.000.220) in the *End Device Address* parameter
4. Click the **APPLY** button.
5. Perform the same procedure for the *ICX35-2*.



11.1.3 End Device Parameter Notes

When configuring the end device, keep the following points in mind:

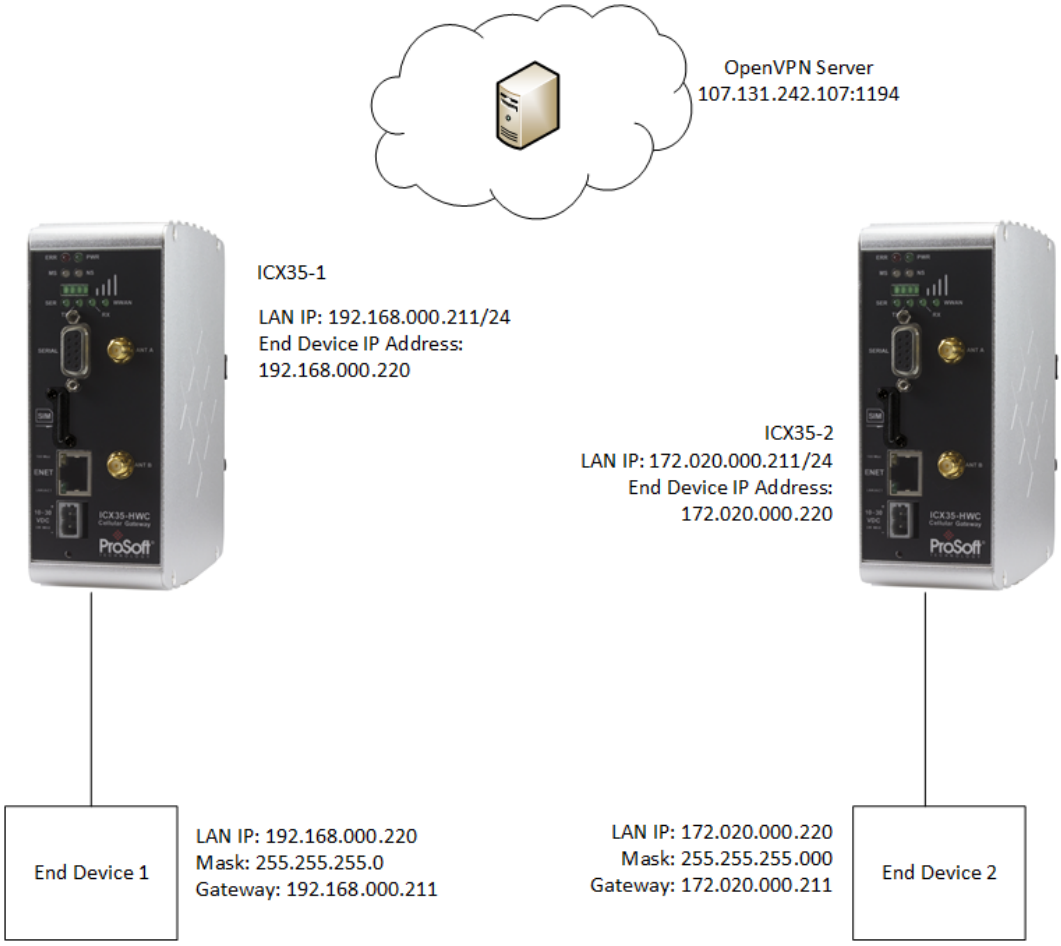
- The IP Address of the end device must match the value entered in the *End Device Address* parameter in the ICX35-HWC.
- The gateway address on the end device must point to the ICX35-HWC *IP Address* and *Subnet Mask* addresses.

11.1.4 Obtaining Data from the End Device

A user trying to reach the end device through the ICX35-HWC must address the WAN ID (in this case, 166.132.10.56 provided by the cellular provider).

11.2 Pass Through and OpenVPN Example

The following diagram illustrates using a Pass Through scenario with OpenVPN:



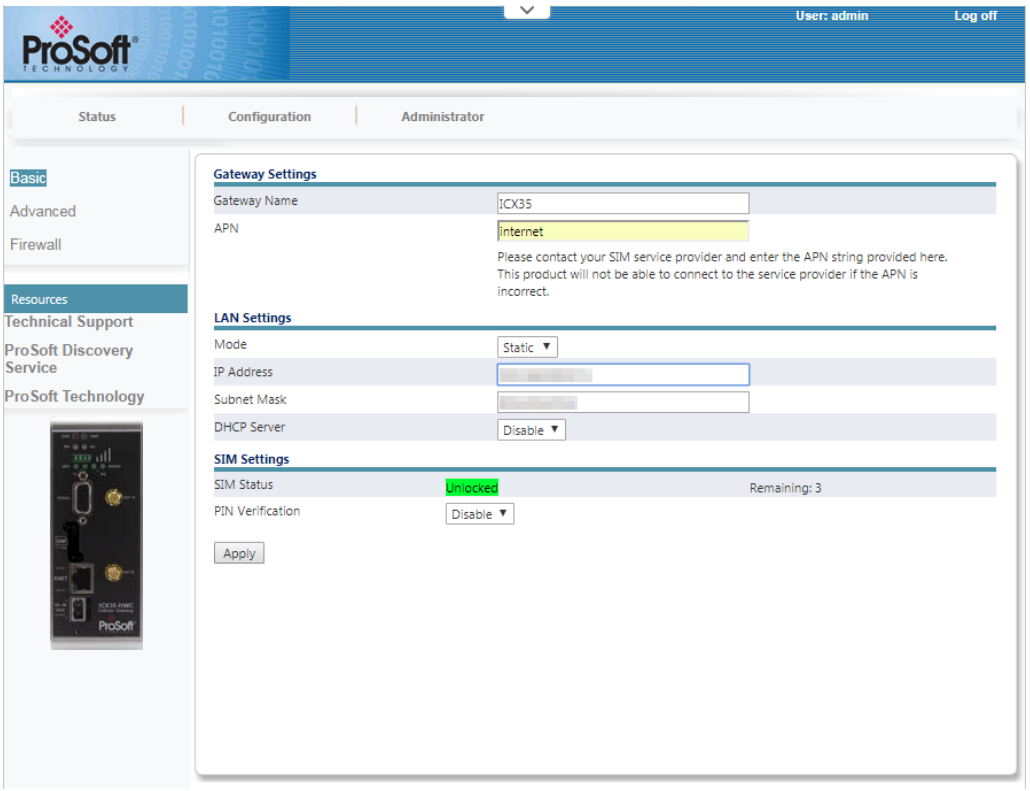
In this scenario, Virtual OpenVPN addresses are assigned by the VPN server. If the end device 172.020.000.220 wants to communicate with 192.168.000.211, it must address the device through the ICX35-HWC VPN address. The ICX35-HWC routes the request as it would a Pass Through device.

