

Where Automation Connects.



PLX35-NB2

Network Bridge

November 8, 2024

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.

How to Contact Us

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

PLX35-NB2 User Manual
For Public Use.

November 8, 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.

Copyright © 2024 ProSoft Technology, Inc. All Rights Reserved.



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

Important Installation Instructions

Power, Input, and Output (I/O) wiring must be in accordance with Class I, Division 2 wiring methods, Article 501-4 (b) of the National Electrical Code, NFPA 70 for installation in the U.S., or as specified in Section 18-1J2 of the Canadian Electrical Code for installations in Canada, and in accordance with the authority having jurisdiction. The following warnings must be heeded:

WARNING - EXPLOSION HAZARD - SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIV. 2;

WARNING - EXPLOSION HAZARD - WHEN IN HAZARDOUS LOCATIONS, TURN OFF POWER BEFORE REPLACING OR WIRING MODULES

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

Class 2 Power

Agency Approvals and Certifications

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

Contents

Your Feedback Please	2
How to Contact Us.....	2
Content Disclaimer	2
Important Installation Instructions.....	3
Agency Approvals and Certifications.....	3
1 Start Here	6
1.1 About the PLX35-NB2 Network Bridge.....	6
1.1.1 Specifications.....	7
1.2 PLX35-NB2 Package Contents	7
1.3 Jumper Information.....	8
1.4 Failover and Automatic Backup & Factory Reset	8
1.4.1 Failover	8
1.4.2 Automatic Backup & Factory Reset.....	8
2 Quick Start	9
2.1 Local Configuration.....	9
2.2 Belden Horizon Setup and Configuration	9
3 Installing the PLX35-NB2	10
3.1 LED Indicators	11
3.1.1 Ethernet Port LEDs.....	12
4 Local Configuration Using the PLX35-NB2 Configuration Webpage	13
4.1 Connecting to the PLX35-NB2 Webpage	13
4.2 Using the Overview Tab	15
4.3 Setting Gateway Configuration Parameters	15
4.3.1 Open Source Software and License Information.....	18
4.4 Configuring Login Credentials	20
4.4.1 Advanced Configuration	21
4.4.2 Initial / Factory Reset Login	22
4.5 File Relay	25
4.5.1 Example #1: Transferring Files Across Segmented Networks Using FTP	29
4.5.2 Example #2: Transferring Files Across Segmented Networks Using SFTP	35
4.6 SD Card	40
4.7 Viewing Gateway Log file Activity	41
4.8 Importing a Configuration File.....	42
4.9 Exporting a Configuration File	43
4.10 Updating the Firmware	44
4.11 Rebooting the Gateway	45
4.12 Factory Reset.....	46
5 Cloud-based Management Using Belden Horizon	48
5.1 Log In and Activate Belden Horizon	48
5.1.1 Belden Horizon On-Prem.....	51
5.2 Creating and Connecting a New VPN Client.....	52

5.2.1	Verifying the VPN Connection	55
5.3	Using Belden Horizon to Configure the PLX35-NB2	57
5.4	Adding Team Members	58
5.4.1	Editing Team Member Access.....	60
5.5	Changing Firmware	61
5.6	Remote Packet Capture	65
6	Easy Bridge	67
6.1	VPN Tunnel Connection	67
6.1.1	Verifying VPN Tunnel Connection	73
6.2	Configuring a New Driver in RSLinx	75
6.3	Uploading .ACD Project File	77
6.4	Ending the Tunnel Connection	80
7	Ethernet Cable Specifications	82
7.1	Ethernet Cable Configuration	82
8	Appendix	83
8.1	PLX35-NB2 Network Requirements	83
8.1.1	PLX35-NB2 LAN Port	83
8.1.2	PLX35-NB2 WAN Port.....	83
8.2	PDN & SRA Tunnel Server IP/DNS Addresses.....	84
9	Support, Service & Warranty	85
9.1	Contacting Technical Support.....	85
9.2	Warranty Information	86

1 Start Here

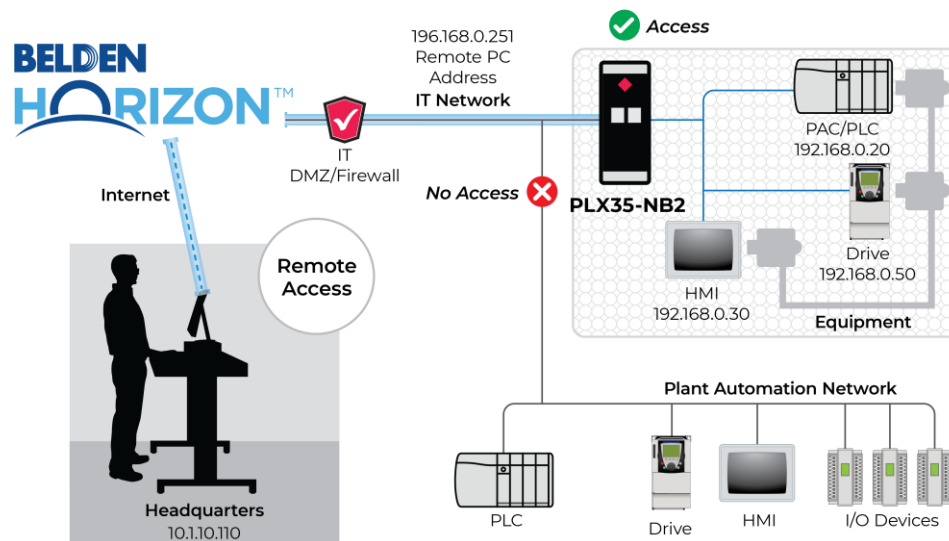
1.1 About the PLX35-NB2 Network Bridge

The PLX35-NB2 Network Bridge is the ideal solution for system integrators, machine builders, and OEMs requiring remote system access for commissioning, troubleshooting, or network maintenance.

During the commissioning phase, a network bridge is deployed on site with automation equipment. Once the equipment is installed and ready for configuration and programming, the bridge allows the user to remotely access the network to commission, maintain, and troubleshoot the system, thereby reducing travel time costs.

By deploying a network bridge to an existing network, the network bridge allows access from anywhere by authorized personnel. In the event of unscheduled downtime, an authorized user can connect to the network to minimize downtime and loss of profit.

Module configuration and remote connections are accomplished through Belden Horizon™, ProSoft Technology's secure, cloud-native platform for the Industrial Internet of Things (IoT).



The PLX35-NB2 allows users to:

- Securely connect to remote devices from any PC without having to use a 3rd-party software application
- Locally control the VPN connection through an EtherNet/IP® message.

The PLX35-NB2 provides 2 Ethernet ports. One port is used for the local network requiring remote access. The second port is used to connect to the internet.

1.1.1 Specifications

Power	Description
Power	24 VDC nominal, 10 to 36 VDC allowed, Positive, Negative, and GND terminals
Power Connector	Three pin, screw terminal, screw retention, black
Current Load	24 VDC nominal @300 mA

Internal Specifications	Description
EtherNet/IP	Supports local control of VPN access through MSG instruction.
Network Ports	HTTP or HTTPS ports 80

Physical	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	(2) 10/100 Base-T, RJ45 connector

Environmental	Description
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 PLX35-NB2 Package Contents

The following components are included with the PLX35-NB2 and are required for installation and configuration.

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

Qty.	Part Name	Part Number	Part Description
1	PLX35-NB2 Network Bridge	PLX35-NB2	2-port Network Bridge
1	2-pin Power Connector	002-0116	Power Connector

If any of these components are missing, please contact ProSoft Technology Technical Support for replacement parts. See Contacting Technical Support (page 85).

1.3 Jumper Information

The module has one visible set of jumper pins on the back of the gateway. These pins should only be jumped/shunted when resetting the gateway back to factory defaults.

To perform a factory reset:

- 1 Set the jumper on both pins and power-cycle the module.
- 2 Wait until the FLT, CFG and ERR LED's flash in a reverse-clockwise direction (the gateway should boot twice by then).
- 3 You will notice all the LED's flashing twice (except interface LED's).
- 4 Remove the jumper and wait for the gateway to finish the power-cycle.
- 5 When the factory reset has finished, the CFG LED flashes.

1.4 Failover and Automatic Backup & Factory Reset

1.4.1 Failover

The Failover process provides a recovery mechanism whenever a serious malfunction renders the main filesystem inoperable.

If the system fails to boot up (all LEDs are solid on) 4 times in a row, on the 5th boot up the gateway will enter a failover state (the FLT LED is solid red and the CFG LED blinks amber). While in this state, the PLX35-NB2 can be accessible using its default configuration. A new upgrade can be performed on the gateway which should fix the serious malfunction that led to the failover state.

1.4.2 Automatic Backup & Factory Reset

If the system fails to boot up (all LEDs are solid on) 10 times in a row, on the 11th boot up the gateway tries to restore the backup firmware and configuration. The backup firmware and configuration are in place before the last upgrade was performed.

If the backup restore procedure has performed correctly, only the PWR LED will be lit upon boot up.

The automatic factory reset process takes place when the PLX35-NB2 needs to return to the default configuration. This is because the backup restore process has not succeeded. After this process is completed, it will run the factory default image with the default configuration, in an out-of-the-box condition. In this case, there is no need to use a jumper to perform a factory reset.

If the factory reset has performed correctly, the CFG LED will blink amber.

2 Quick Start

2.1 Local Configuration

Task	Page
Install the module	10
Connect to the PLX35-NB2 webpage	13
Set gateway configuration parameters	15
Configure login credentials	20
Update firmware	44

2.2 Belden Horizon Setup and Configuration

Belden Horizon allows you to remotely configure, maintain, and troubleshoot the gateway.

Task	Page
Obtain an activation key and login to Belden Horizon	48
Create a VPN client	52
Establish a VPN Connection	52
Perform configuration functions in Belden Horizon	57
Add Team Members	58
Change Firmware if required	61

3 Installing the PLX35-NB2

Mount the PLX35-NB2 such that:

- There is easy access for the cables to ensure that they are not bent, constricted, near high amperage, or exposed to extreme temperatures.
- The LEDs on the front panel are visible for troubleshooting and verifying the gateway status.
- There is adequate airflow around the gateway, but also protected from direct exposure to the elements, such as sun, rain, and dust.

Caution: The PLX35-NB2 is in a hardened case and is designed for use in industrial and extreme environments; however, unless the cables are expressly designed for such environments, the cables can fail if exposed to the same conditions the PLX35-NB2 can withstand.

3.1 LED Indicators

The following table describes the diagnostic LEDs on the PLX35-NB2.

LED	State	Description
MGMT	Off	The module cannot reach the internet and is not managed by Belden Horizon (default).
	Flashing Green	The module can reach the internet.
	Solid Green	The module is managed by a Belden Horizon account.
	Solid Red	N/A
	Flashing Red	The module is configured to be managed by Belden Horizon but cannot reach Belden Horizon.
	Alternating Red/Green	N/A
VPN	Off	Belden Horizon is not enabled (default).
	Flashing Green	VPN is possible (normal).
	Solid Green	A VPN tunnel is established.
	Solid Red	The module is managed by Belden Horizon and EIP has disabled VPN tunneling.
	Flashing Red	VPN connection failed.
	Alternating Red/Green	N/A
PWR (Power)	Off	Power is not connected to the power terminals or source is insufficient to properly power the module.
	Solid Green	Sufficient power is connected to the power terminals.
FLT (Fault)	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 <i>Reset</i> button or cycle power to clear the error.
CFG	Off	Normal operation
	Flashing Amber	The module has no configuration.
	Solid Amber	The module is in configuration mode. Either a configuration error exists, or the configuration file is currently being downloaded or read. After power-up or after the <i>Reset</i> button is pressed, the configuration is read and the module implements the configuration values and initializes the hardware.
ERR	Off	Normal operation
	Flashing Amber	An error condition has been detected and is occurring on one of the application ports. Check configuration and troubleshoot for communication errors.
	Solid Amber	The ERR LED is cleared on receipt of a well-formed allowed packet. On receipt of data packet containing an unsupported protocol, the LED is lit. If the LED is solid, a large number of errors are occurring on one or more ports (network communication errors).

3.1.1 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.

4 Local Configuration Using the PLX35-NB2 Configuration Webpage

The PLX35-NB2 contains a browser-based configuration webpage used for configuration. The following sections describe the configuration process.

4.1 Connecting to the PLX35-NB2 Webpage

- 1 Ensure that the module is connected to the network through the LAN port.
- 2 Apply power to the module.
- 3 To log into the PLX35-NB2 configuration webpage through the network, your PC must be able to connect to the PLX35-NB2. The default IP address of the PLX35-NB2 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 (where xxx is an available address on the network).

IP address:	<input type="text" value="192 . 168 . 0 . "/>
Subnet mask:	<input type="text" value="255 . 255 . 255 . 0"/>

Note: ProSoft Discovery Service can be used to discover the IP address. Download and install ProSoft Discovery Services from the ProSoft website at www.prosoft-technology.com.

- 4 In a web browser, enter the PLX35-NB2 default address of **192.168.0.250**. Minimum browser requirements: Chrome 58, Firefox 54, and Internet Explorer 10.
- 5 In the PLX35-NB2 configuration webpage, enter the **USERNAME** and **PASSWORD** to log in. The default **USERNAME** is *admin* and the default **PASSWORD** is *password*.

ProSoft

Login here:

Remember me

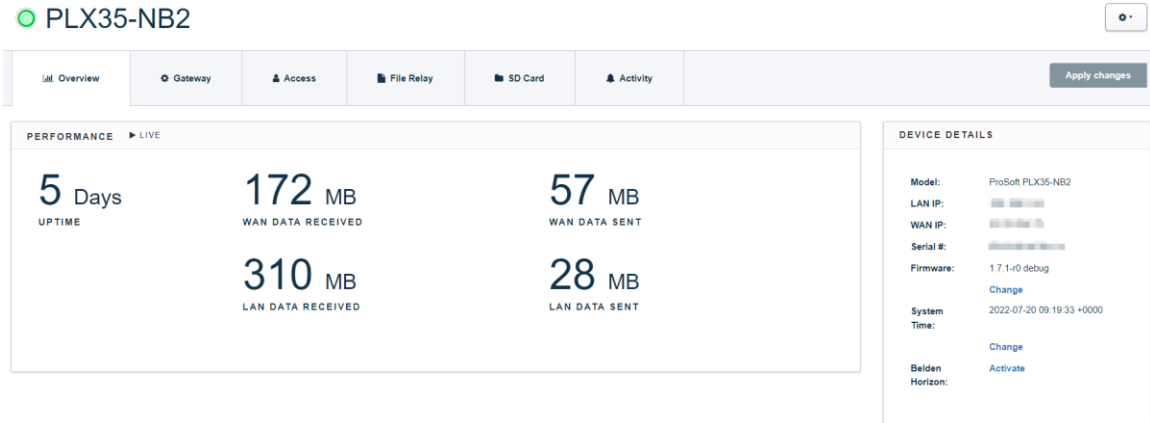
Login

PLX35-NB2

Minimum browser requirements:
Chrome 58, Firefox 54, Internet Explorer 10

Note: For security purposes, it is required to change the default username and password after initial login or factory reset. See *Initial / Factory Reset Login* on page 22.

6 After successful log in, the configuration webpage displays the *Overview* tab.



This page allows you to:

- View Performance Information
- View Device Details
- Update Firmware
- Manually enter a custom date and time

7 After 5 consecutive failed login attempts, login is suspended for 10 minutes. The login details and status is logged in *syslog* and */psft/loginRecords.txt* (The last 100 login attempts are logged).



4.2 Using the Overview Tab

The *Overview* tab contains performance information as well as device details, access information, and module location information.

In addition, this page allows you to make firmware updates to the gateway. You can view this tab at any time by simply clicking on the *Overview* tab.

Tip: This tab provides an *Activation Code* that allows you to take advantage of configuring and maintaining your gateway using Belden Horizon. See *Cloud-based Maintenance using Belden Horizon on page 48* for details on using this code.

4.3 Setting Gateway Configuration Parameters

- 1 Click on the *Gateway* tab.

The screenshot shows the configuration interface for the Gateway tab. At the top, there are navigation tabs: Overview, Gateway (selected), Access, File Relay, SD Card, and Activity. Below the tabs, the configuration is organized into sections:

- GATEWAY**
 - Gateway Name: PLX35-NB2
 - Description: Prosoft
 - Address: [Empty field]
 - Advanced configuration... (link)
- LOCAL AREA NETWORK**
 - IP: 192.168.0.26
 - Subnet: 255.255.255.0
 - Default Gateway: 192.168.0.1
 - DHCP Server: Disabled
 - NTP: Enabled
 - NTP Server 1: 0.us.pool.ntp.org
 - NTP Server 2: 1.us.pool.ntp.org
 - NTP Server 3: 2.us.pool.ntp.org
 - NTP Mode: Client
- WIDE AREA NETWORK**
 - DHCP Client: Disabled
 - IP Address: 10.20.254.70
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 10.20.254.1
 - DNS 1: 10.11.200.201
 - DNS 2: 10.11.200.202
 - VLAN ID: [Empty field]
- BELDEN HORIZON**
 - URL: wss://belden.io
 - On-Prem IP Address: [Empty field]

2 Use the following table to enter the appropriate parameters:

Parameter	Description
Gateway	
Gateway Name	Enter a name for this gateway.
Description	Enter a description to describe the gateway. For example, <i>Network Bridge - Bakersfield</i> .
Address	Enter the street address of the gateway (i.e., where the gateway resides)
Advanced configuration (link)	This link allows you to provide GPS coordinates of the gateway's location.
Local Area Network	
IP	Enter the IP address of the gateway. This is a static IP address. The default IP address is 192.168.0.250. (The netmask is always 255.255.255.0).
Subnet	Subnet mask of the PLX35-NB2 Ethernet port.
Default Gateway	Default gateway of the PLX35-NB2 Ethernet port.
DHCP Server	Use this parameter to enable or disable DHCP. The default is Disabled . If you want to use a DHCP server to select an IP, select Enabled .

Selecting **Enabled** displays a number of additional DHCP-related parameters

DHCP Server

DHCP Lease Time

DHCP Lease Units

DHCP Pool Low

DHCP Pool High

DHCP Lease Time - Allows you to select lease times in hour, minutes, or seconds. This is the amount of time an IP address remains available on a particular device before releasing the IP address for use by another device.

DHCP Lease Units - Allows you to specify Hours and Minutes and works in conjunction with *DHCP Lease Time*.

DHCP Pool Low - DHCP uses a pool of assigned addresses that are available to requests. *DHCP Pool Low* allows you to set the last octet to the low end number of the pool. (See example below)

DHCP Pool High - DHCP uses a pool of assigned addresses that are available for use. *DHCP Pool High* allows you to specify the high-end last octet of the pool

For example:

DHCP Pool Low

DHCP Pool High

This example specifies that the range of addresses that may be used is between 192.168.72.100 through 192.168.72.249.

NTP	This parameter specifies whether or not the Network Time Protocol (NTP) is enabled or disabled. The default is Enabled . If Disabled , the following two parameters are not present.
NTP Server 1	Default set to: 0.us.pool.ntp.org . Enter a different NTP server, if needed.
NTP Server 2	Default set to: 1.us.pool.ntp.org . Enter a different NTP server, if needed.
NTP Server 3	Default set to: 2.us.pool.ntp.org . Enter a different NTP server, if needed.
NTP Mode	Default is Client . This can be edited to Client/Server mode.

Wide Area Network	
DHCP Client	<p>This is set to Enabled by default. If your administrator wants to assign a static IP, this should be set to Disabled.</p> <p>If Disabled, you must supply the following information: IP: The IP address assigned to the WAN port. Subnet: Enter the subnet address. Gateway: Enter the gateway address for this subnet. DNS 1: Enter the Domain Name Server IP provided to your system. DNS 2: Enter the backup Domain Name Server IP provided to your system.</p>
VLAN ID	<p>If the gateway is part of a VLAN, enter the VLAN ID.</p>
Belden Horizon	
URL	<p>By default, <i>URL</i> is set to wss://belden.io. If the PLX35-NB2 needs to be activated on premises then the <i>URL</i> must be set as wss://onprem.belden.io. If the PLX35-NB2 is activated to the cloud, this parameter cannot be modified.</p> <p>Note: Only wss://belden.io and wss://onprem.belden.io can be configured as the <i>URL</i>.</p>
On-Prem IP Address	<p>This section is disabled by default. If the <i>URL</i> is configured as wss://onprem.belden.io, then the On-Prem server IP address must be entered here. If the PLX35-NB2 is activated to the cloud, this parameter cannot be modified.</p> <p>Note: If the <i>URL</i> is configured as wss://belden.io, this parameter will be disabled</p>

- 3 Click the **APPLY CHANGES** button when complete.

4.3.1 Open Source Software and License Information

To view a list of the software and licenses contained in the PLX35-NB2, click on the **LICENSES** link at the bottom of the *Gateway* tab.

The screenshot shows the configuration interface for the PLX35-NB2. At the top, there is a 'TUNNEL CONNECTED' status and a 'DISCONNECT' button. Below this is a navigation bar with tabs for Overview, Gateway, Access, File Relay, SD Card, and Activity. The 'Gateway' tab is selected. Under 'LOCAL AREA NETWORK', the IP is set to 192.168.0.250, DHCP Server is Disabled, NTP is Enabled, and three NTP Servers are listed with addresses 0.us.pool.ntp.org, 1.us.pool.ntp.org, and 2.us.pool.ntp.org. The NTP Mode is set to Client. Under 'WIDE AREA NETWORK', the DHCP Client is Enabled and the VLAN ID is blank. At the bottom right, a 'Licenses' link is highlighted with a red box. The footer of the configuration area says 'Powered by ProSoft Technology'.

