Where Automation Connects.

ICX35-HWC

Industrial Cellular Gateway

3G/4G LTE

April 21, 2016

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
9201 Camino Media, Suite #200
Bakersfield, CA 93311
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
www.prosoft-technology.com
support@prosoft-technology.com

ICX35-HWC User Manual
Rev. 1.1.0

April 21, 2016

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 on the enclosed DVD and are available at no charge from our web site: http://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.

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

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 OUVERT UN DISPOSITIF DE TYPE ET EST DESTINE A ETRE INSTALLE DANS UNE ENCEINTE ADAPTÉ POUR L'ENVIRONNEMENT TELS QUE L'ÉQUIPEMENT EST ACCESSIBLE SEULEMENT AVEC L'UTILISATION D'UN OUTIL.

ADAPTÉ POUR UNE UTILISATION EN CLASSE emplacements non dangereux SEULEMENT I, Division 2, Groupes A, B, C ET D LIEUX DANGEREUX OU.

AVERTISSEMENT - RISQUE D'EXPLOSION - NE PAS COUPER EQUIPEMENT LORSQUE LE CIRCUIT EST EN DIRECT ou si la zone est connue pour être dépourvue de concentrations inflammables.

AVERTISSEMENT - RISQUE D'EXPLOSION - SUBSTITUTION DE TOUT COMPOSANT PEUT NUIRE CONFORMITÉ À CLASS I, DIVISION 2.

Agency Approvals and Certifications

Agency
ATEX
CE
CB Safety
ETSI
FCC/IC
PTCRB
UL/cUL

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.

Important Notice

Due to the nature of wireless communications, data transmission and reception can never be guaranteed. Data may be delayed, corrupted (that is, it may have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as ProSoft Technology Wireless products are used in a normal manner with a well-constructed network. Nevertheless, the ICX35-HWC should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. ProSoft Technology accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using ProSoft Technology products, or for failure of the ICX35-HWC to transmit or receive such data.

Limitation of Liability

The information in this manual is subject to change without notice, and does not represent a commitment on the part of ProSoft Technology.

PROSOFT TECHNOLOGY, INC AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY PROSOFT TECHNOLOGY PRODUCT, EVEN IF PROSOFT TECHNOLOGY AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall ProSoft Technology and/or its affiliates aggregate liability arising under or in connection with the ProSoft Technology product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the ProSoft Technology product.

WARNING – EXPLOSION HAZARD – DO NOT REPLACE ANTENNAS UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NON-HAZARDOUS.

“THIS DEVICE CONTAINS A TRANSMITTER MODULE:
FCC ID: N7NMC7355
PLEASE SEE FCC ID LABEL ON BACK OF DEVICE."
"THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS: (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION."
"CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER’s AUTHORITY TO OPERATE THE EQUIPMENT."
“THIS DEVICE IS CONFIGURED FOR OPERATION IN THE USA DURING MANUFACTURING. THESE CONFIGURATION CONTROLS ARE NOT PRESENT IN THE SOFTWARE WITH WHICH THE UNIT IS SHIPPED; THEREFORE THE END USER CANNOT CHANGE THE POWER SETTINGS, FREQUENCY OR THE COUNTRY/REGION. THE MODELS SOLD & SHIPPED WITHIN THE U.S. ARE IDENTIFIED WITHIN THE MODEL NUMBER WITH –A AS PART OF THE IDENTIFIER.” THE MODELS SOLD & SHIPPED OUTSIDE OF THE U.S. ARE IDENTIFIED WITH A –E AS PART OF THE MODEL NUMBER DESIGNATING THE REGION OF USE.

Industry Canada Requirements:

THE INSTALLER OF THIS RADIO EQUIPMENT MUST INSURE THAT THE ANTENNA IS LOCATED OR POINTED SUCH THAT IT DOES NOT EMIT RF FIELD IN EXCESS OF HEALTH CANADA LIMITS FOR THE GENERAL POPULATION; CONSULT SAFETY CODE 6, OBTAINABLE FROM HEALTH CANADA.

Contents

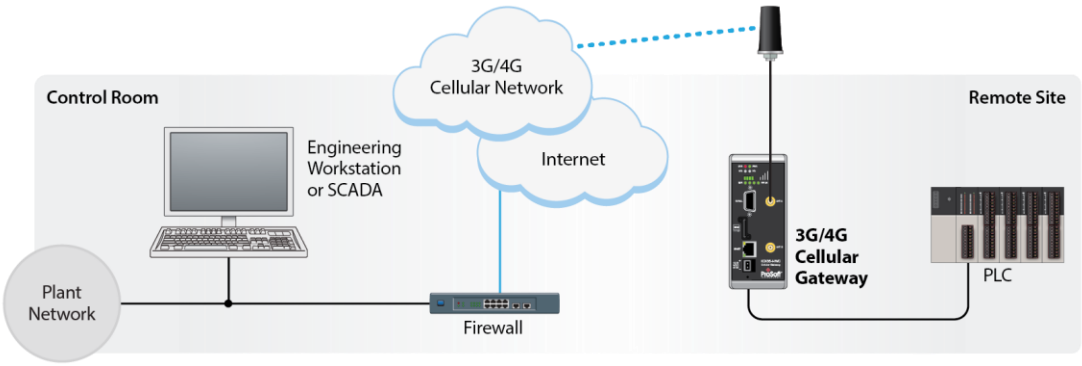
1 Start Here

In This Chapter

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 networks with a single device.



The ICX35-HWC supports:

- 4G LTE with GSM
- 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

Cellular Technology	LTE, GSM, UMTS/HSPA+, GPRS, EDGE
Frequency/Bands	**ICX35-HWC-A**: Freq: 700/850/900/1700/1800/1900/2100 MHz HSPA and HSPA+ Bands: 1,2,4,5,8 LTE Bands: 2,4,5,13,17,25 Quad-band EDGE/GPRS/GSM **ICX35-HWC-E**: Freq: 700/800/850/900/1700/1900/2100/2600 MHz HSPA and HSPA+ Bands: 1,2,5,6,8 LTE Bands: 1,3,7,8,20 Quad-band EDGE/GPRS/GSM
Max Downlink Speeds	Up to 100 Mbps maximum (network dependent)
Max Uplink Speeds	Up to 50 Mbps maximum (network dependent)
Activation	SIM Slot
Security	OpenVPN client, IPSec client, IP Address Filtering

Physical

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

Operating Temperature	IEC 60068 -22°F to +158°F (-30°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.

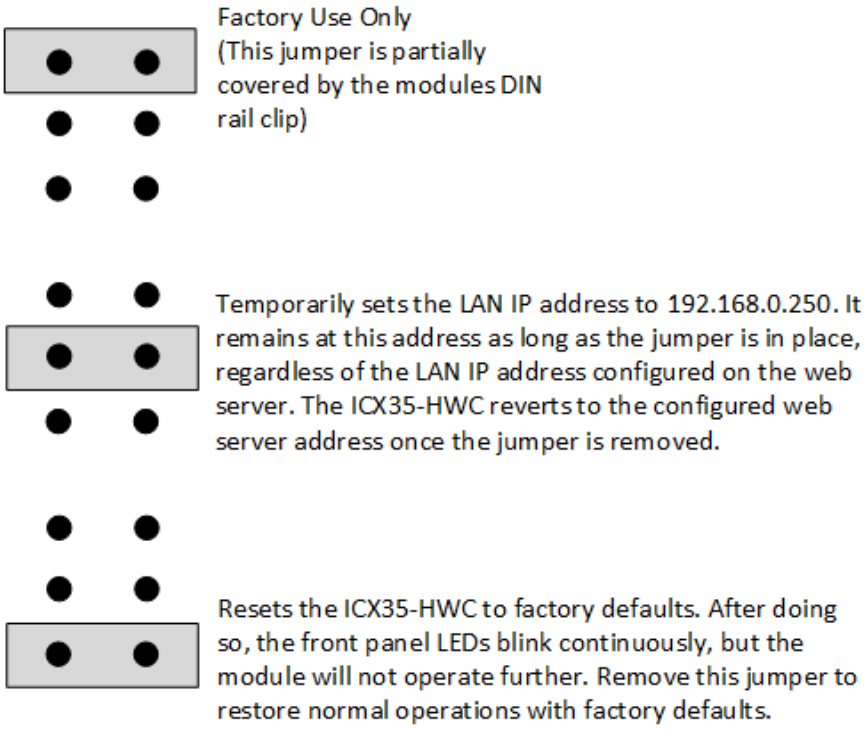
Important: Before beginning the installation, please verify all of the following items are present.

Qty.	Part Name	Part Number	Part Description
1	ICX35-HWC Cellular Gateway	ICX35-HWC	3G/4G LTE
1	ProSoft Solutions DVD	DVD-001	Contains documentation for the ICX35-HWC
1	2-pin Power Connector		Power Connector
1	Connector Lever		
1	Jumper for rear pins		

If any of these components are missing, please contact ProSoft Technology Support for replacement parts.

1.3 Jumpers

There are three jumpers located on the rear of the unit.



1.4 Power Requirements

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

2 Connecting to the ICX35-HWC

In This Chapter

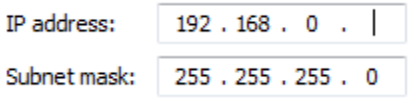
The configuration webpage is used to configure and manage the ICX35-HWC. First-time setup must be performed over a wired network, where provider-specific cellular configuration details are configured. Once initially set up, you can access the webserver over the LAN and cellular networks (unless LAN access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

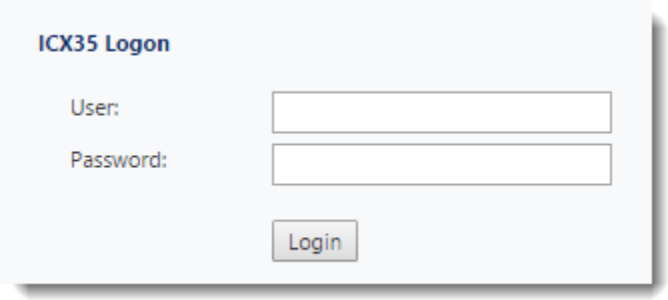
2.1 Configuration Webpage Setup

1. Insert the SIM card 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 radio's 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

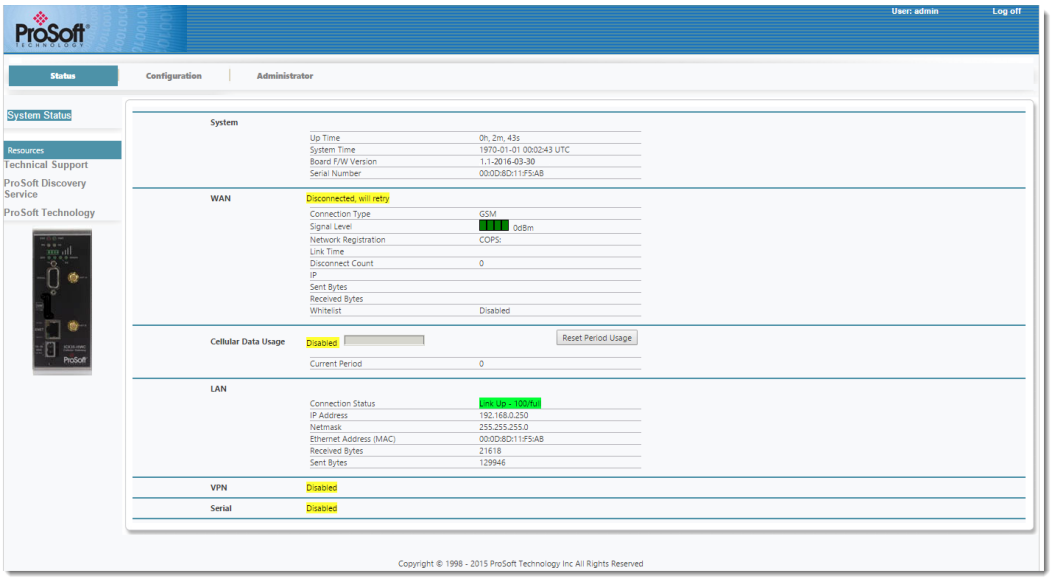


5. Open a web browser and enter the ICX35-HWC default address of http://192.168.0.250:8080
   You can also use ProSoft Discovery Service to set a temporary IP address. You can download and install ProSoft Discovery Services from the ProSoft website at www.prosoft-technology.com.
6. Once the ICX35-HWC homepage opens, enter the **USERNAME** and **PASSWORD** to log in. You will be able to customize these later. The default **USERNAME** is '*admin*' and the default **PASSWORD** is '*password*'.

Note: Be sure to change your password once you log in. You can do this by navigating to **Administrator > Access Control > Web Login**. Be sure to click **Apply** after entering your new credentials.

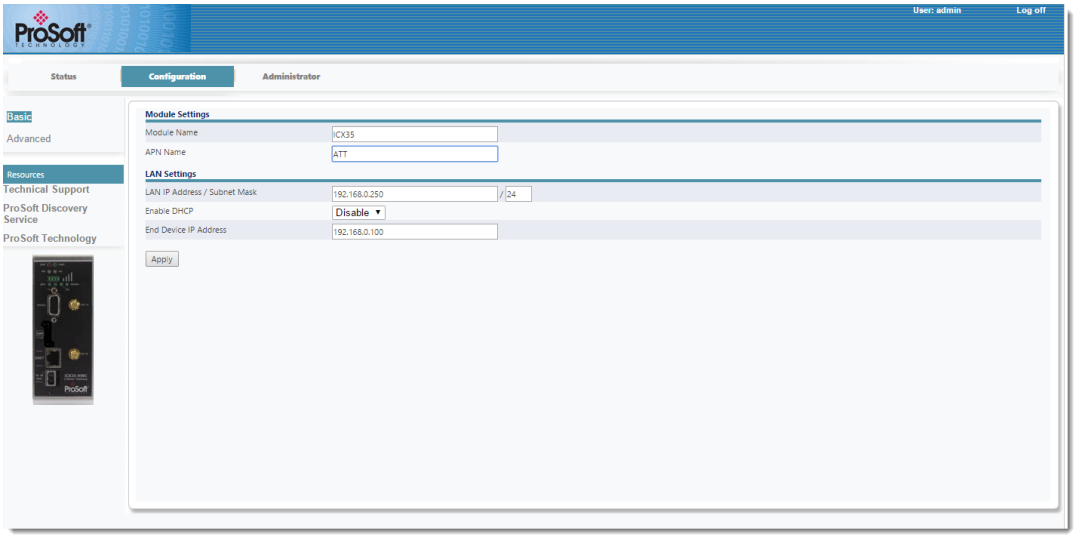


7 After successful login, the homepage displays data from the *Status* tab.



2.2 Assigning a LAN IP Address to the ICX35-HWC

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

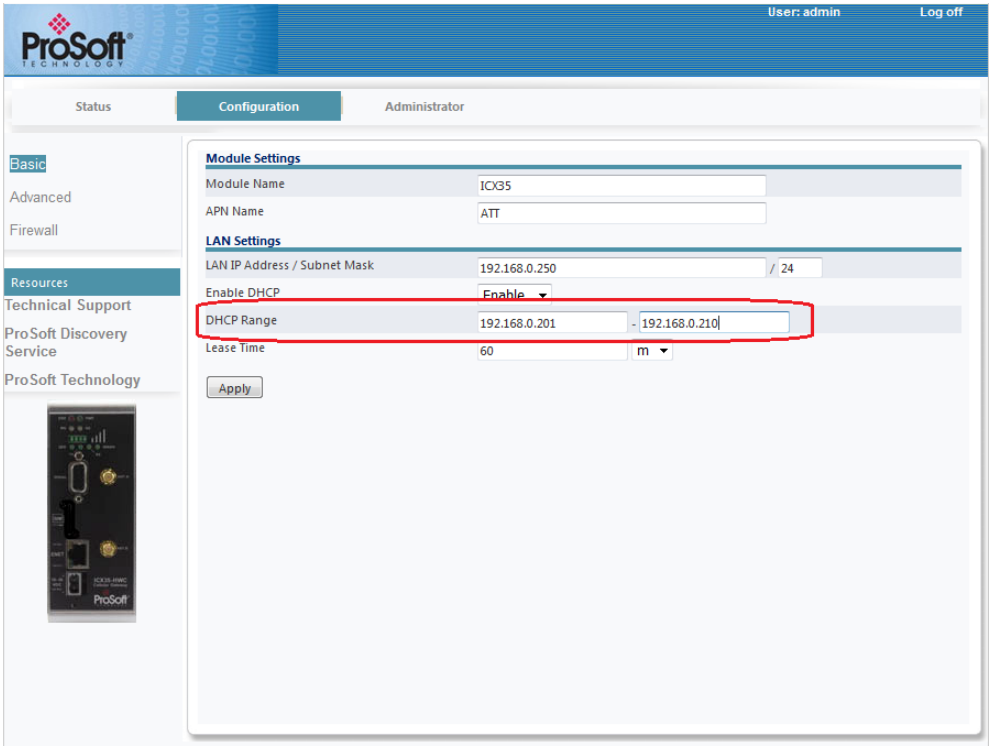


2 Enter a name for the module in the **Module Name** field.
3 Enter the APN (Access Point Name). This information is provided by your cellular provider.
4 Enter the **LAN IP Address/Subnet Mask** of the ICX35-HWC.

5 Enter the **End Device IP Address** of the end device if you only have one device. The end device is the device connected to the LAN port of the device that the ICX35-HWC will access.

6 Choose whether or not to use DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) for end devices.

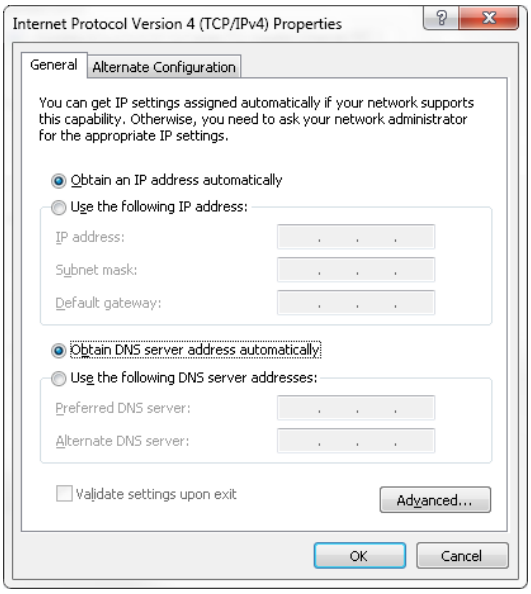
a) If YES, **Enable** the DHCP option and select a **DHCP Range** of IP addresses applicable to multiple End Devices.



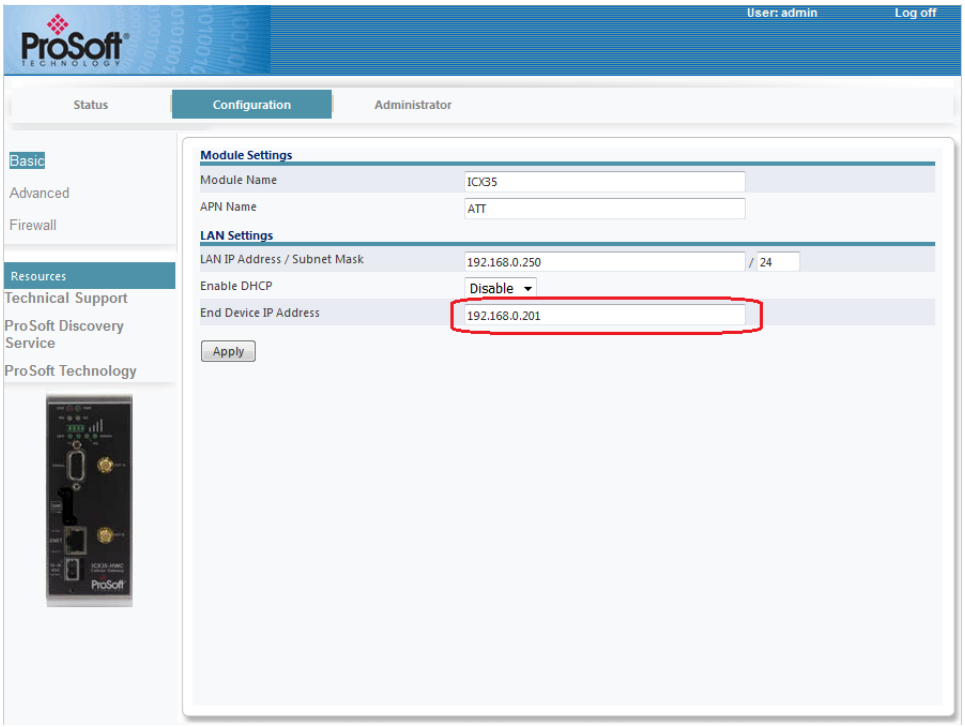
- **DHCP Range** – This allows you to enter a range of IP addresses that can be addressed. For example, if you have a number of devices connected to a remote ICX35-HWC, you can enter the DHCP range to use on devices connected to the remote ICX35-HWC.