You must establish standard End Device-to-End Device communications before attempting to configure an OpenVPN tunnel.

11.2.1 ICX35-1 Configuration Parameters

In this scenario, configure the ICX35-1 for Pass Through.

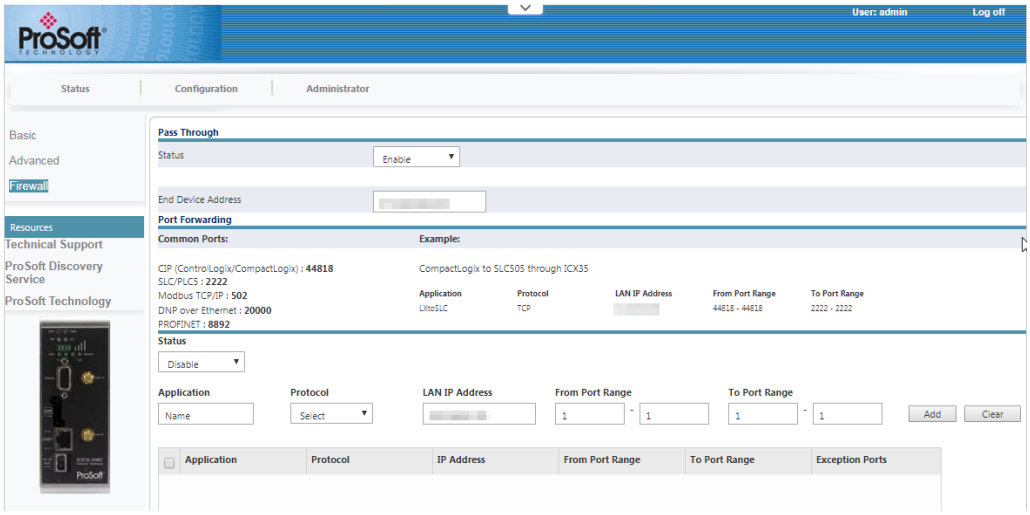
1. Log in to the *ICX35-1* built-in web server.
2. Navigate to **Configuration > Basic**.



3. Enter the *Gateway Name* and *APN* of the network.
4. In the example, the *ICX35-1* IP Address is **192.168.000.211**. This is configured in the *IP Address* and *Subnet Mask* fields.
5. Click the **APPLY** button.
6. Perform the same procedure for the *ICX35-2*.

11.2.2 Enable Pass Through

1. Navigate to **Configuration > Firewall**.
2. Enable the *Status* parameter under the *Pass Through* heading.
3. Enter the IP Address of the device connected to the *ICX35-1* (172.020.000.220) in the *End Device Address* parameter
4. Click the **APPLY** button.
5. Perform the same procedure for the *ICX35-2*.



11.2.3 Configuring End Device 1

When configuring the end device, keep the following points in mind:

- The IP Address of the end device connected to *ICX35-1* must match the value entered in the *End Device Address* parameter in the *ICX35-1*.
- The gateway address on the end device must point to the *ICX35-1 IP Address* and *Subnet Mask* addresses.

11.2.4 Configuring End Device 2

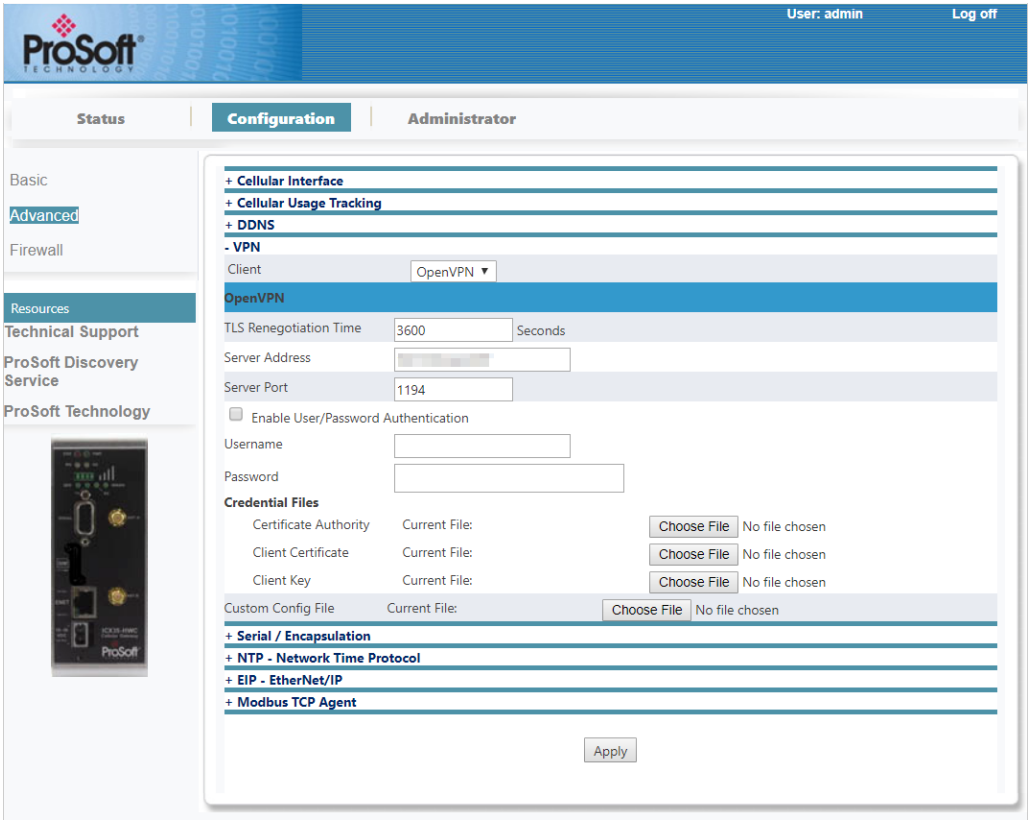
When configuring the end device, keep the following points in mind:

- The IP Address of the end device connected to *ICX35-2* must match the value entered in the *End Device Address* parameter in the *ICX35-2*.
- The gateway address on the end device must point to the *ICX35-2 IP Address* and *Subnet Mask* addresses.

11.2.5 Configuring OpenVPN Parameters

You must now configure OpenVPN parameters on both ICX35-HWC radios.

1. Navigate to **Configuration > Advanced**.
2. Click on the **VPN** link.
3. Select **OPENVPN** from the drop-down list box.