A list of the Open Source software and its license terms are displayed:

The screenshot shows the 'Licenses' page. At the top, there is a navigation bar with tabs for Overview, Gateway, Access, File Relay, SD Card, and Activity. An 'Apply changes' button is visible on the right. Below the navigation bar is the heading 'Software contained in the product' and a sub-heading 'You can find the detailed list of used Open Source Software and its license terms in the section below:'. A table follows with the following data:

Package Name	License	Point of Contact	Source Link
ac1-2.2.53	LGPL-2.1 GPU-2.0	https://github.com/matorchak	https://github.com/openwrt/packages/tree/openwrt-19.07/utls/ac1
atn-2.4.48	LGPL-2.1 GPU-2.0	https://github.com/matorchak	https://github.com/openwrt/packages/tree/lede-17.01/utls/atn
bash-4.4.18	GPLv3+ or later	https://github.com/ja-pa	https://github.com/openwrt/packages/tree/openwrt-19.07/utls/bash
binutils-2.27	GPLv3	Felix Fietkau mbd@openwrt.org	https://github.com/openwrt/packages/tree/openwrt-19.07/package/development/binutils
busybox-1.25.1	GPLv2	Felix Fietkau mbd@openwrt.org	https://github.com/openwrt/packages/tree/lede-17.01/package/utls/busybox
bcq2-1.0.6	bcq2	https://github.com/ibyx	https://github.com/openwrt/packages/tree/openwrt-19.07/package/utls/bcq2
curl-7.50.3	MIT	https://github.com/kaloa	https://github.com/openwrt/packages/tree/openwrt-19.07/package/network/utls/curl
dnsmasq-2.73	GPLv2	LEDE team	https://github.com/openwrt/packages/tree/lede-17.01/package/network/services/dnsmasq
dooftools-4.1	GPLv3+ or later	https://github.com/hoibart	https://github.com/openwrt/packages/tree/lede-17.01/utls/dooftools
eno6-2.2.6	MIT	https://github.com/ibyx	https://github.com/openwrt/packages/tree/lede-17.01/utls/eno6

License Details:

TUNNEL CONNECTED
DISCONNECT

Overview
Gateway
Access
File Relay
SD Card
Activity

Apply changes

ipaddr	MIT	https://github.com/whitequark	https://github.com/whitequark/ipaddr.js
eonasdan-bootstrap-datetimepicker	MIT	https://github.com/Eonasdan	https://github.com/Eonasdan/bootstrap-datetimepicker

License Details

Packages: busybox-1.25.1, dnsmasq-2.78, fstools-2016-09-31, libcap-2.25, iproute2-4.4.0, led-e-keyring-2016-04-30, lzo-2.09, mbedtls-1.3.17, mbedtls-2.3.0, mtd-ubifs-1.5.2, netifd-2016-11-21, popl-1.16, procd-2016-10-19, u-boot-2016.05, ubus-2016-10-12, ubox, uci-2016-07-04.1, uclibc-2.28

Packages: curl-7.50.3, expat-2.2.6, json-c-0.12.1, libxml2-2.9.8, ncurses-5.9, go-syslog, lua-5.1.5, httprouter, pty, orcman, go-uuid, atomictestify, server, httpunix, gorml2json, jquery, bootstrap, underscore, backbone, backbone-forms, handlebars, swag, js-cookie, bootstrap3-dialog, backbone-deep-model, file-saver, he, JQuery-slimScroll, ipaddr, eonasdan-bootstrap-datetimepicker, gorml2json, httpunix

Packages: go-avro, softethervpn-psft-4.29-9680, glog

Packages: acl-2.2.53, attr-2.4.48, libiconv, libnl-tiny-0.1, Linux-PAM-1.2.0, userspace-rcu-0.9.4, xz-5.2.4, zlib-1.2.8

Packages: bash-4.4.18, binutils-2.27, dosfstools-4.1, fvttool, readline-7.0

Packages: pflag, fsnotify, snappy, iperf-1.3.4

Packages: gorilla-websockets, libarchive-3.3.2

Packages: jsonfilter-2016-07-02, firewall-2016-11-07, libubox, usign-2015-07-04, go-sphew

Package: zlib

Package: bzip

Powered by ProSoft Technology

Each entry can be expanded:

TUNNEL CONNECTED
DISCONNECT

Overview
Gateway
Access
File Relay
SD Card
Activity

Apply changes

License Details

Packages: busybox-1.25.1, dnsmasq-2.78, fstools-2016-09-31, libcap-2.25, iproute2-4.4.0, led-e-keyring-2016-04-30, lzo-2.09, mbedtls-1.3.17, mbedtls-2.3.0, mtd-ubifs-1.5.2, netifd-2016-11-21, popl-1.16, procd-2016-10-19, u-boot-2016.05, ubus-2016-10-12, ubox, uci-2016-07-04.1, uclibc-2.28

Packages: curl-7.50.3, expat-2.2.6, json-c-0.12.1, libxml2-2.9.8, ncurses-5.9, go-syslog, lua-5.1.5, httprouter, pty, orcman, go-uuid, atomictestify, server, httpunix, gorml2json, jquery, bootstrap, underscore, backbone, backbone-forms, handlebars, swag, js-cookie, bootstrap3-dialog, backbone-deep-model, file-saver, he, JQuery-slimScroll, ipaddr, eonasdan-bootstrap-datetimepicker, gorml2json, httpunix

Packages: go-avro, softethervpn-psft-4.29-9680, glog

Packages: acl-2.2.53, attr-2.4.48, libiconv, libnl-tiny-0.1, Linux-PAM-1.2.0, userspace-rcu-0.9.4, xz-5.2.4, zlib-1.2.8

Packages: bash-4.4.18, binutils-2.27, dosfstools-4.1, fvttool, readline-7.0

Packages: pflag, fsnotify, snappy, iperf-1.3.4

Packages: gorilla-websockets, libarchive-3.3.2

BSD 2-Clause License
 Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Packages: jsonfilter-2016-07-02, firewall-2016-11-07, libubox, usign-2015-07-04, go-sphew

Package: zlib

4.4 Configuring Login Credentials

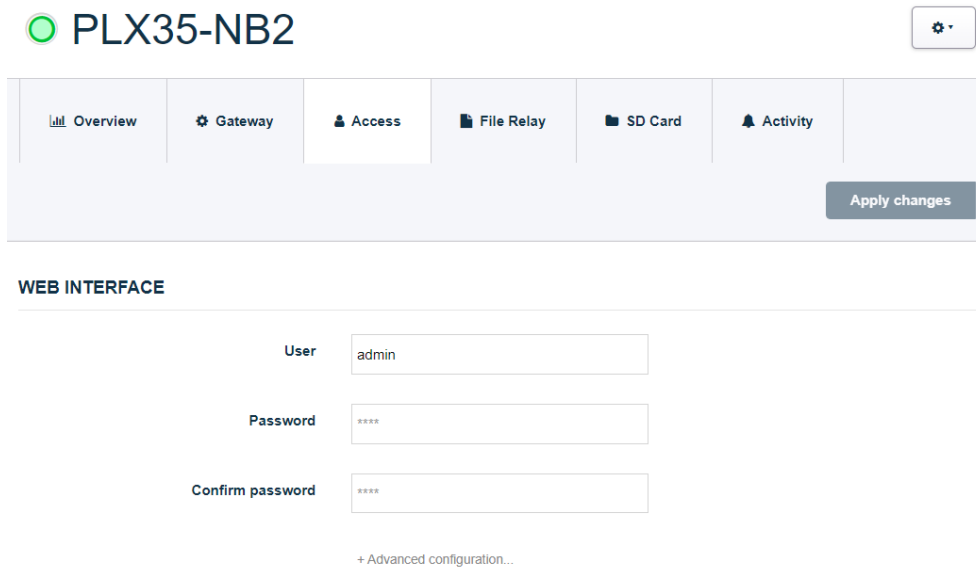
The gateway is shipped with the following login defaults:

User: **admin**

Password: **password**

The *Access* tab allows you to change the default user name and password.

- 1 Click on the *Access* tab.



The screenshot shows the configuration interface for the PLX35-NB2 gateway. At the top, there is a header with the device name "PLX35-NB2" and a settings icon. Below the header is a navigation menu with tabs for "Overview", "Gateway", "Access", "File Relay", "SD Card", and "Activity". The "Access" tab is currently selected. To the right of the navigation menu is an "Apply changes" button. Below the navigation menu is a section titled "WEB INTERFACE" containing three input fields: "User" with the value "admin", "Password" with masked characters "****", and "Confirm password" with masked characters "****". Below these fields is a link labeled "+ Advanced configuration...".

This page allows you to set up the users that can manage and configure this gateway. The *Advanced Configuration* link allows you to restrict access based on user.

- 2 Enter a user name and a password.
- 3 Confirm the password by retyping it.

4.4.1 Advanced Configuration

- 1 Click on the *Advanced Configuration* link.

The screenshot shows the configuration interface for the PLX35-NB2 device. At the top, there is a header with the device name 'PLX35-NB2' and a settings icon. Below this is a navigation menu with tabs for 'Overview', 'Gateway', 'Access', 'File Relay', 'SD Card', and 'Activity'. An 'Apply changes' button is located at the bottom right of the navigation area. The main content area is titled 'WEB INTERFACE' and contains several configuration fields: 'User' (admin), 'Password' (masked with asterisks), 'Confirm password' (masked with asterisks), a link for '- Advanced configuration...' (highlighted with a red box), 'Web Protocol' (a dropdown menu currently set to 'HTTP'), and 'HTTP port' (8080).

- 2 Select the *Web Protocol*. Select **HTTP** or **HTTPS**.
- 3 Choose the port depending on what protocol is selected.
- 4 Click **APPLY CHANGES** when complete.

4.4.2 Initial / Factory Reset Login

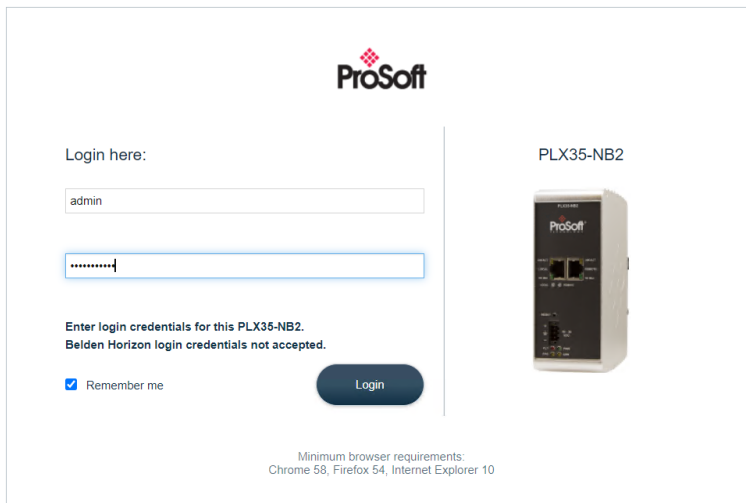
This procedure is used for brand new units, or resetting the PLX35-NB2 to the default configuration. The default credentials are as follows:

User: admin

Password: password

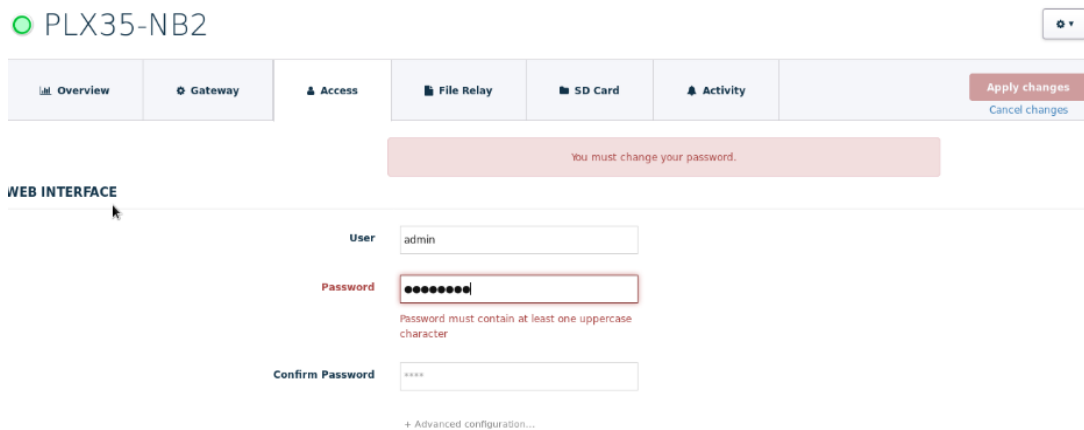
Note: Beginning with PLX35-NB2 firmware v1.5, this process requires you to change the default password on initial/reset login.

- 1 Connect to the PLX35-NB2 webpage using the default credentials.

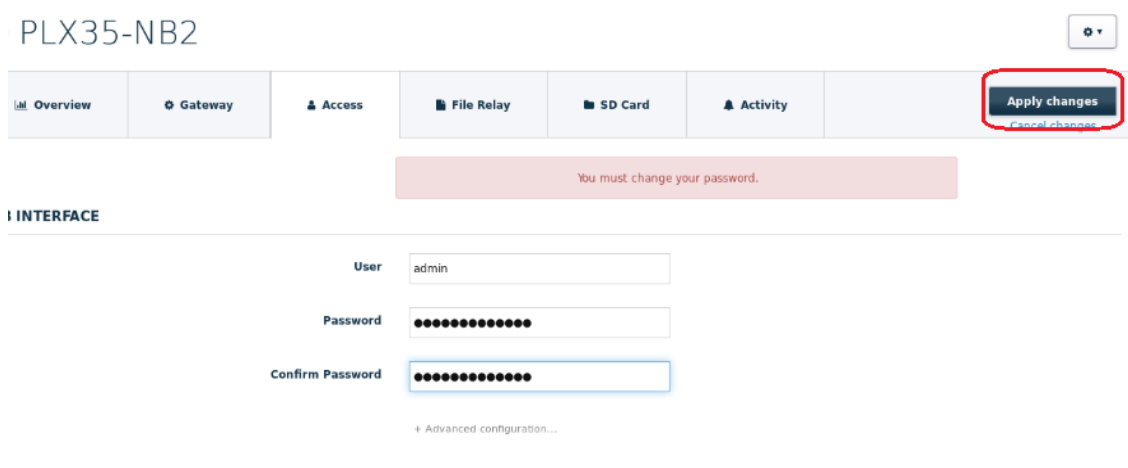


- 2 After logging in, the Access tab will be displayed to change the password.

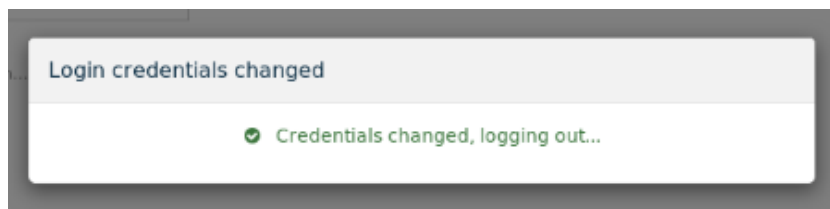
Note: Beginning with PLX35-NB2 firmware v1.5, this process requires you to change the default password on initial/reset login.



- 3 Select a password that is compatible with the following rules:
 - Between 8 and 40 characters
 - At least one upper case letter
 - At least one lowercase letter
 - Contains at least one digit (0 through 9)
 - Contains at least one special character: !@#\$%^&*()_+=-~
- 4 Re-enter the new password in the *Confirm Password* field.
- 5 After confirming the new password in the *Confirm Password* field, click the **APPLY CHANGES** button in the top right corner of the page.

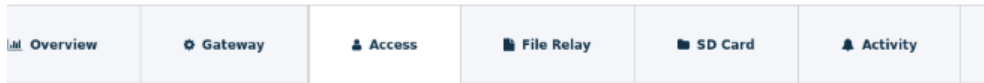


- 6 After the changes are applied, you will be logged out and redirected to the login page.



- 7 After logging in using the username and the new password, future password changes can be done from the *Access* tab as in the *Configuring Login Credentials* section on page 20.

PLX35-NB2



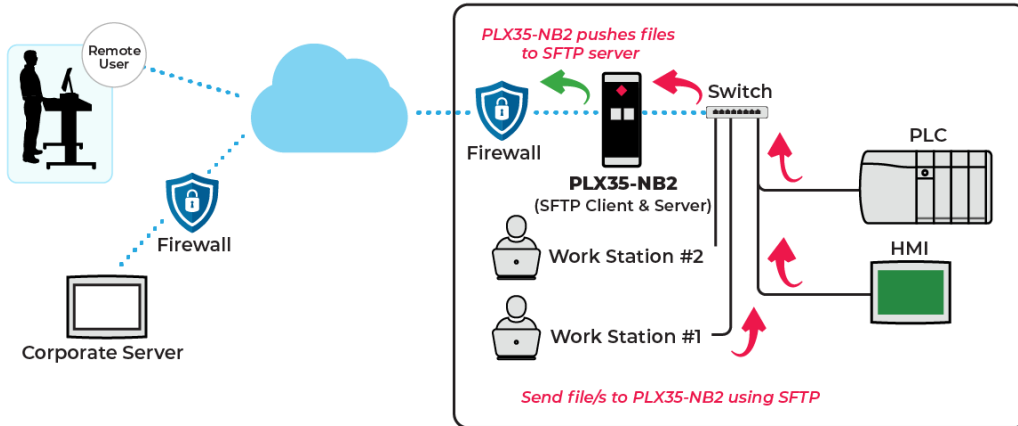
INTERFACE

User	<input type="text" value="admin"/>
Password	<input type="password" value="****"/>
Confirm Password	<input type="password" value="****"/>

+ Advanced configuration...

4.5 File Relay

The LAN and WAN ports on the PLX35-NB2 are physically isolated. The File Relay functionality enables simple and secure transfer of files across segmented networks. For example, if the customer would like to back up their OT equipment configuration files on the server without wanting to create a link between the IT and OT network, the PLX35-NB2 can be used to segment between the two networks.



The *File Relay* tab allows you to use the SD card port on the device as a temporary storage medium for large files that can be automatically transferred to a remote location. Files can be copied to the PLX35-NB2 SD card from an FTP/SFTP Client. The files can then be transferred to a remote FTP/SFTP Server, or via Belden Horizon.

- 1 In the *Incoming* section of the *File Relay* tab, select the **FTP** or **SFTP** protocol to enable FTP or SFTP Incoming file transfer.

PLX35-NB2

Overview	Gateway	Access	File Relay	SD Card	Activity
----------	---------	--------	-------------------	---------	----------

INCOMING

Protocol:

User:

Password:

Confirm Password:

2 Use the following table to enter the appropriate parameters:

Parameter	Description
Incoming	
Protocol	FTP (File Transfer Protocol) SFTP (Secure File Transfer Protocol)
User	The username is for uploading files through FTP to the module's SD card. The default value is f-relay .
Password	Password for FTP access. The password must have at least 8 characters, contain at least one uppercase letter, one lowercase letter, and one special character.
Outgoing	
Protocol	Protocol of the server used as final destination for the File Relay. Supported protocols for upload are FTP/SFTP/Belden Horizon
URL	URL of the server used as final destination for the File Relay. Supported protocols for upload are FTP/SFTP/Belden Horizon For FTP the format is specified in the field: ftp://user@host:port/path/ For SFTP the format is: sftp://user@host:port/path/
Password	Password used to upload to the remote server. You can view the configured value by pressing the "eye" button. Password is used only for FTP. This field is greyed out for SFTP. This field is removed for Belden Horizon.

- | | |
|----------|--|
| Host Key | <p>Public Key that authenticates SFTP Server and proves its identity to PLX35-NB2 client. This should be copied from SFTP Server and pasted here.</p> <ul style="list-style-type: none"> • Used only for SFTP • This field is greyed out for FTP • This field is removed for Belden Horizon • Keys supported: RSA 2048, RSA 3072, RSA 4096, Ed25519 255, ECDSA nistp256, ECDSA nistp384, ECDSA nistp521 • Keys unsupported: DSA 1024, ECDSA secp256k1 |
|----------|--|

Public Key from SFTP Server should be exported as **OpenSSH** format.
Example:

- ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDAE1+/MsozGfb5JF6g6y1dh1YfeyPTrsforNIKKfQRElKACOF3c6eRsSkUnOazfUWHLtCT2B49sXgpteidU4Phg01kECKjCvISeUuRmWX9CDbGUJNQBeawapZ7WRBIOsBh0aualywcndMZ0dd16J9t+T49KRJtxG8iw17AKE5yTzBEGsRmIv2IWQV444w7+Z/DcLR5BmSxuXA/Mm6VCvMpkp60xdfVFzKEkVWSgIAi8E3quMH3+UOJHfCK3yH4byUFvhJqFfcqMsOHe/QaiblNl jpvGL7VB0gdAln2Igt5nmyKUPHkbn/vB26/YKsa69P2Z8qfkmZV3jKp0xHu5CLEYG4fj1BKLSDVY49AU2oT6CS+ad++vMdD0boALiJfM08ztUbMBKVkQDZ4FJD/n418HZjJnOU8Ax3Jw7jghkisES3J4sKIPsvse8DR8+iGzg6oYplZJhk bzEGJgHE46hIM8OvOYcsU7hfyaSRZOZtA0+UIg7tKkraWofa8eZFa7OxEH8iJSW15Qcp2QMniDy6vd+QPuZr3byu0EVw6Px6vqI PhKKLKEoz3lUxxH3c+T6CfP/CVzSuhik523ZAZyjK0Nnimc+MSmROE8hrPWSCg9uimIzGHWLWxjxbSmHRz42EdUilrWA5Uv8q7vK19xfgwji0wNLjlx8I3ZmcIehQ==
- ecdsa-sha2-nistp384
AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBDBbqQXJXwsBDy+kGaAZbeHC02FL8p0xmXEQfy9X1yuXQTTbw5UH/QgiBzrj2hIEm/njbPG2ybOa98pUBuw1mM5ftDjKVTF35Ilave96BqJEYyJYYH2y8Ve5qDDliwvZzyg==

Standard SSH2 format is NOT supported:

```

---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAQGDanO7WbWaw1+Ukd2RjfvNTS1f
eNULkzaQS17fCYfAX
GuAHjrVi3WxynQF9vyV/an+0XAsfiFUhmRE+DaaLMzvjnmXIMFhcjhM
FshZk3RUOfF5d5Syd
1fuqMDj2+s2dcjidnkBRXF2Nq+Ii7rPChtjmDgwe7b7dzxgG6erVs61
Ybbr9dAuUs7i5ri79
m3BCHtxLvF/OOm1R27jEyizMRyOBswa5DJBL6skl8oK5fdgSdmVyy6i
I88cedD0lipwCt+X9
5l1jeFzX1Ia/L+NzshBs4vAjr3obgHWNiwEDdckw0RU/FDFdbjmH55f
vWAa7M7lE+A8/UFEa
MZ2LMqLdULwiOHb4TtVCoYfnQlrcqEl8Vfw8A77vH8KadGpZ2EuLZPo7
cdYUgovb5pzgmbVHh
MiMaRjkVtdc118nPwdeO4CUnlMIWROSLf2JGTg2GTZipbT1Fge8e2
wEO9bHiDBORRU5PZP
RQOlQDnbtFnE4gswFdhvs4+tHaunw4wBVDIo10=
---- END SSH2 PUBLIC KEY ----

```

Note: Host Key will be removed from the outgoing server configuration upon downgrade from PLX35-NB2 1.5 release to any older firmware.