- **Lease Time** – Enter the desired lease time using seconds, minutes, or hours. This setting depends on your cellular plan.

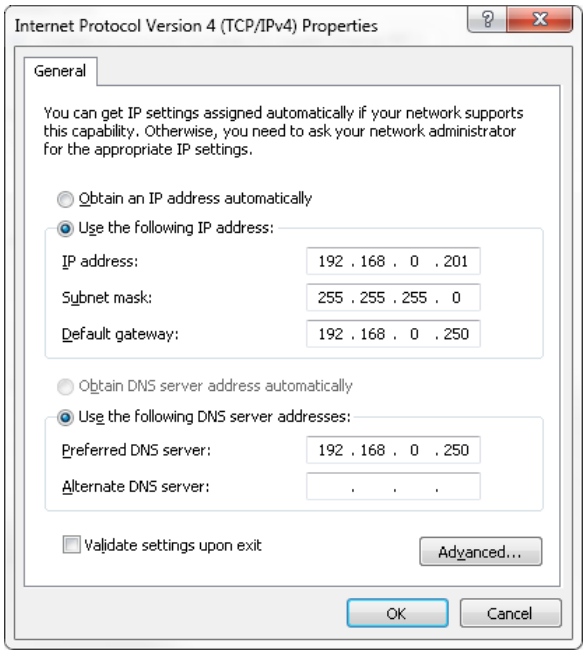
b) For each End Device, set the TCP/IPv4 properties (Found at **Control Panel\Network and Internet\Network Connections**) as follows:



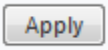
c) If NO, **Disable** the DHCP option and enter an applicable **End Device IP Address**.



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



7 In the ICX35-HWC configuration webpage, click **Apply**. The module reboots and should connect to the cellular provider.



8 Once the reboot is complete, reset your PC back to its original IP address. This IP address should now 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 web page. Add **:8080** to specify the correct port (192.168.0.250**:8080).**

2.3 Connecting to your Cellular Provider

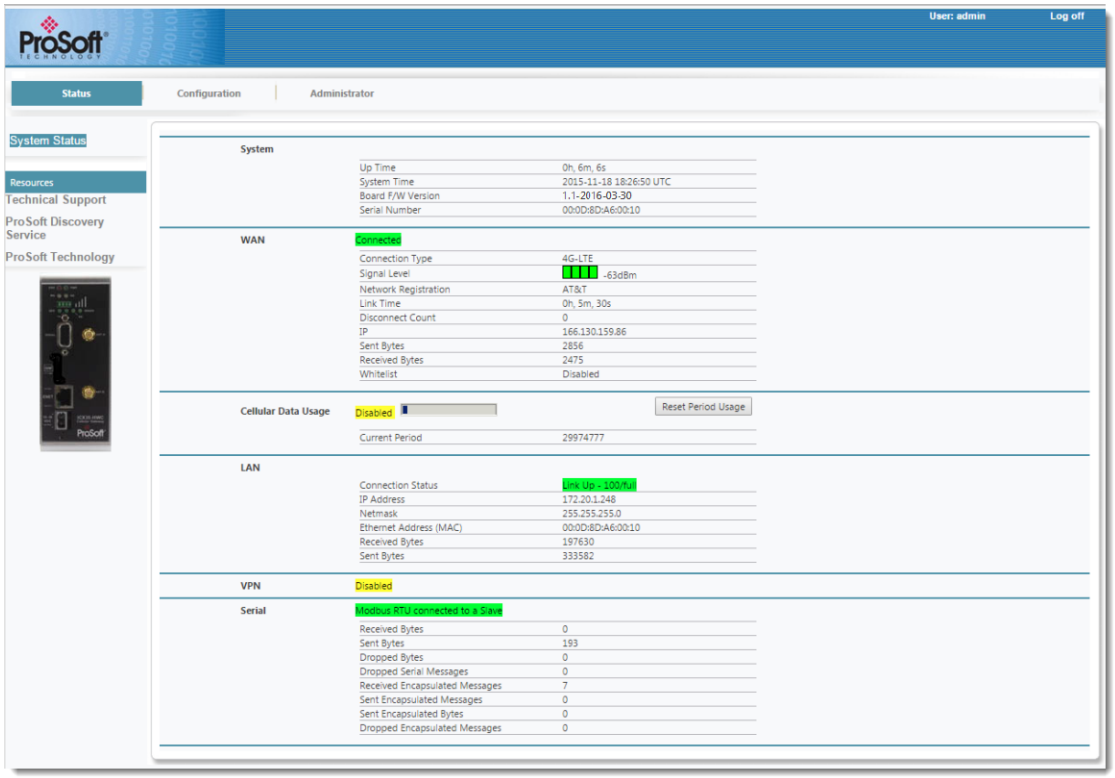
The ICX35-HWC supports 3G GSM/GPRS and 4G LTE (where applicable) networks. It uses your cellular provider as an ISP (Internet Service Provider) to connect to the Internet. Cellular devices using GSM technology, such as AT&T, require a SIM (Subscriber Identity Module) card to be installed in the radio.

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.

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 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. 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.
5. 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.
6. The GSM network information is now displayed on the *Status* web page.



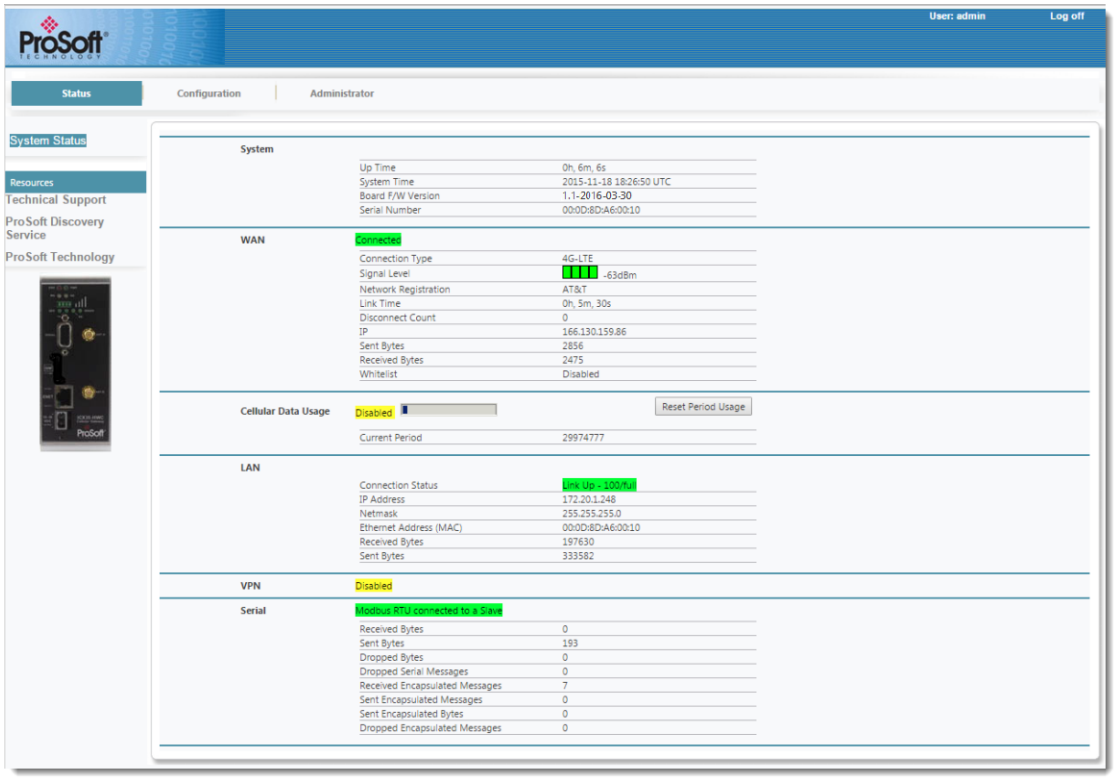
3 ICX35-HWC Webpage

There are three main tabs of the ICX35-HWC web pages:

- Status
- Configuration
- Administrator

3.1 Status

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

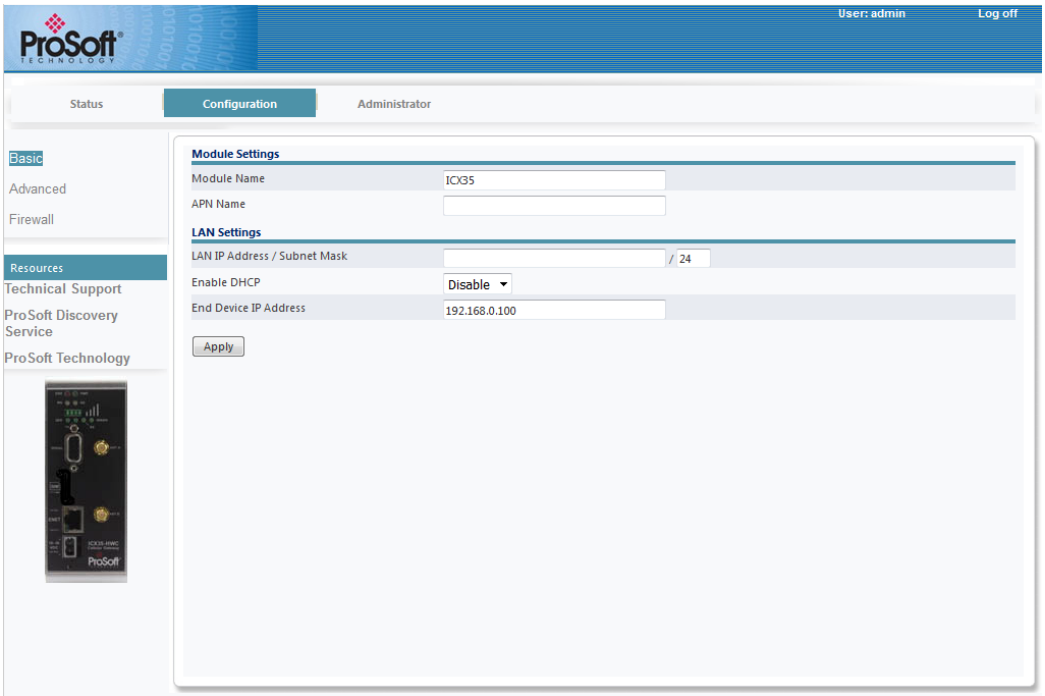


System	Description
Up Time	Amount of time the cellular gateway has been active since the last power cycle or a reset
System Time	Current date and time of the ICX35-HWC
Board F/W Version	Firmware version of the cellular hardware
Serial Number	Serial number of the ICX35-HWC
WAN	
Connection Type	The type of connection. For example, GSM
Signal Level	Signal Level of cellular network (dBm)
Network Registration	Registered local cellular network
Link Time	The number of days, hours, minutes, seconds connected to the WAN
Disconnect Count	Indicates the time that the unit has lost communication to a cell tower and has/is attempting to reconnect back to the cellular service. It counts each time that 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
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. 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. This value is set during Advanced Configuration.
VPN	Set in Advanced Configuration Settings
Serial	Based on Advanced Configuration settings. For example, this displays a serial status based on selections in Advanced Configuration.

3.2 Configuration

3.2.1 Basic

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



Module Settings

Parameter	Description
Module Name	Name of ICX35-HWC on network
APN Name	Access Point Name of the network path for cellular connectivity

LAN Settings

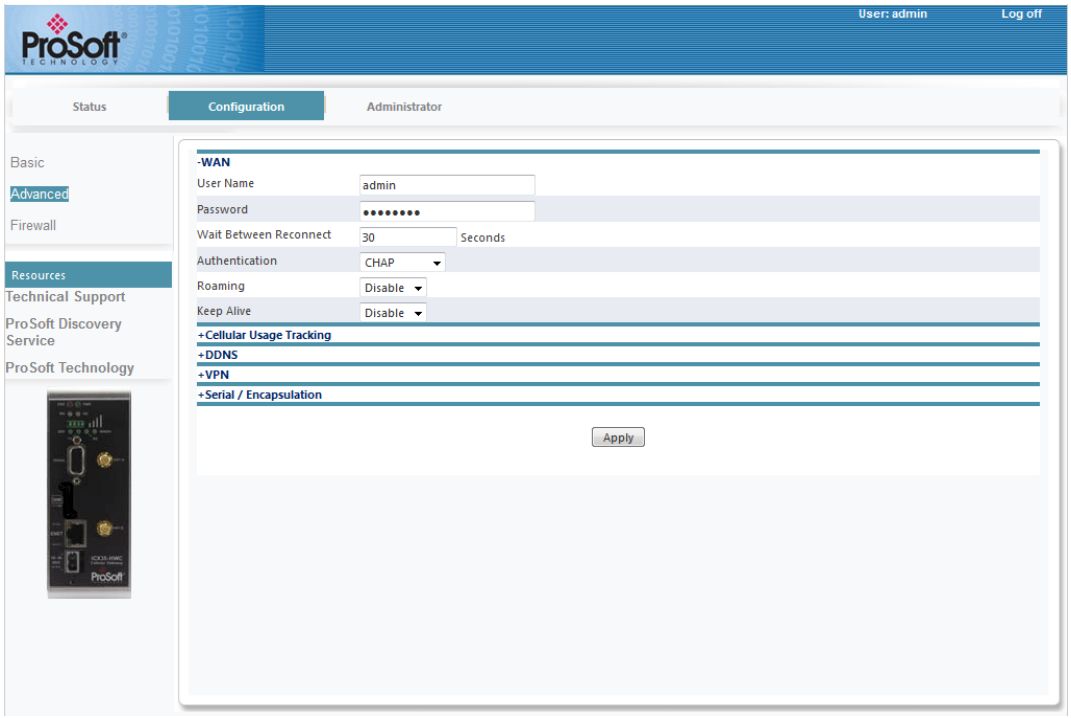
Parameter	Description
LAN IP Address / Subnet Mask	IP address of the ICX35-HWC ethernet port
Enable DHCP	Enables/Disables DHCP functionality
End Device IP Address	Used when DHCP is disabled. IP address of end device.
DHCP Range	Used when DHCP is enabled. DHCP range of end devices
Lease Time	Used when DHCP is enabled. Enter the desired lease time using seconds, minutes, or hours. This setting depends on your cellular plan.

3.2.2 Advanced

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

- WAN
- Cellular Usage Tracking
- DDNS
- VPN
- Serial/Encapsulation

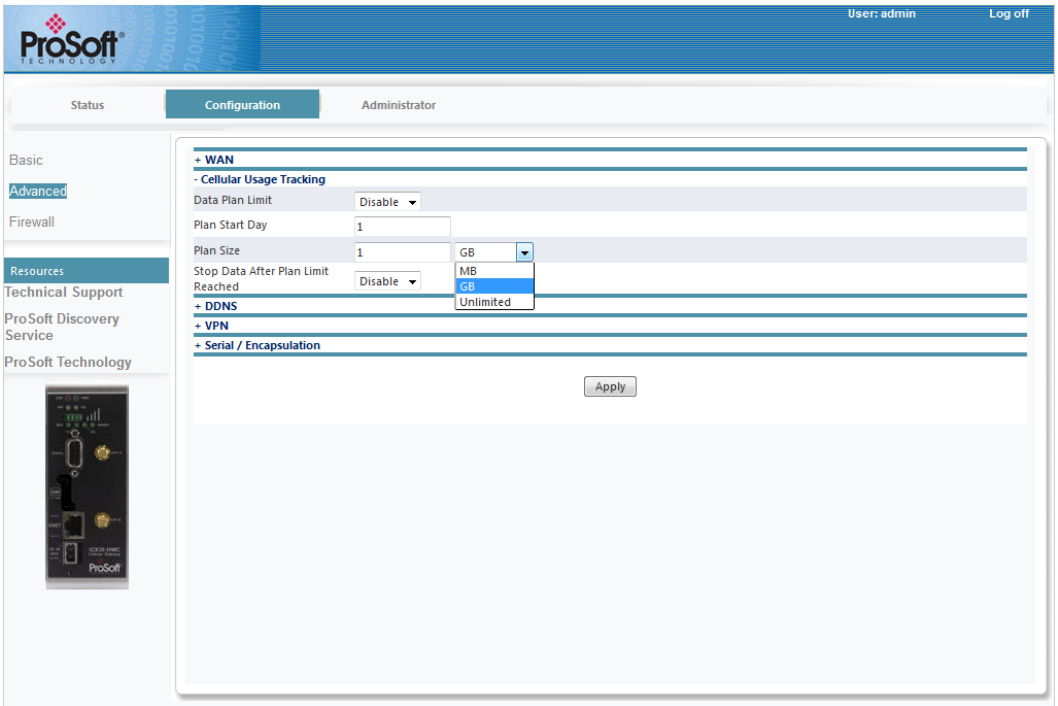
WAN



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	PAP - Password Authentication Protocol CHAP - Challenge Handshake 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 Usage Tracking

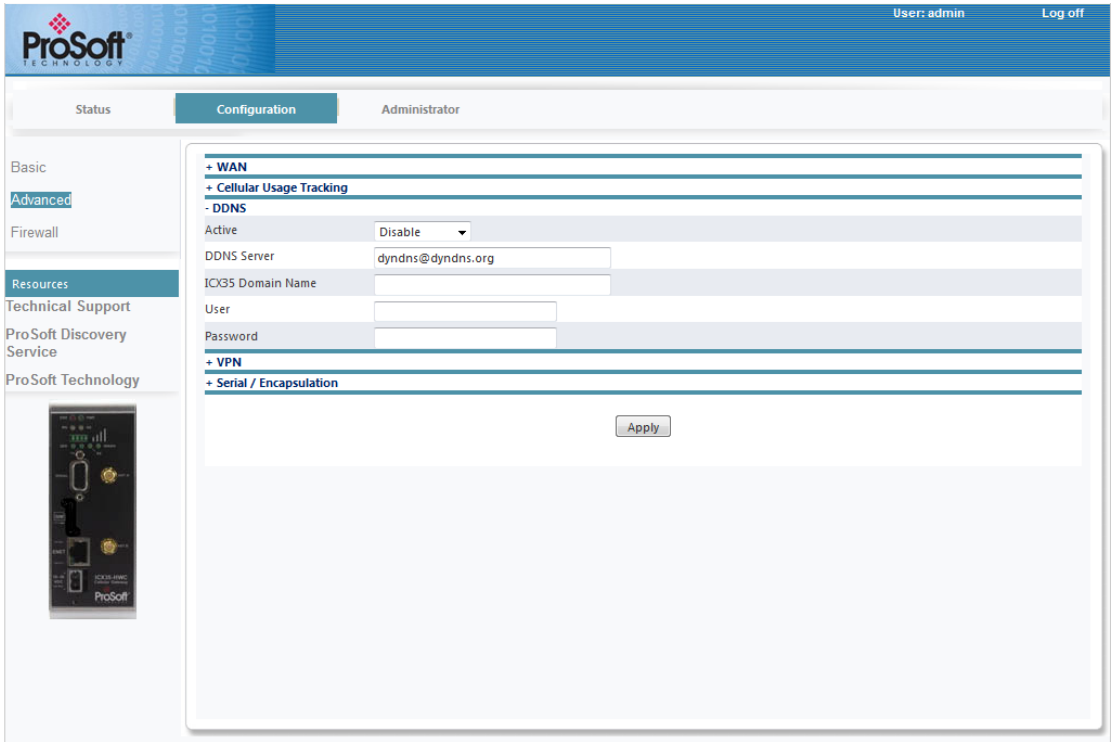
Note: The Cellular Usage Tracking feature is not an official value of the usage a carrier would report. Due to possible differences in these values, cellular usage tracking should be used as an aid for gauging how much data the system is using over a period rather than as a reliable method to determine 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. *Enabled* tells the ICX35-HWC to stop transferring data after the Plan (size) limit is reached.