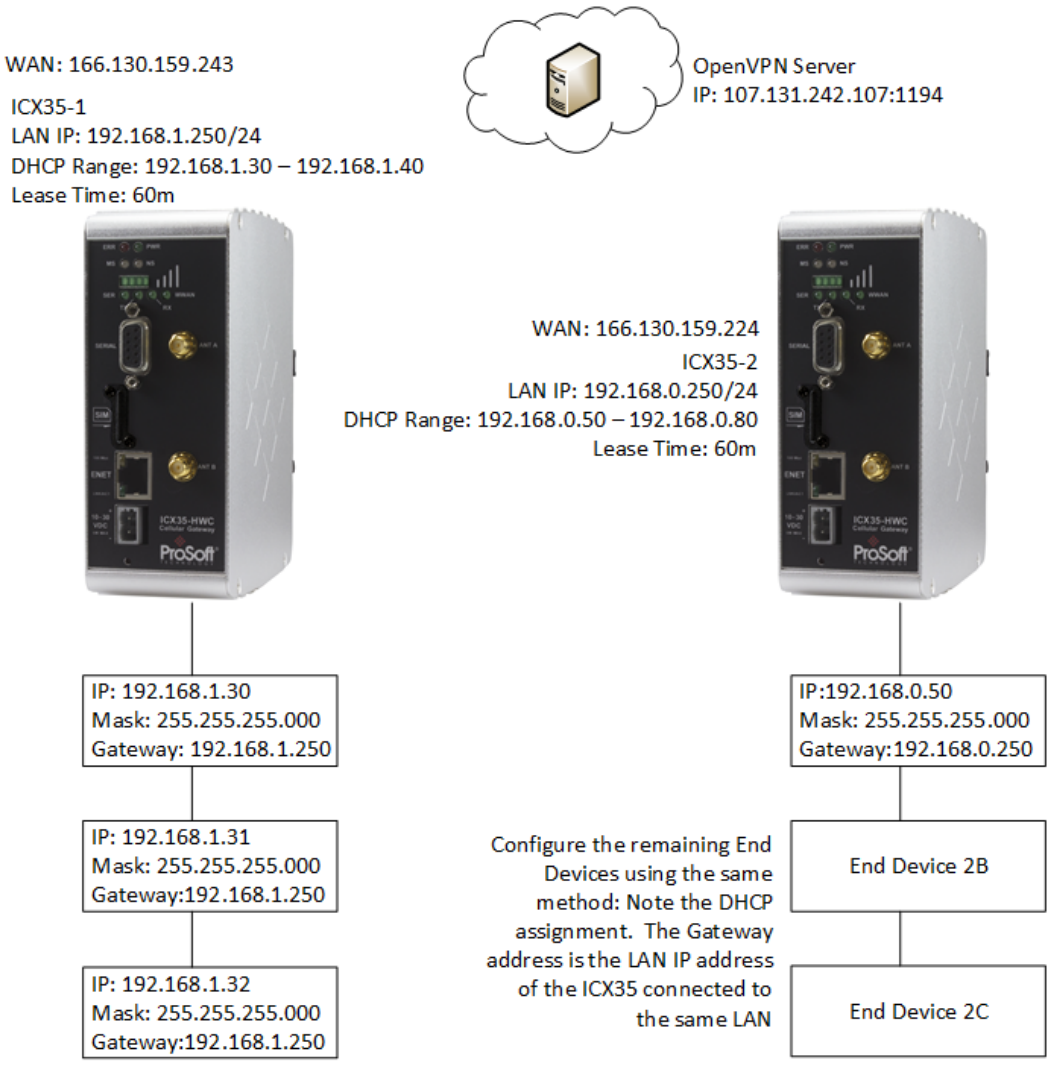
4. Enter the number of seconds in the *TLS RenegotiationTime* field.
5. Enter the OpenVPN server's IP Address in the *Server IP* field.
6. Enter the Server Port number in the *Server Port* field. This is the port assigned to the OpenVPN Server shown at the top of the diagram.
7. If user/password authentication is configured on the server, enable the *User/Password Authentication* box and provide credentials in the *User* and *Password* fields.
8. Browse and select the *Certificate Authority*, *Client Certificate*, and *Client Key* Credential Files. Your Server Administrator provides the three certificate files.

> **Note:** Certificate/keys are mandatory as separate files if a custom configuration file is not used, or if a custom configuration file is provided but does not contain the certificates and keys inline. If the certificates and keys are provided both inline in the custom configuration file and uploaded in the UI, the uploaded files will take precedence.

9. Click the **APPLY** button.
10. Perform the same procedure for the *ICX35-2*.

11.3 OpenVPN with DHCP Enabled Example

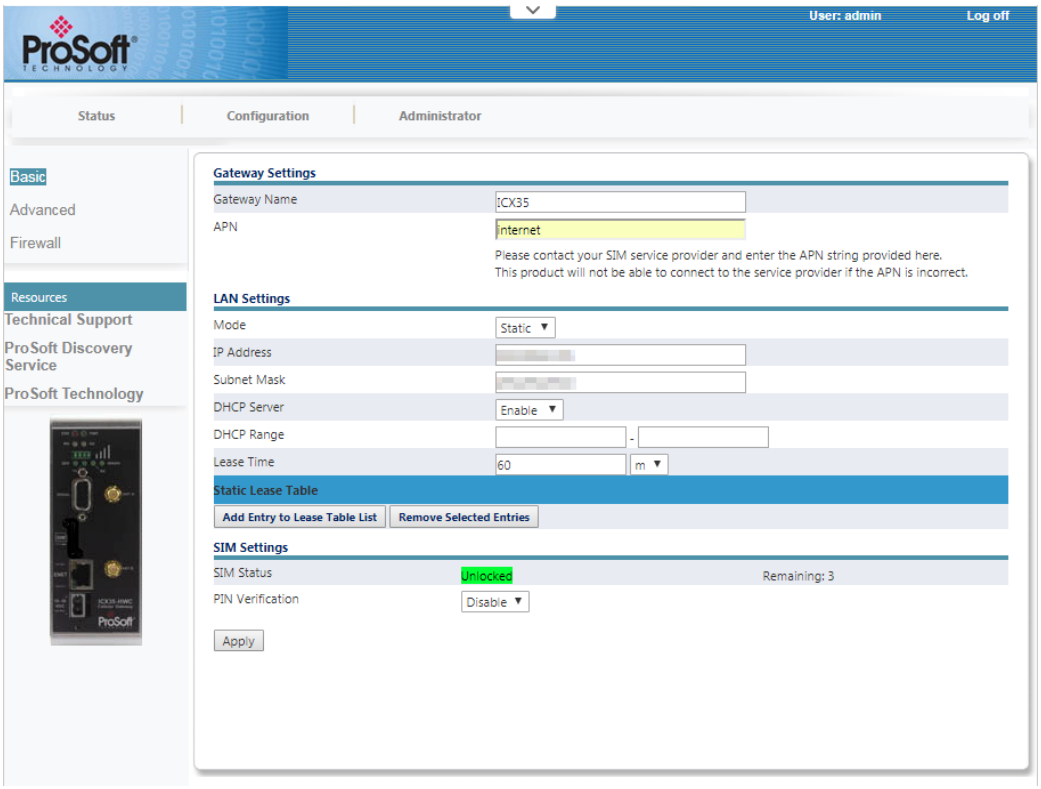
The following diagram illustrates the use of OpenVPN with DHCP enabled.