OUTGOING

Protocol: SFTP

URL: sftp://admin@192.168.0.13:22/

Password: ****

Host Key: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQD

SSH-Key:

Daily Upload Time: 07:56

SSH-Key

SSH-Key is the public key that authenticates the SFTP Server user for file transfer. Once generated, it should be copied to the SFTP Server as a .pub file and associated with the designated user. The SSH-Key pair generation takes place the first time it is requested. Subsequent requests return the same public key.

SSH keys will be removed upon gateway factory reset.

- Used only for SFTP
- This field is greyed out for FTP
- This field is removed for Belden Horizon

OUTGOING

Protocol: SFTP

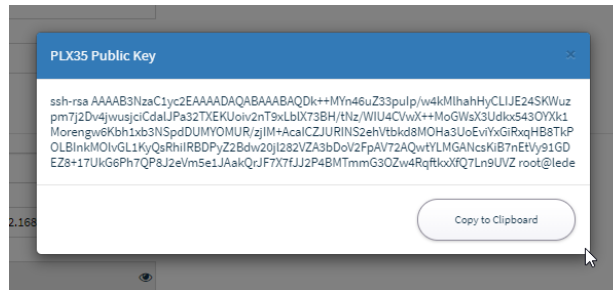
URL: sftp://admin@192.168.0.13/

Password: ****

Host Key: `ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDk++Myn46uZ33pulp/w4kMlhahHyCLJE24SKWuz
pmTj2Dv4jwusjciCdaLJP832TXEKUoiv2nT9xLbIX73BH/nlz/WIU4CVwX++MoGIWx3JdKx543OYXk1
Morengv8Kbh1xb3NSpdDUMYOMUR/zjIM+AcalCZJURINS2eh/tbkd8MOHa3UoEvYxGIRxqHB8TkP
OLBlnkMOlvGL1KyQsRhlIRBDPyZ2Bdv20jI282VZA3bDdV2FpAV72AQwtYLMGANcsKiB7nEHYy91GD
Ez8+17UkG6Ph7QP8J2eVmsE1JAakQrJF7X7J2P4BMTmmG3OZw4RqtKxXQ7Ln9UVZ root@lede`

SSH-Key:

Daily Upload Time: 03:00



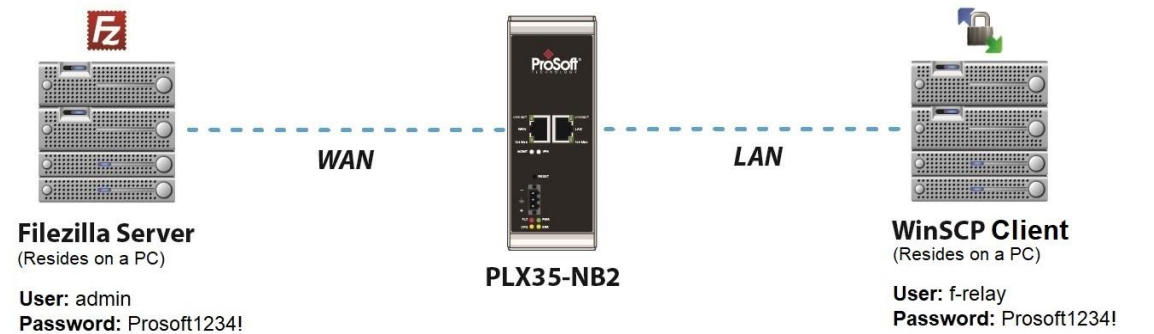
Daily Upload Time The upload time, shown in the Local UI is UTC – similar with the time on the *Overview* page. Default time value is 03:00.

3 Click APPLY CHANGES when complete.

4.5.1 Example #1: Transferring Files Across Segmented Networks Using FTP

This example shows an incoming FTP to an outgoing FTP.

- On the LAN port, the PLX35-NB2 acts as an FTP Server for the incoming files to a WinSCP Client, The files are temporarily stored in the PLX35-NB2 SD card.
- On the WAN port, the PLX35-NB2 acts as an FTP Client to a Filezilla Server. The files are pushed from the PLX35-NB2 to the Filezilla FTP Server.



PLX35-NB2 ⚙️

[Overview](#) [Gateway](#) [Access](#) [File Relay](#) [SD Card](#) [Activity](#) [Apply changes](#)

INCOMING

Protocol:

User:

Password:

Confirm Password:

OUTGOING

Protocol:

URL:

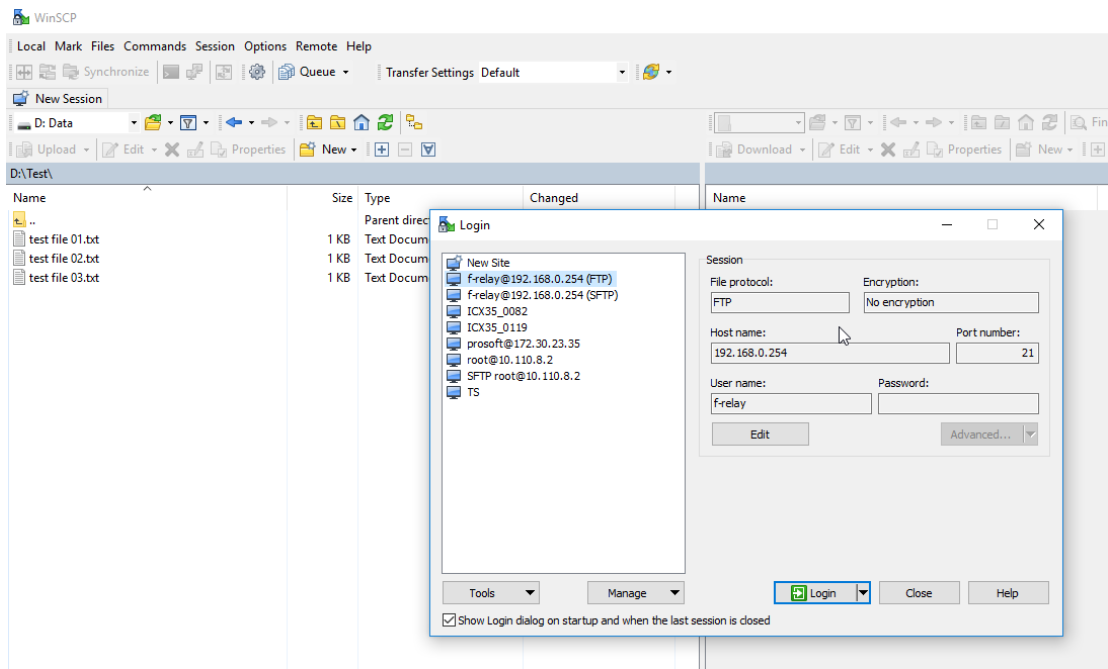
Password:

Host Key:

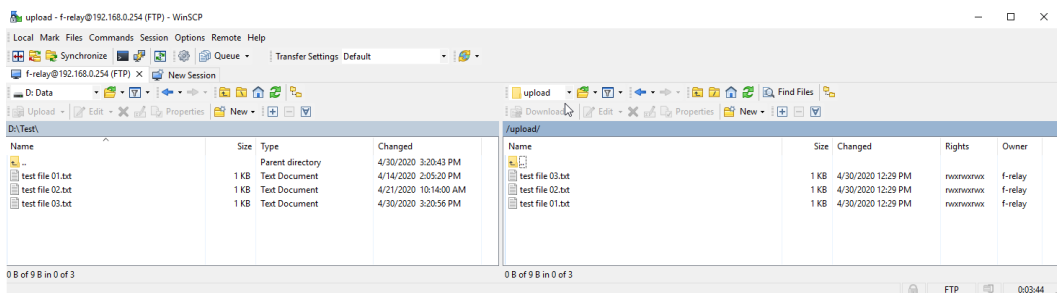
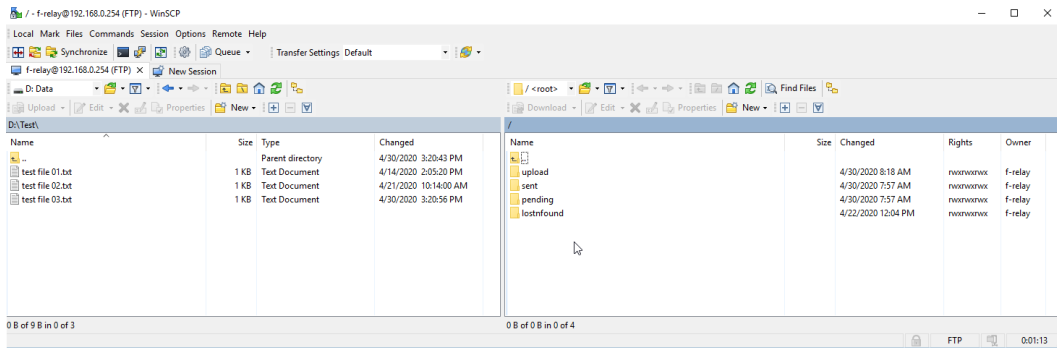
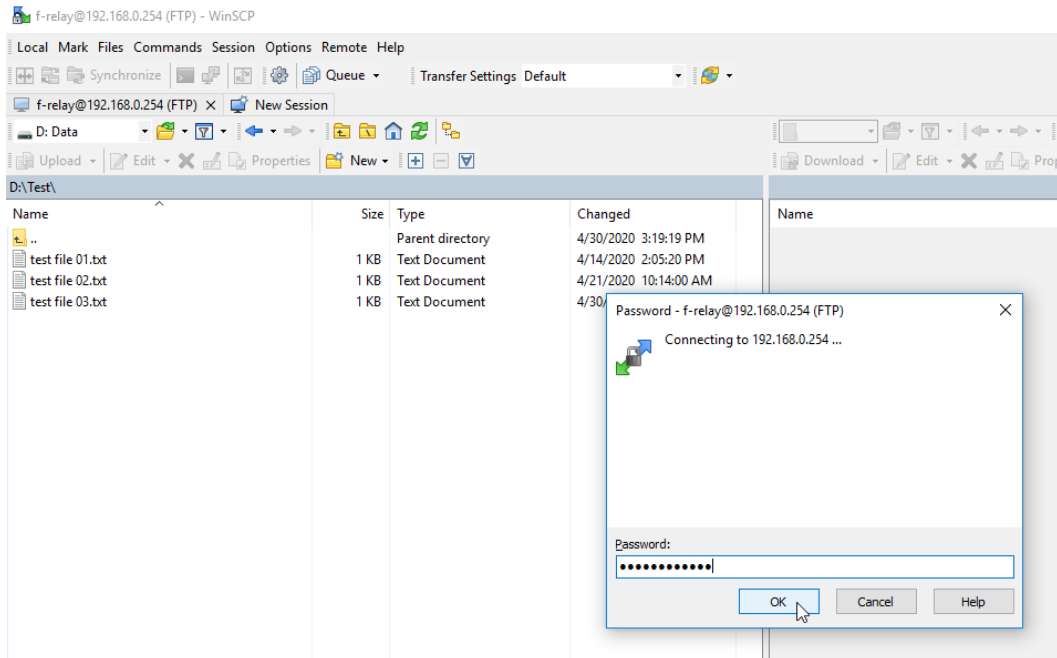
SSH-Key:

Daily Upload Time:

- 1 From the WinSCP Client, open a FTP session to PLX35-NB2 and transfer a few files to the *Upload* folder on the PLX35-NB2 SD card:

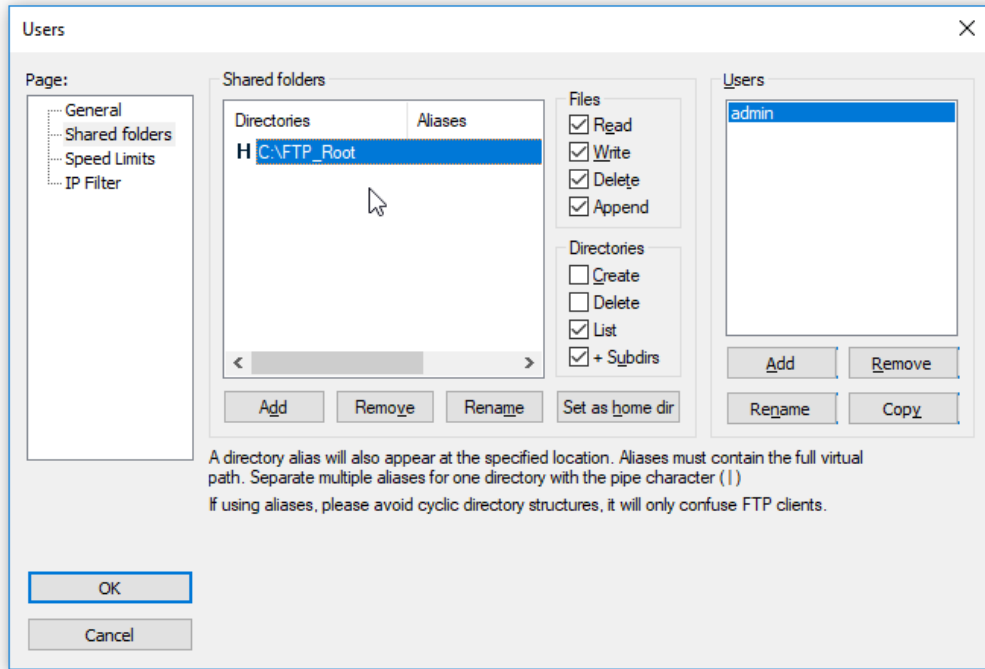
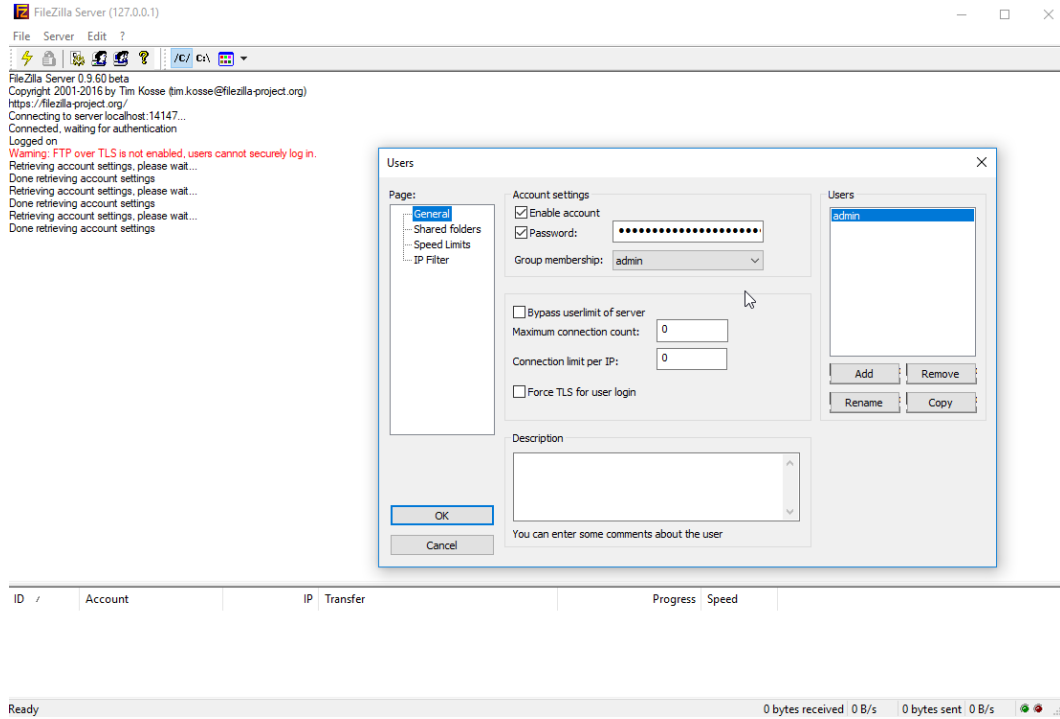


2 Click Ok.

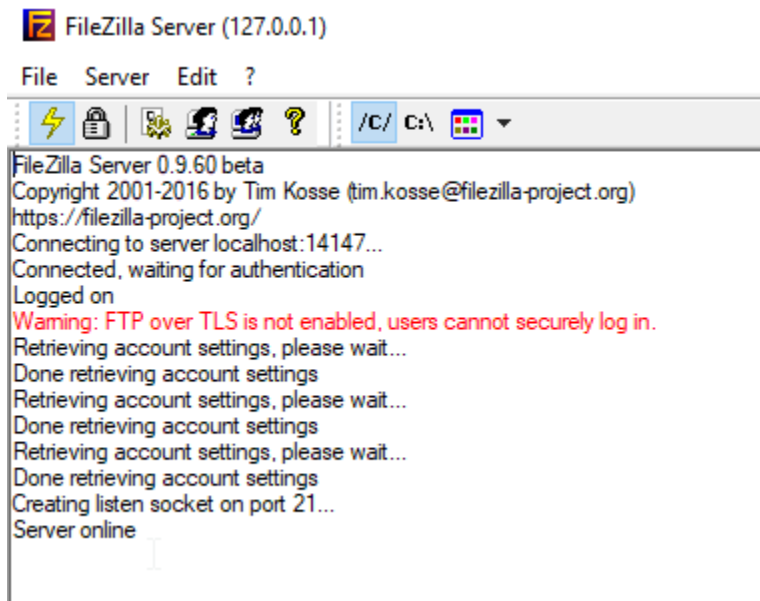


3 Log into the FTP Filezilla Server.

User: admin
Password: Prosoft1234!
Folder: C:\FTP_Root):



4 Start the server:



- At the configured *Daily Upload Time*, set (hh:mm, default is 03:00). The files from the PLX35-NB2 SD card *Upload* folder will be time-stamped (yyyy-mm-dd) and transferred to the FTP Filezilla Server on folder C:\FTP_Root.

The screenshot shows the FileZilla Server interface with a log window displaying server activity. The log includes connection details, user authentication for 'admin', and file transfer operations for '2020-04-30test file 01.txt', '02.txt', and '03.txt'. Below the log, a Windows File Explorer window is open to the 'Local Disk (C:) > FTP_Root' directory, showing three files: '2020-04-30test file 01.txt', '2020-04-30test file 02.txt', and '2020-04-30test file 03.txt'.

```

FileZilla Server (127.0.0.1)
File Server Edit ?
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Retrieving account settings, please wait...
Done retrieving account settings
Creating listen socket on port 21...
Server online
(0001364/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> Connected on port 21, sending welcome message...
(0001364/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220-FileZilla Server 0.9.60 beta
(0001364/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(0001364/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220 Please visit https://filezilla-project.org/
(0001364/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> USER admin
(0001364/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 331 Password required for admin
(0001364/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> PASS *****
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> 230 Logged on
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> PWD
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> 257 "/" is current directory.
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> EPSV
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> 229 Entering Extended Passive Mode (||60833|)
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> TYPE I
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> 200 Type set to I
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> STOR 2020-04-30test file 01.txt
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> 150 Opening data channel for file upload to server of "/2020-04-30test file 01.txt"
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> 226 Successfully transferred "/2020-04-30test file 01.txt"
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> QUIT
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> 221 Goodbye
(0001364/30/2020 15:41:02 PM - admin (192.168.0.254)> disconnected.
(0001374/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> Connected on port 21, sending welcome message...
(0001374/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220-FileZilla Server 0.9.60 beta
(0001374/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(0001374/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220 Please visit https://filezilla-project.org/
(0001374/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> USER admin
(0001374/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 331 Password required for admin
(0001374/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> PASS *****
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> 230 Logged on
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> PWD
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> 257 "/" is current directory.
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> EPSV
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> 229 Entering Extended Passive Mode (||61831|)
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> TYPE I
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> 200 Type set to I
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> STOR 2020-04-30test file 02.txt
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> 150 Opening data channel for file upload to server of "/2020-04-30test file 02.txt"
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> 226 Successfully transferred "/2020-04-30test file 02.txt"
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> QUIT
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> 221 Goodbye
(0001374/30/2020 15:41:02 PM - admin (192.168.0.254)> disconnected.
(0001384/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> Connected on port 21, sending welcome message...
(0001384/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220-FileZilla Server 0.9.60 beta
(0001384/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220-written by Tim Kosse (tim.kosse@filezilla-project.org)
(0001384/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 220 Please visit https://filezilla-project.org/
(0001384/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> USER admin
(0001384/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> 331 Password required for admin
(0001384/30/2020 15:41:02 PM - (not logged in) (192.168.0.254)> PASS *****
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> 230 Logged on
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> PWD
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> 257 "/" is current directory.
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> EPSV
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> 229 Entering Extended Passive Mode (||59867|)
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> TYPE I
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> 200 Type set to I
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> STOR 2020-04-30test file 03.txt
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> 150 Opening data channel for file upload to server of "/2020-04-30test file 03.txt"
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> 226 Successfully transferred "/2020-04-30test file 03.txt"
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> QUIT
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> 221 Goodbye
(0001384/30/2020 15:41:02 PM - admin (192.168.0.254)> disconnected.