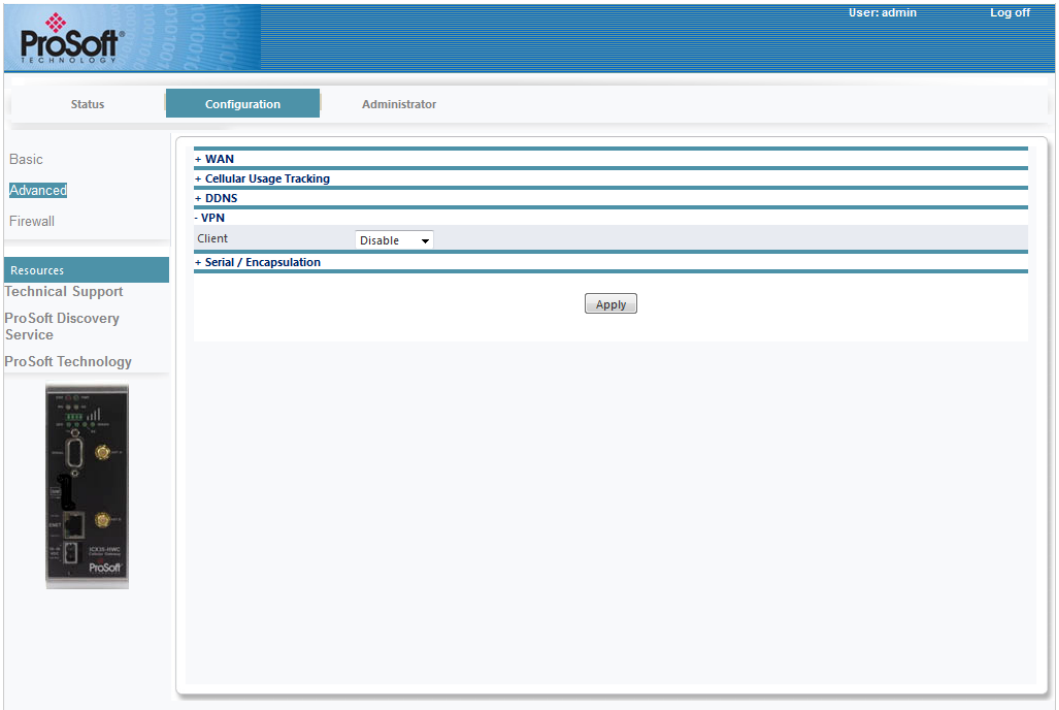
DDNS

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:

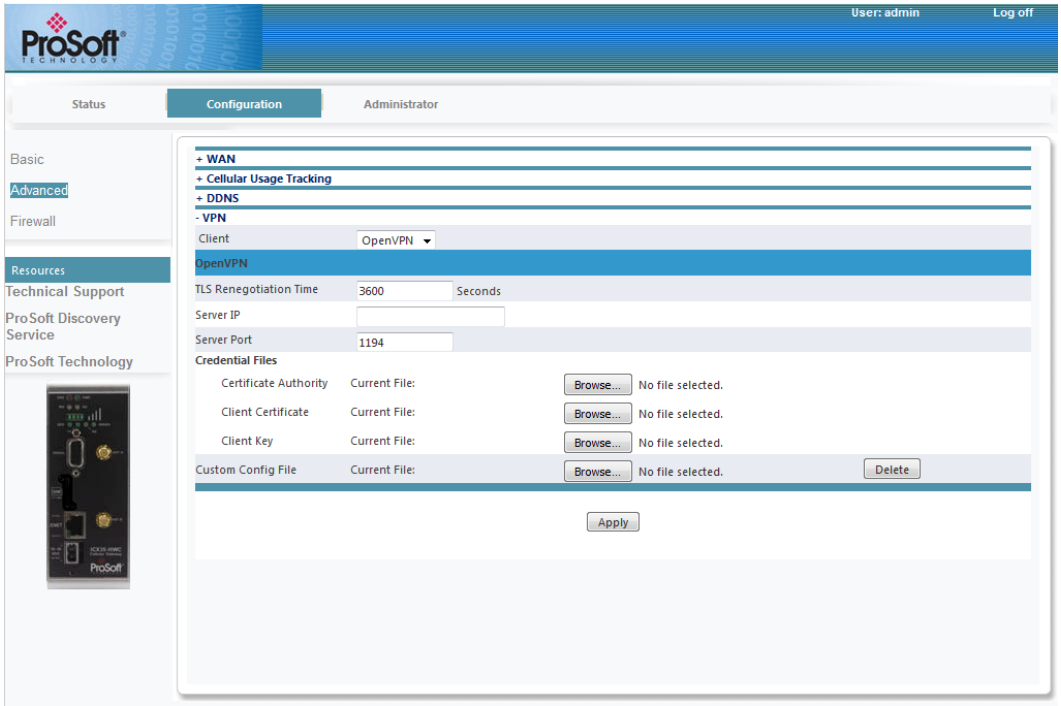
- Disable
- OpenVPN
- IPSec

Select **Disable** to disable VPN functionality.

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 4 provides details on using OpenVPN.

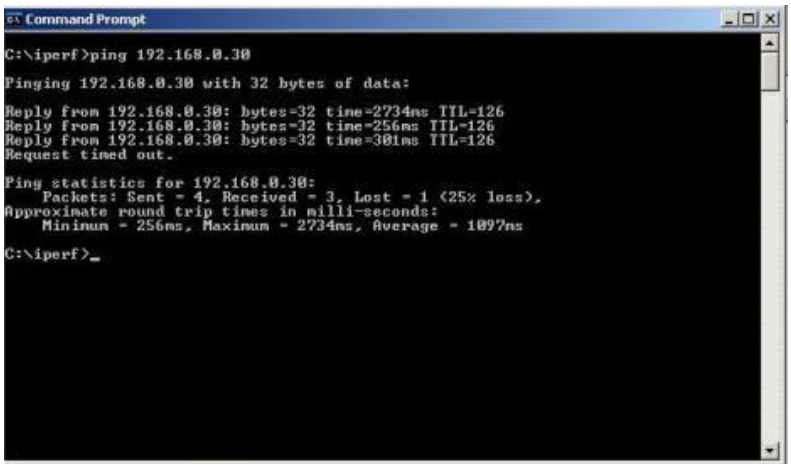
Parameter	Description
TLS Renegotiation Time	Transport layer Security renegotiation time in seconds. This controls how often the underlying SSL/TLS session renegotiates. This provides additional security by frequently rekeying the session keys. This is set to 3600 by default.
Server IP	IP address of 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 generally accepted default port designated for OpenVPN. This is the port number that is used for the previous example.

Parameter	Description
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. Once you have all of the files, click the browse button to locate them on the file system. Once all of the files are uploaded, the actual files appear in the appropriate Current File area.
Custom Config File	Allows you to choose and upload a custom OpenVPN configuration file, which overrides any credential files previously loaded. The Delete button allows you to delete the Custom Configuration file.

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 web page will indicate that an OpenVPN connection is established.

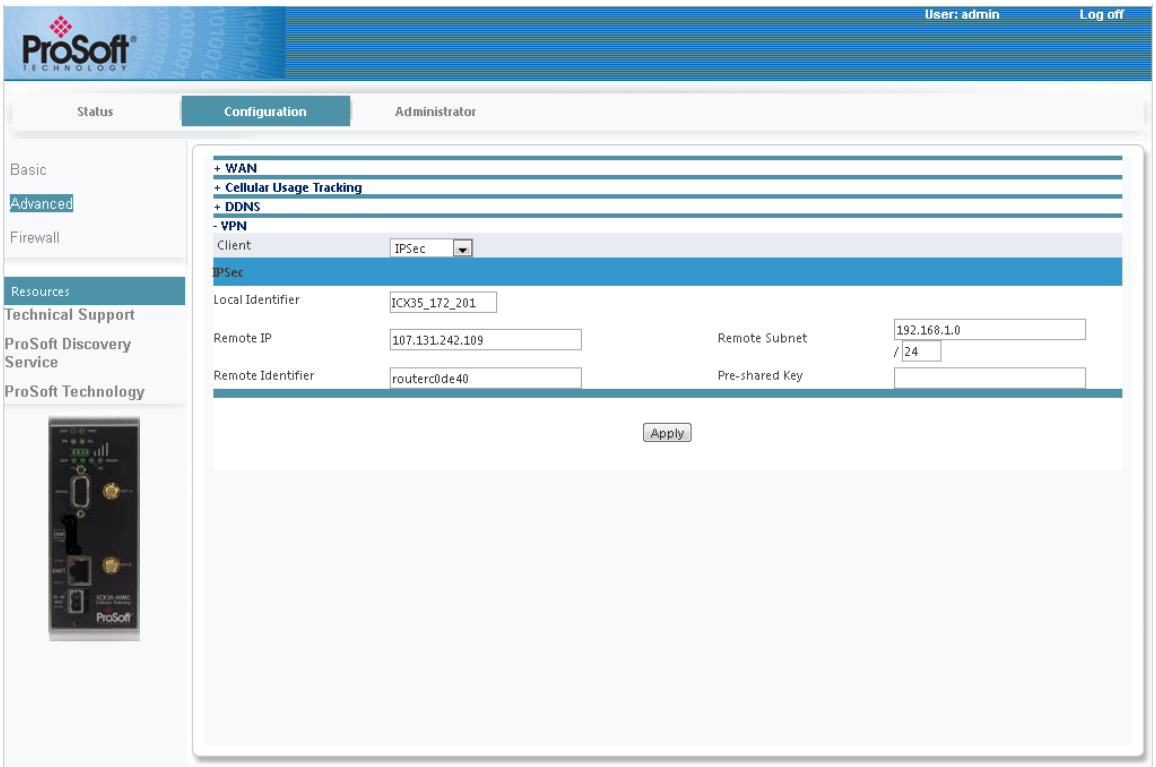
You can now pass secured data between the two LAN devices. Verify this with a simple ping from one LAN device to the other.



IPSec

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

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

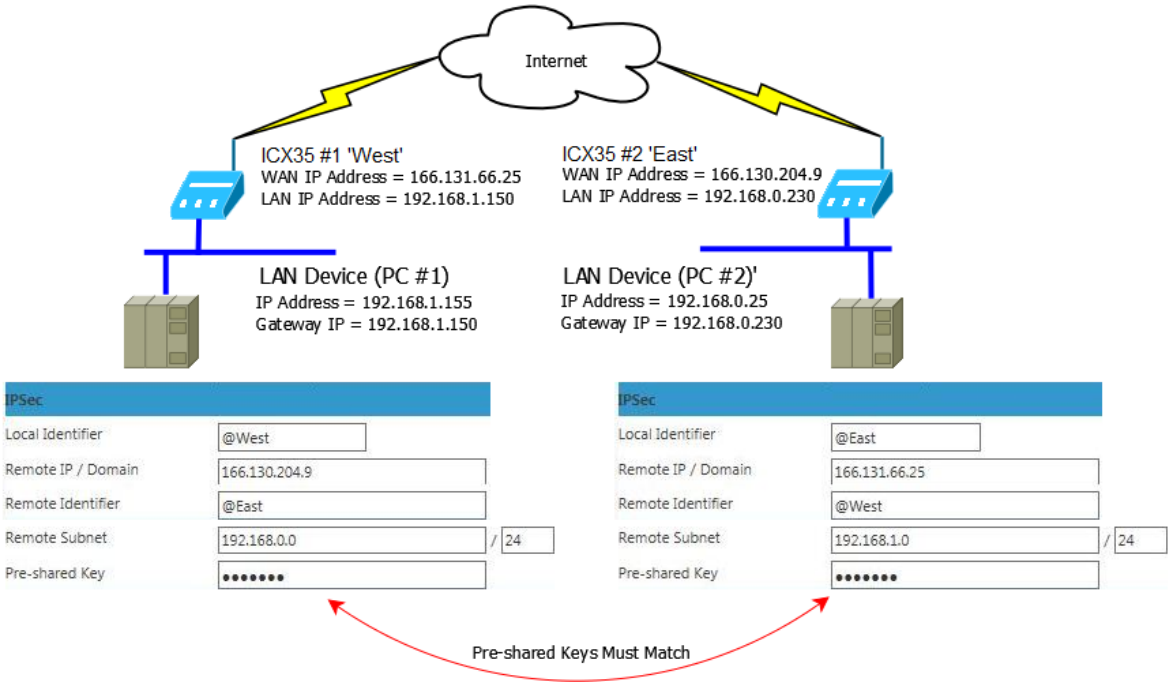


Parameter	Description
Local Identifier	Specifies the identifier to be used for the local side of the IPsec connection. This is used during authentication of the tunnel. It is a free-form string, although typically it is a Fully Qualified Domain Name, or an IP address. Max length is 28. **Note:** Use 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 IP	This parameter specifies the IPsec remote IP.
Remote Identifier	This parameter 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	This parameter 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)
Pre-shared Key	Specifies the pre-shared key that needs to 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.

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"

Name	ICX35 #1 West
WAN IP	WAN IP Address of ICX35 #1
LAN IP	192.168.1.150
Local Identifier	@West
Remote IP	WAN IP Address of ICX35 #2
Remote Identifier	@East
Remote Subnet	192.168.0.0/24
Preshared Key	presharedkey (this can be any string)
End Device	192.168.1.155 (IP address of LAN Device #1)

LAN Device #1 (Connected to ICX35 #1)

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

ICX35 #2 "East"

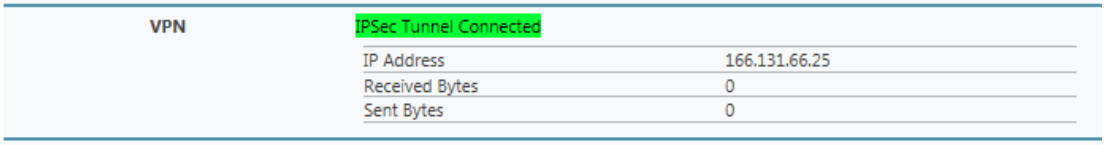
Name	ICX35 #2 East
WAN IP	WAN IP address of ICX35 #2
LAN IP	192.160.0.230
Local Identifier	@East
Remote IP	WAN IP address of ICX35 #1
Remote Identifier	@West
Remote Subnet	192.168.1.0/24
Preshared Key	presharedkey (this can be any string)
End Device	192.168.0.30 (IP address of LAN Device #2)

LAN Device #2 (Connected to ICX35 #2)

IP Address	192.168.0.30 (ICX35s end device IP address)
Gateway	192.168.0.230 (ICX35s LAN IP address)

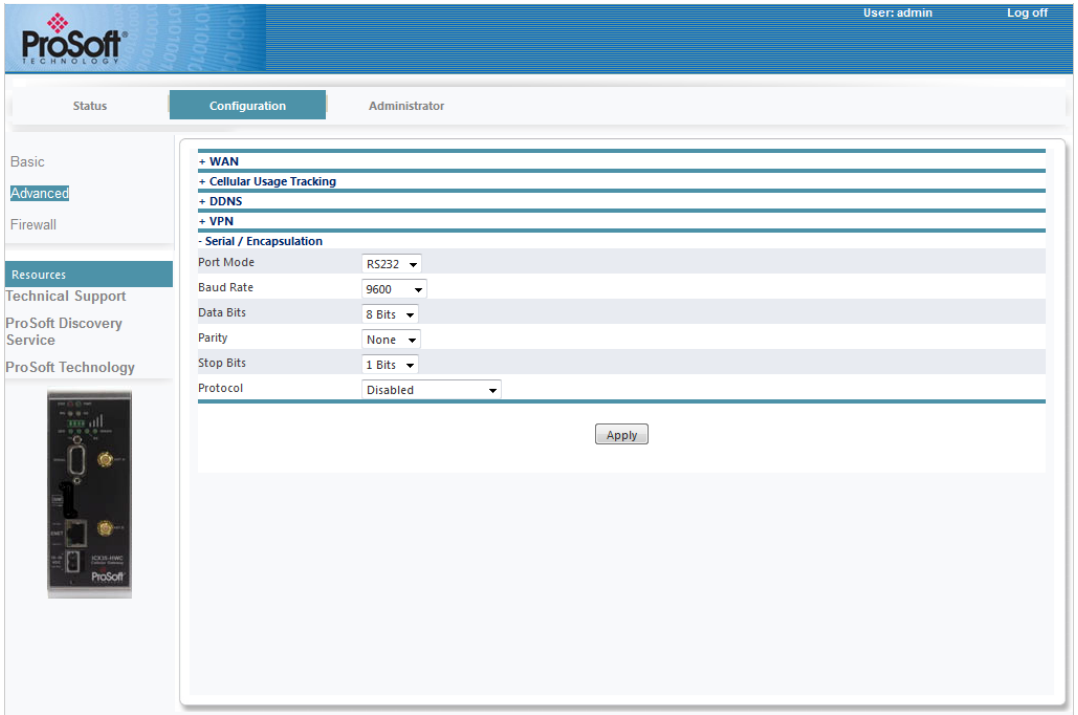
Verification

Once all four devices are configured, the status web page in both of the ICX35s will indicated that an IPSec VPN connection is made.



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

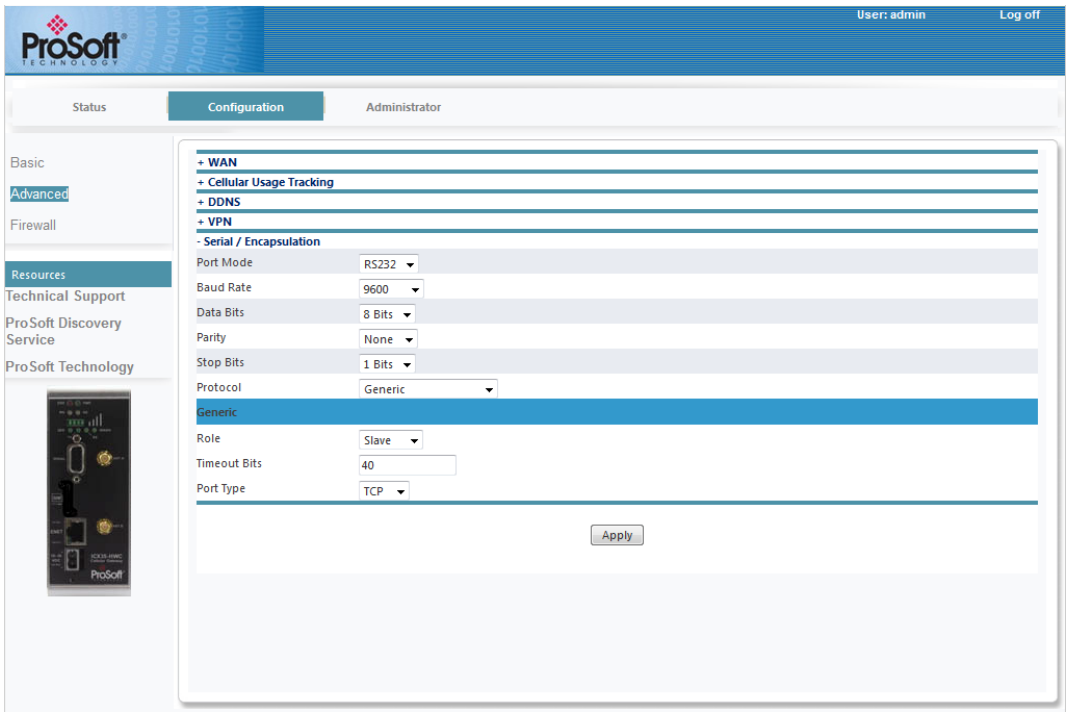
Serial / Encapsulation



Parameter	Description
Port Mode	This parameter sets the scheme for the serial port (RS-232, RS-485, or RS-422)
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: ○ **Disabled** ○ **Generic** ○ **Modbus RTU** ○ **Modbus ASCII** ○ **Modbus RTU to TCP** ○ **Modbus ASCII to TCP** ○ **DF1 Full-Duplex (Not available for RS485 port mode)** ○ **DF1 Radio Modem (Not available for RS485 port mode)**

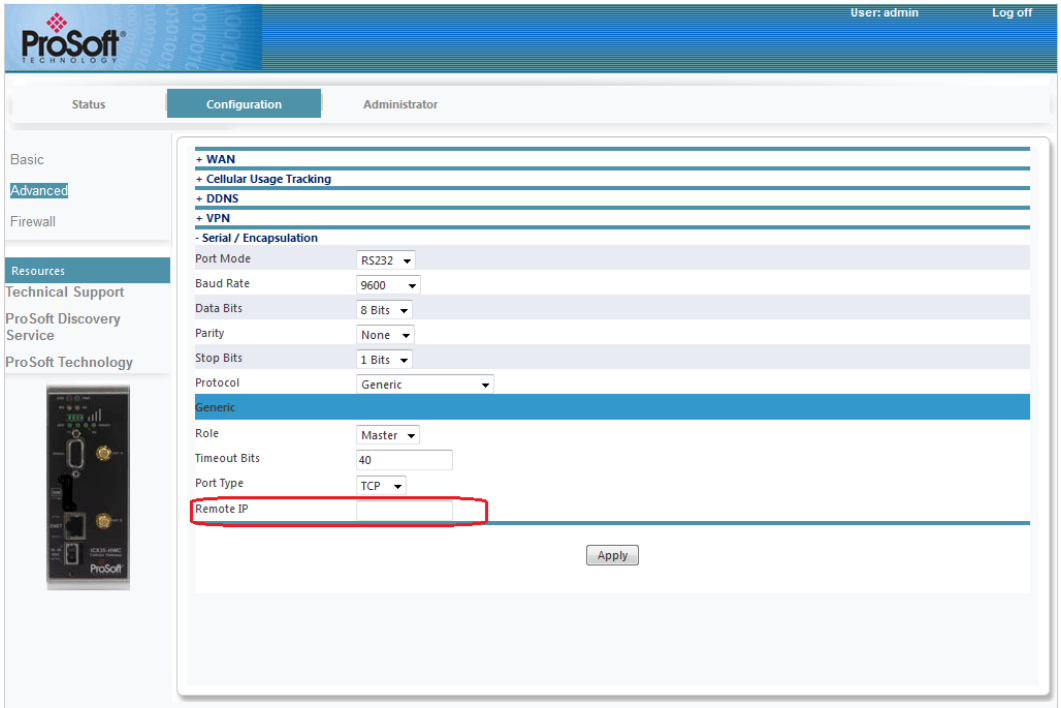
Generic

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.