11.3.1 ICX35-1 Configuration

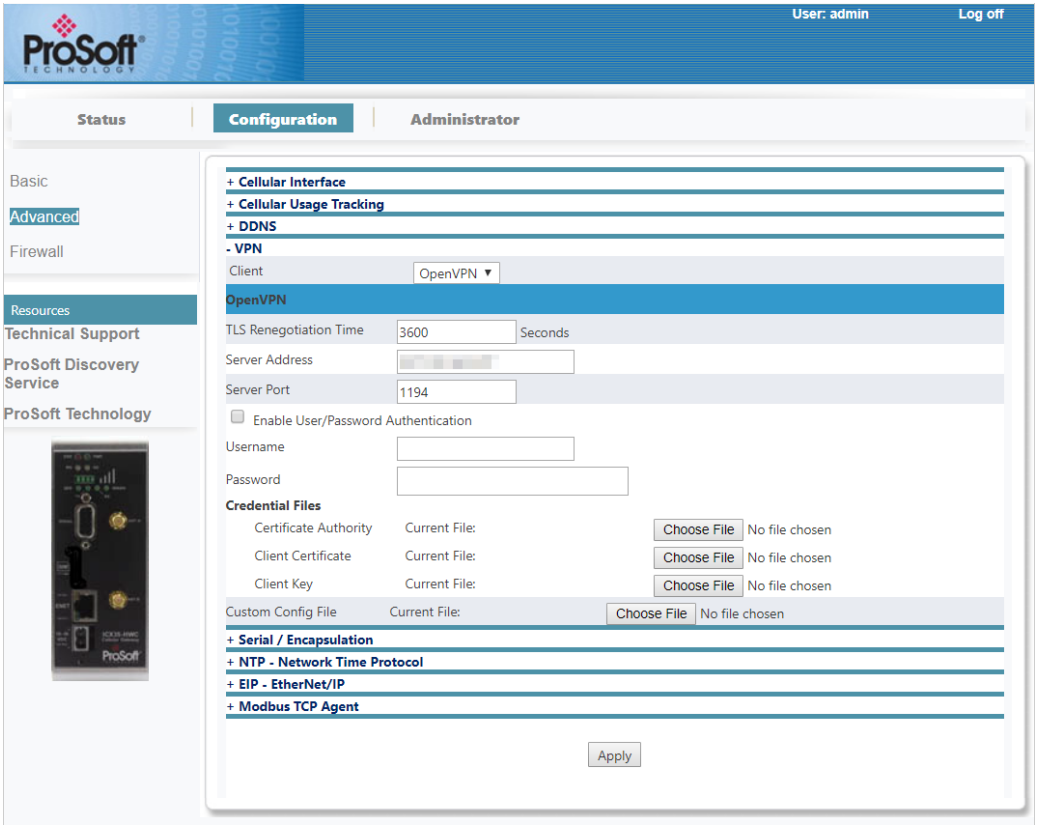
The ICX35-1 shown in the diagram is configured in the ICX35-1 webpage as follows:

1. Login to the *ICX35-1* web server.
2. Navigate to **Configuration > Basic**.



3. Enter the name of the module in the *Gateway Name* field.
4. Enter the access point name in the *APN* field. Get this from your cellular provider.
5. Enter the LAN IP and subnet mask in the *IP Address* and *Subnet Mask* fields for the *ICX35-1*.
6. Select **ENABLE** from the DHCP Server drop-down list box.
7. Enter the *DHCP Range* for the connected end devices.
8. Enter the appropriate lease time in the *Lease Time* field. See the *Lease Time* field description in the manual for detailed info.
9. Click the **APPLY** button.
10. Navigate to **Configuration > Advanced**.

11 Click on the **VPN** link and select **OPENVPN** from the *Client* drop-down list.



12 Enter the *TLS Renegotiation Time* in the appropriate field (see TLS).

13 Enter the OpenVPN server's IP address in *Server IP*.

14 Enter the *Server Port* shown.

15 If user/password authentication is configured on the server, enable the *User/Password Authentication* box and provide credentials in the *User* and *Password* fields.

16 Choose and upload the *Credential Files*. Your Server Administrator will provide you with the certificate files and location.

17 Click the **APPLY** button.

11.3.2 ICX35-2 Configuration

The *ICX35-2* is configured using the exact same procedure as the *ICX35-1* in this example. Use the diagram as a guide to fill in the appropriate fields as described.

11.3.3 End Device Configuration

End devices must be configured based on the DHCP assignments. The *Gateway* settings must match the LAN IP of the ICX35-HWC. This must be done on both ICX35-HWC radios.

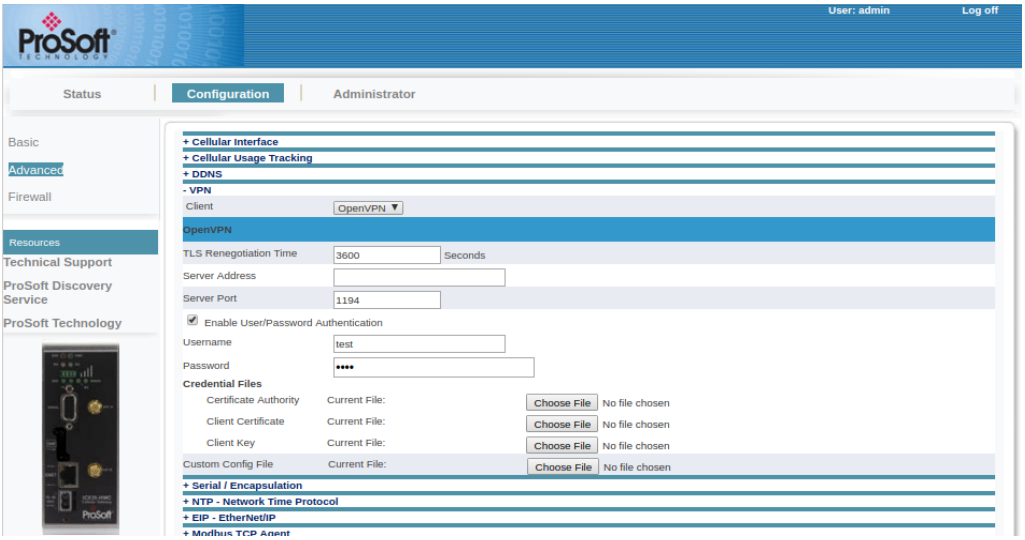
When setting up *Ethernet Bridges*, set the IP address to the DHCP assigned addresses.