```

ID	Account	IP	Transfer	Progress	Speed
Ready					

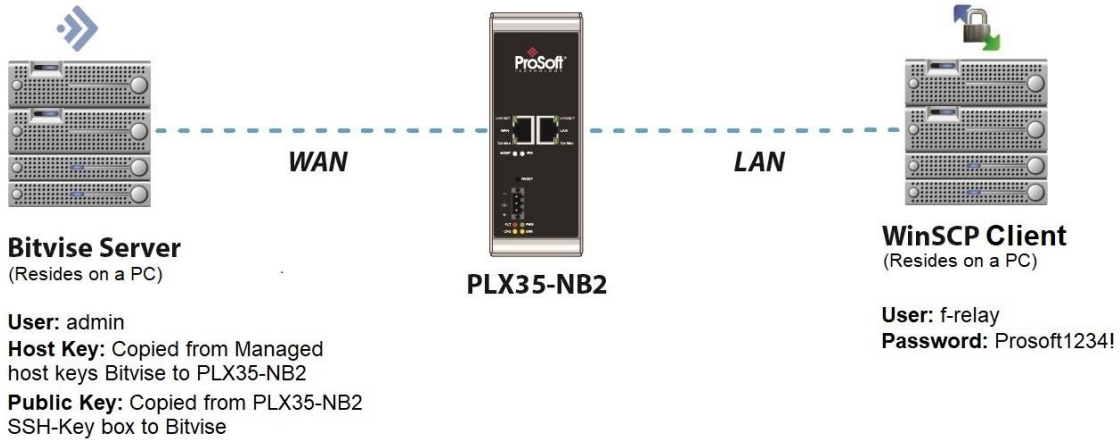
Local Disk (C:) > FTP_Root

- 2020-04-30test file 01.txt
- 2020-04-30test file 02.txt
- 2020-04-30test file 03.txt

4.5.2 Example #2: Transferring Files Across Segmented Networks Using SFTP

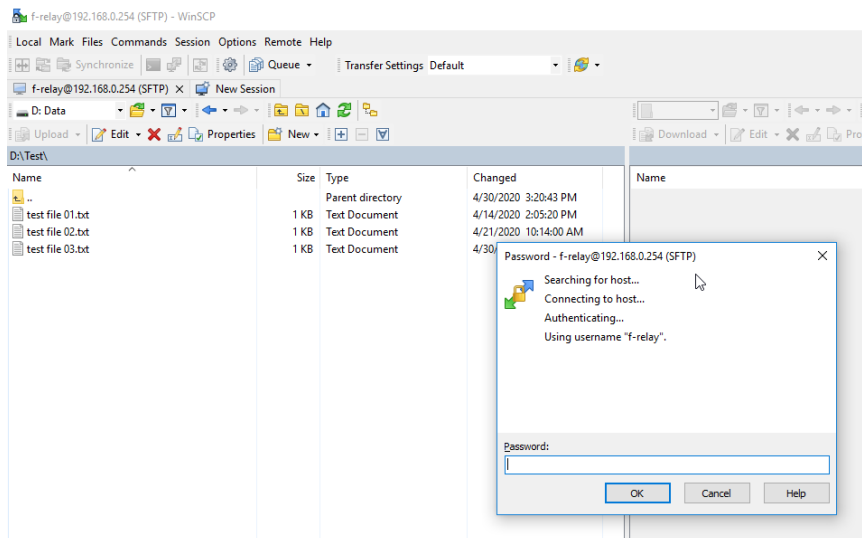
This example shows an incoming SFTP to Outgoing SFTP.

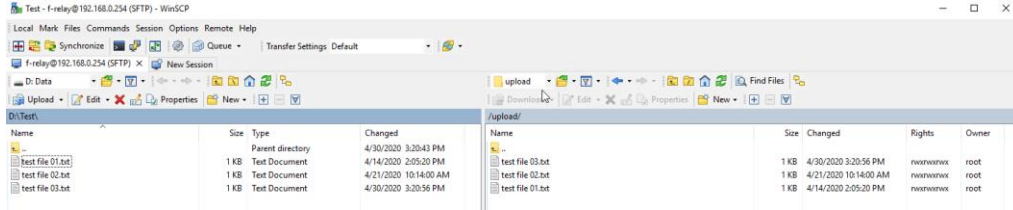
- On the LAN port, the PLX35-NB2 acts as a SFTP Server for the incoming files from the WinSCP Client. The files will be temporarily stored on the SD card.
- On the WAN port, the PLX35-NB2 acts as a SFTP Client to a Bitwise Server. The files are pushed from the PLX35-NB2 to the Bitwise SFTP Server.



- 1 From the WinSCP Client, open a SFTP session to PLX35-NB2 and transfer few files to the *Upload* folder on PLX35-NB2 SD card:

The screenshot shows the configuration interface for PLX35-NB2. At the top, there is a navigation bar with tabs: Overview, Gateway, Access, File Relay, SD Card, and Activity. Below this, the 'INCOMING' section is visible, with fields for Protocol (SFTP), User (f-relay), Password (masked with ****), and Confirm Password (masked with ****). The 'OUTGOING' section below it has fields for Protocol (SFTP), URL (sftp://admin@192.168.0.13:22/), Password (masked with ****), Host Key (ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD), a 'Generate SSH Key' button, and a Daily Upload Time field set to 12:41.





PLX35-NB2

Overview Gateway Access **File Relay** SD Card Activity

INCOMING

Protocol: SFTP

User: f-relay

Password: ****

Confirm Password: ****

OUTGOING

Protocol: SFTP

URL: sftp://admin@192.168.0.13:22/

Password: ****

Host Key: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQD

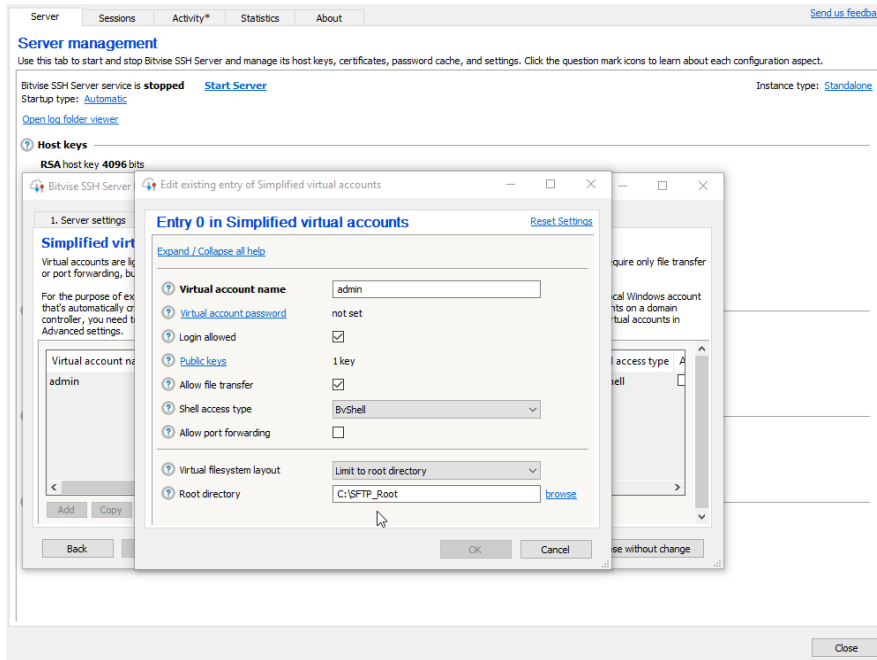
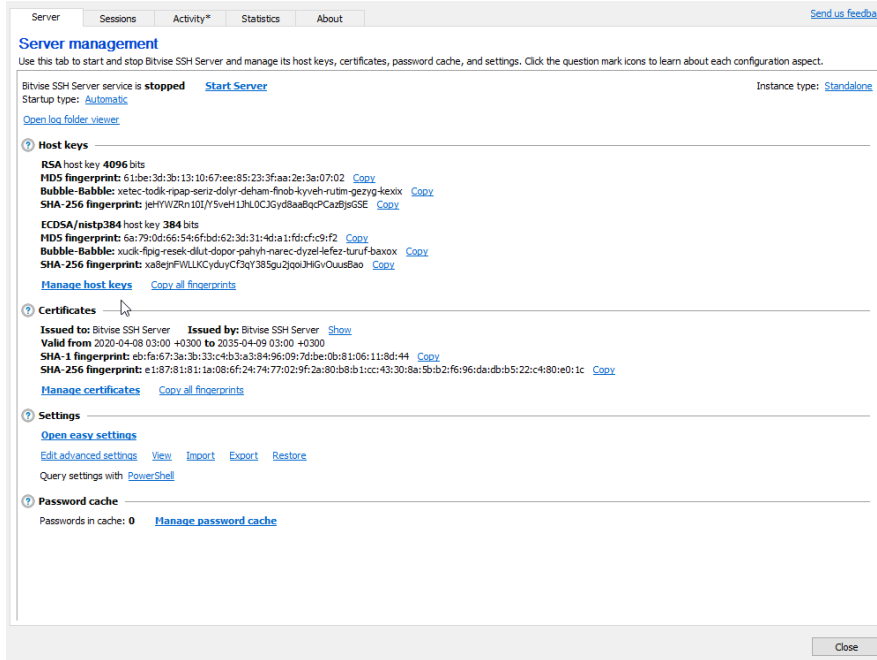
SSH-Key:

Daily Upload Time: 12:41

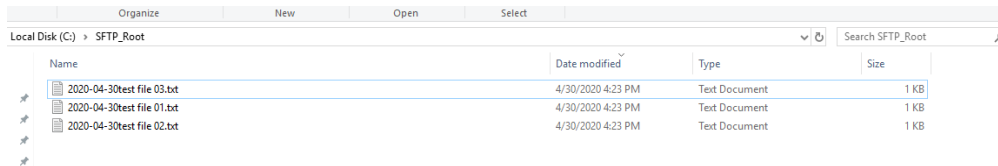
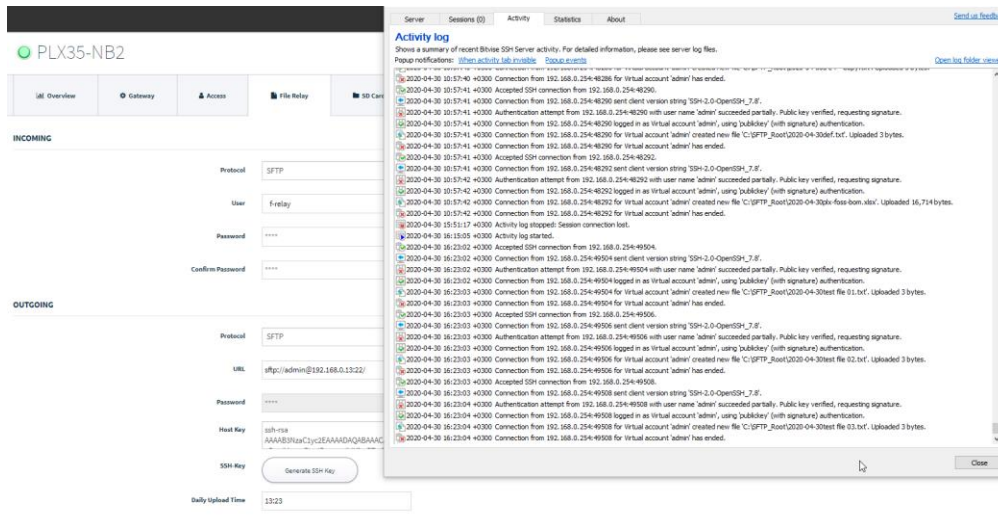
PLX35 Public Key