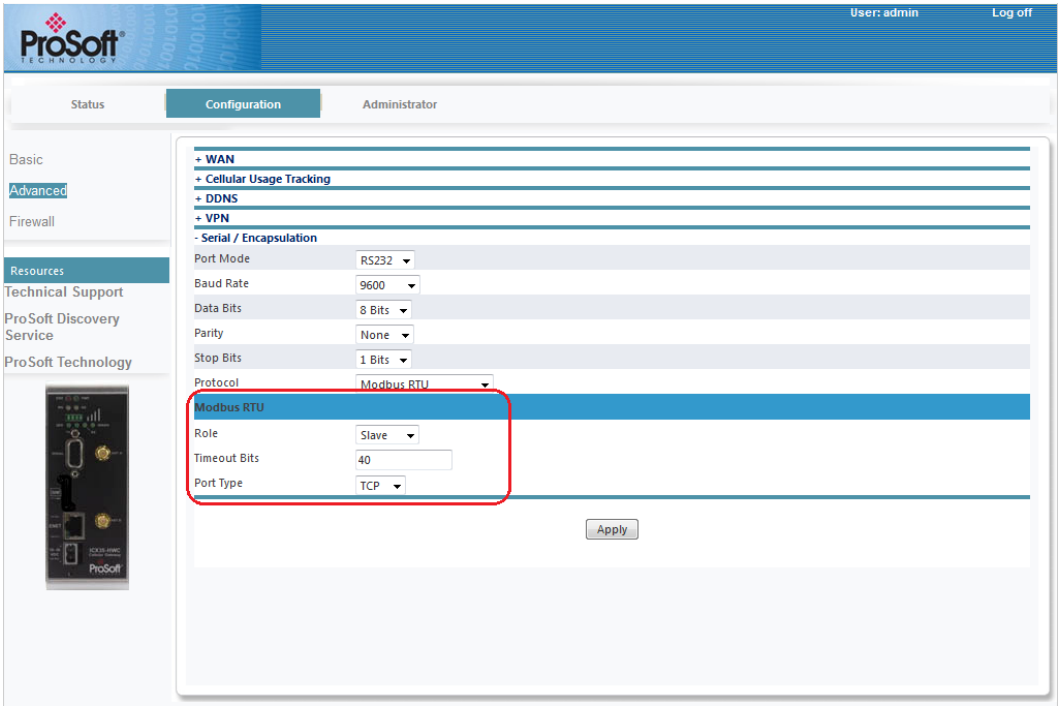
The **Master** role contains an additional parameter:



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

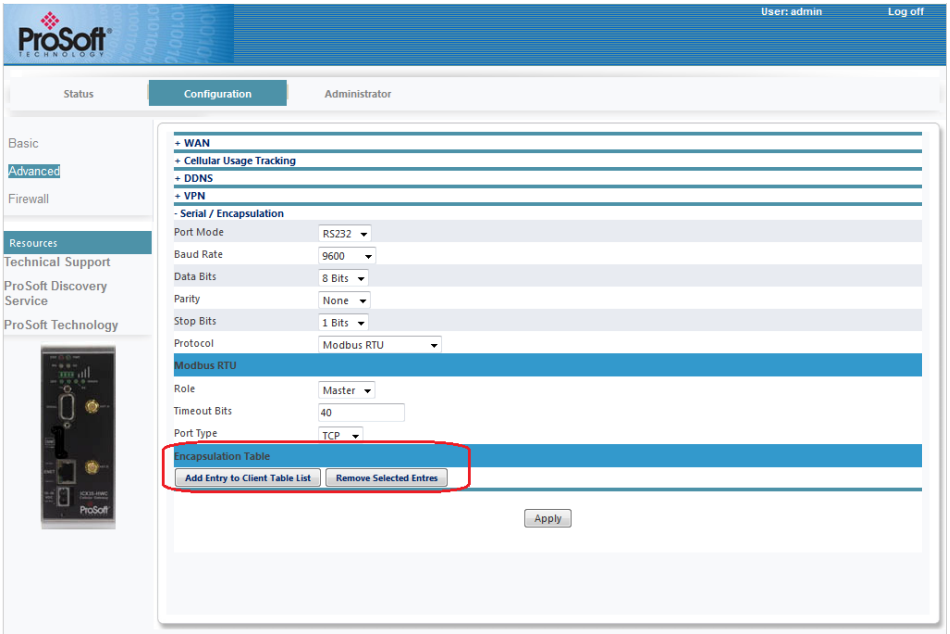
Modbus RTU

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



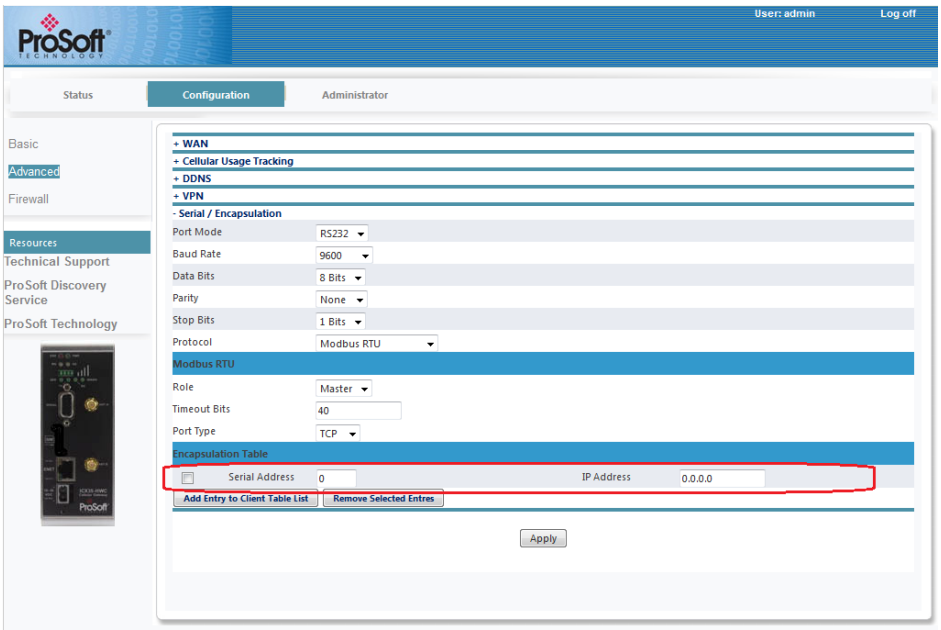
Parameter	Description
Role	Network role for the encapsulation process (Master, Slave, Master/Slave).
Timeout Bits	Sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Type of IP connection (TCP or UDP)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

The **Master** role contains additional parameters:



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

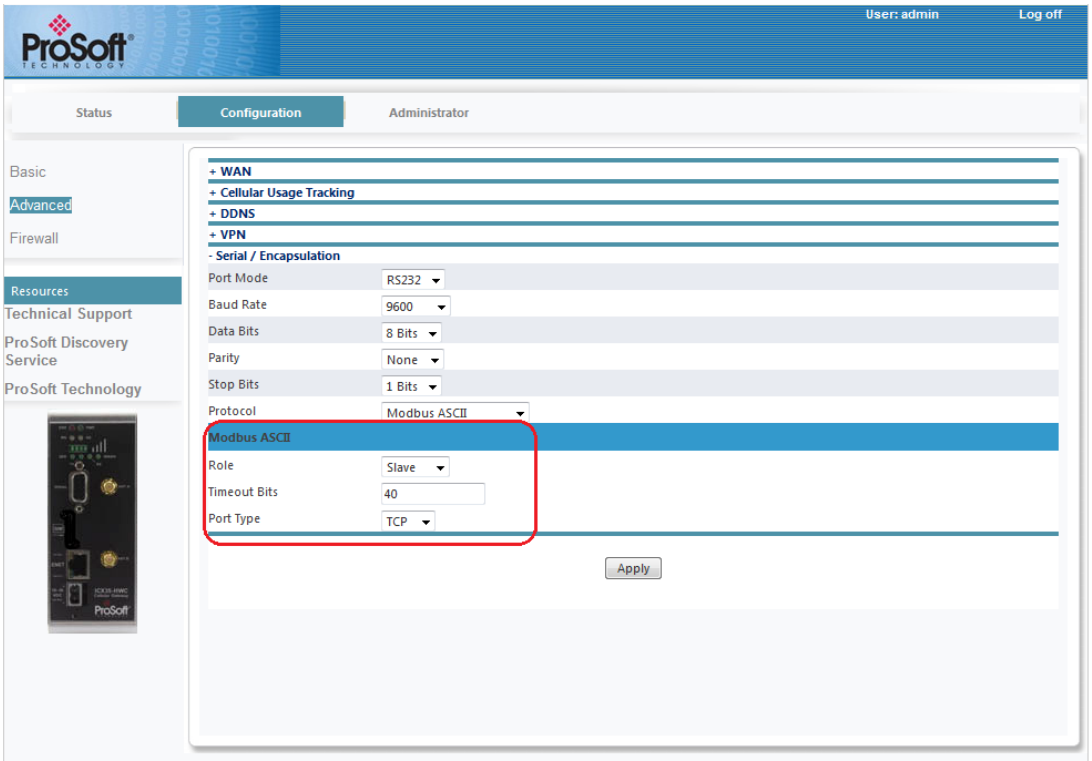
If **Slave** is selected, the *Encapsulation* table is not visible. You can add an entry to the *Client Table* list. Click on the **Add Entry to Client Table List** button.



The **Remove Selected Entries** button selects and removes entries from this list.

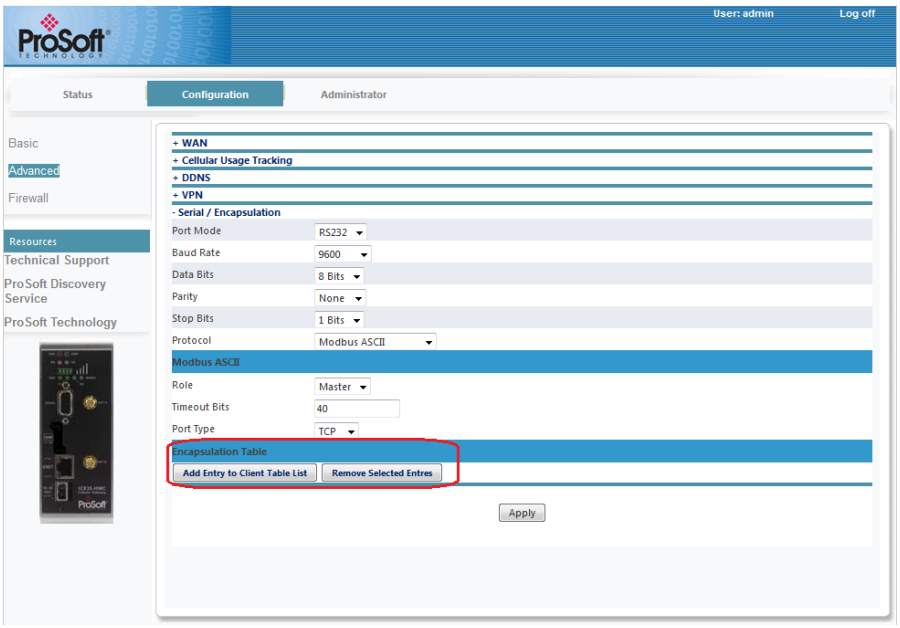
Modbus ASCII

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



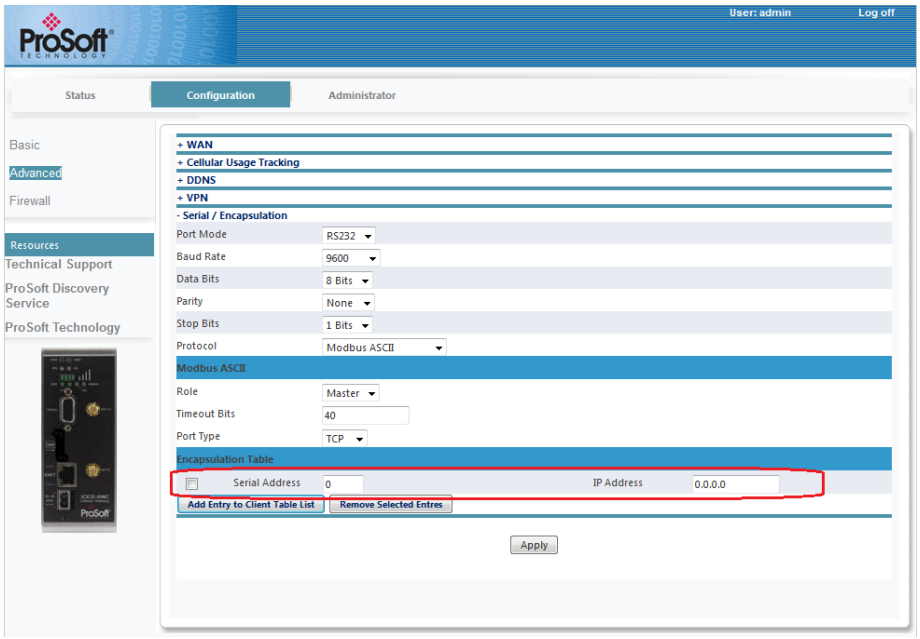
Parameter	Description
Role	Network role for the encapsulation process (Master, Slave, Master/Slave).
Timeout Bits	Sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Type of IP connection (TCP or UDP)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

The **Master** role contains additional parameters:



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

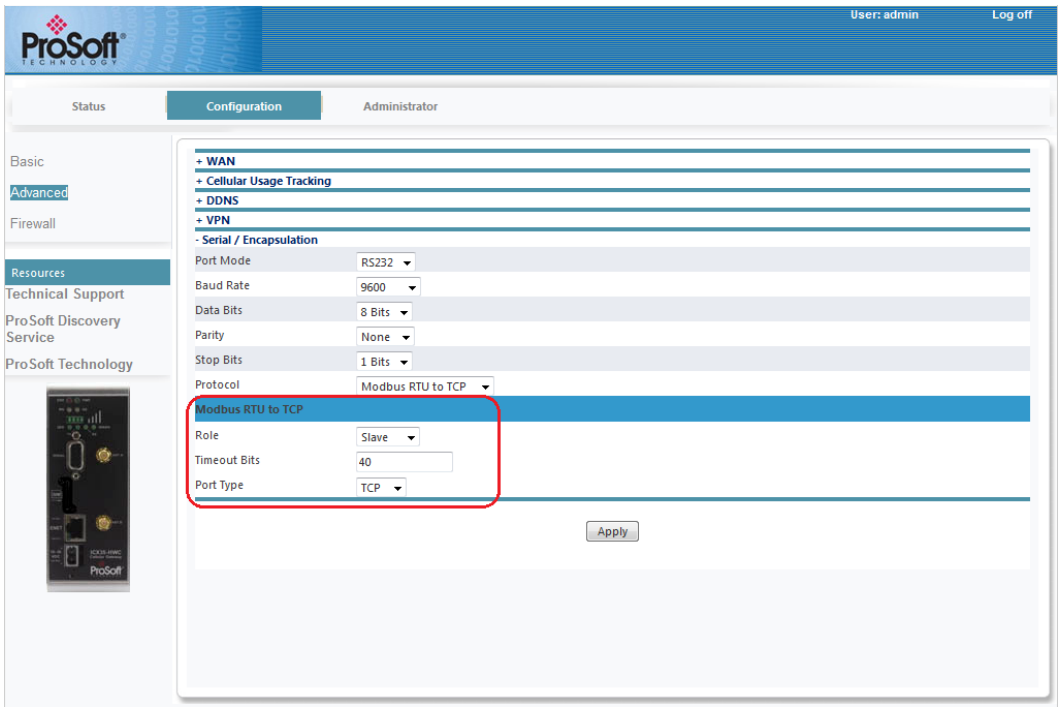
If **Slave** is selected, the *Encapsulation* table is not visible. You can add an entry to the *Client Table* list. Click on the **Add Entry to Client Table List** button.



The **Remove Selected Entries** button selects and removes entries from this list.

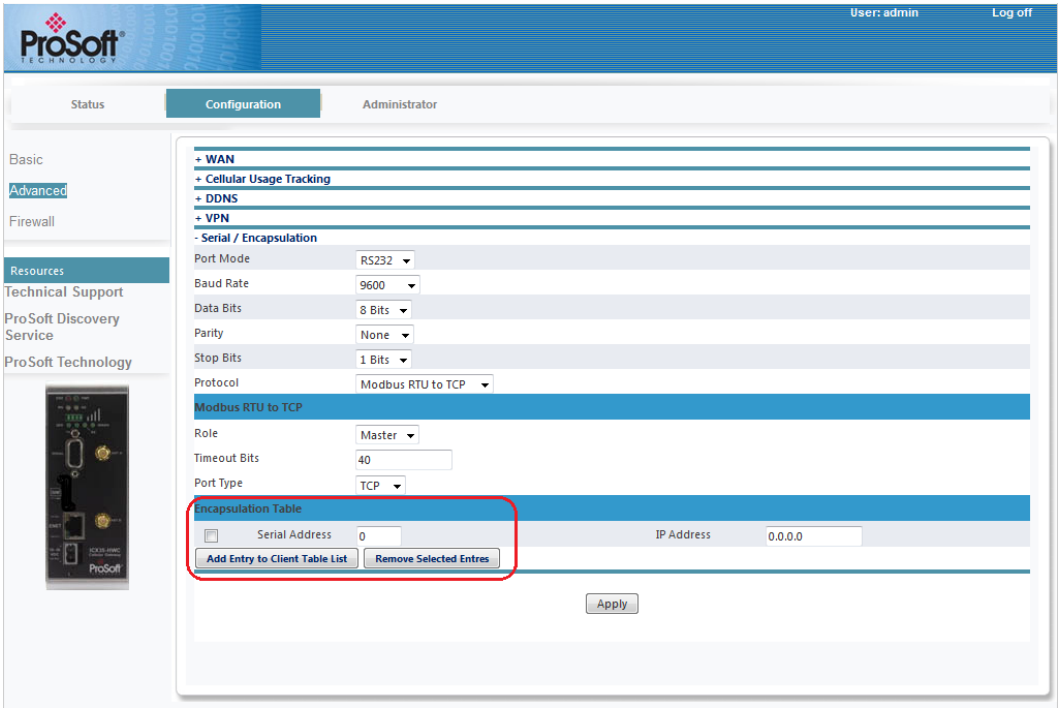
Modbus RTU to TCP

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 or UDP) for the encapsulated data.