11.4 OpenVPN with Username and Password Authentication

11.4.1 Configuring the Username/Password as the Only Method of Authentication

Configuring the Client

1. Enable **USER/PASSWORD AUTHENTICATION** by checking the box.
2. Enter the *Username* and *Password*.
3. Provide the Certificate Authority file.



Note: The Client Certificate and Client Key files are not used with this type of authentication. Therefore, this type of authentication is less secure than the default method using certificates.

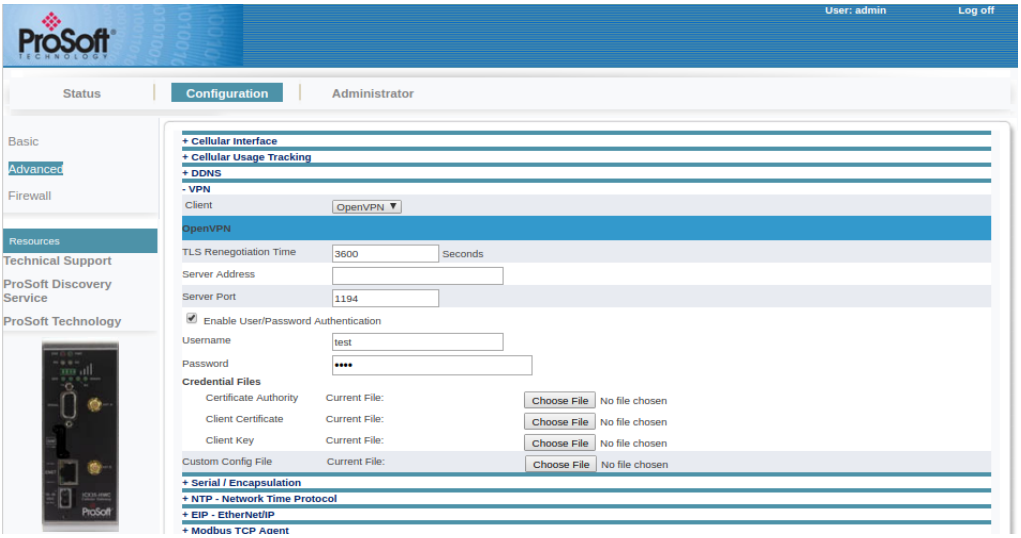
Configuring the Server

1. Log into the Openvpn server.
2. Create a user by typing: **`useradd <username>`**
3. Add a password to the new user: **`passwd <username>`** and enter the password.
4. Edit the server configuration file by adding the following lines:
   `username-as-common-name`
   `client-cert-not-required`
   `plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so login`

11.4.2 Configuring the Username and Password with Certificates

Configuring the Client

1. Enable **USER/PASSWORD AUTHENTICATION** by checking the box.
2. Enter the *Username* and *Password*.
3. Provide the *Certificate Authority*, *Client Certificate*, and *Client Key* files.



Note: All authentication methods (Username/Password, Certification, and Key) must be valid in order for the client to connect to the server.

Configuring the Server

1. Log in Openvpn server.
2. Create a user by typing: **`useradd <username>`**
3. Add a password to the new user: **`passwd <username>`** and enter the password.
4. Edit the server configuration file by adding the following line:
   `plugin /usr/lib/openvpn/openvpn-plugin-auth-pam.so login`

11.5 Connecting to Multiple OpenVPN Servers

This section details the connection between an ICX35-HWC and two OpenVPN servers.

1. Navigate to **Configuration > Advanced**.
2. Click on the VPN link.
3. Select **OPENVPN** from the drop-down list box.
4. Select the *Default Gateway*. The default is the Cellular Gateway provided by the SIM carrier. Choose between that and the *OpenVPN Server 1* or *OpenVPN Server 2* gateways.

Configuration Options for OpenVPN Server 1

1. Enter the number of seconds in the *TLS Renegotiation Time* field.
2. Enter the OpenVPN server's IP Address in the *Server IP* field.
3. Enter the Server Port number (OpenVPN Server 1)in the *Server Port* field.
4. Select the *Encryption Cipher* to match the OpenVPN Server 1 cipher.
5. If user/password authentication is configured on the OpenVPN Server 1, enable the **USER/PASSWORD AUTHENTICATION** box and provide credentials in the *User* and *Password* fields.
6. Browse and select the *Certificate Authority*, *Client Certificate*, and *Client Key* credential files. Your OpenVPN Server 1 Administrator provides the three certificate files.

> **Note:** Certificate/keys are mandatory as separate files if a custom configuration file is not used, or if a custom configuration file is provided but does not contain the certificates and keys inline. If the certificates and keys are provided both inline in the custom configuration file and uploaded in the UI, the uploaded certificate and key files will take precedence.

7. Select *Protocol* to match the OpenVPN Server 1 protocol.
8. Click **ADD NEW OPENVPN SERVER** to add configuration options for a secondary server. This will apply the values entered for OpenVPN Server 1.

Configuration Options for OpenVPN Server 2

1. Select **OPENVPN SERVER 2** to be configured.
2. Enter the number of seconds in the *TLS Renegotiation Time* field.
3. Enter the OpenVPN Server 2 IP Address in the *Server IP* field.
4. Enter the Server Port number (OpenVPN Server 2) in the *Server Port* field.
5. Select the *Encryption Cipher* to match the OpenVPN Server 2 cipher.
6. If user/password authentication is configured on the OpenVPN Server 2, enable the **USER/PASSWORD AUTHENTICATION** box and provide credentials in the *User* and *Password* fields.

7 Browse and select the *Certificate Authority*, *Client Certificate*, and *Client Key* credential files. Your OpenVPN Server 2 Administrator provides the three certificate files.

> **Note:** Certificate/keys are mandatory as separate files if a custom configuration file is not used, or if a custom configuration file is provided but does not contain the certificates and keys inline. If the certificates and keys are provided both inline in the custom configuration file and uploaded in the UI, the uploaded certificate and key files will take precedence.