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDwo8Jed6nijAzOFLzmZNzLEA7PFsehuMeW3XnacZ4yGaxTvx1McKdkO4egu8cbV5filF+A3luHr6O8t/hMepVUHvhH3Dlr1WlW0XE298NuzK8lgpGcFfiOSJwdYFOcTtTqzaUZUJSXkqKS2J88Fk8y0AfoC9IXUPmWJ4DthkVnQs6AZJV48fEUbxRL31xMo9mAYKyTDTAXyE14w0Gf8Ks5bH6uZ1k4XvjFl5vpZoeWGr2F44QM35sjCG3+MDbEyZRXaWmJhxtfAsimPnnS4jQMr3x6qUQqH/ZiNPraLnuXz6Bu1fyB2DoHhLliSdxnWeyGdQunP/x31tsMlerZ5 root@lede
```

- 2 On the Bitvise server, managing public keys:
 - Generate a key on Bitvise Manage host keys, export it as OpenSSH format, then copy the key to Host Key box into the PLX35-NB2
 - Generate SSH Key on PLX35-NB2, copy into a .pub file and add it on admin account on Bitvise server



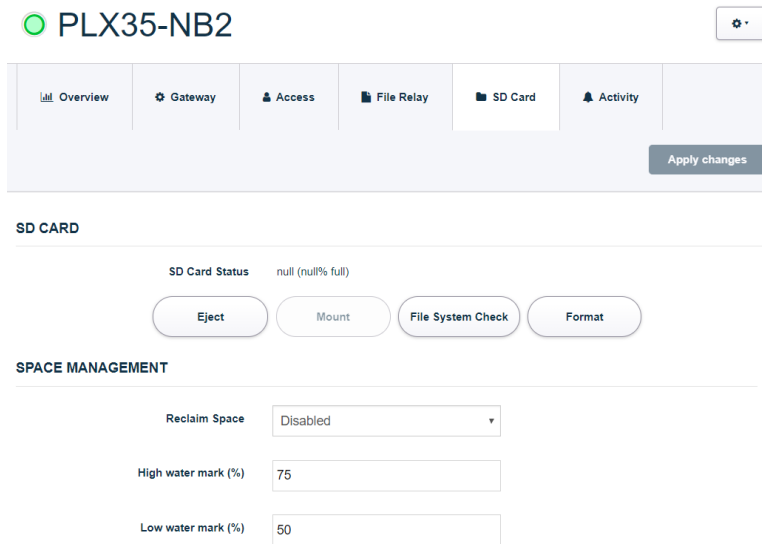
- After the Bitwise server is started, set the *Daily Upload Time* (hh:mm, default is 03:00). The files from the PLX35-NB2 SD card *Upload* folder will be time-stamped (yyyy-mm-dd) and transferred to PC 2 FTP Bitwise Server on folder C:\SFTP_Root.



4.6 SD Card

The *SD Card* tab allows you to Eject, Mount, Format, and diagnose the PLX35-NB2 SD Card. You can also optimize the SD Card in this tab.

You can only access the SD Card from a FTP/SFTP Client.



- 1 Use the following table to enter the appropriate parameters:

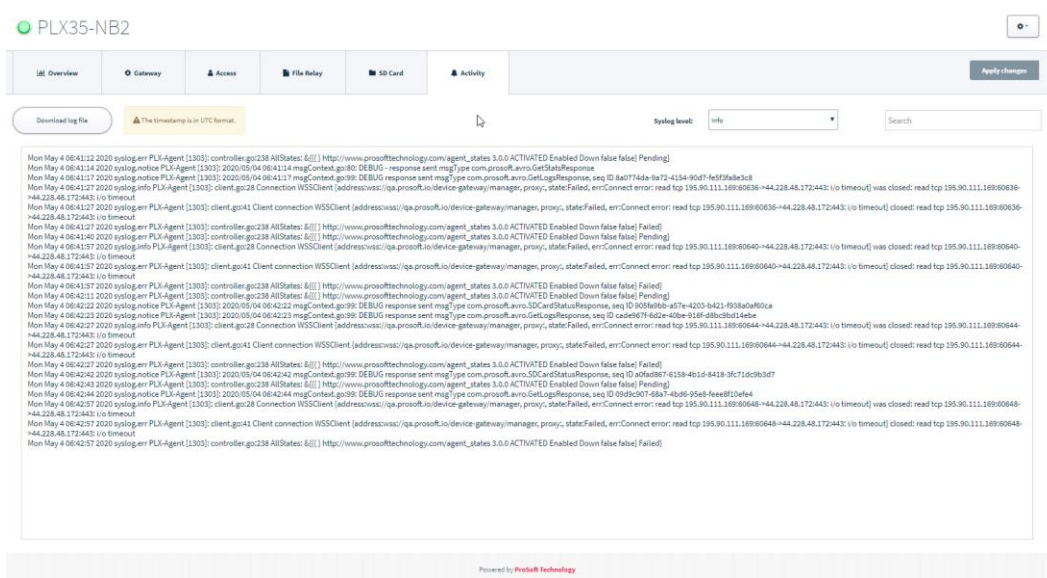
Parameter	Description
SD Card	Note: The <i>SD Card</i> options may be greyed out according to the SD card status. If the SD Card is not present, the SD Card options are greyed out. If the SD Card is not mounted, the Eject and Format buttons are greyed out. If the SD Card is mounted, the Mount button is greyed out.
Eject	Recommended to be done before manually removing SD Card.
Mount	This allows the SD card to be visible to the PLX35-NB2. When the SD Card is not 'mounted', it will not be visible to the PLX35-NB2.
File System Check	Checks the SD Card for errors. This should be used in case the SD Card cannot be mounted. The page will be refreshed after the File System Check process is finished, then the user can manually mount the SD Card using Mount button.
Format	Removes the data from the SD Card and creates a new file system (FAT32 type).
Space Management	
Reclaim Space	Automatically cleans up the SD Card. Default value is Disabled .
High Water Mark (%)	The system will start deleting files from the SD Card when this threshold is reached.
Low Water Mark (%)	The system will delete files from the SD Card until this threshold is reached.

Note: The High and Low Water Mark values should be based on the size of the SD Card and the sizes of the uploaded files. Inappropriate values may cause the deletion of files before the upload is performed.

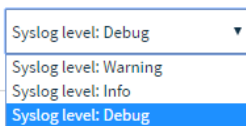
- 2 Click **APPLY CHANGES** when complete.

4.7 Viewing Gateway Log file Activity

- 1 Click on the *Activity* tab.



Options on this page include search, search filter options, and a Download log file option.

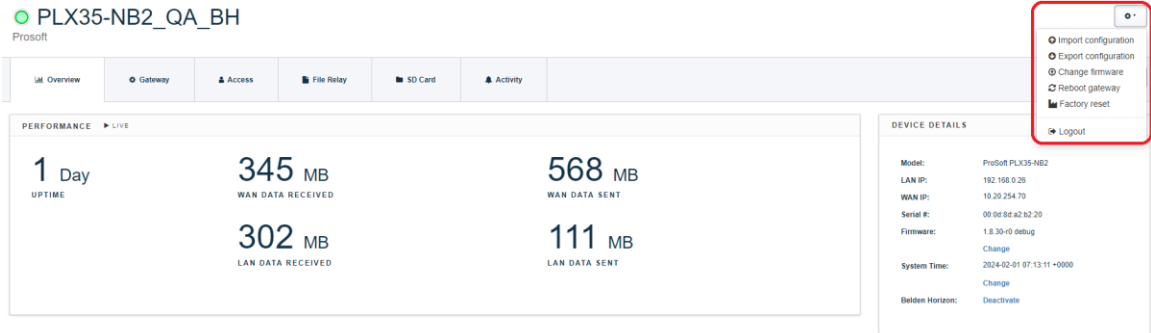


- 2 Click on the **DOWNLOAD LOG FILE** button to download a .txt file to the download folder of your PC or laptop.

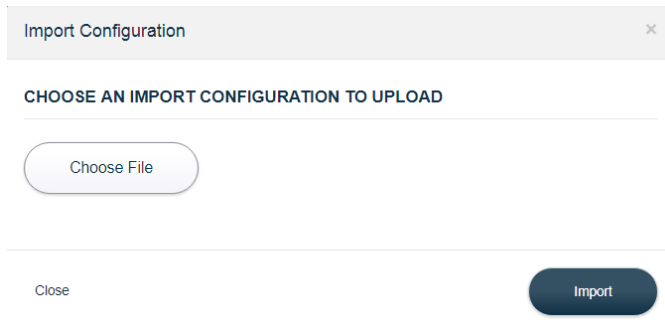
Note: Some options that appear in the configuration UI may not be available during management or configuration options within Belden Horizon.

4.8 Importing a Configuration File

- 1 Select **IMPORT CONFIGURATION** from the **SETUP** icon located in the upper-right corner of any configuration page.

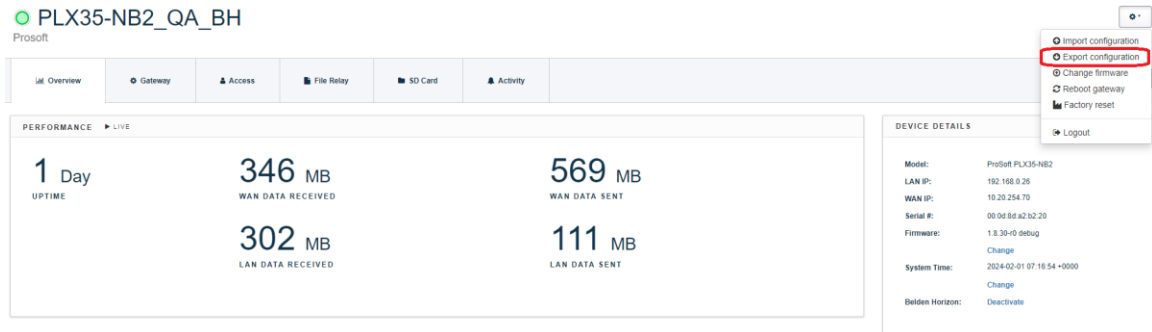


- 2 Locate and select a configuration file to import and then click the **IMPORT** button.



4.9 Exporting a Configuration File

- 1 In the upper-right corner of any configuration page, select **EXPORT CONFIGURATION** from the setup icon.



- 2 The gateway downloads a **tar.gz** file to your PC or laptop. Do not modify this file.

4.10 Updating the Firmware

Note: Downgrading to old firmware versions:

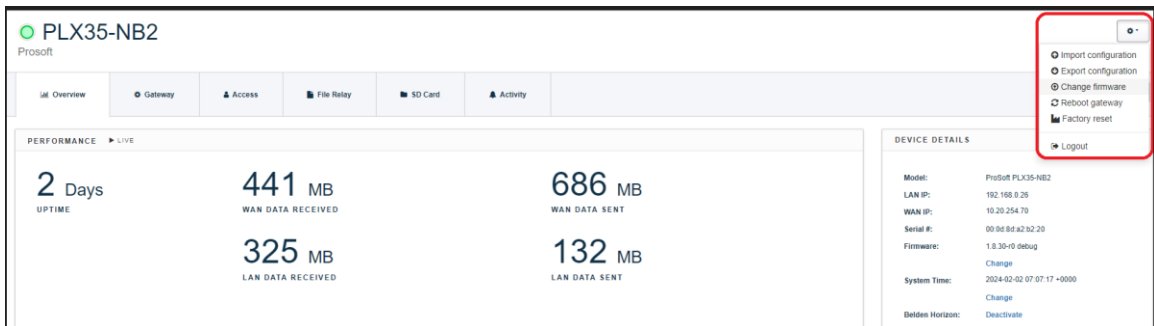
If running firmware version is 1.2.13 or higher, performing a downgrade to versions 1.1.57 or 1.0.24 is not supported.

If running firmware version is 1.2.31 or higher, performing a downgrade to versions 1.2.13, 1.1.57 or 1.0.24 is not supported.

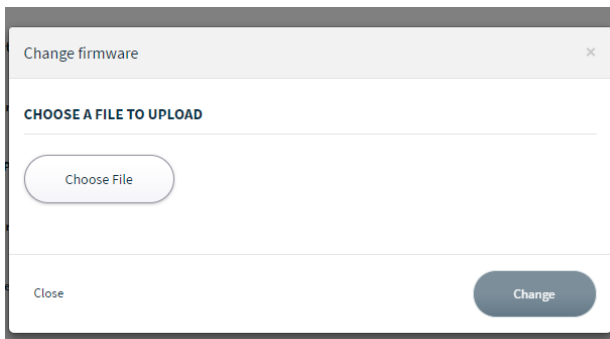
If running firmware version 1.7.1 or higher, users cannot downgrade to versions 1.6.90 and lower due to a new signing key method implementation.

Note: Belden Horizon can also schedule updates to the latest firmware for multiple PLX35-NB2 gateways.

- 1 Click the **SETUP** icon in the top-right corner of the page and then click **CHANGE FIRMWARE**.



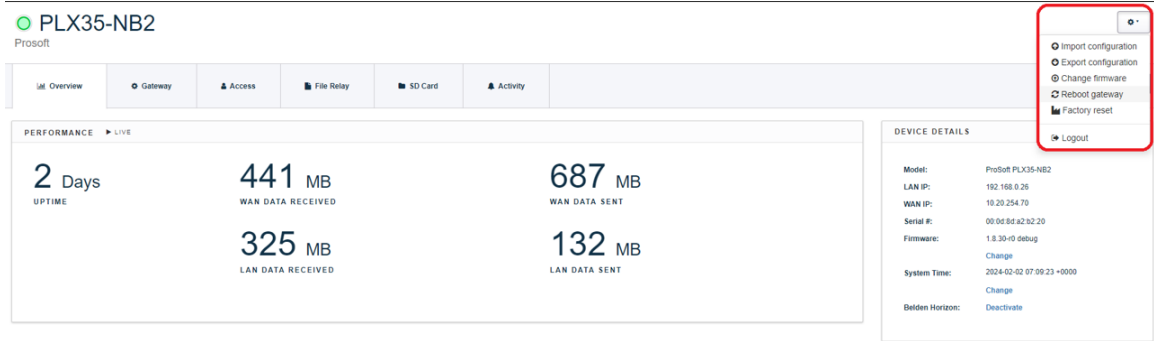
This opens the *Change firmware* dialog.



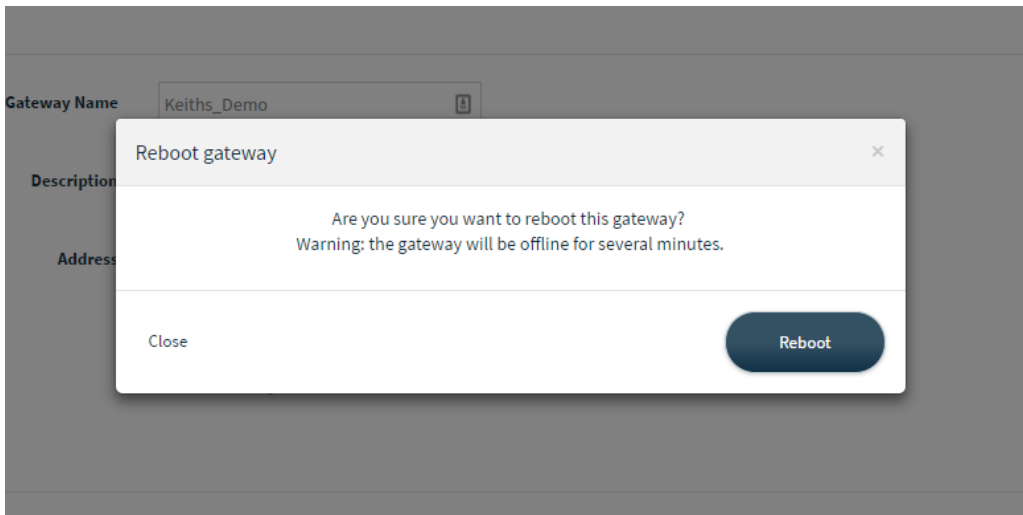
- 2 Click the **CHOOSE FILE** button and locate the firmware file.
- 3 Select the file and click **OPEN**.
- 4 Click the **CHANGE** button to load the new firmware.
- 5 After the firmware update is complete, refresh PLX35-NB2 webpage.

4.11 Rebooting the Gateway

- 1 Click the **SETUP** icon in the top-right corner of the page and then click **REBOOT GATEWAY**.



This opens the *Reboot gateway* dialog.

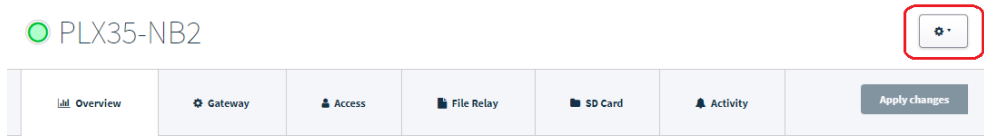


- 2 Click the **REBOOT** button when ready.

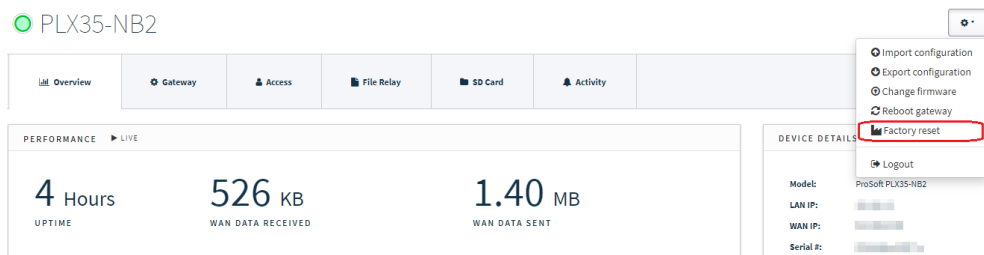
4.12 Factory Reset

The *Factory Reset* option will reset the PLX35-NB2 to its default configuration. All custom configuration changes will be lost after this procedure.

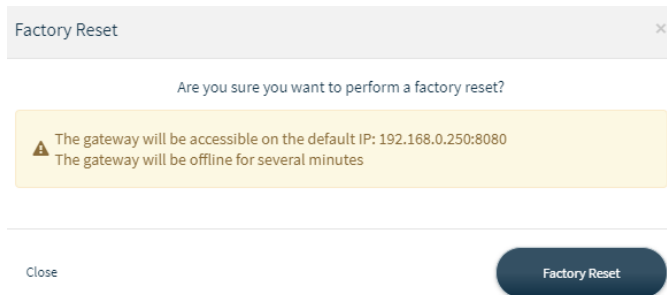
- 1 Click the **SETUP** icon in the top-right corner of the page.



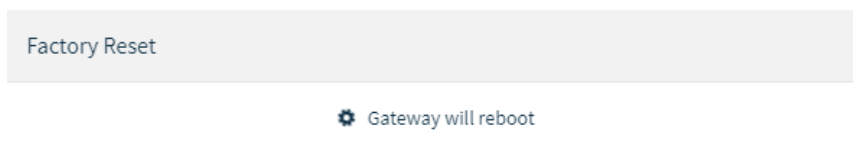
- 2 In the drop down, select the **FACTORY RESET** option.



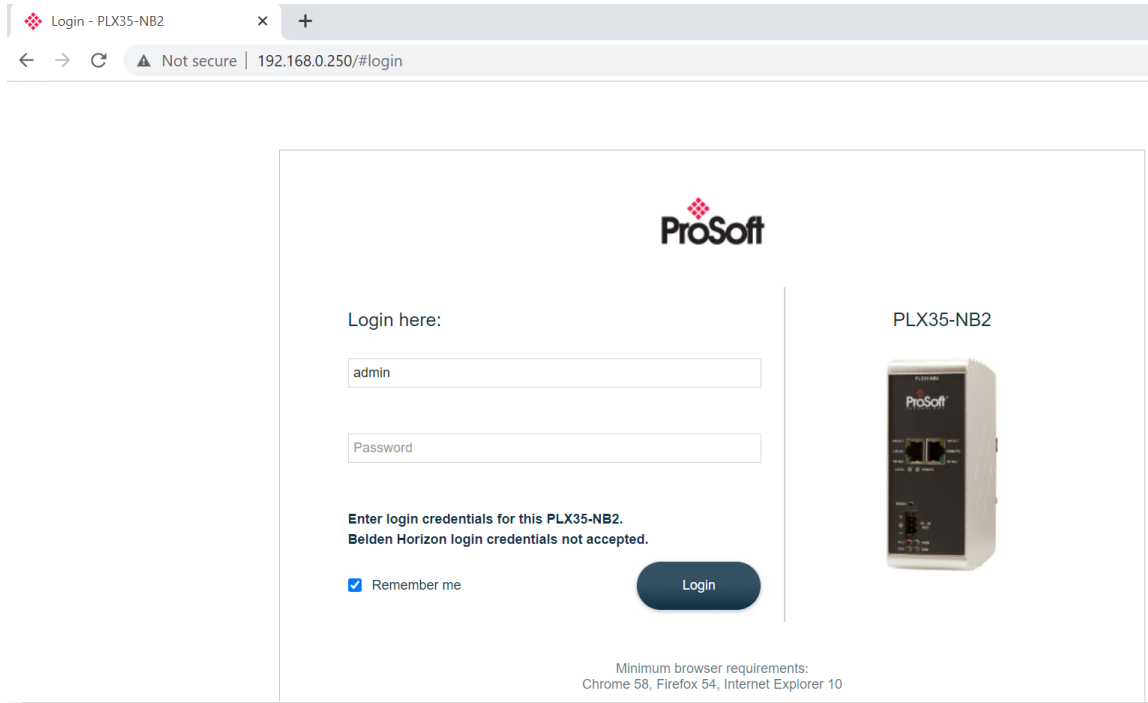
- 3 Click the **FACTORY RESET** button in the pop-up message that appears on the screen.



A pop-up message will indicate the factory reset procedure has begun.



- 4 After a few minutes, the PLX35-NB2 UI will be available by using the default IP address **192.168.0.250**.



- 5 After the factory reset is complete, the first login will be done using the default credentials (admin/password). It will then require you to change the password as shown in the See *Initial / Factory Reset Login* section on page 22.

5 Cloud-based Management Using Belden Horizon

Belden Horizon allows you to manage multiple gateways on the network through a secure VLAN tunnel via a webpage. You can perform multiple tasks, including activating, setting up VPN clients, perform configuration and maintenance, and invite team members.

5.1 Log In and Activate Belden Horizon

Belden Horizon requires that you activate the PLX35-NB2 the first time you use it. You must obtain an activation key from the gateway.

- 1 Connect your gateway WAN port to a network that can reach the internet. The MGMT LED will flash green if the PLX35-NB2 can reach the internet and is not yet activated.
- 2 Log in to the module from the LAN port as described in the section entitled "Connecting to the PLX35-NB2 Webpage" (page 13). This takes you to the *Overview* tab.
- 3 Under *Device Details*, click the **ACTIVATE** link to the right of the *Belden Horizon* label.

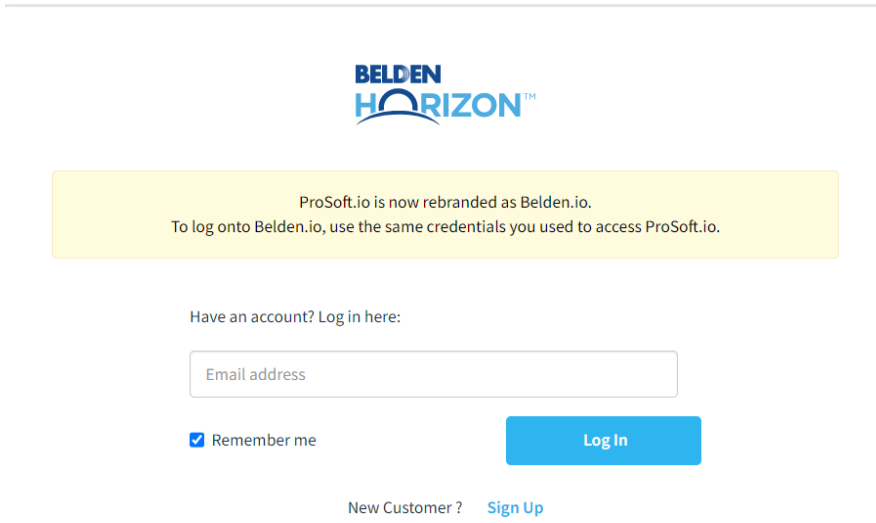
Note: If the gateway is already connected to a Belden Horizon account, the link reads "Deactivate".

- 4 The gateway securely retrieves an alphanumeric activation key from Belden Horizon that is only valid for three (3) hours. Record this activation key.

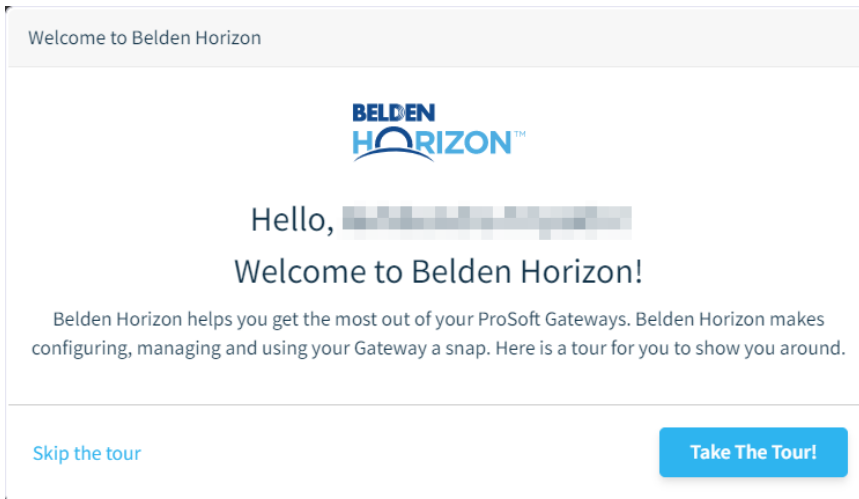
Note: The module must be connected to the internet through the WAN port in for the module to retrieve an activation key.