The **Master** role contains additional parameters:



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

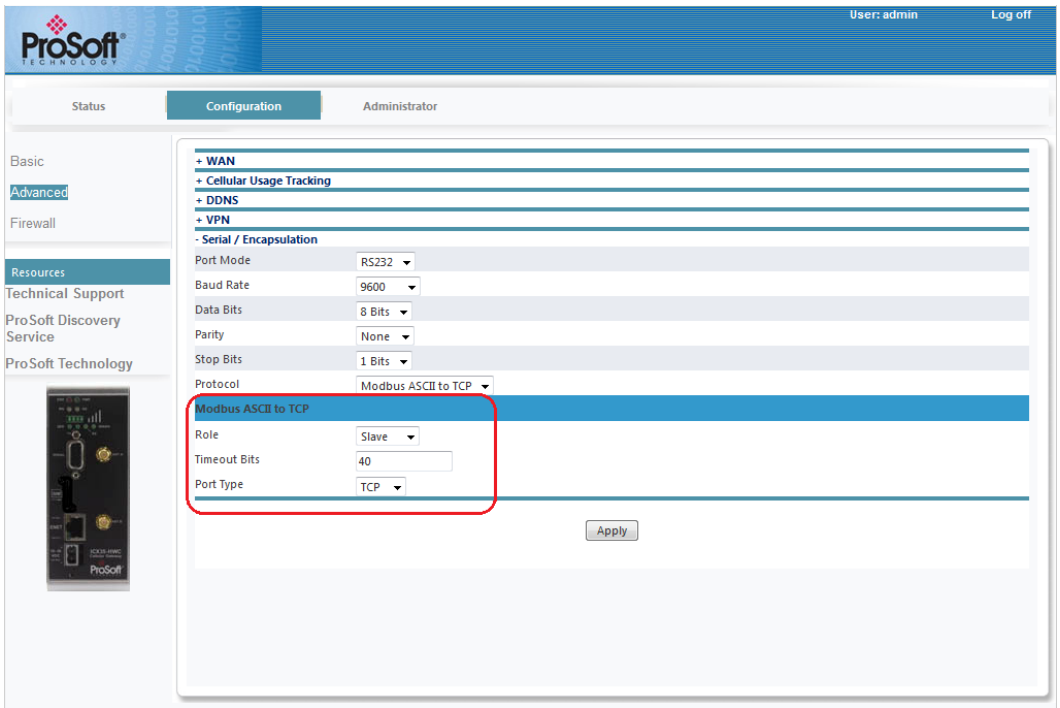
If **Slave** is selected, the Encapsulation table is not visible.

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.

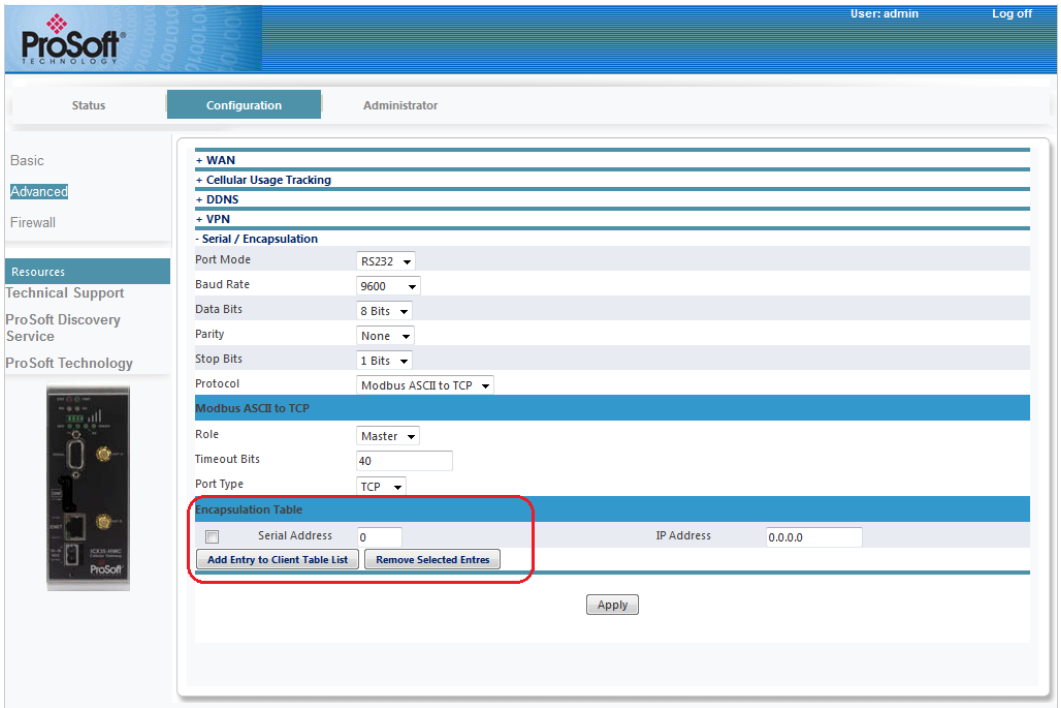
Modbus ASCII to TCP

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 or UDP) for the encapsulated data.

The **Master** role contains additional parameters:



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

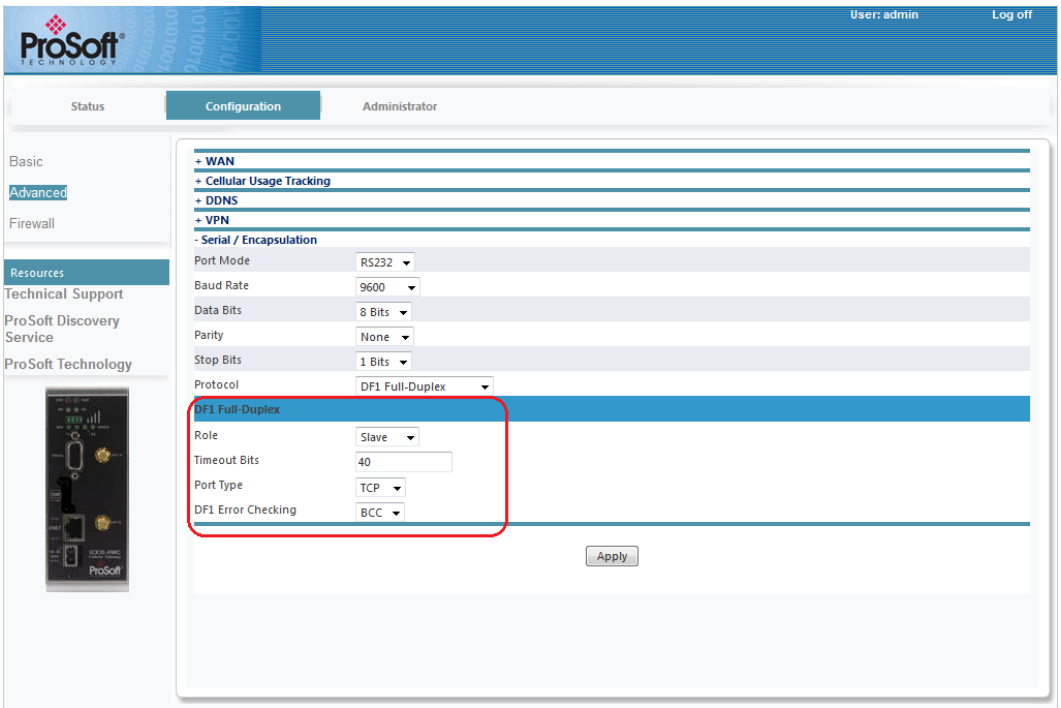
If **Slave** is selected, the Encapsulation table is not visible.

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.

DF1 Full Duplex

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



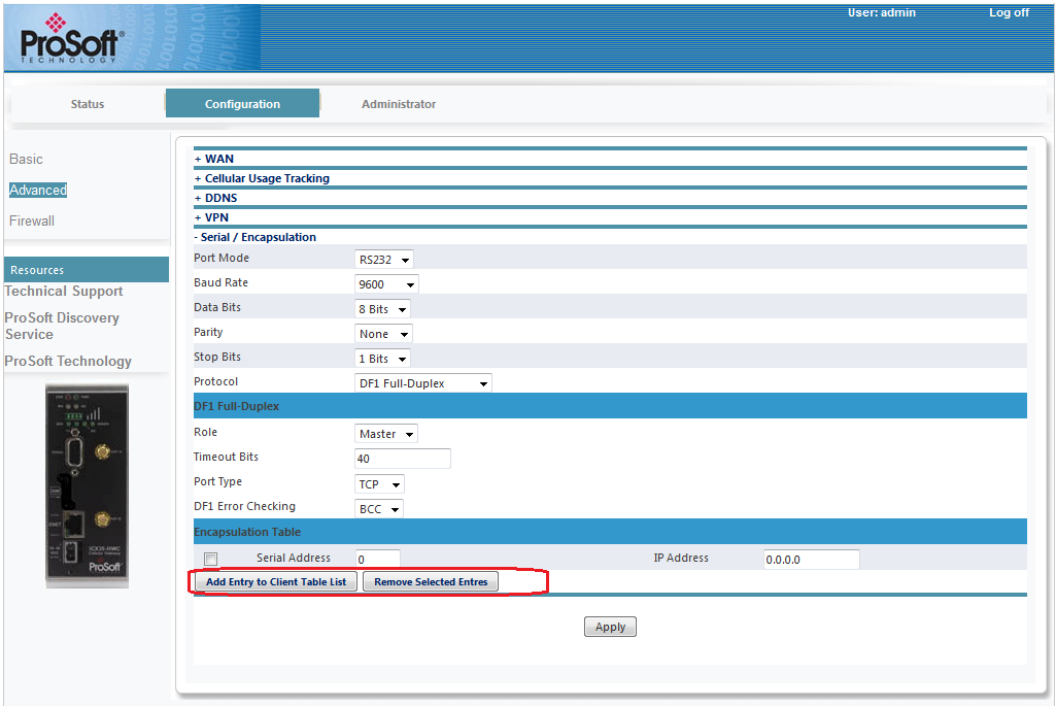
Parameter	Description
Role	Specifies the network role for the encapsulation process (Master, Slave).
Timeout Bits	Sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	Specifies the type of IP connection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

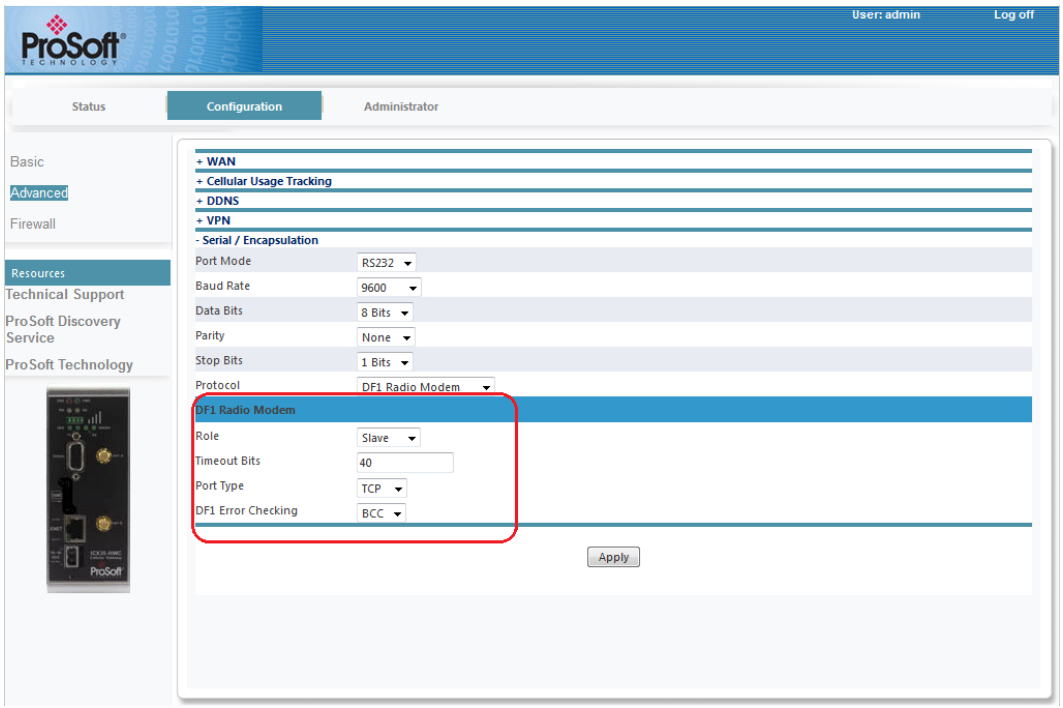
You can add an entry to the *Client Table* list. Click on the **Add Entry to Client Table List** button.



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:



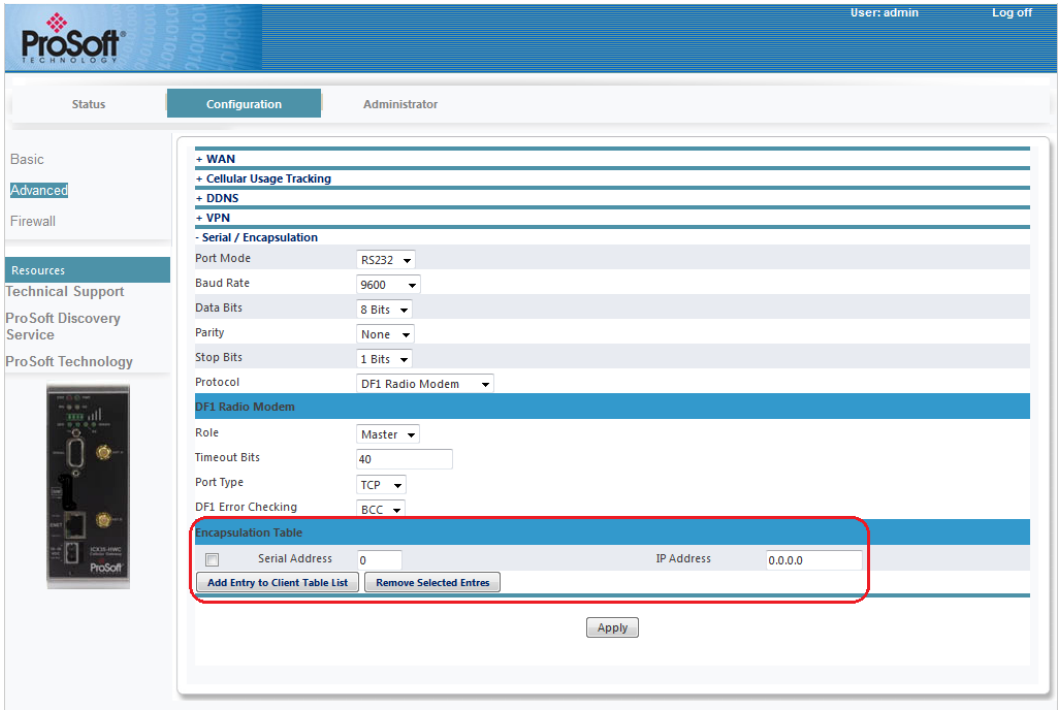
Parameter	Description
Role	Specifies the network role for the encapsulation process (Master, Slave).
Timeout Bits	This parameter sets the length of time the gateway will wait when no further serial data is received before encapsulating and transmitting data (0 to 65535).
Port Type	This parameter specifies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

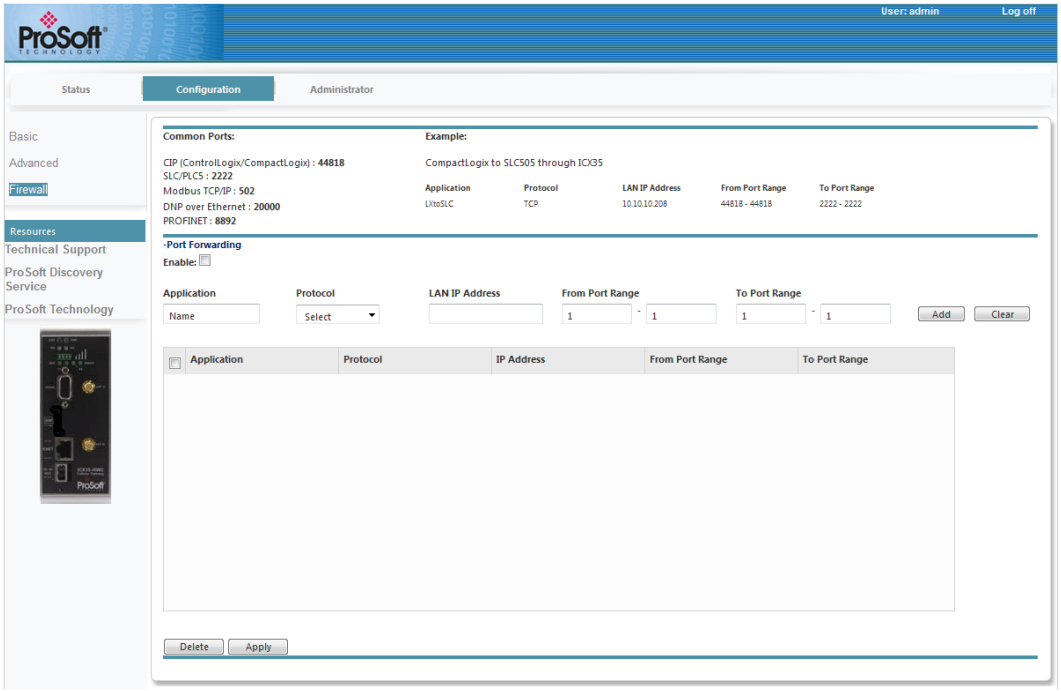
You can add an entry to the *Client Table* list. Click on the **Add Entry to Client Table List** button



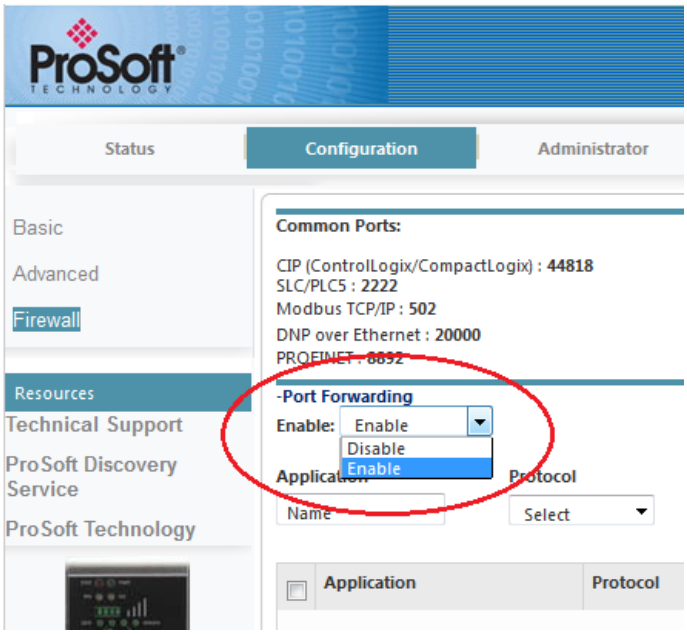
The **Remove Selected Entries** button selects and removes entries from this list.

3.2.3 Firewall

The **Configuration > Firewall** tab displays the following fields for Port Forwarding. Up to 10 mappings can be created.