8 Select *Protocol* to match the OpenVPN Server 2 protocol.

11.5.1 Troubleshooting Multiple OpenVPN Servers

Below are items to consider when connecting the ICX35-HWC to multiple OpenVPN servers:

- **Using the same IP address for OpenVPN servers.**
  OpenVPN server has a default IP address 10.8.0.1/24. It also leases to clients from the same subnet 10.8.0.0/24.When using the ICX35-HWC with multiple OpenVPN servers, it is imperative to reconfigure each OpenVPN server to avoid overlap of these default subnets. Failure to reconfigure the overlapping subnets may lead to incorrect routing at the ICX35-HWC level.
- **OpenVPN servers are using the same IP subnet or overlapping IP subnets for route injection.**
  The system administrator should monitor this to avoid the overlap of the subnets used for route injection.
- Configuring one of the OpenVPN Server connections as Default Gateway implies that all network traffic will be passed through the tunnel. The server administrator should be aware of the filters put in place on the server side, and how the OpenVPN server configuration might impact the network traffic. When using Belden Horizon together with the OpenVPN setup in this scenario, make sure that traffic to the Belden Horizon is reachable through the connection configured as a Default Gateway.

12 Cellular Technology Definitions

Many GSM Networks have been upgraded to support HSUPA. GSM Networks use SIM cards which are smart cards containing the account holder's details. A SIM can generally be moved from one device to another allowing for account flexibility.

CDMA (Code Division Multiple Access) is the cellular technology used by Verizon in the United States. The ICX35-HWC is certified by Verizon. To provide backward compatibility and seamless connections in a wider range of locations, the ICX35-HWC will fall back to 1x when EV-DO is not available.

1x
1x provides a digital cellular telephony system and can provide wireless Internet access at speeds between 60 and 80 kbps, with bursts up to 144 kbps.

EDGE
EDGE (Enhanced Data rates for GSM Evolution) provides end-to-end packet data services with an enhanced connectivity building on GPRS technology and using the established GSM networks. EDGE provides higher transmission rates and better transmission quality for data than GPRS. EDGE can carry data at speeds typically up to 384 kbit/s in packet mode.

When EDGE is not available, your ICX35-HWC will fall back to GPRS for the connection to your cellular provider to provide continued connectivity.

EV-DO
EV-DO (Evolution Data Optimized) provides a broadband-like cellular data connection that is 10 times faster than 1x/CDMA service. With the high-speed connection, users can experience faster downloading when accessing the Internet and retrieving e-mails, including large attachments and other bandwidth-intensive applications. EV-DO is often referred to as Mobile Broadband and Cellular Broadband.

EV-DO revision A is an enhancement on the original revision 0 adding expanded upload capabilities and a more robust connection overall. In addition to increasing the downlink speed, revision A also increases the uplink speed. In addition, it is backwards compatible and automatically connects with existing and broadly deployed EV-DO Rev. 0 and 1x networks ensuring reliable and pervasive connectivity.

GPRS
General Packet Radio Service (GPRS) is packet-switched with many users sharing the same transmission channel, but only transmitting when they have data to send. This means that the total available bandwidth can be immediately dedicated to those users who are actually sending at any given moment, providing higher utilization where users only send or receive data intermittently. GPRS provides speeds of 30-70 kbps with bursts up to 170 kbps.

HSDPA
HSDPA (High-Speed Downlink Packet Access) is a cellular technology allowing for higher data transfer speeds. In HSDPA mode of operation, max speeds are up to 7.2 Mbit/s in the downlink and 384 kbit/s in the uplink. HSDPA uses Adaptive Modulation and Coding (AMC), fast packet scheduling at the Node B (Base Station) and fast retransmissions from Node B (known as HARQ-Hybrid Automatic Repeat Request) to deliver the improved downlink performance vs. UMTS and EDGE. HSPDA (and HSUPA) falls back to UMTS, EDGE or GPRS (in order of precedence). This feature allows you to have seamless connectivity no matter where your ICX35-HWC is located.

HSUPA
HSUPA (High-Speed Uplink Packet Access) is a cellular technology which most closely resembles a broadband synchronous connection. The upload and download speeds are maximized to provide a faster throughput, reaching speeds up to 2.0 Mbit/s for the uplink and 7.2 Mbit/s for the downlink. Please check with your network provider on the availability of HSUPA.

LTE
Long Term Evolution (LTE) commonly referred to at 4G LTE, is based on the GSM/EDGE and UTMS/HSPA network technologies, increasing the capacity and speed using a different radio interface together with core network improvements.

LTE offers the highest link rates currently available.

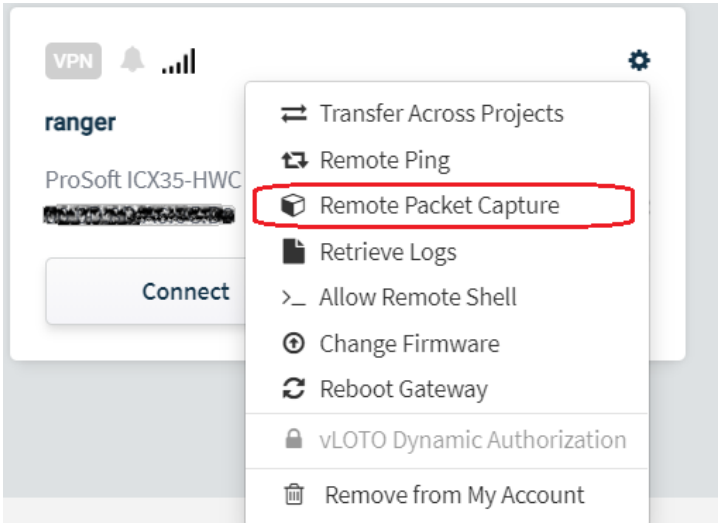
Security
1x and EV-DO data transmissions are highly secure. Originally developed based upon the "spread spectrum" pioneered by the US Department of Defense, security in CDMA technologies is obtained by spreading the digital information contained in a particular signal of interest over multiple coded paths, over a much greater bandwidth than the original signal.

UMTS
UMTS (Universal Mobile Telecommunications System) supports up to 1920 kbit/s data transfer rates, although most users can expect performance up to 384 kbit/s. A UMTS network uses a pair of 5 MHz channels, one in the 1900 MHz range for uplink and one in the 2100 MHz range for downlink.