- 5 Open a new tab in your web browser, enter **www.belden.io** in the address bar, and then press **ENTER**.

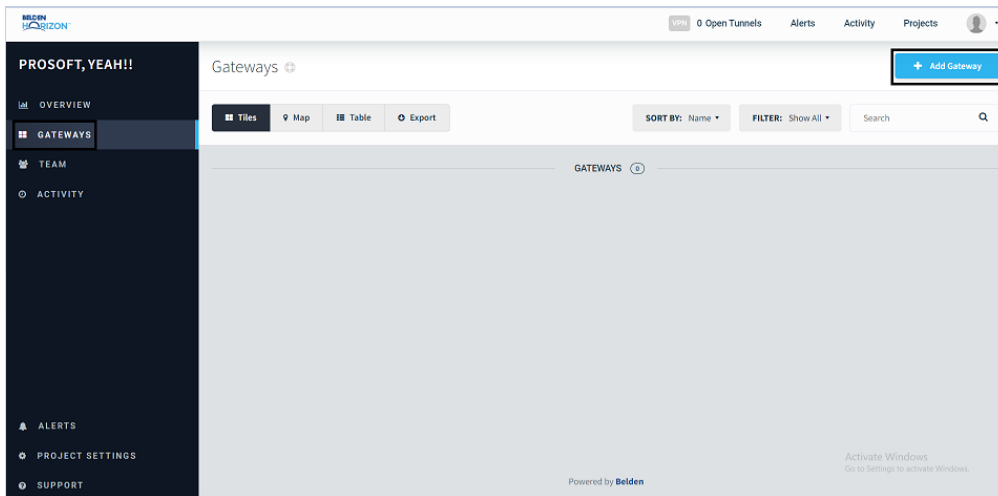
- 6 In the *Belden Horizon Login* screen, enter your Belden Horizon login email and password and click **LOGIN**, or click **SIGN UP** to create a new account. Login credentials are not interchangeable between Belden Horizon and the local interface.



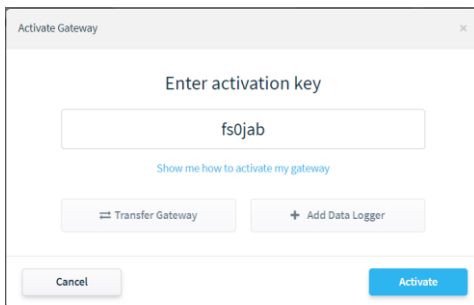
- 7 After you are logged in, you can take a tour of the features of Belden Horizon by clicking **TAKE THE TOUR**. Or you can skip the tour to configure the gateway.



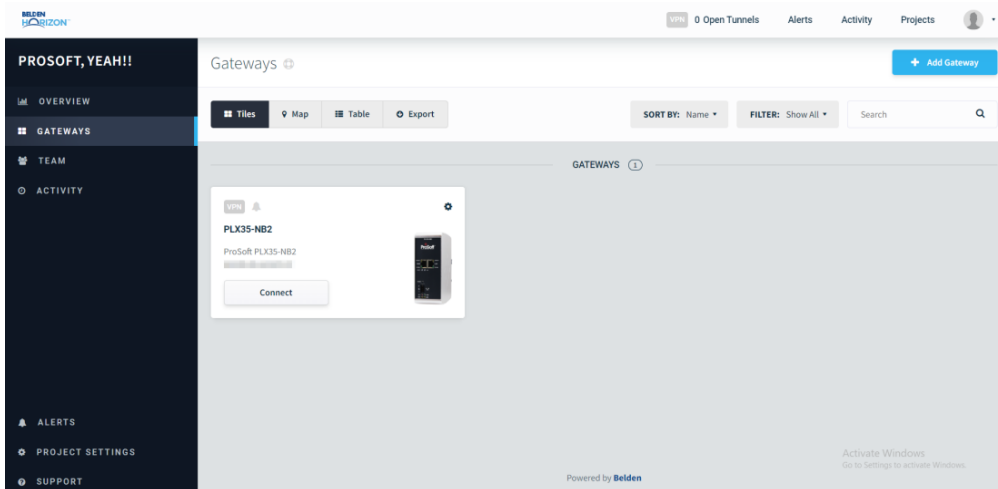
- 8 When ready, activate the PLX35-NB2 within the tour, or you can click on the **ADD GATEWAY** button from the *Gateways* tab.



- 9 Belden Horizon prompts you for the activation key that you recorded earlier. Click **ACTIVATE**.



- 10 Upon successful activation, the PLX35-NB2 appears on the *Gateways* page.



5.1.1 Belden Horizon On-Prem

Belden Horizon On-Prem requires that you activate the PLX35-NB2 the first time you use it. To do this, you must obtain an activation key from the gateway.

- 1 Connect your gateway WAN port to On-Prem server.
- 2 Log in to the PLX35-NB2 from the LAN port as described in the section entitled "Connecting to the PLX35-NB2 Webpage" (page 13). The *Overview* tab displays.
- 3 In the *Overview* tab > *Device Details*, click the **ACTIVATE** link to the right of the *Belden Horizon* label.

Note: If the PLX35-NB2 is already connected to a Belden Horizon account, the link reads "Deactivate".

- 4 The PLX35-NB2 securely retrieves an alphanumeric activation key from Belden Horizon On-Prem. It is valid for three (3) hours. Record this activation key.

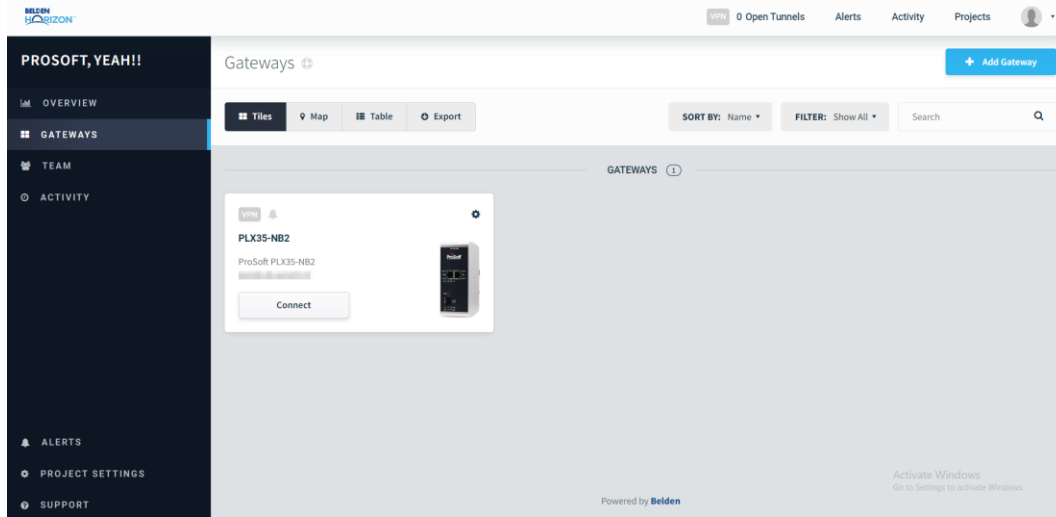
Note: Access to Internet is not necessary for generating a key or adding it to Belden Horizon On-Prem server.

- 5 Open a new tab in a web browser, enter **www.onprem.belden.io** and press **ENTER**.
- 6 In the Belden Horizon On-Prem Login screen, enter the user credentials or click **SIGN UP** to create a new account. The login credentials are not interchangeable between Belden Horizon On-Prem and the local interface.
- 7 After logging in, you can take a tour of the features of Belden Horizon On-Prem by clicking **TAKE THE TOUR**. Or you can skip the tour to configure the gateway.
- 8 When ready, activate the PLX35-NB2 within the tour, or click on the **ADD GATEWAY** button from the *Gateways* tab.
- 9 Belden Horizon On-Prem prompts you for the activation key that you recorded earlier. Click **ACTIVATE**.
- 10 Upon successful activation, the PLX35-NB2 appears on the *Gateways* page.

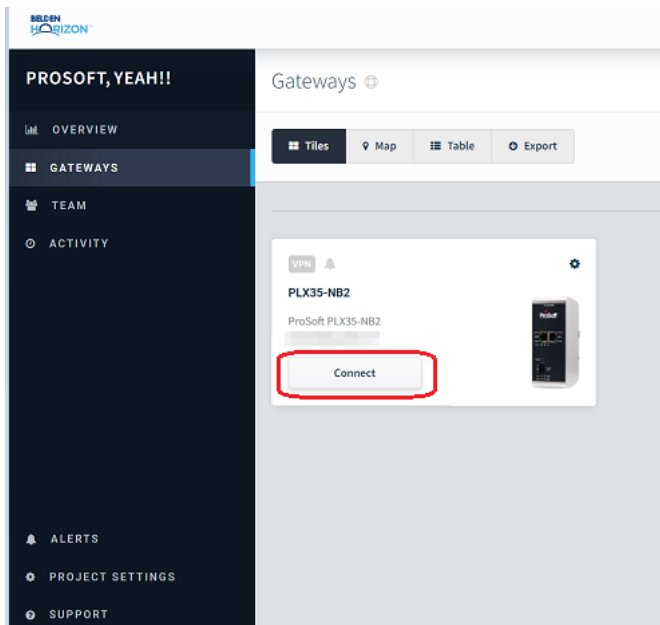
5.2 Creating and Connecting a New VPN Client

Belden Horizon uses your native Windows VPN client for secure remote access. The first time you intend to establish a VPN connection, you must set up the client and then connect to it. Initial VPN client configuration is only done once and is described in the following steps. If you already have a Belden Horizon VPN Client established in your Network Connections folder, you do not need to perform these steps.

Once the PLX35-NB2 is activated, the gateway is displayed on the *Gateways* page.



- 1 In the *Gateways* tab, click on the **CONNECT** button of the gateway profile.



2 Assign the PC's IP address and subnet mask.

Assign local IP address

Assign IP address to computer when tunneling

Enter an IP address below. Your computer will be given this IP address when connecting through the gateway to devices at the remote site. This IP address must not be in use by the end devices at your remote site.

This configuration only has to be set one time per gateway

Client IP

IP address

Client Subnet Mask

IP address

Cancel Save & Connect

3 The system generates a unique secure one-time use username.

Open Tunnel for PLX35-NB2

✓ Username generated

This username is only valid for a single session. Copy and paste the username below into your VPN client to connect. (Don't worry, you won't need a password or domain.)

Region: NA California

51Z082OPKT@Tun-X30RXR93RYMR8LY7Z

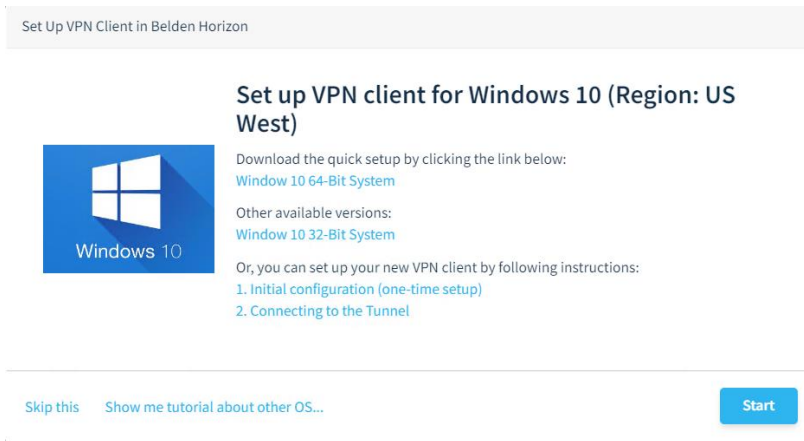
Copy To Clipboard

[Show me how to setup my VPN client](#)

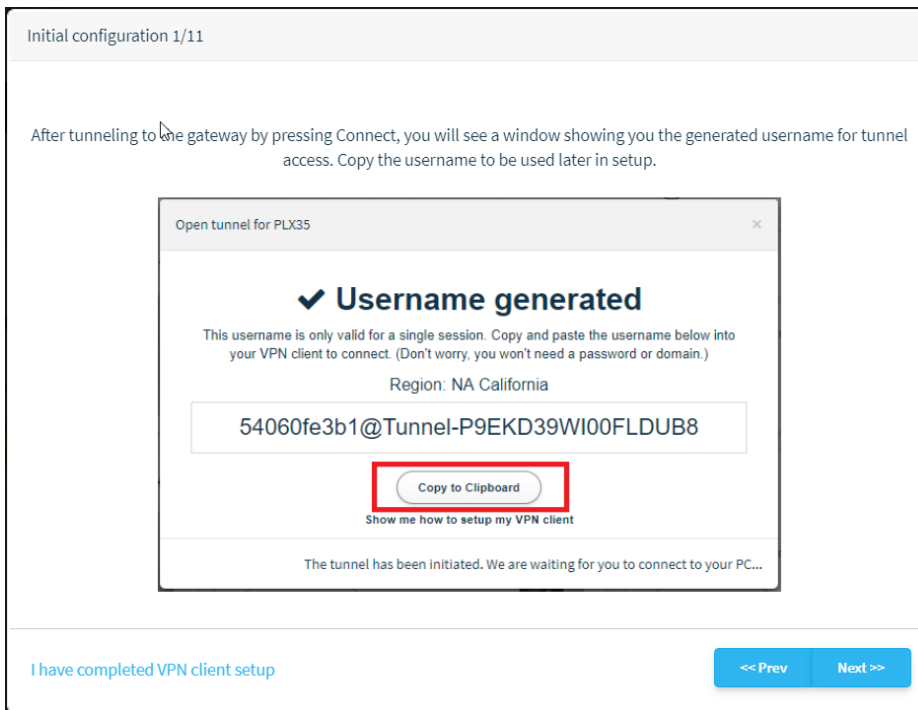
The tunnel has been initiated. We are waiting for you to connect to your PC...

4 Click the **COPY TO CLIPBOARD** button to save this username.

- 5 Click "**SHOW ME HOW TO SETUP MY VPN CLIENT.**" This opens the *Set Up VPN Client in Belden Horizon* dialog.

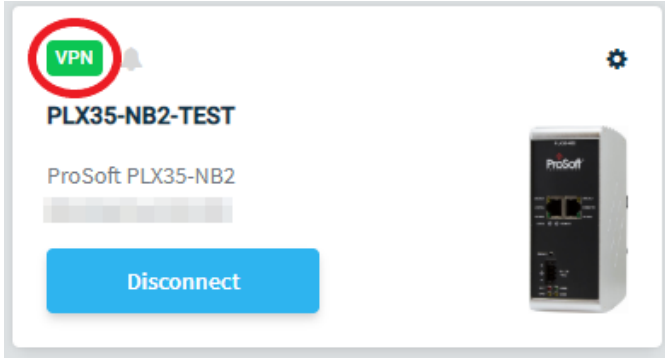


- 6 Click on the **INITIAL CONFIGURATION (ONE-TIME SETUP)** option. Follow the tutorial to complete the setup. The tutorial also shows you how to connect to the VPN tunnel.



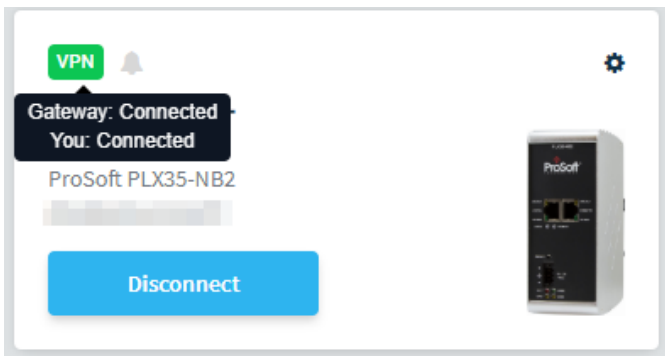
5.2.1 Verifying the VPN Connection

The module on the Gateways page of Belden Horizon provides a VPN indicator as shown:



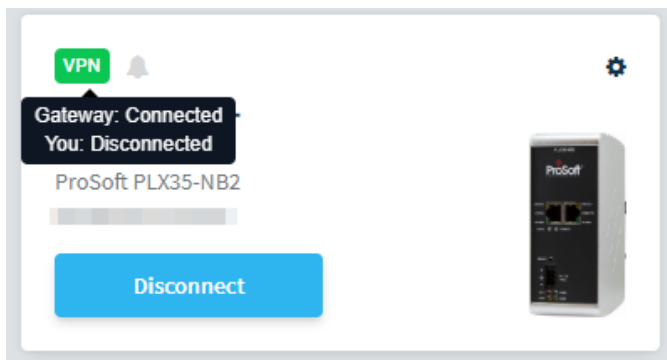
You can view the connection status by hovering over the VPN icon or by hovering over the status at the top of the page. See the next section for more details.

This indicator is grayed out if there is no connection established. However, you can hover over this indicator to obtain more information about the connection.



The example above shows both the gateway and the user are connected to the VPN server.

If only one part of the tunnel connection is established, the indication may appear as shown below:

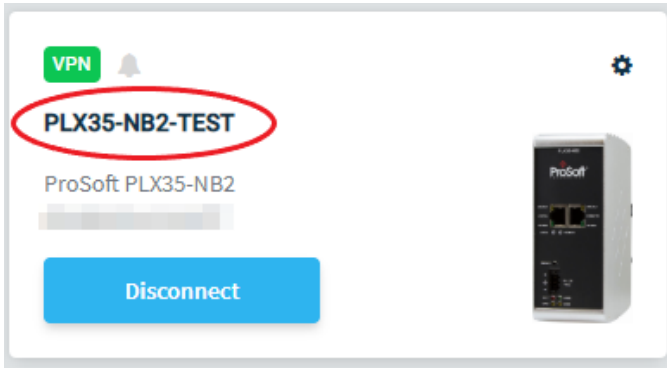


This example shows a connection between the gateway and the VPN server. However, it shows the user as "Disconnected". In this case, Belden Horizon may be waiting for the user to provide a user name in order to connect to the VPN.

5.3 Using Belden Horizon to Configure the PLX35-NB2

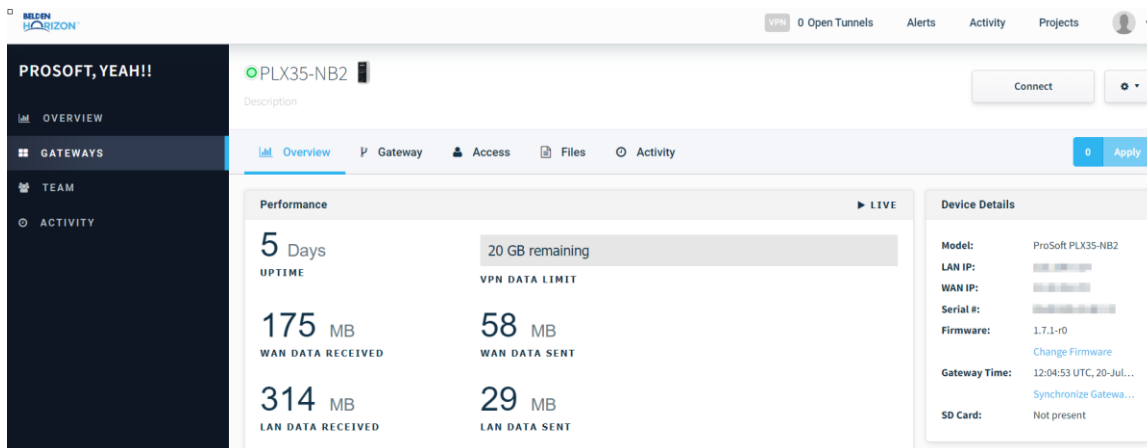
All configuration tasks may be performed using Belden Horizon. You do not need to use the module's internal web server to configure the module or edit existing configurations.

To access configuration parameters, click on the module name.



This opens the gateway's configuration pages.

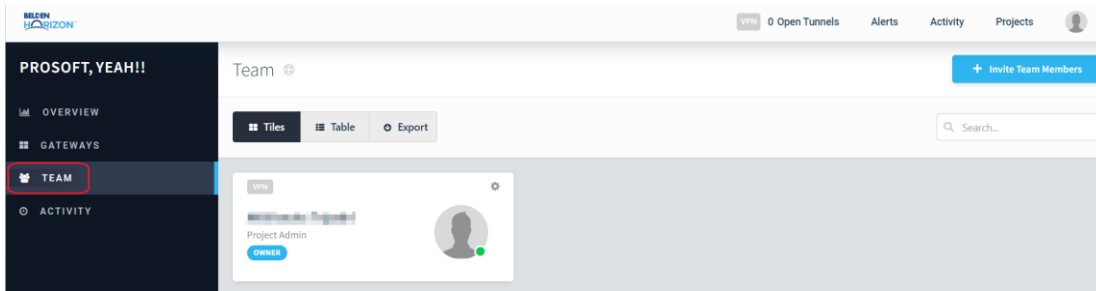
In addition to the normal features of Belden Horizon, these configuration pages are exclusive to the PLX35-NB2. The configuration tabs are the same as those described under "Local Configuration using the Gateway's Configuration Webpage" on page 13.



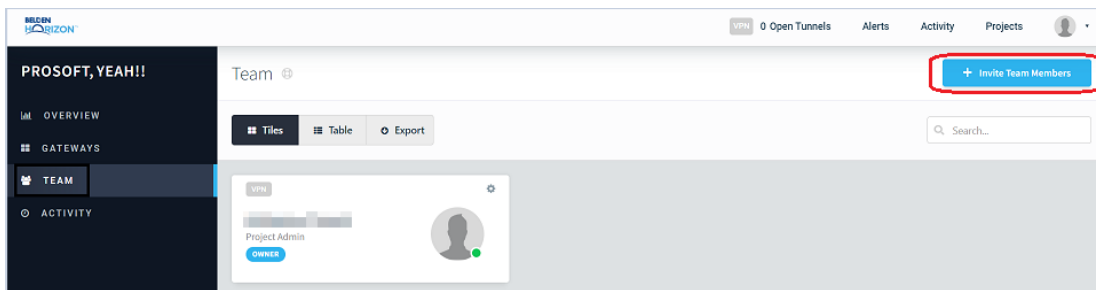
5.4 Adding Team Members

Within Belden Horizon, you can invite team members to your account. This allows others to securely access the remote site and perform maintenance and configuration functions on the gateway once invites are accepted.

- 1 Click on the **TEAM** icon.



- 2 Click on the **INVITE TEAM MEMBERS** button located in the upper-right hand corner of the page.



3 The *Invite New Team Member* dialog opens.

Invite New Team Member

An email with an activation link will be sent to the provided email address. The link will expire in 5 days (Jul 25 2022 @ 17:46). If the user does not activate their account until then, they will have to manually reset their password.

Message

Please join me on Belden Horizon.
You can use this account to manage ProSoft gateways.
You can also use this account to access any device connected to a ProSoft gateway using a tunnel.

Email

E-mail address

First Name

First Name

Last Name

Last Name (optional)

Choose project role