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



Port Forwarding

Parameter	Description
Application	Name of particular mapping
Protocol	Packet delivery method (TCP, UDP, both)
LAN 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

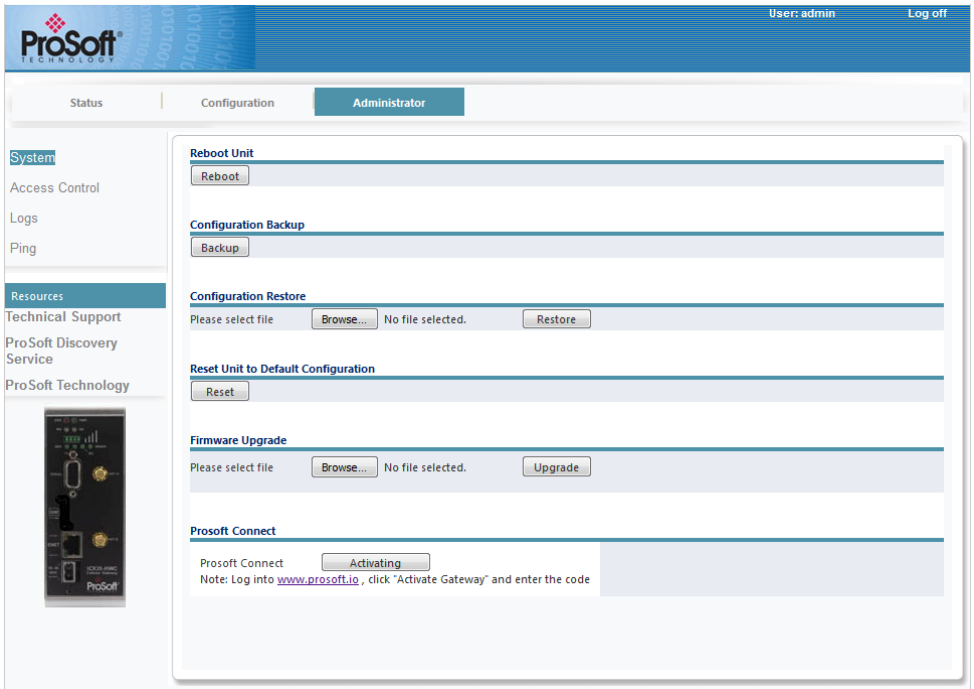
When the fields above are complete, click the **Add** button to load the parameters into the table. To remove an existing mapping in the table, highlight it and click **Delete**.

When complete, click **Apply**.

3.3 Administrator

The *Administrator* tab allows you to configure the password, record logs, update firmware, etc.

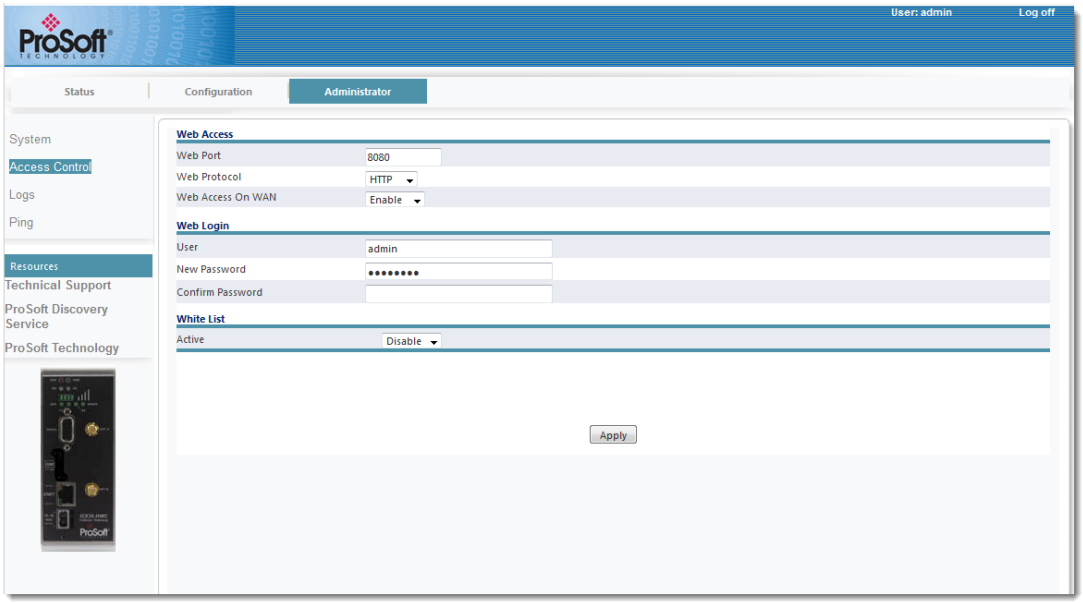
3.3.1 System



The ICX35-HWC configuration can be saved to a file for backup. The file can also be loaded back into the ICX35-HWC. Restoring to factory defaults is accomplished here as well.

Parameter	Description
Reboot Unit	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 that you want to restore. The **Restore** button restores the file.
Reset Unit to Default Configuration	Restores the ICX35-HWC to factory defaults – the previous configuration is lost.
Firmware Upgrade	Performs a firmware upgrade to the module. The **Choose File** button allows you to locate the firmware upgrade file. The **Upgrade** button allows you to upgrade the firmware using the selected file.
ProSoft Connect	Secure webpage interface to activate, setup VPN clients, invite team members, and manage multiple ProSoft cellular radios on the network.

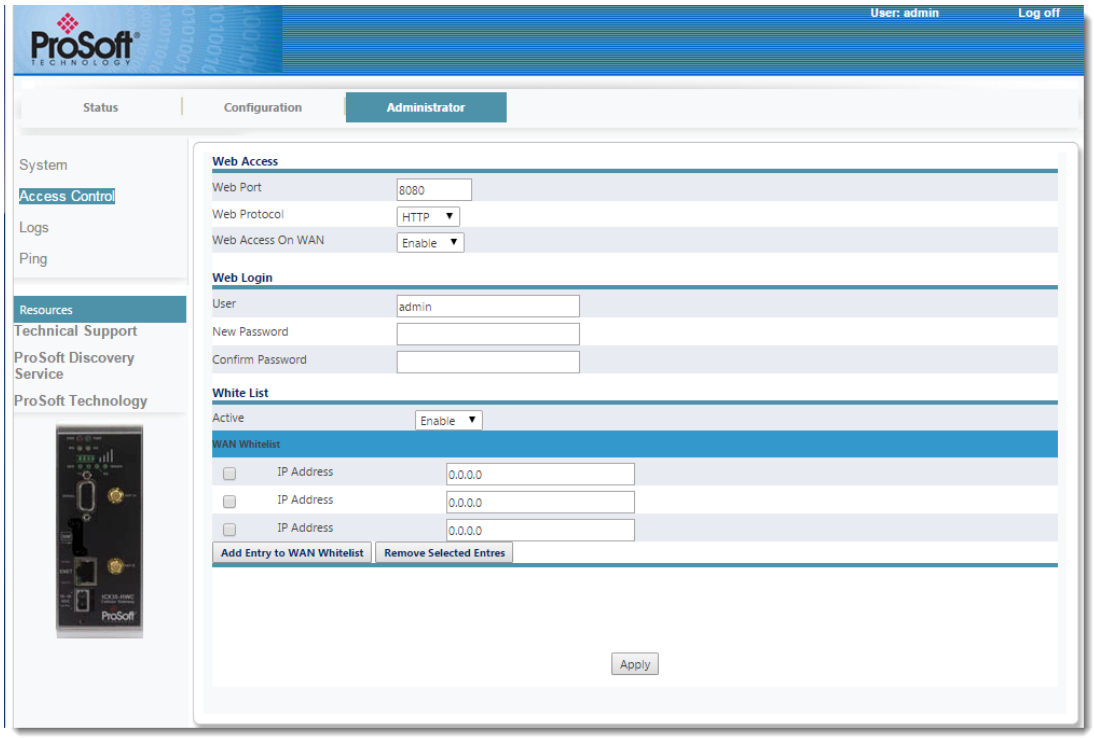
3.3.2 Access Control



Parameter	Description
Web Access	
Web Port	Web access port number
Web Protocol	HTTPS or HTTP
Web Access on WAN	Allows or blocks web page access from the WAN
User	
User Name	New login user name
New Password	New login password
Confirm Password	Confirm new password
White List	
Active	Choose **Enable** or **Disable**. If you choose **Enable**, the unit displays the **Add Entry to WAN Whitelist** button.

Adding Entries to the Whitelist

Click on the **Add Entry to WAN Whitelist** button. This unit 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.

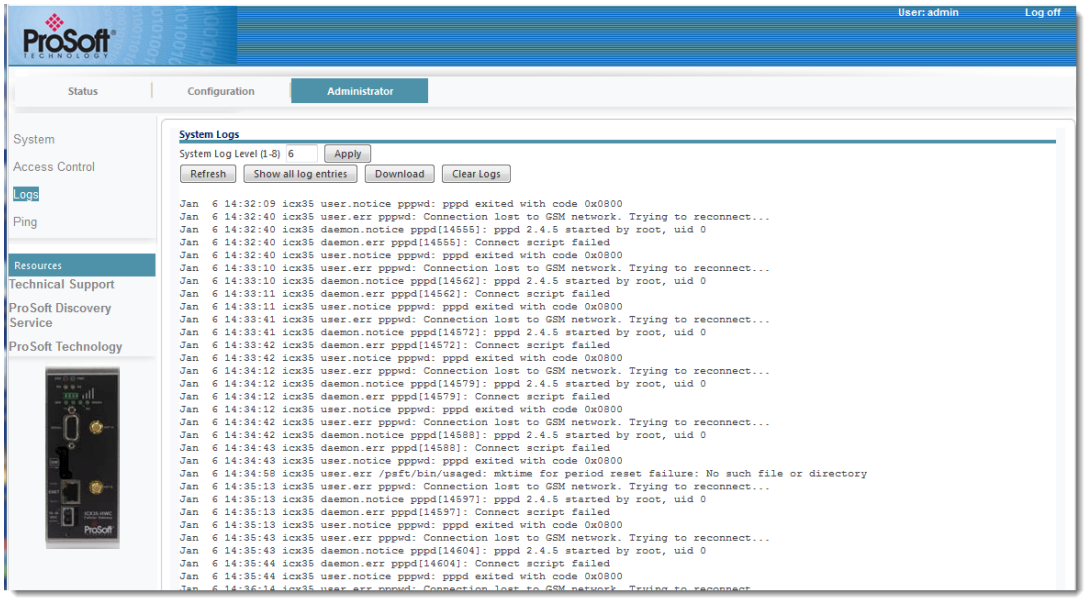
Since all VPN traffic is presumably between trusted hosts, whitelist entries are ignored (but not deleted) when an OpenVPN or IPsec tunnel is configured.

Add your entry. Use the **Add Entry to WAN Whitelist** button to add additional IPs.

To remove whitelist entries, click the checkbox of the entry and click on the **Remove Selected Entries** button.

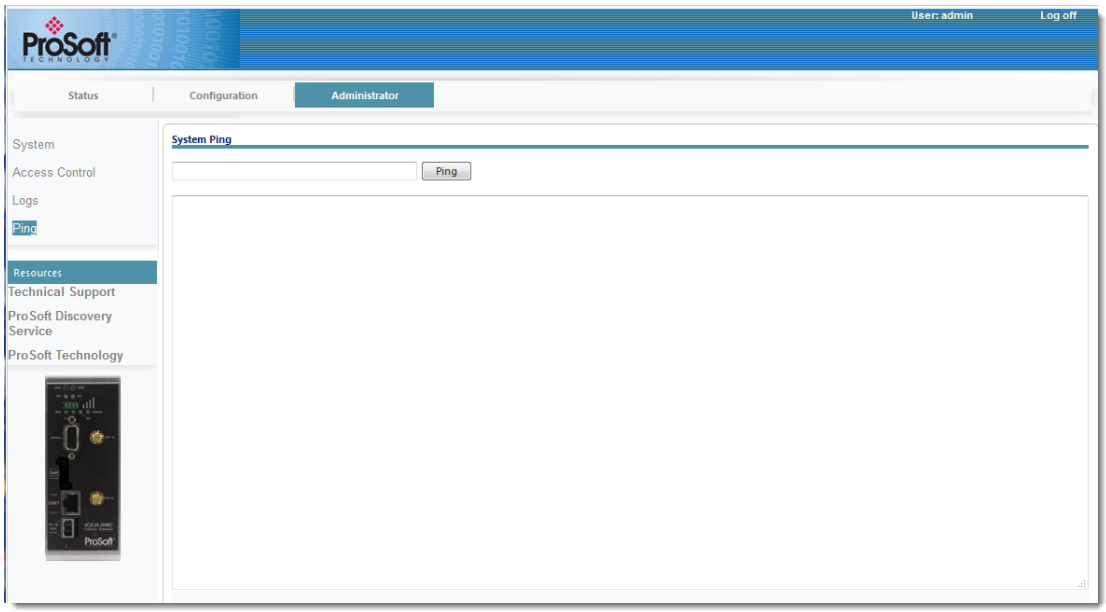
Click **Apply** when done.

3.3.3 Logs



Parameter	Description
System Log Level	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.
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

3.3.4 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 **Ping**.

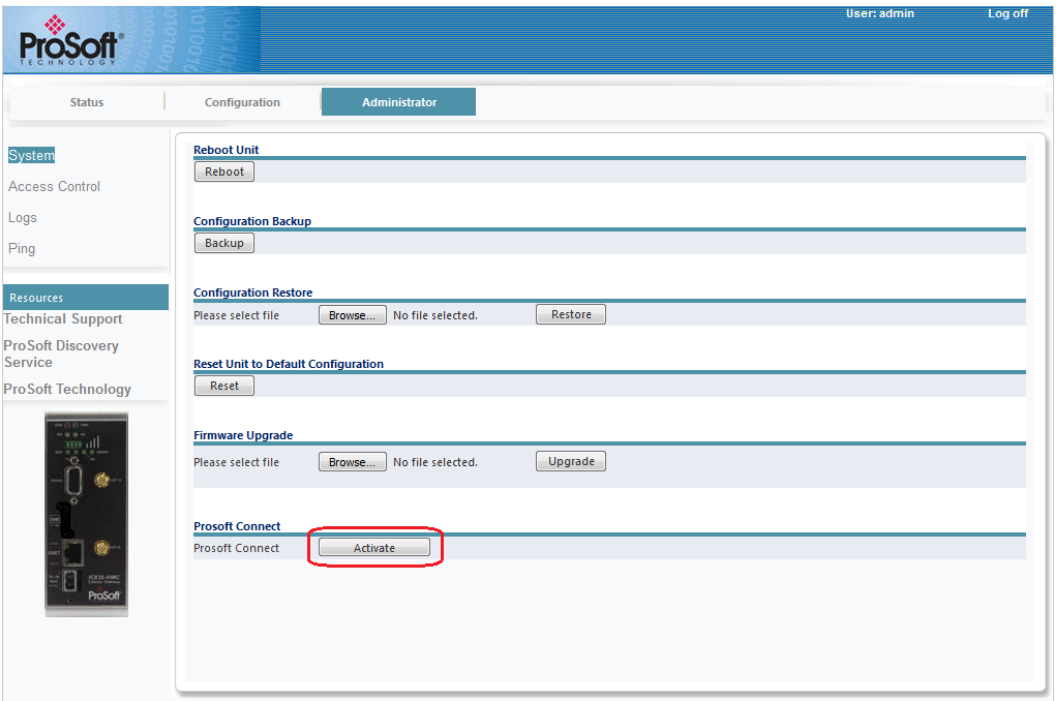
4 ProSoft Connect

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

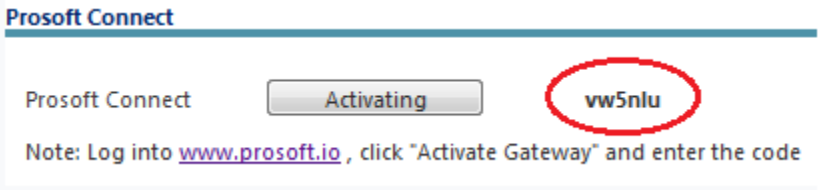
4.1 Activation

ProSoft Connect requires you to activate the ICX35-HWC upon initial use.

1. On the Configuration webpage, click on **Administrator > System.**
2. Under the *ProSoft Cloud Connect* section, click on the **Activate** button.

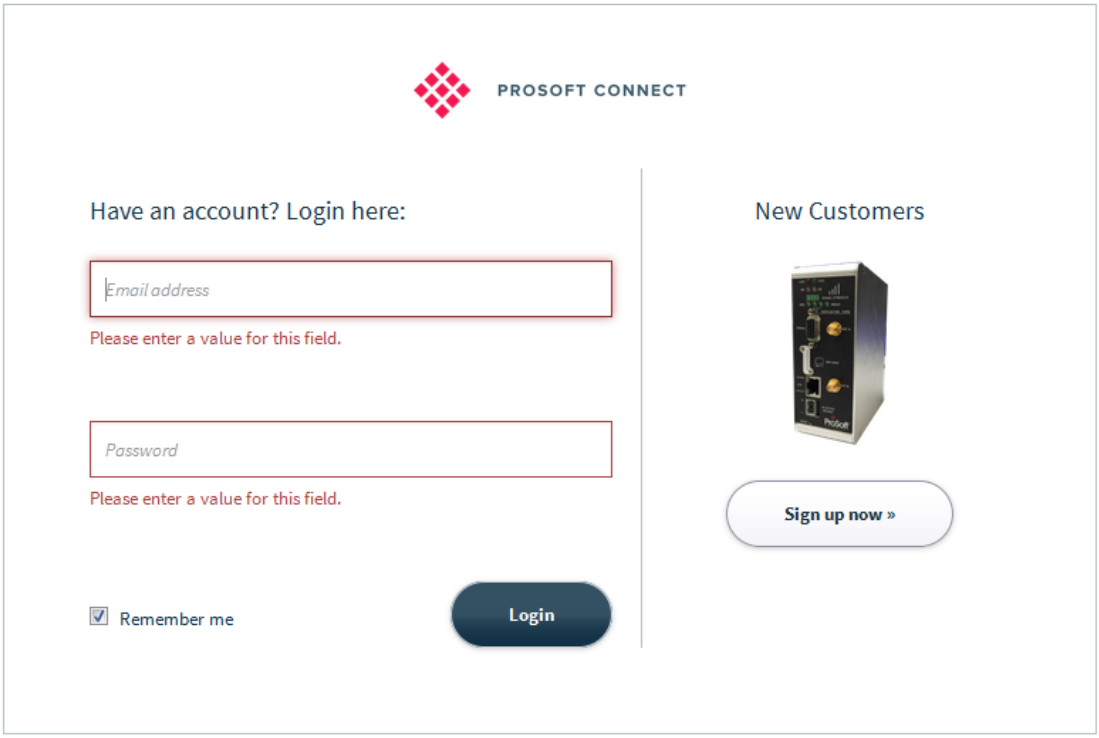


3. A six-character alphanumeric Activation Key is generated. Record this key for later use.

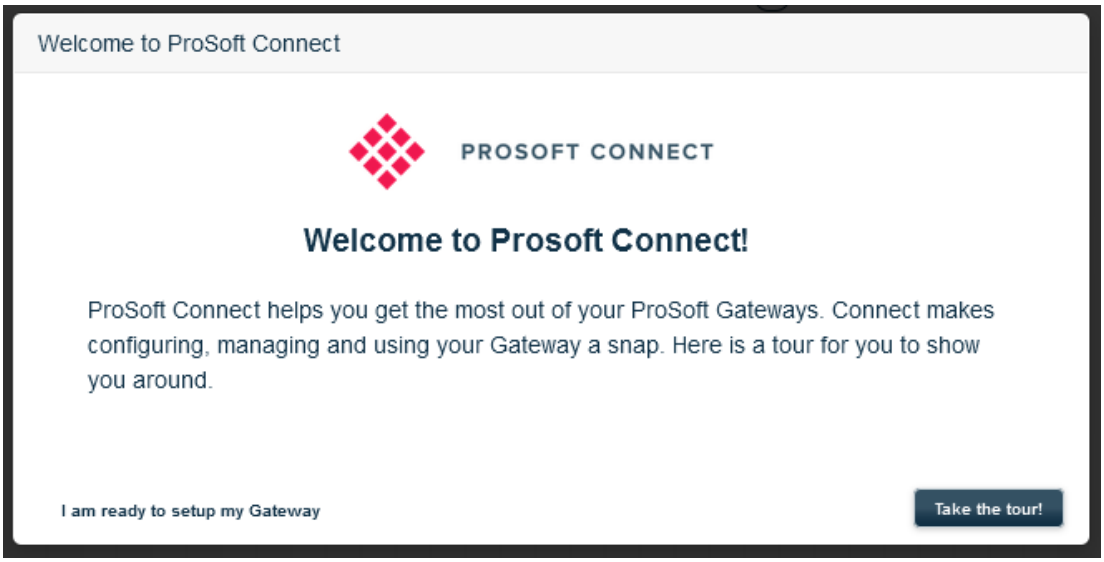


4 Click on the www.prosoft.io link. Or open a new tab in your web browser, enter www.prosoft.io, then press **Enter**.

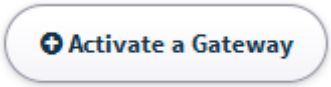
5 Enter or create an account in the ProSoft Connect log-in screen.