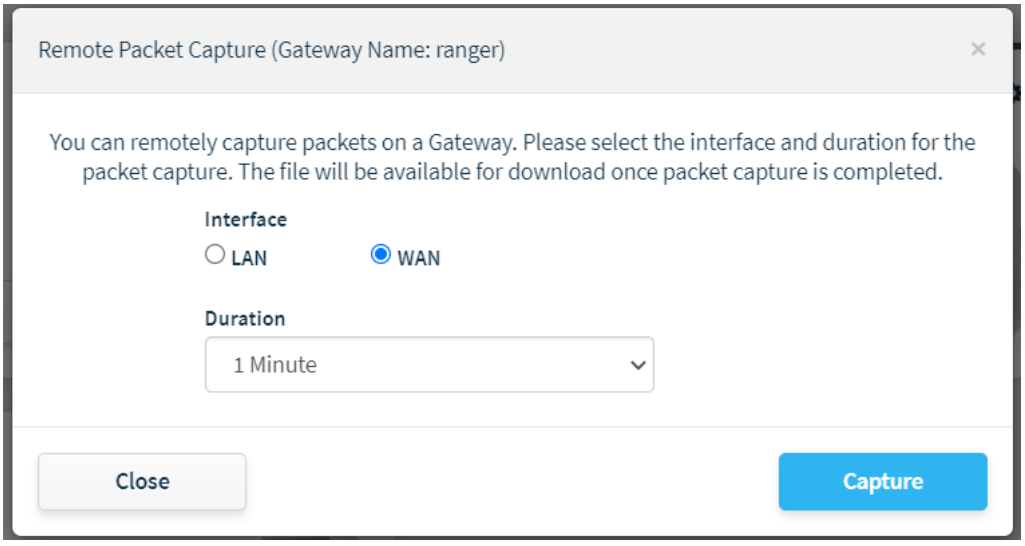
13 Appendix A – Belden Horizon Remote Packet Capture

A remote packet capture option is enabled from Belden Horizon to capture the tcpdump on LAN or WAN interface for a specified duration.

1 Under *Settings*, click on the **REMOTE PACKET CAPTURE** option.



2 Select the *Interface* and *Duration*, then click the **CAPTURE** button.



3 The captured tcpdump is stored in Belden Horizon. Once the file capture is complete, follow the prompts to save to your desktop. The file can be opened with Wireshark for analysis.

14 Proxy ARP

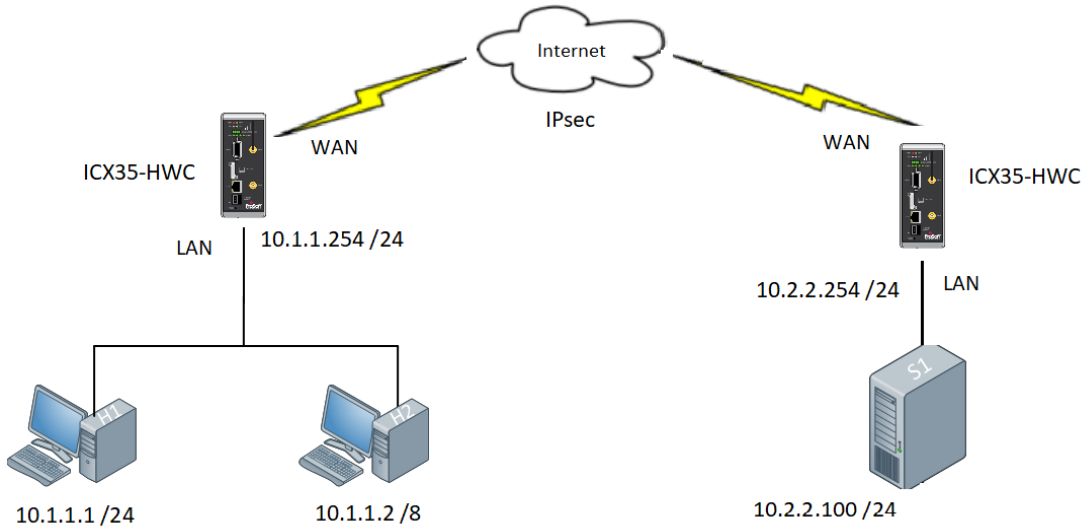
Proxy ARP is a technique in which a proxy server on a given network answers the Address Resolution Protocol (ARP) queries for an IP address that is not on that network.

The proxy is aware of the destination location and offers its own MAC (Media Access Control) address as the (ostensibly final) destination. The traffic directed to the proxy address is typically routed by the proxy to the intended destination via another interface or tunnel.

The process results in the proxy server responding with its own MAC address to an ARP request for a different IP address for proxy purposes.

Proxy ARP can be used when clients are on different physical networks but configured as if they are all on the same subnet. It can be used to create a subnet effect without changing the network configuration of the devices.

14.1 Proxy ARP Sample Topology



The example above has two subnets: **10.1.1.0 /24** and **10.2.2.0 /24**. The routers (ICX35-HWC) are connected to both subnets via WAN connections. One ICX35-HWC network includes two hosts (H1 and H2), and the other ICX35-HWC network includes a server (S1).

The H1 host has a /24 subnet mask and the H2 host has a /8 subnet mask. When H1 tries to reach the S1 server at 10.2.2.100, the following occurs:

1) H1 compares its IP address and subnet mask to the S1 server IP address (10.2.2.100) and decides that the server is on another subnet.

2) H1 sends the packet to its default gateway (10.1.1.254).

3) H1 checks its ARP table to see if there is an entry for 10.1.1.254, if not it will send an ARP request.

4) The ICX35-HWC router will respond to the ARP request, sending its MAC address of its Fast Ethernet (LAN) interface.

When H2 tries to send an IP packet to the S1 server:

1) H2 compares its IP address and subnet mask to the S1 server IP address (10.2.2.100) and decides that the server is on the same subnet (/8).
2) H2 checks its ARP table to see if there is an entry for 10.2.2.100, if not it will send an ARP request.

Since the S1 server is not on the 10.1.1.0 /24 subnet, the ICX35-HWC routers do not forward the broadcast and the ARP request never makes it to the S1 server.

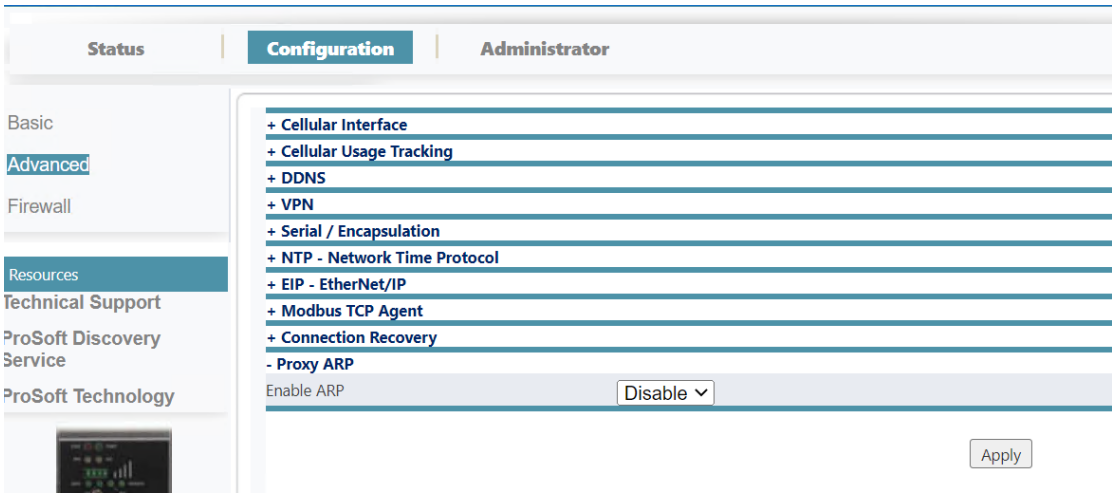
However, when the Proxy ARP is enabled on the ICX35-HWC router:

1) The ICX35-HWC router sees the ARP request from H2 on the 10.1.1.0 /24 subnet and responds with its own MAC address on behalf of destination IP address.
2) The router sends an ARP reply to H2 with its MAC address on the FastEthernet (LAN) interface.
3) Once the H2 resolves the MAC via ICX35-HWC router, it can communicate with the S1 server.

14.2 Configuring Proxy ARP in ICX35-HWC

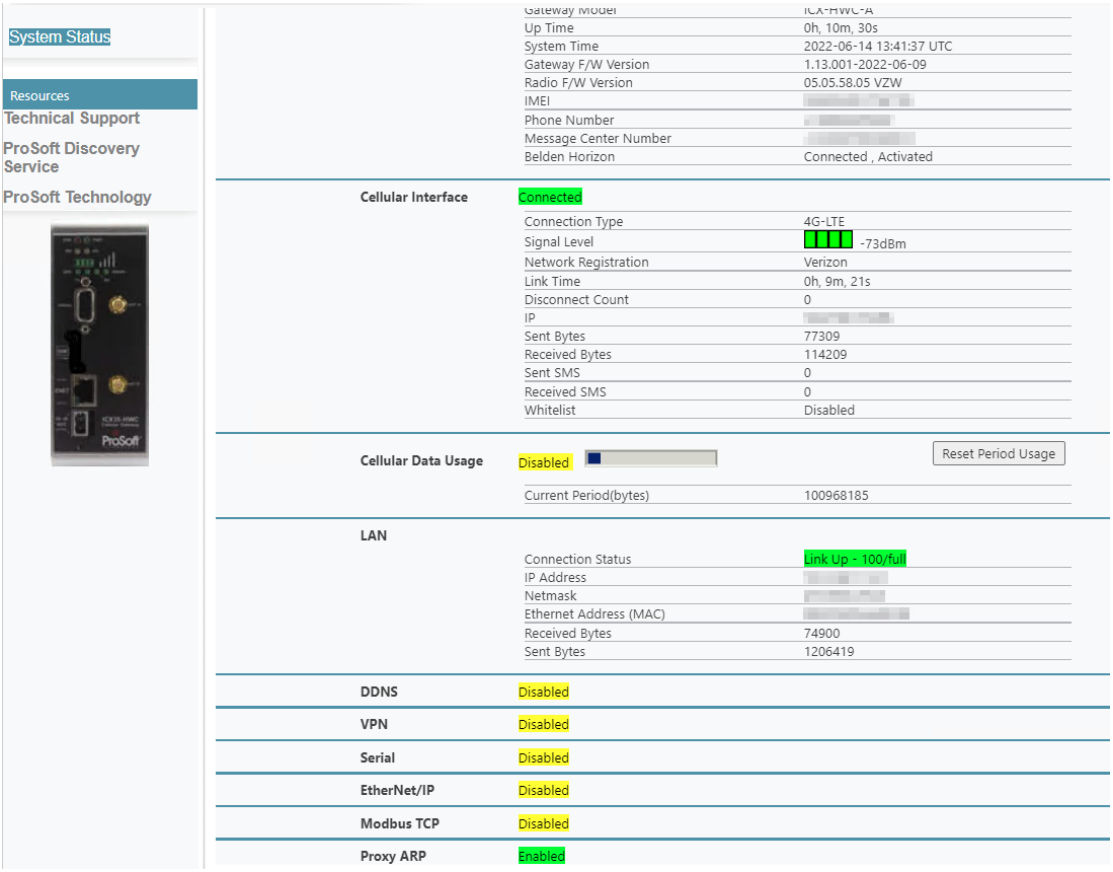
To configure the Proxy ARP, go to **Configuration** > **Advanced** > **Proxy ARP**.

Note: Proxy ARP cannot be enabled or disabled via Belden Horizon. It can be done only via the ICX35-HWC UI.



14.3 Proxy ARP Status Check

To view the status of the Proxy ARP, go to **Status** > **System Status** > **Proxy ARP**.



15 Support, Service & Warranty

15.1 Contacting Technical Support

ProSoft Technology, Inc. is committed to providing the most efficient and effective support possible. Before calling, please gather the following information to assist in expediting this process:

- Product Version Number
- System architecture
- Network details

If the issue is hardware related, we will also need information regarding:

- Module configuration and associated ladder files, if any
- Module operation and any unusual behavior
- Configuration/Debug status information
- LED patterns
- Details about the interfaced serial, Ethernet or Fieldbus devices

Note: For technical support calls within the United States, ProSoft Technology's 24/7 after-hours phone support is available for urgent plant-down issues.

North America (Corporate Location)	**Europe / Middle East / Africa Regional Office**
Phone: +1.661.716.5100 info@prosoft-technology.com Languages spoken: English, Spanish REGIONAL TECH SUPPORT support@prosoft-technology.com	Phone: +33.(0)5.34.36.87.20 france@prosoft-technology.com Languages spoken: French, English REGIONAL TECH SUPPORT support.emea@prosoft-technology.com
Latin America Regional Office	**Asia Pacific Regional Office**
Phone: +52.222.264.1814 latinam@prosoft-technology.com Languages spoken: Spanish, English REGIONAL TECH SUPPORT support.la@prosoft-technology.com	Phone: +60.3.2247.1898 asiapc@prosoft-technology.com Languages spoken: Bahasa, Chinese, English, Japanese, Korean REGIONAL TECH SUPPORT support.ap@prosoft-technology.com

For additional ProSoft Technology contacts in your area, please visit: www.prosoft-technology.com/About-Us/Contact-Us.

15.2 Warranty Information

For complete details regarding ProSoft Technology's TERMS & CONDITIONS OF SALE, WARRANTY, SUPPORT, SERVICE AND RETURN MATERIAL AUTHORIZATION INSTRUCTIONS, please see the documents at: www.prosoft-technology/legal.