Project Admin Configure & Connect **Connect Only** Custom

Cancel Send Invitation

4 Enter the information and the project role of the person you want to invite.

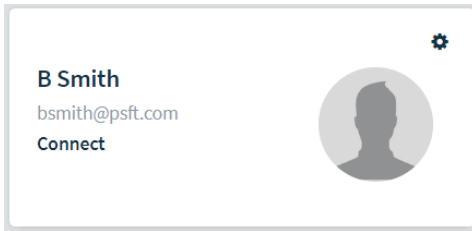
Note: An email address can only be associated with one Belden Horizon account at a time.

5 Modify the *Message* dialog to send a unique message to the invitees.

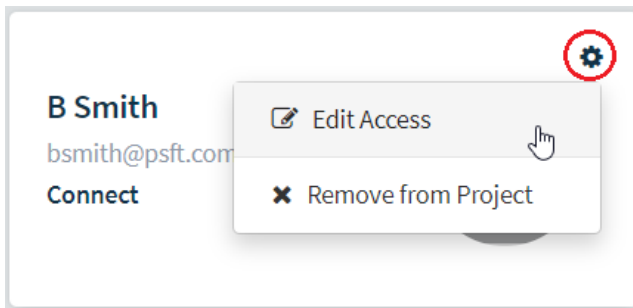
6 When you are done, click the **SEND INVITATION** button. You should receive an “invitation sent successfully” message if the email address was valid. You can edit a member’s access rights once the invite is sent.

5.4.1 Editing Team Member Access

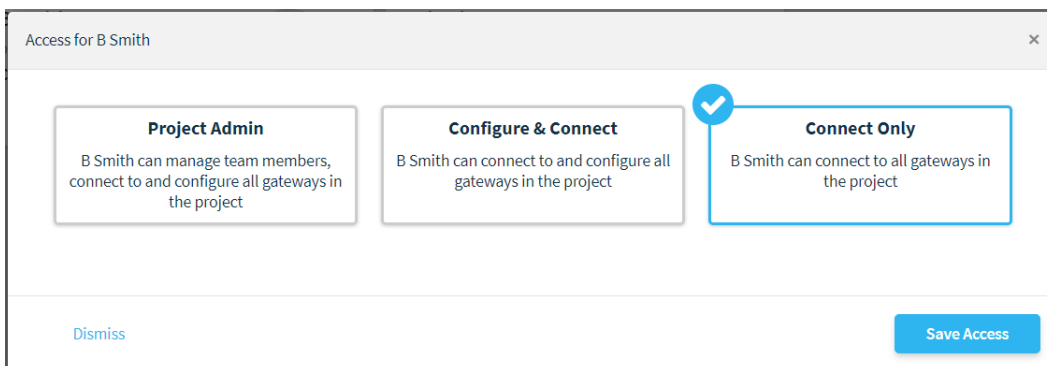
As an administrator, you can control the type of access rights assigned to your team members. When a team member accepts an invitation, a card appears on the *Team* page of Belden Horizon.



- 1 Click on the **EDIT ACCESS** option.



- 2 This opens the access dialog for the new team member. Initially, access defaults to "Connect only" which means that that user is allowed to create a tunnel, but is not allowed to configure a gateway.

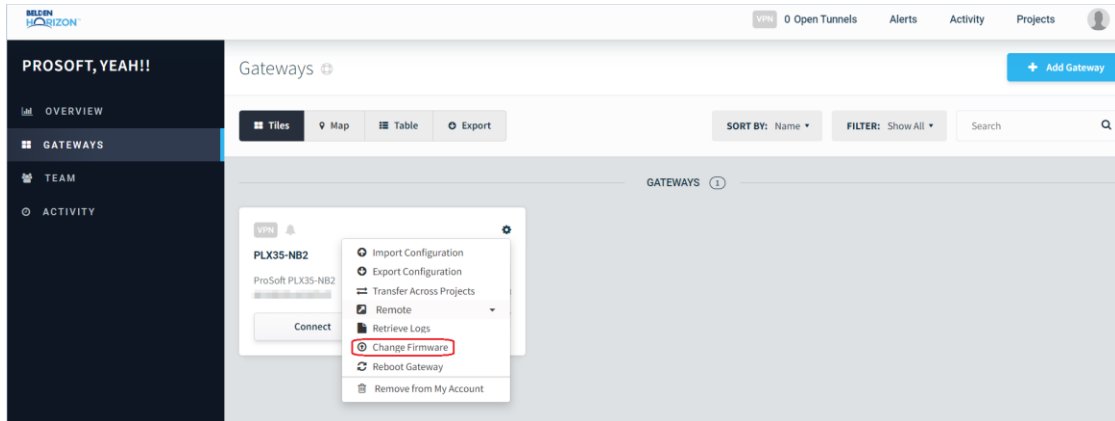


- 3 Change this user's access rights by clicking on any of the first 3 access selections and then click the **SAVE ACCESS** button.

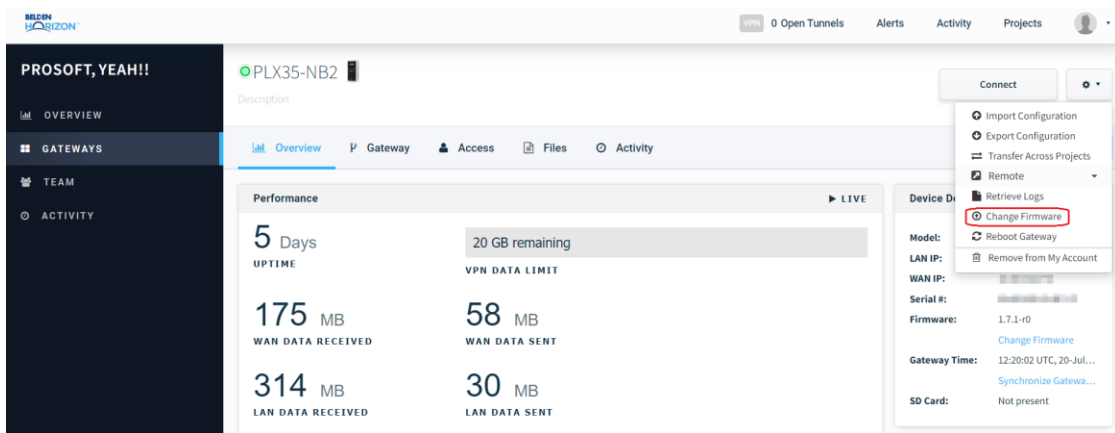
5.5 Changing Firmware

You can schedule a firmware change for multiple gateways or a single gateway through Belden Horizon. There are two ways to start the firmware change process:

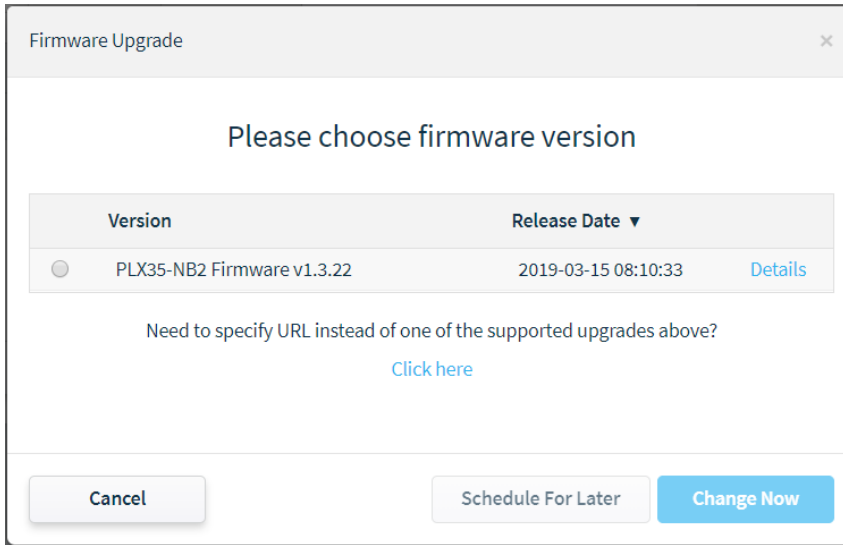
- Click the firmware **CHANGE** option in the *Device Details* block.



- Select **CHANGE FIRMWARE** from the setup icon in the top-right corner of every configuration page.

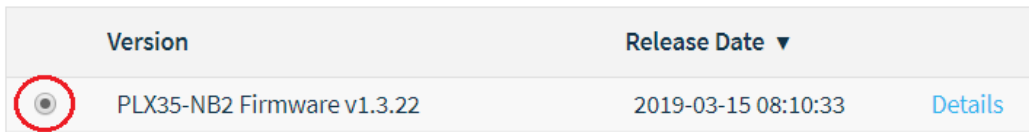


- 1 Click on the **CHANGE FIRMWARE** option to open the *Firmware Upgrade* dialog.



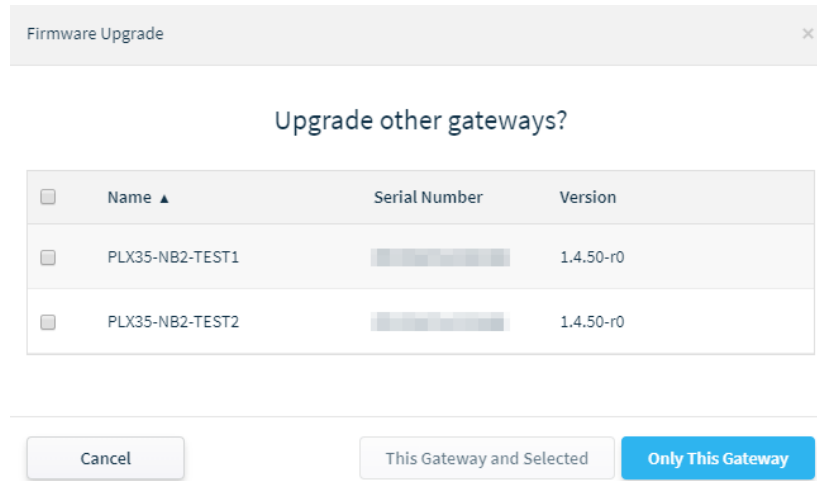
This dialog lists the most recent firmware versions and details about this version.

- 2 Select the version to install by clicking the radio button.



There are options to upgrade now or schedule for later.

- i. **Change Now** - Allows you select additional gateways for upgrade and then immediately performs the upgrade.
 - 1 With the correct firmware version selected, click the **CHANGE NOW** button. You are prompted as to whether or not you want to upgrade other gateways.



- 2 Choose any available gateways that you want to upgrade, if applicable.
- 3 Click the **APPLY ONLY TO THIS GATEWAY** button if you do not need to upgrade additional gateways or click the **APPLY TO THIS GATEWAY AND SELECTED** button to upgrade firmware on the current gateway and any selected gateways.
- 4 The firmware upgrade starts immediately.

ii. **Schedule for Later** - Allows you to select additional gateways for upgrade and then allows you to schedule a date and time for the upgrade to occur.

- 1 With the correct firmware version selected, click the **SCHEDULE FOR LATER** button. You are prompted as to whether or not you want to schedule upgrades for other gateways.

<input type="checkbox"/>	Name ▲	Serial Number	Version
<input type="checkbox"/>	PLX35-NB2-TEST1	[REDACTED]	1.4.50-r0
<input type="checkbox"/>	PLX35-NB2-TEST2	[REDACTED]	1.4.50-r0

- 2 If you don't want to schedule upgrades for other gateways, click the **APPLY ONLY TO THIS GATEWAY** button to schedule the upgrade.

Version: PLX35-NB2 Firmware v1.3.22
Gateway: PLX35-NB2-TEST

Please select a date and time

01/08/2020 9:05 AM

January 2020

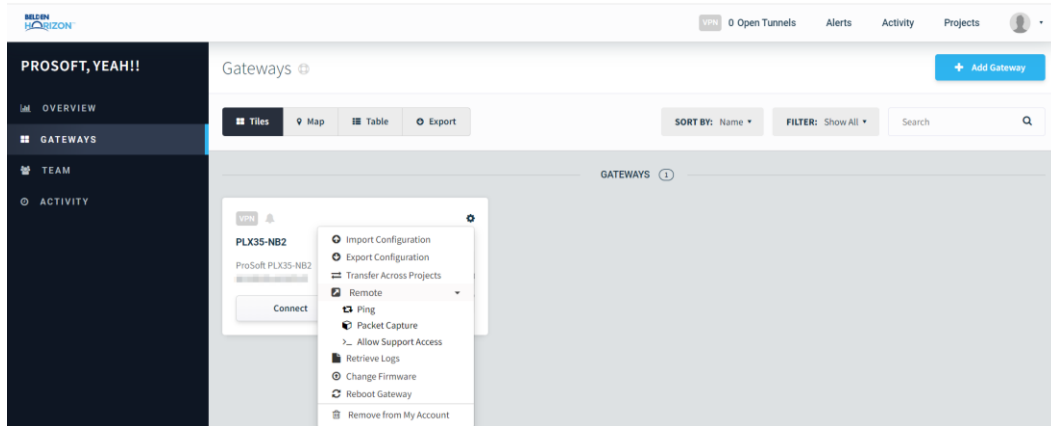
Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

- 3 Schedule the date and time for the firmware change to occur.
- 4 Click the **SCHEDULE** button.
If you want to schedule changes for other gateways, use the **APPLY TO THIS GATEWAY AND SELECTED** button and follow the same procedure.

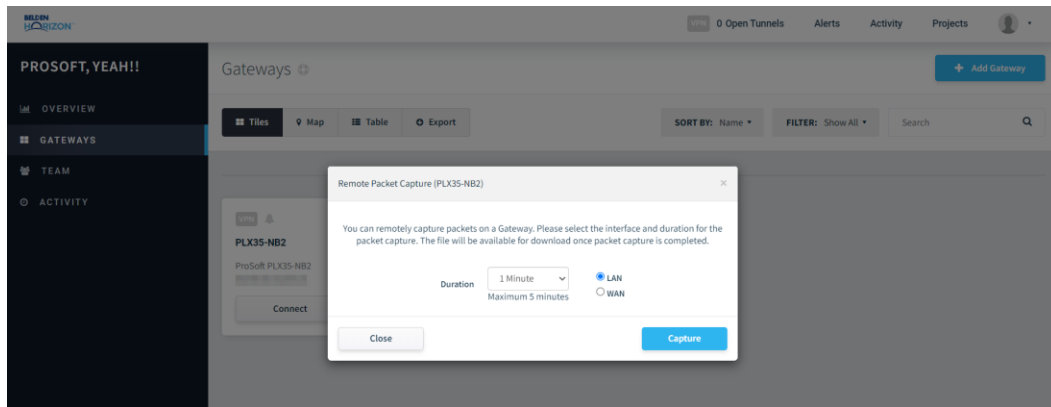
5.6 Remote Packet Capture

The following procedure describes a remote packet capture. This feature is available in firmware version v1.6.60 and newer.

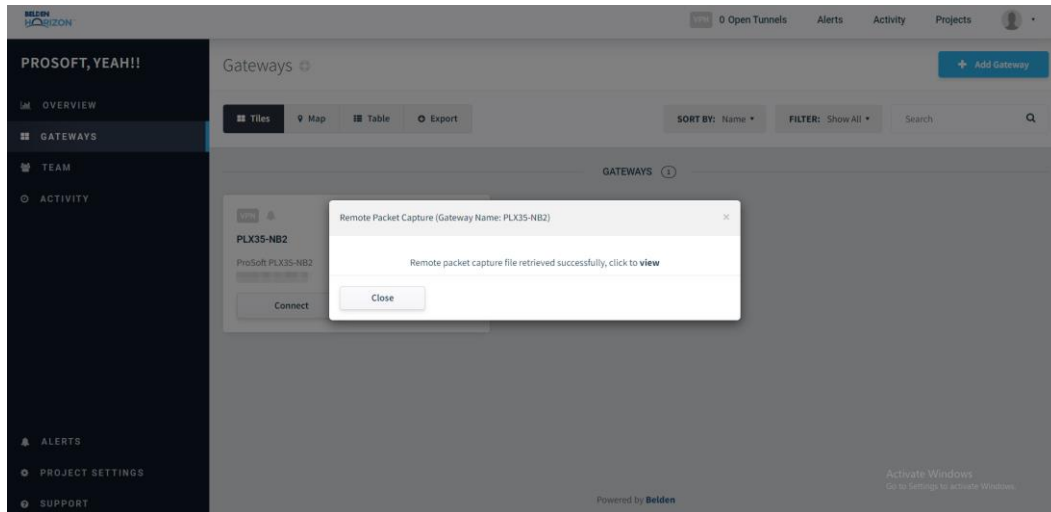
- 1 Right-click on the **SETUP** icon of the PLX35-NB2, and select **PACK CAPTURE**.



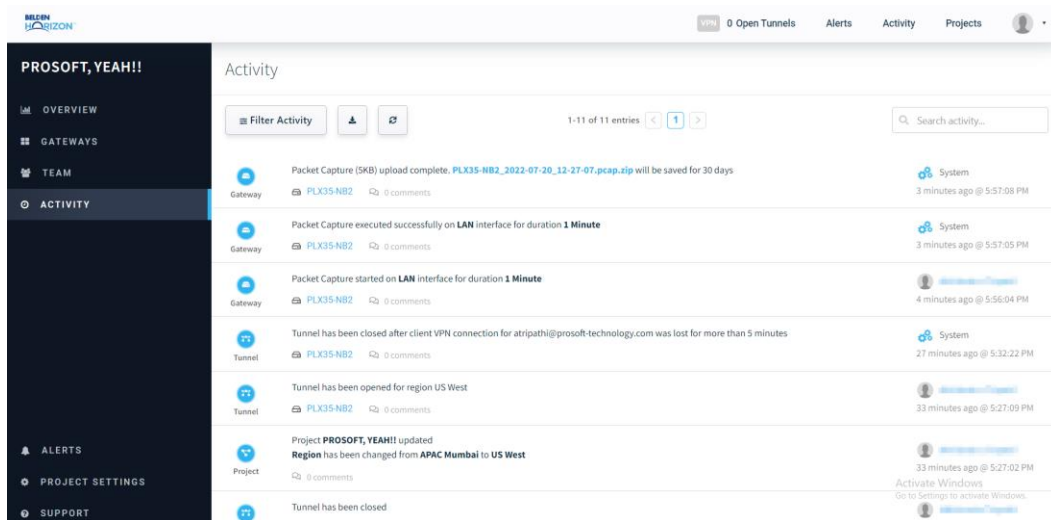
- 2 Select the duration and interface to be used in the capture. Click **CAPTURE** to begin.



- 3 Once the capture is complete, the captured file can be viewed.

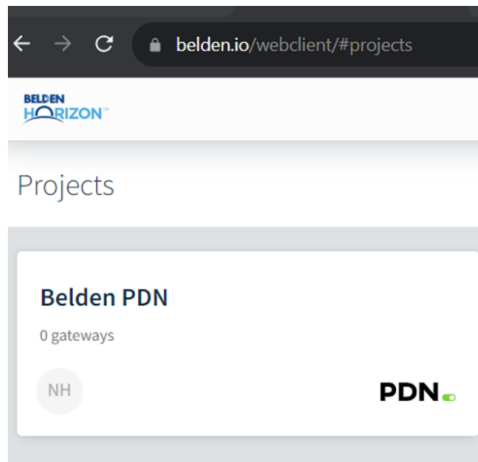


- 4 The captured files are saved in Belden Horizon for few days. It can also be downloaded from the *Activity* tab as shown below:



6 Easy Bridge

The PLX35-NB2 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 (Persistent Data Network) Projects in **Belden.io**.

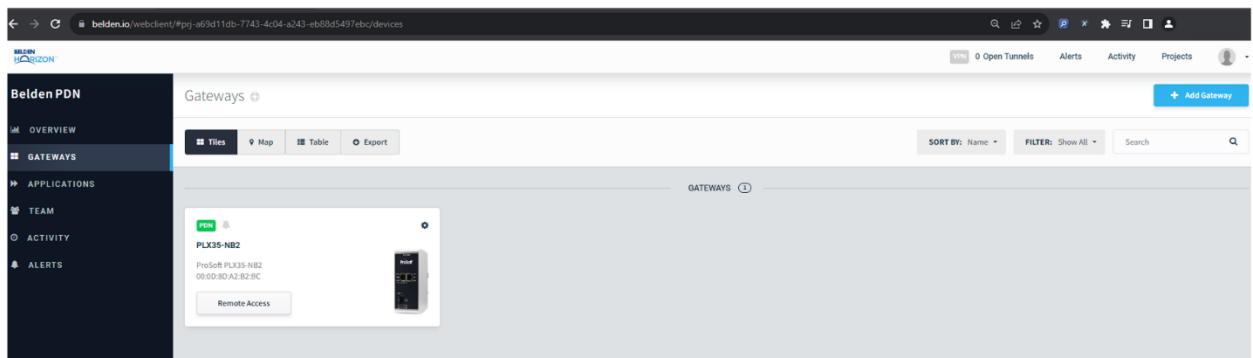


6.1 VPN Tunnel Connection

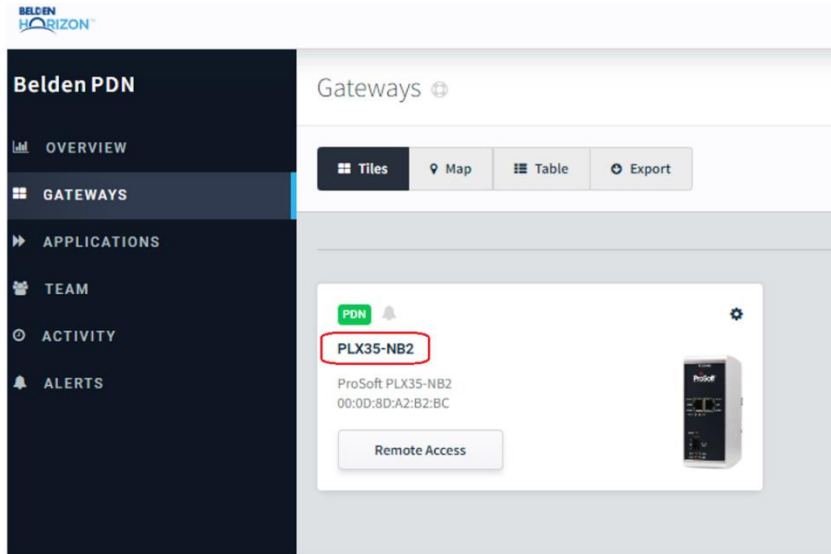
Once a local connection to the PLX35-NB2 gateway has been established (see *Connecting to the PLX35-NB2 Webpage* on page 13 for more information), ensure the following:

- WAN port has internet access (see *Setting Gateway Configuration Parameters* page 15 for more information).
- Activation is successful through the Belden Horizon UI (see *Cloud-based Management Using Belden Horizon* page 48 for more information).

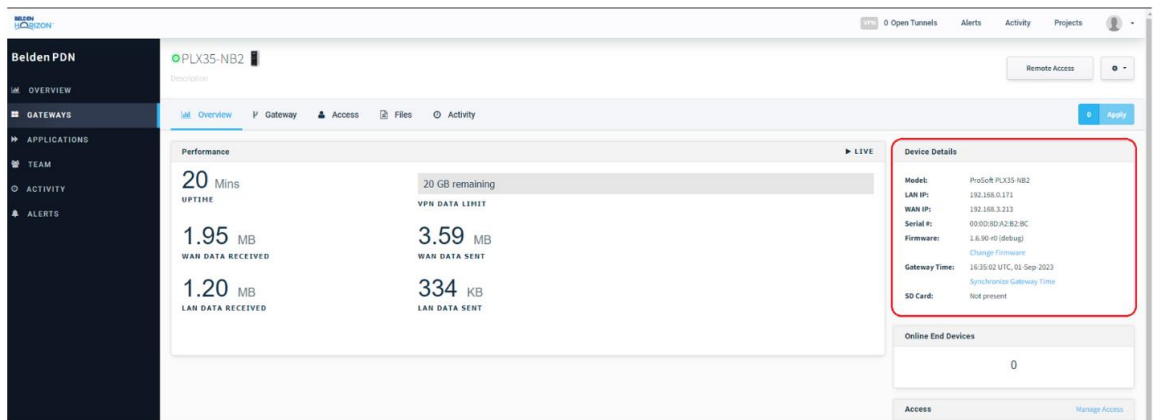
Once the PLX35-NB2 is activated, it will be listed in the *Gateways* section of the **Belden.io** page.



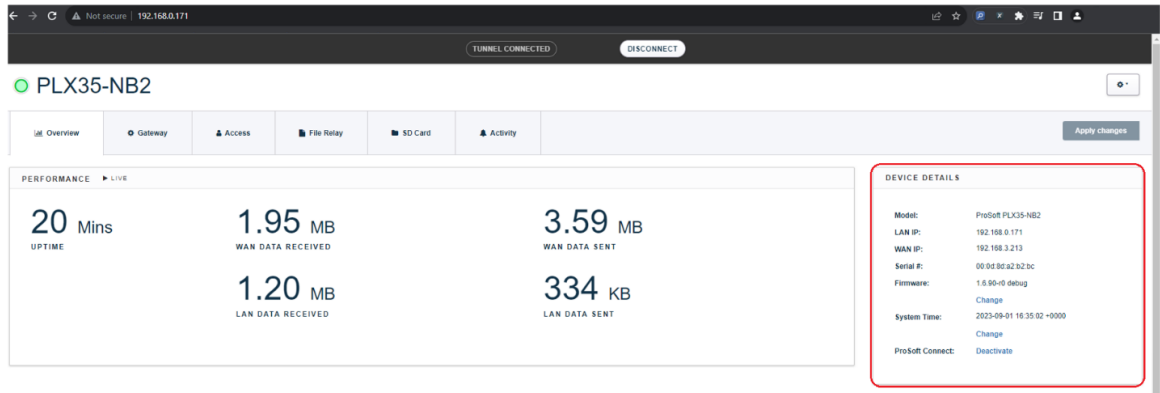
- 1 Click on the **PLX35-NB2** name within the tile.



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

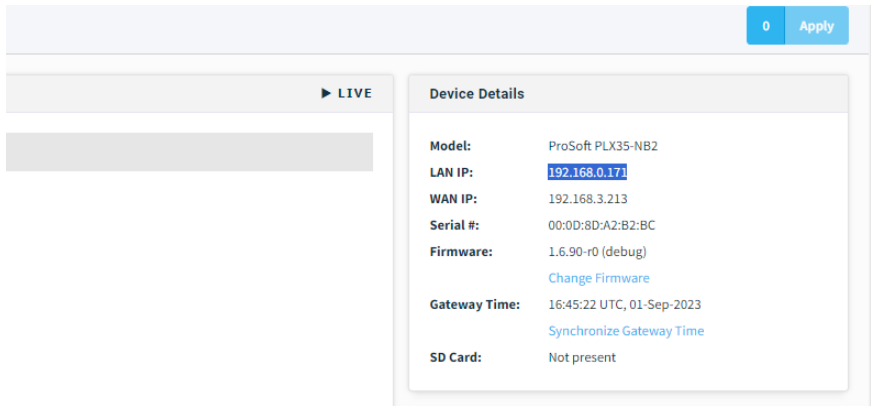


- The *Device Details* should match the *Device Details* on the module's webpage (see below). This confirms the Activation and PDN are operating prior to starting the VPN Tunnel.

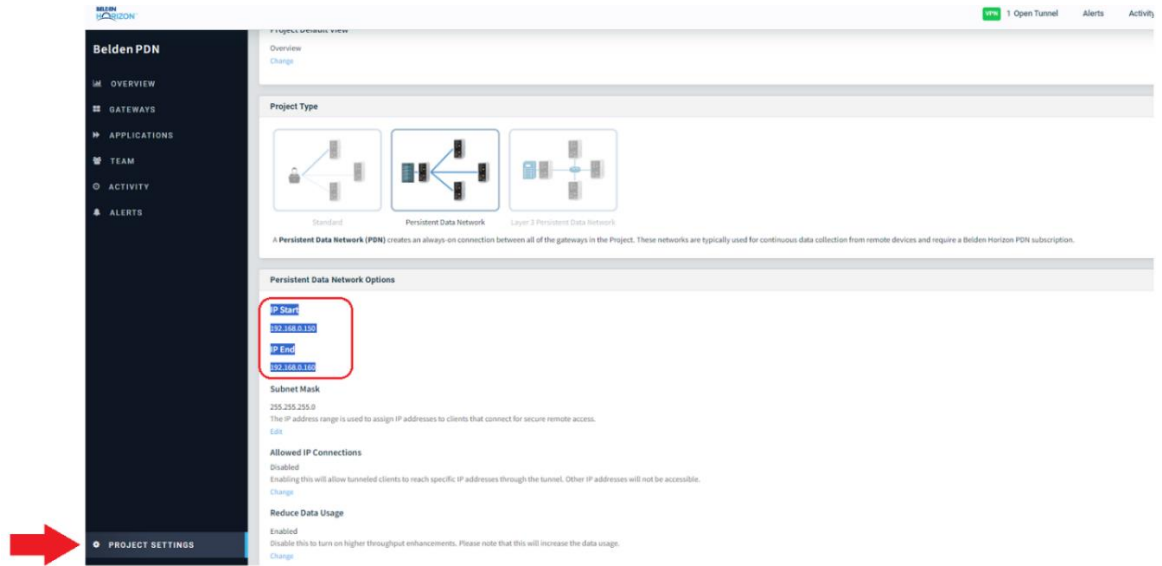


- Ensure the PLX35-NB2 LAN IP address is on the same network as the PLC Controller IP address.

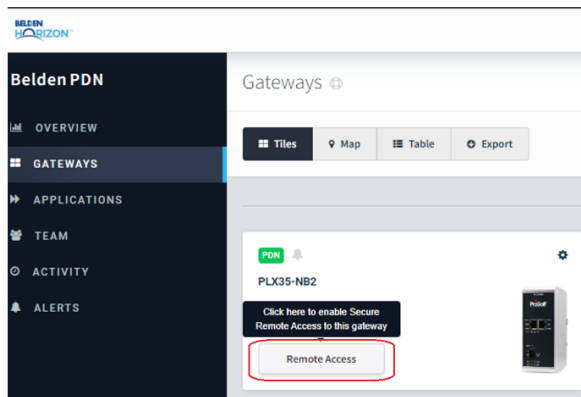
This exercise uses the following IP address examples:
PLX35-NB2 LAN IP: **192.168.0.171**
PLC Controller: **192.168.0.215**



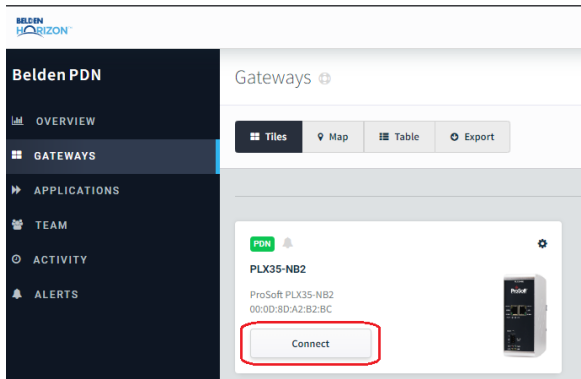
- 5 On the left tab of **Belden.io** page, click on the **PROJECT SETTINGS** button. Under the *Persistent Data Network Options* section, verify the PLX35-NB2 IP address range is correct.



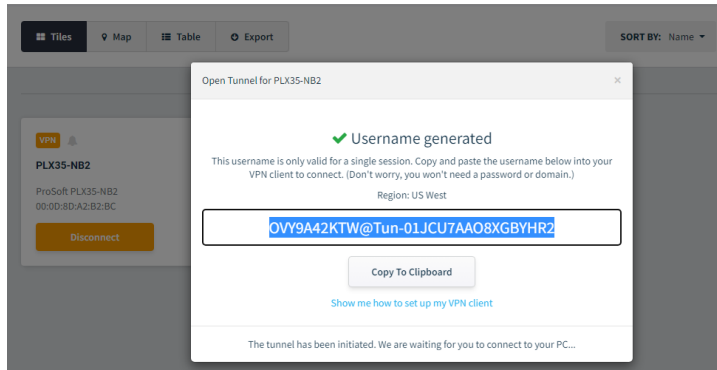
- 6 From the *Gateways* tab, click on the **REMOTE ACCESS** button to enable a secure, remote access to the PLX35-NB2.



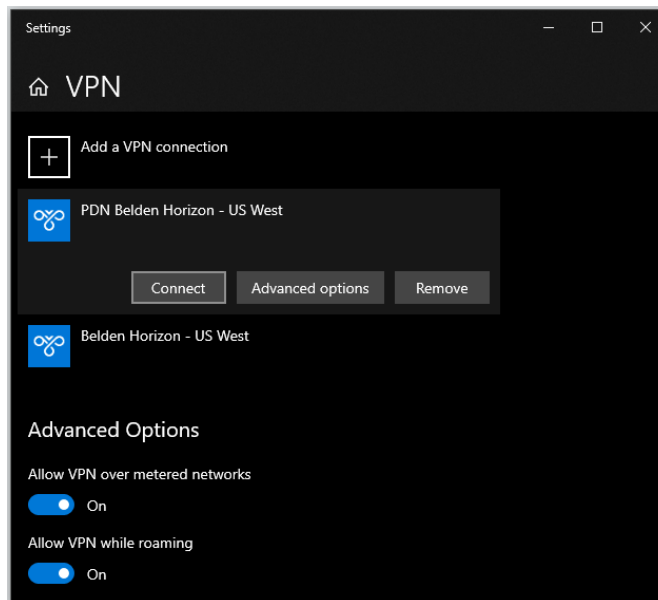
Then click on the **CONNECT** button.



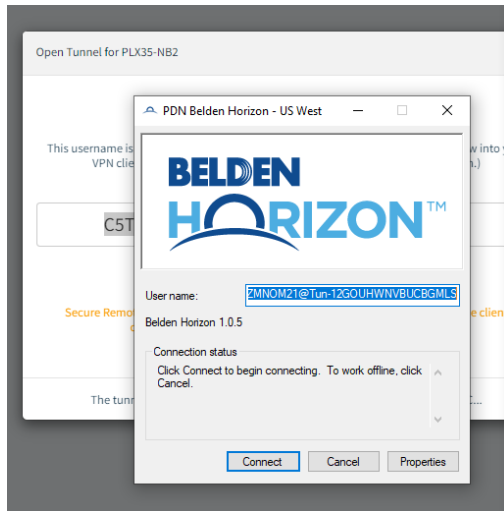
- 7 In the *Open Tunnel for PLX35-NB2* dialog, a username is automatically generated. Click the **COPY TO CLIPBOARD** button. This is a one-time use username key. This key is needed to connect the VPN Client to the Belden Horizon Tunneling Server.



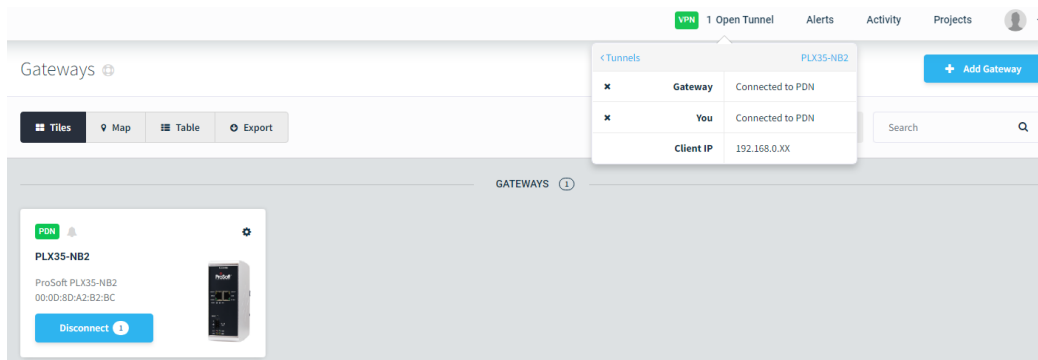
- 8 Open the **WINDOWS SETTINGS > NETWORK & INTERNET > VPN** selection. Under the *PDN Belden Horizon – US West* VPN option, click the **CONNECT** button.



- 9 In the VPN Client dialog, paste the one-time username key and click the **CONNECT** button.

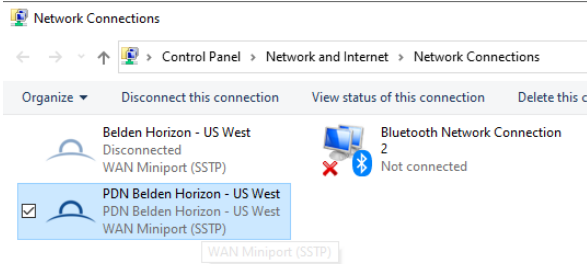


- 10 Upon successful VPN Tunnel connection, the status is shown in the **OPEN TUNNEL** option in the **Belden.io** menu.

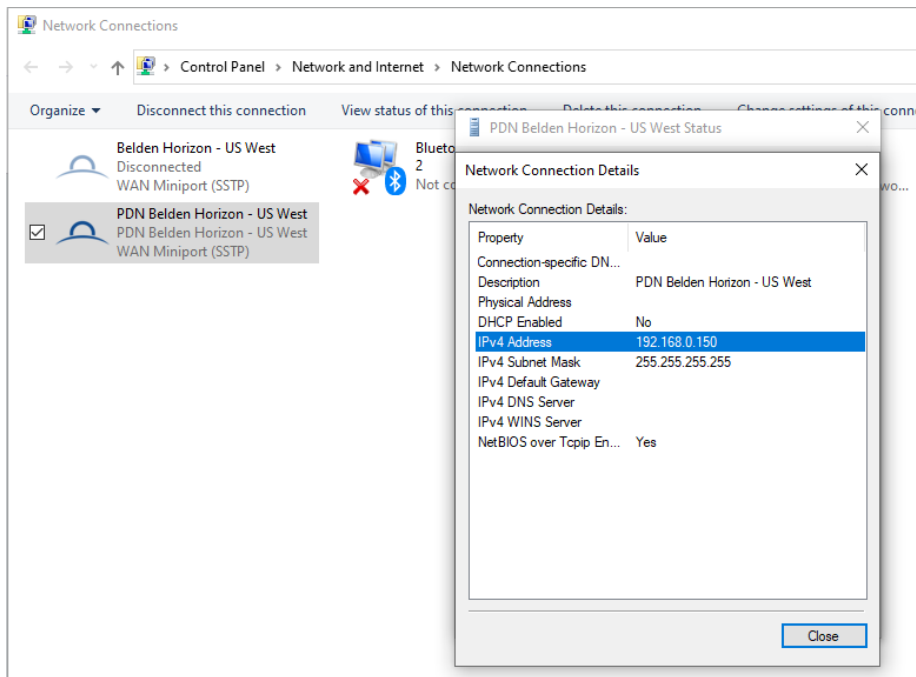


6.1.1 Verifying VPN Tunnel Connection

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



- 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.