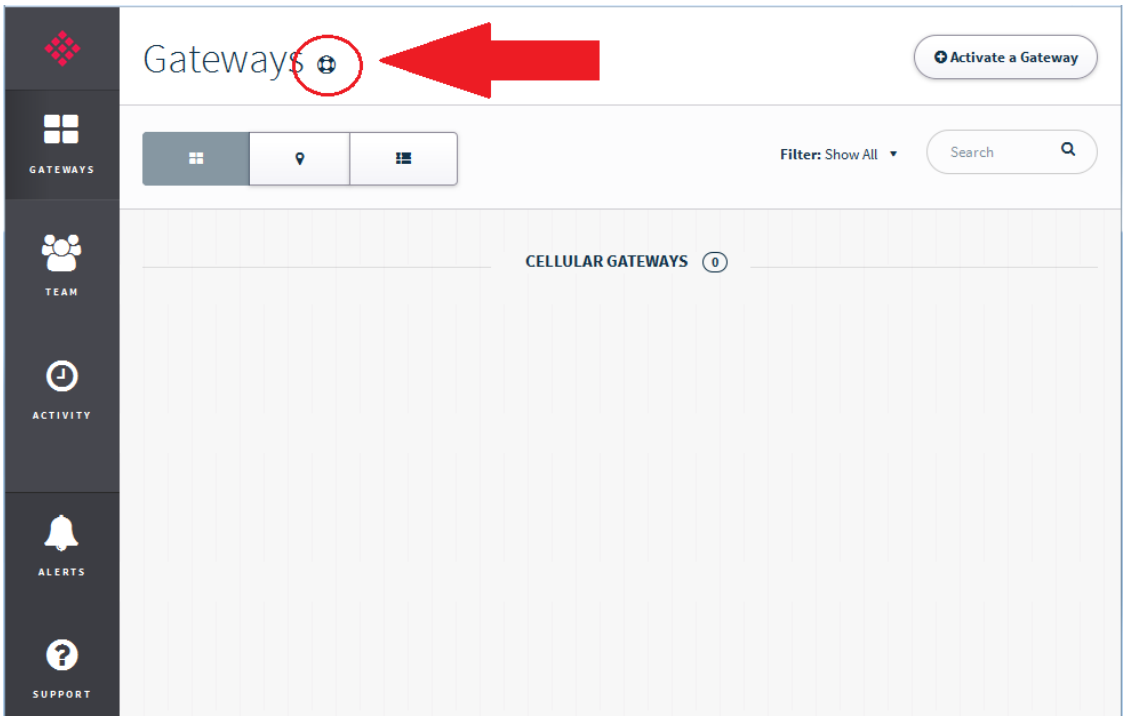
6 Once logged in, you can take a tour of the features of the ProSoft Connect utility.



7 When ready, activate the ICX35-HWC within the tour, or you can click on the **Activate 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 is in a hardened case, and designed for use in industrial and extreme environments. However, 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 a 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.

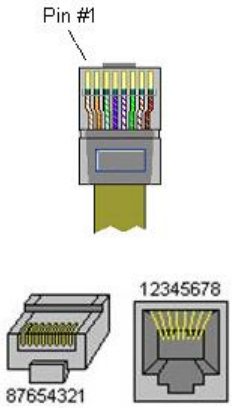
The Ethernet port on the module is Auto-Sensing. Use either a standard Ethernet straight-through cable or a crossover cable when connecting the module to an Ethernet hub, a 10/100/1000 Base-T Ethernet switch, or directly to a PC. The module will detect the cable type and use the appropriate pins to send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

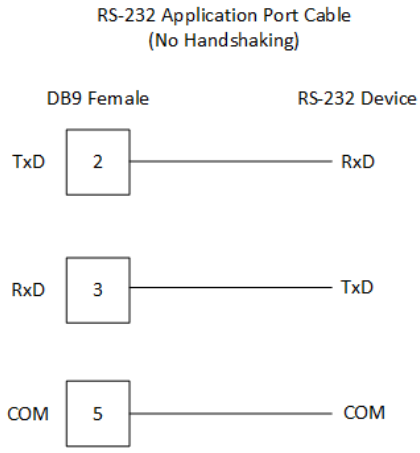
Crossover cable			Straight- through cable	
RJ-45 PIN	**RJ-45 PIN**		**RJ-45 PIN**	**RJ-45 PIN**
1 Rx+	3 Tx+		1 Rx+	1 Tx+
2 Rx-	6 Tx-		2 Rx-	2 Tx-
3 Tx+	1 Rx+		3 Tx+	3 Rx+
6 Tx-	2 Rx-		6 Tx-	6 Rx-



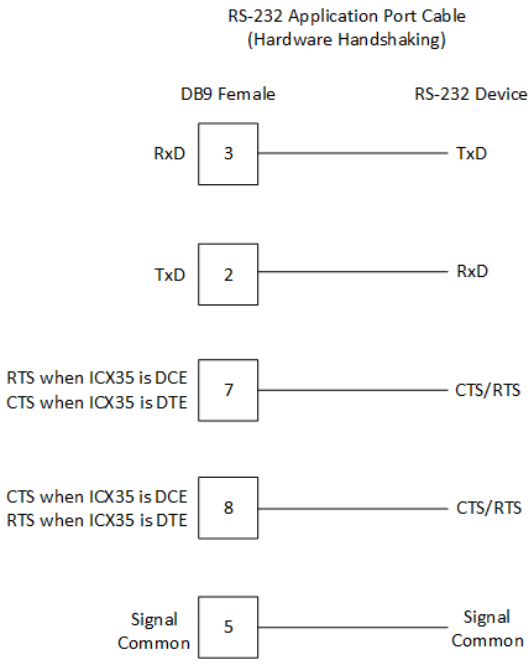
5.2.2 Serial Port Basics

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:

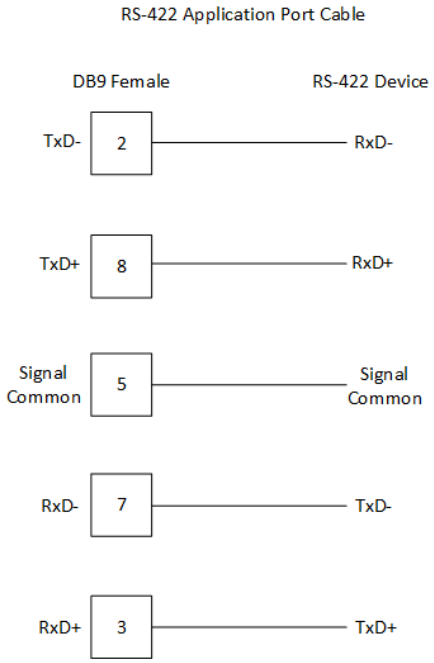


If hardware handshaking is required, the cable to connect to the port is as shown below:



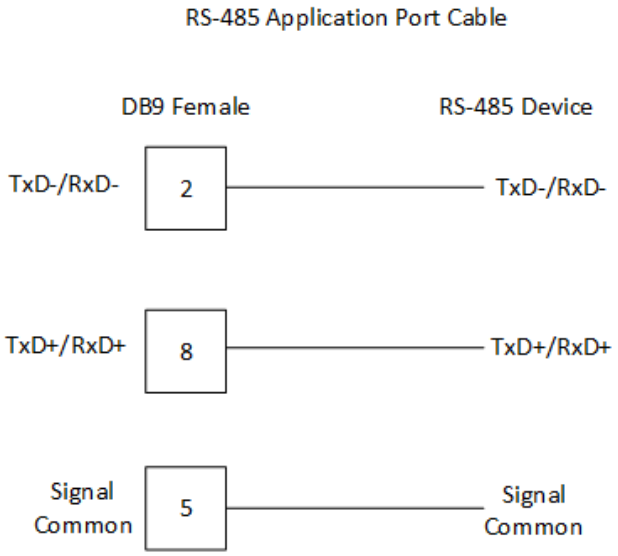
RS422

The RS-422 interface requires a single four or five wire cable. The Common connection is optional, depending on the RS-422 network devices being used. The cable required for this interface is shown in the following diagram:



RS-485 Application Port(s)

The RS-485 interface requires a single two or three wire cable. The Common connection is optional, depending on the RS-485 network devices used. The cable required for this instance is shown in the following diagram:



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 config/minor error/No SIM
NS (Network Status)	Off	ICX35-HWC is powered off
	Solid Green	Connected to cellular tower
	Blinking Green	Attempting to connect to cellular tower
	Solid Red	Duplicate IP (E/IP) /Non-recoverable network fault
	Blinking Red	Established connection timeout (E/IP) / Minor network fault

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	The port is actively transmitting data
RX	Off	No Activity on the port
	Flashing Green	The 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	LED flashes at a steady, slow rate: *0.2 Hz (5 sec) ON *4 Hz (250 ms) OFF	ICX35-HWC is powered and searching for a connection.
Faster blink	LED flashes at a steady, faster rate: *About 3 Hz (333 ms) blink rate	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 ICX35-HWC Tech Notes (Example Configurations)

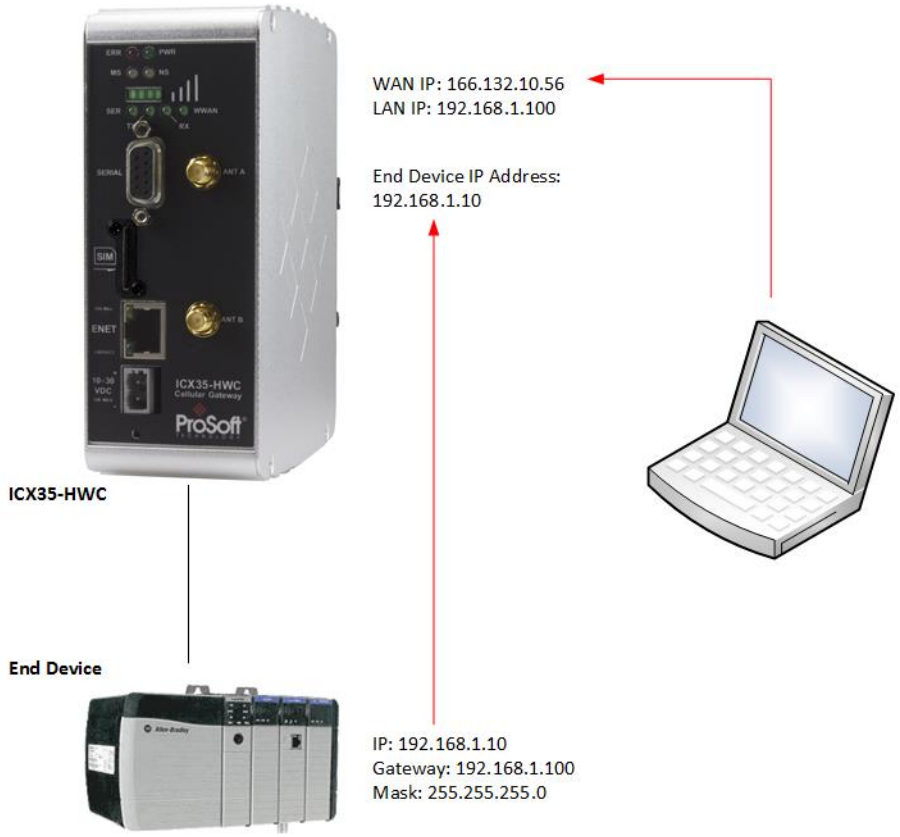
This section describes example configurations of the ICX35-HWC using:

- Pass-thru (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.

6.1 Pass-Thru Mode (End Device to End Device)

The following diagram illustrates a pass-thru mode configuration example:



In this scenario, the user on the laptop wants to communicate with a CLX.

To configure the ICX35-HWC, you must supply:

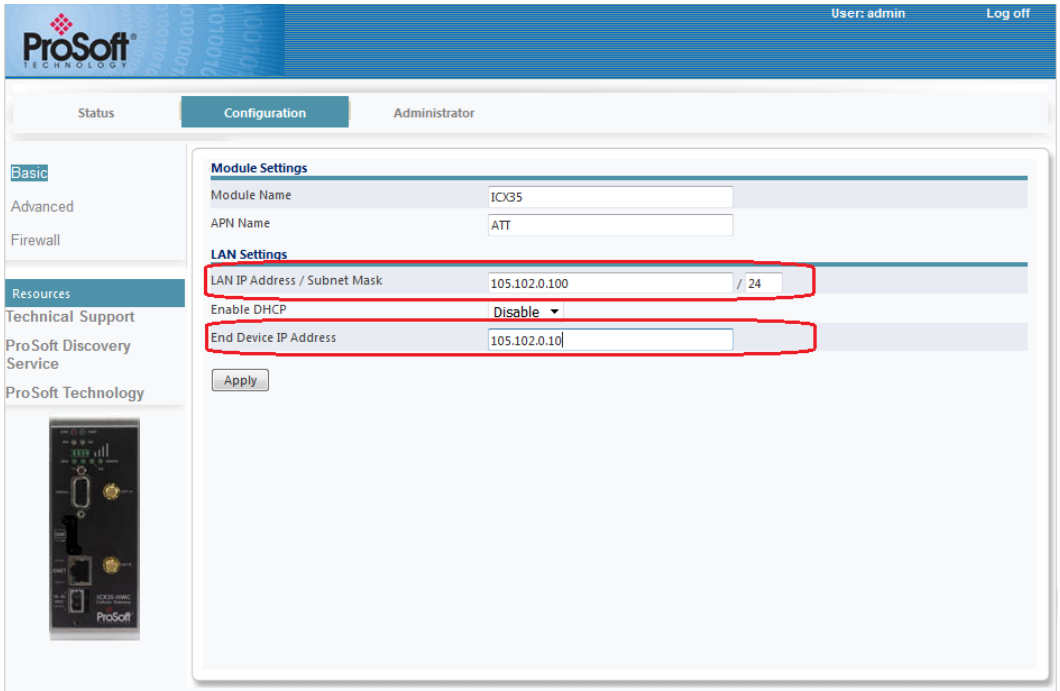
- WAN IP – This number is supplied by the cellular provider.
- Module Name
- APN Name – This is provided by the cellular provider
- LAN IP
- End Device IP Address

To configure the end device, you must supply:

- IP Address
- Mask
- Gateway IP Address

6.1.1 ICX35-HWC Configuration Parameters

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



Using the previous example, the LAN IP of the ICX35-HWC is **192.168.1.100**. This is configured in the **LAN IP Address/Subnet Mask** field as shown.

The *End Device IP Address* (also known as the pass-thru IP) is the IP Address of the device connected to the ICX35-HWC (193.168.1.10).

6.1.2 End Device Parameters

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

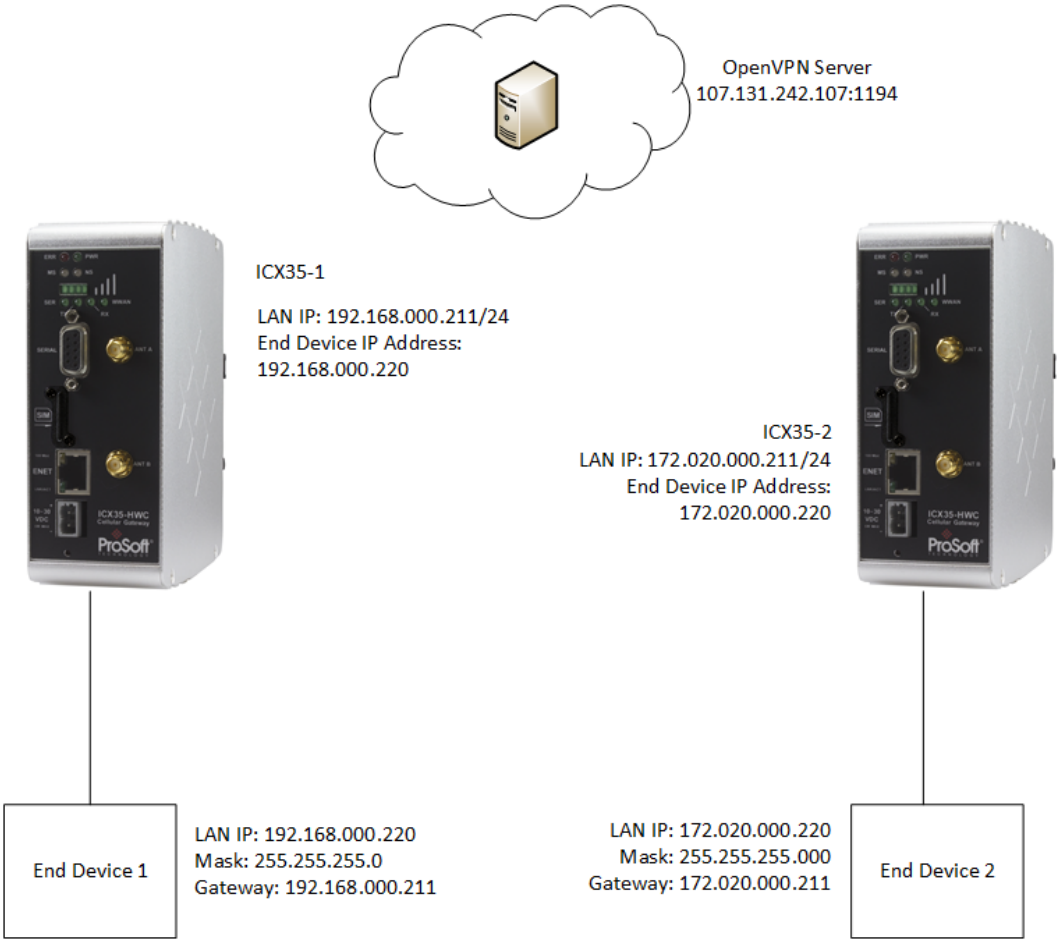
- The IP Address of the end device must match the end device IP Address configured on the ICX35-HWC.
- The Gateway Address on the end device must point to the LAN IP Address/Subnet Mask address of the ICX35-HWC.

6.1.3 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).

6.2 Pass-Thru and OpenVPN Example

The following diagram illustrates using a pass-thru 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-thru device.

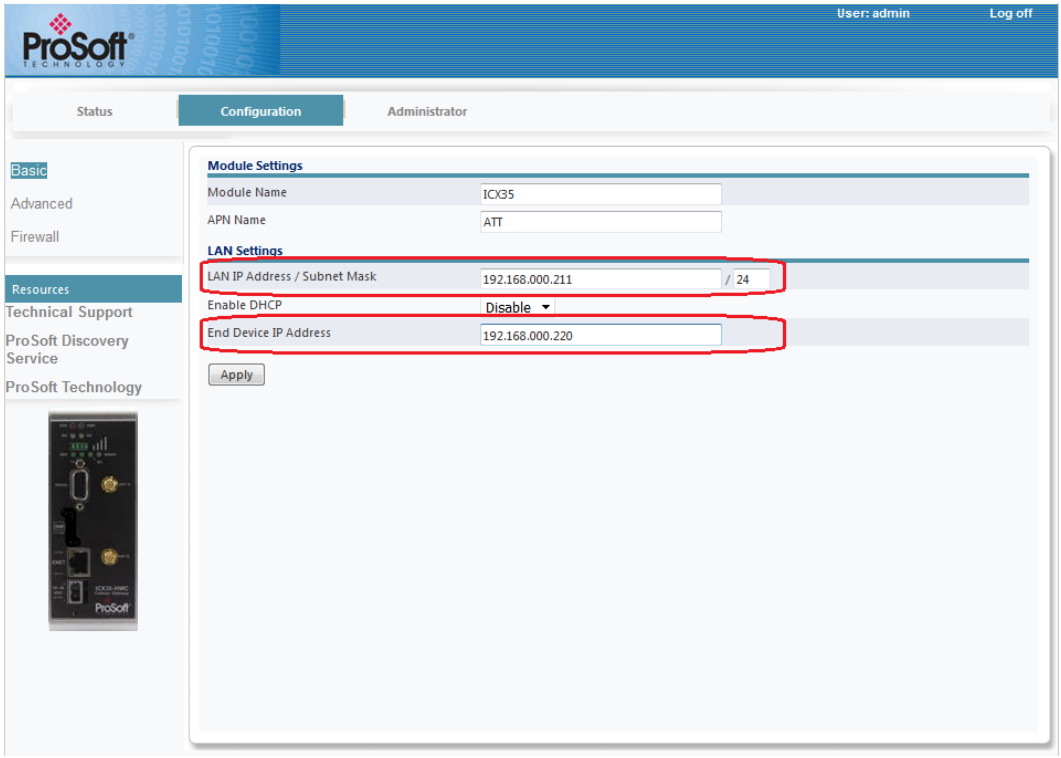
You must establish standard End Device-to-End Device communications before attempting to configure an OpenVPN tunnel.

6.2.1 ICX35-1 Configuration Parameters

In this scenario, configure the *ICX35-1* for pass-thru.

1 Log into the ICX35-1 internal web server.

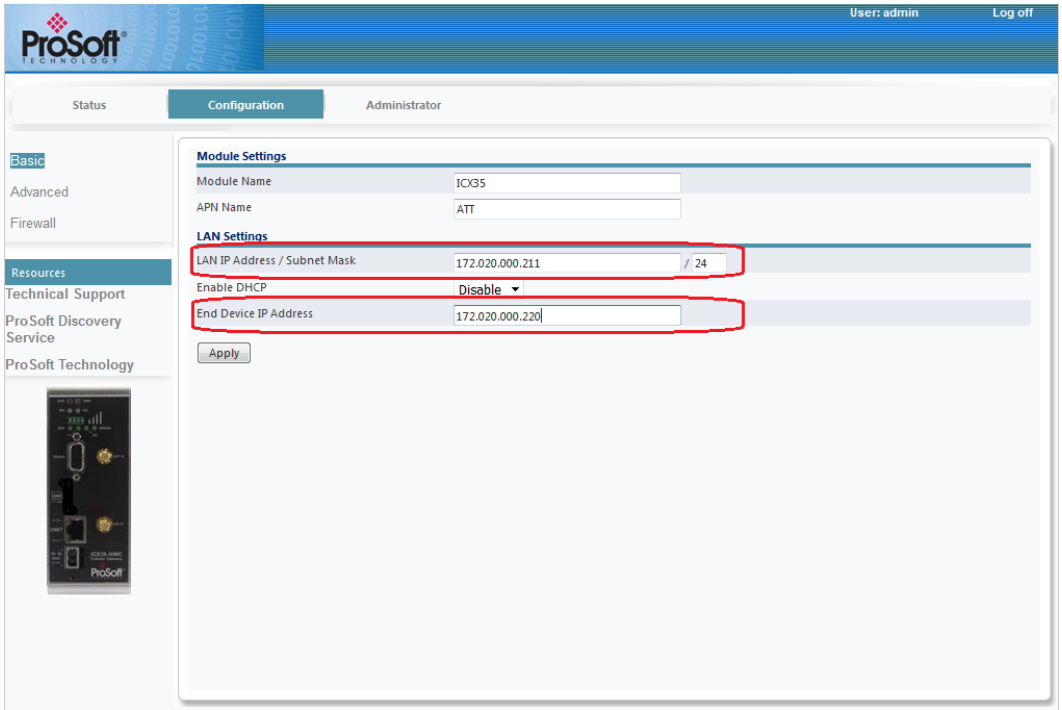
2 Navigate to **Configuration > Basic**.



3 Enter the LAN IP of the *ICX35-1* in the **LAN IP Address/Subnet Mask** field.

4 Enter the LAN IP of End Device 1 in the **End Device IP Address** field. This address must match the IP address configured on the end device. In this case, 192.168.000.211 as shown in the diagram.

5 Perform the same procedure on the *ICX35-2* using the LAN IP of the *ICX35-2* and the End Device IP as shown.



6.2.2 Configuring End Device 1

- The IP address of the end device connected to *ICX35-1* must match the IP address configured on the *ICX35-1 End Device IP Address* field.
- The Gateway parameter must match the VPN address for the *ICX35-1*.

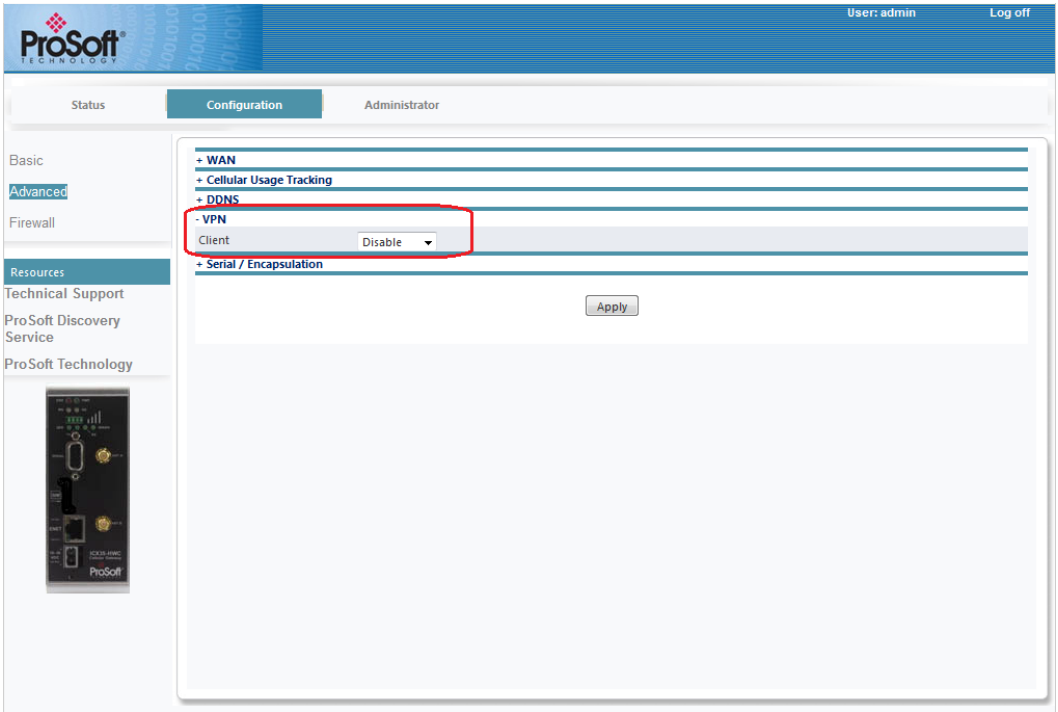
6.2.3 Configuring End Device 2

- The IP address of the end device connected to *ICX35-2* must match the IP address configured on the *ICX35-2 End Device IP Address* field.
- The Gateway parameter must match the VPN IP address for the *ICX35-2* once connected.

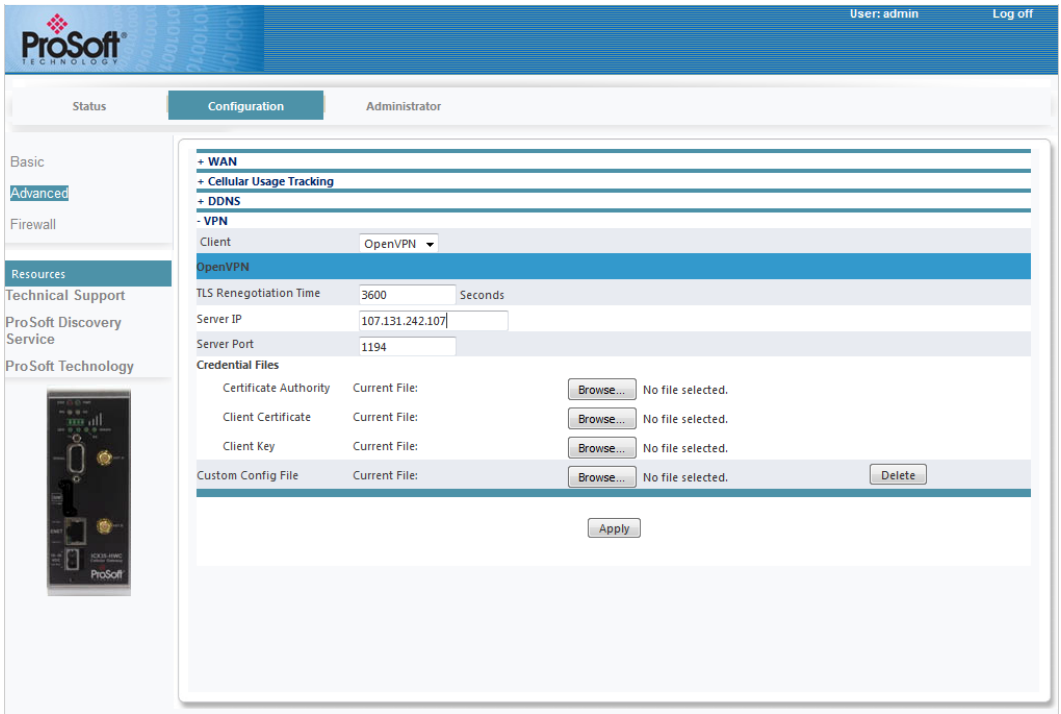
6.2.4 Configuring OpenVPN Parameters

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.

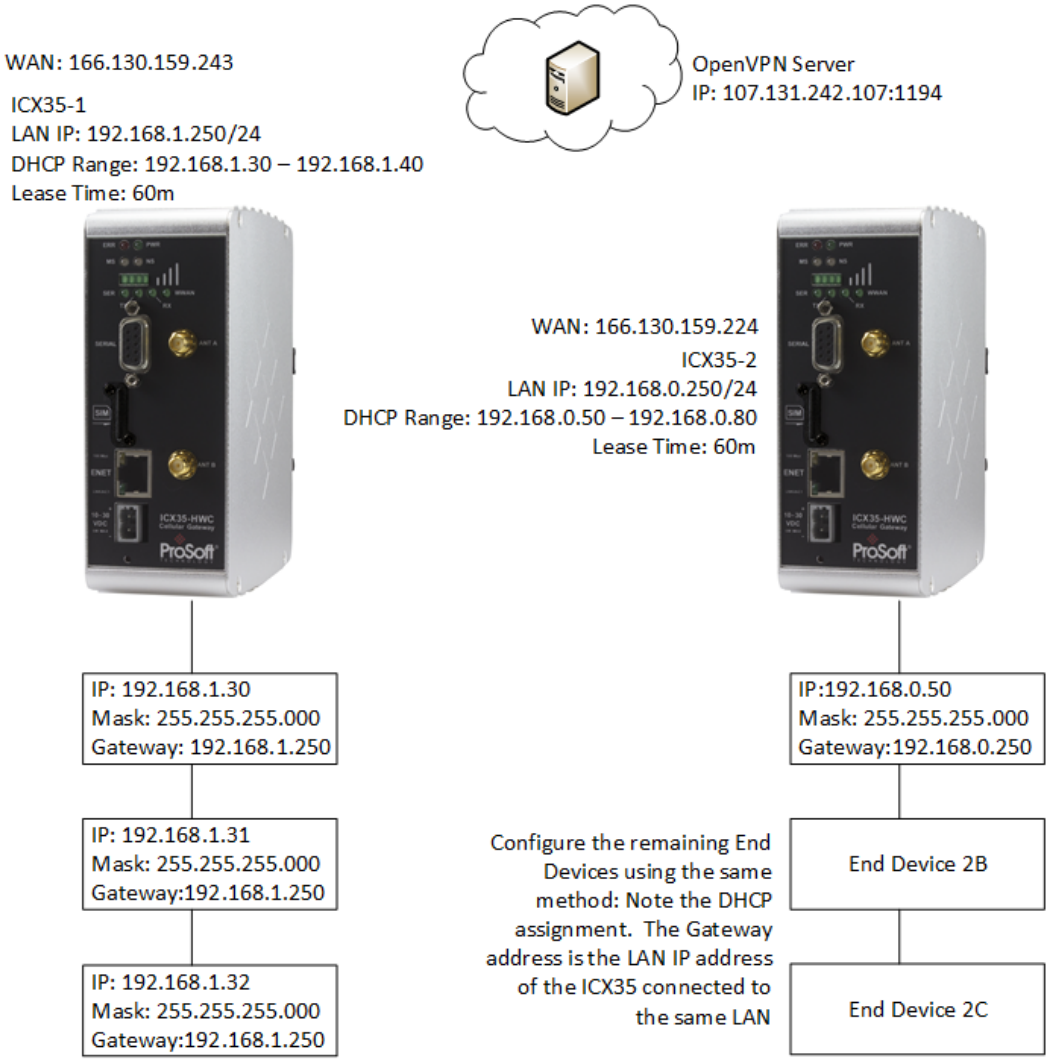


4 Enter the in seconds in the TLS *Time* field.
5 Enter the OpenVPN server's IP Address in the **Server IP** field.
6 Enter the Server Port number in the **Server Port** field. This is the port assigned to the OpenVPN Server shown at the top of the diagram.

7. Choose the **Credential** files. Your Server Administrator will provide three certificate files. Browse to the location of these files and select for all three fields. Your Server Administrator will specify which files should be uploaded to the appropriate fields.
8. Click **Apply**.
9. Perform the same procedure for the *ICX35-2*.

6.3 OpenVPN with DHCP Enabled (Example)

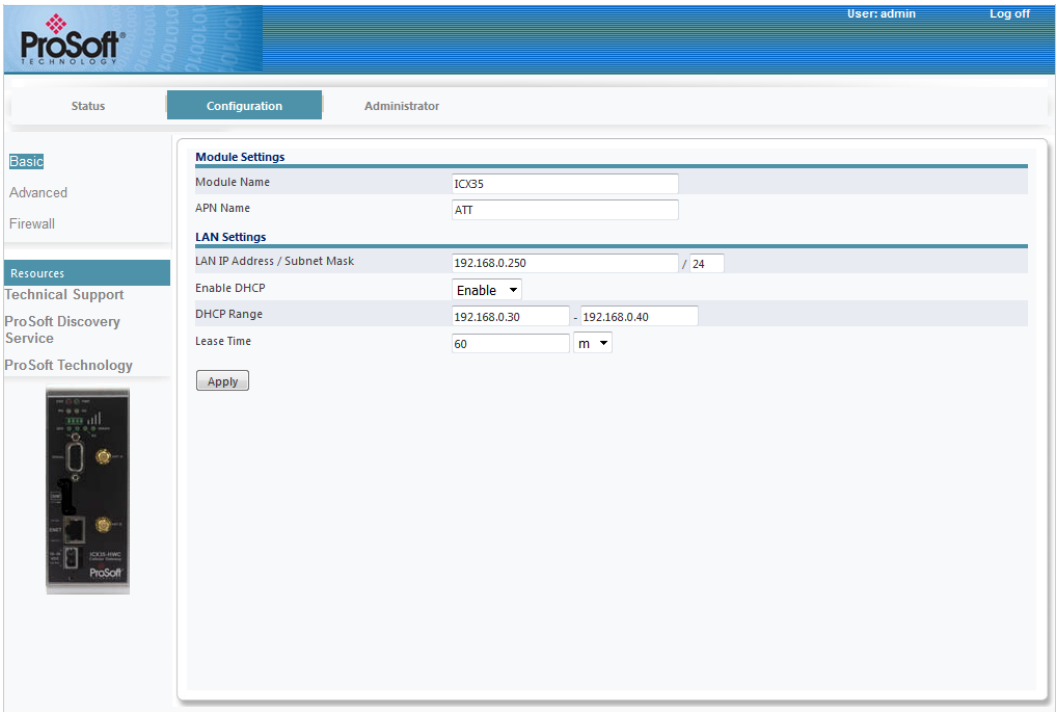
The following diagram illustrates the use of OpenVPN with DHCP enabled.



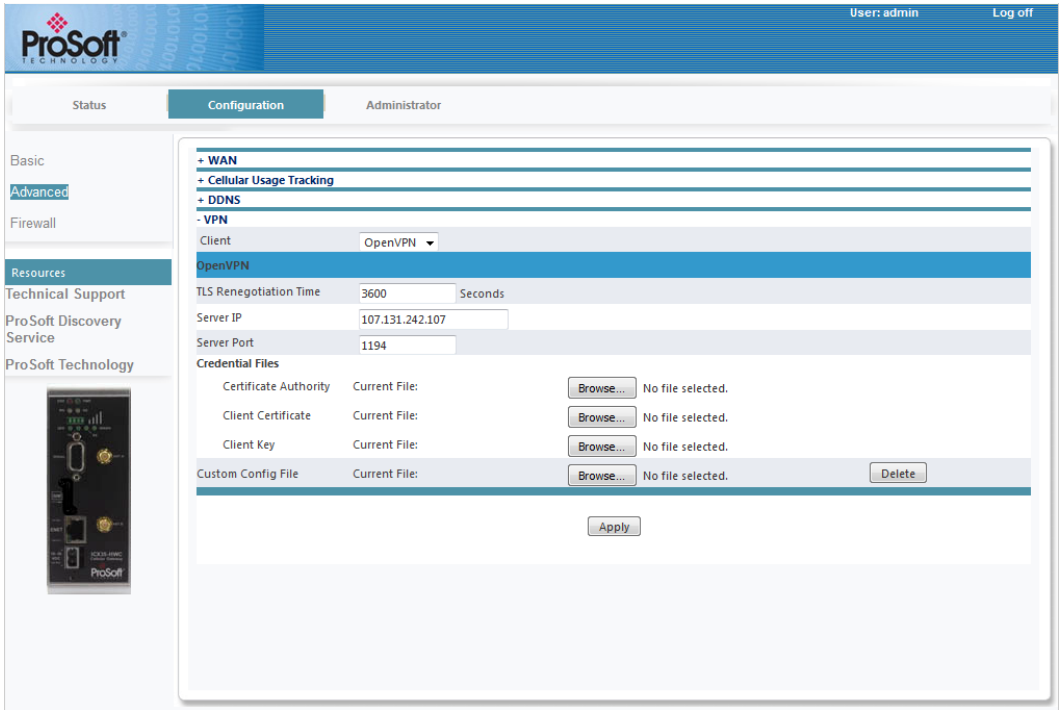
6.3.1 ICX35-1 Configuration

The *ICX35-1* shown in the diagram is configured in the *ICX35-1* web page as follows.

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



3 Enter the name of the module in the **Module Name** field.
4 Enter the APN name in the **APN Name** field. Get this from your cellular provider.
5 Enter the LAN IP and subnet mask in the **LAN IP Address/Subnet Mask** field for the *ICX35-1*.
6 Select **Enable** from the *Enable DHCP* 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 **Apply**.
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 Choose and upload the **Credential Files**. Your Server Administrator will provide you with the certificate files and location.
16 Click **Apply**.

6.3.2 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.

6.3.3 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.

7 GSM Communication (AT&T®)

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.

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

8 Support, Service & Warranty

In This Chapter

8.1 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:

1 Product Version Number
2 System architecture
3 Network details

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

1 Module configuration and associated ladder files, if any
2 Module operation and any unusual behavior
3 Configuration/Debug status information
4 LED patterns
5 Details about the serial, Ethernet or Fieldbus devices interfaced to the module, if any.

Note: *For technical support calls within the United States, ProSoft's 24/7 after-hours phone support is available for urgent plant-down issues. Detailed contact information for all our worldwide locations is available on the following page.*

Internet	Web Site: www.prosoft-technology.com/support E-mail address: support@prosoft-technology.com
Asia Pacific (location in Malaysia)	Tel: +603.7724.2080 E-mail: asiapc@prosoft-technology.com Languages spoken include: Chinese, English
Asia Pacific (location in China)	Tel: +86.21.5187.7337 x888 E-mail: asiapc@prosoft-technology.com Languages spoken include: Chinese, English
Europe (location in Toulouse, France)	Tel: +33 (0) 5.34.36.87.20 E-mail: support.EMEA@prosoft-technology.com Languages spoken include: French, English
Europe (location in Dubai, UAE)	Tel: +971-4-214-6911 E-mail: mea@prosoft-technology.com Languages spoken include: English, Hindi
North America (location in California)	Tel: +1.661.716.5100 E-mail: support@prosoft-technology.com Languages spoken include: English, Spanish
Latin America (Oficina Regional)	Tel: +1-281-2989109 E-Mail: latinam@prosoft-technology.com Languages spoken include: Spanish, English
Latin America (location in Puebla, Mexico)	Tel: +52-222-3-99-6565 E-mail: soporte@prosoft-technology.com Languages spoken include: Spanish
Brasil (location in Sao Paulo)	Tel: +55-11-5083-3776 E-mail: brasil@prosoft-technology.com Languages spoken include: Portuguese, English

8.2 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 on the ProSoft Solutions DVD or go to www.prosoft-technology.com/legal

Documentation is subject to change without notice.

Index