```
C:\Users\Sysadmin>ipconfig -all

Windows IP Configuration

Host Name . . . . . : Win10_VM_ENV
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-64-82-41
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e20d:b291:8b53:f224%2(Preferred)
IPv4 Address. . . . . : 192.168.3.204(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.3.1
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-73-81-6D-00-0C-29-64-82-41
DNS Servers . . . . . : 10.2.10.72
                       10.2.10.73
NetBIOS over Tcpi. . . . . : Enabled

PPP adapter PDN Belden Horizon - US West:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : PDN Belden Horizon - US West
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.0.150(Preferred)
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . :
NetBIOS over Tcpi. . . . . : Enabled
```

- 4 The PLC Controller's IP Address (ex. 192.168.0.215) can now be pinged.

```
Autoconfiguration Enabled . . . . . : Yes

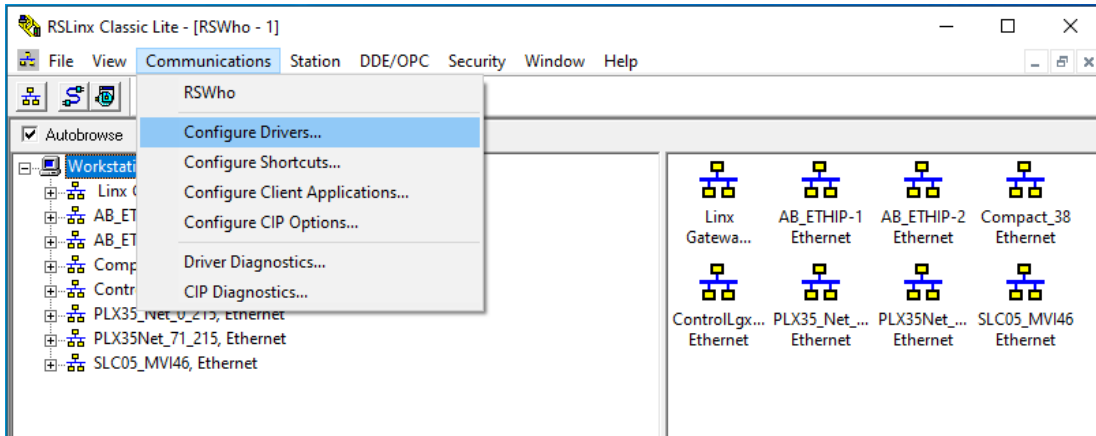
C:\Users\Sysadmin>ping 192.168.0.215

Pinging 192.168.0.215 with 32 bytes of data:
Reply from 192.168.0.215: bytes=32 time=147ms TTL=64
Reply from 192.168.0.215: bytes=32 time=79ms TTL=64
Reply from 192.168.0.215: bytes=32 time=118ms TTL=64
Reply from 192.168.0.215: bytes=32 time=86ms TTL=64

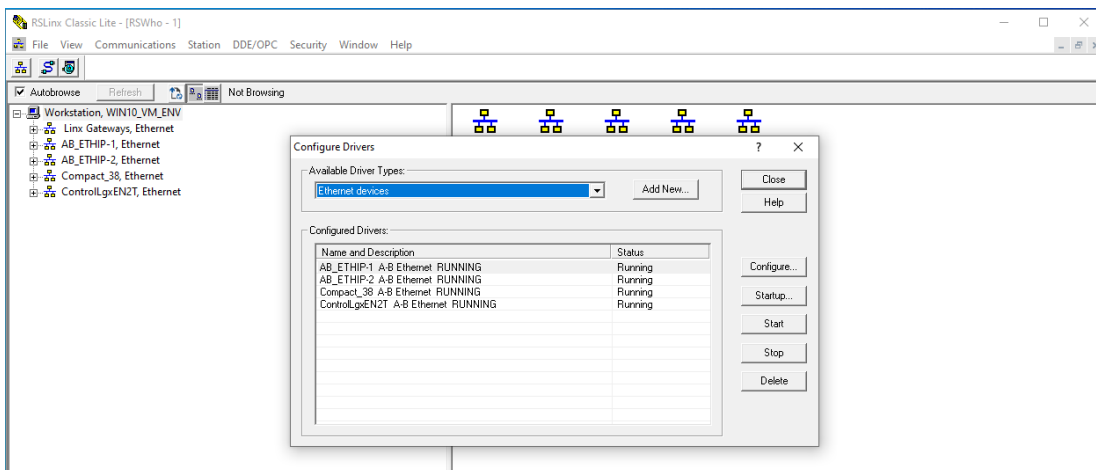
Ping statistics for 192.168.0.215:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 79ms, Maximum = 147ms, Average = 107ms
```

6.2 Configuring a New Driver in RSLinx

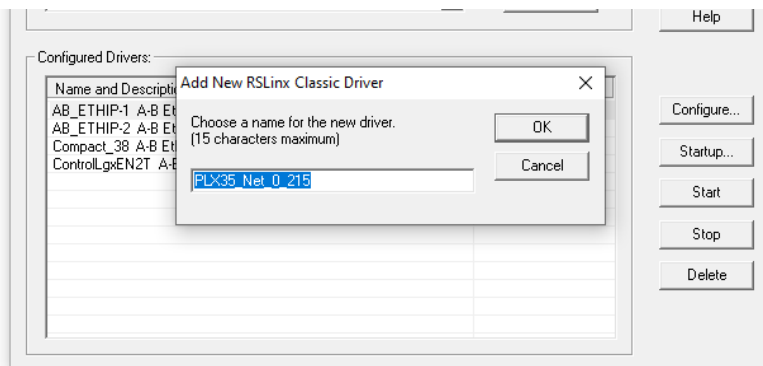
- 1 Open RSLinx to view the available Rockwell Controllers.
- 2 Click on the **COMMUNICATIONS > CONFIGURE DRIVERS** option to configure a new driver.



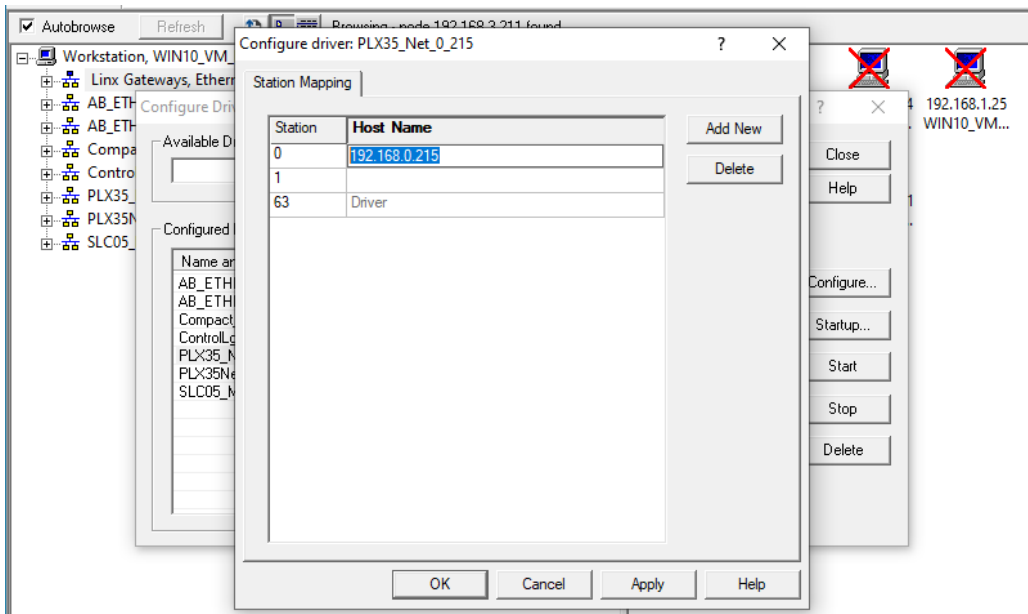
- 3 Click the **ADD NEW** button and select the **ETHERNET DEVICES** Driver Type.



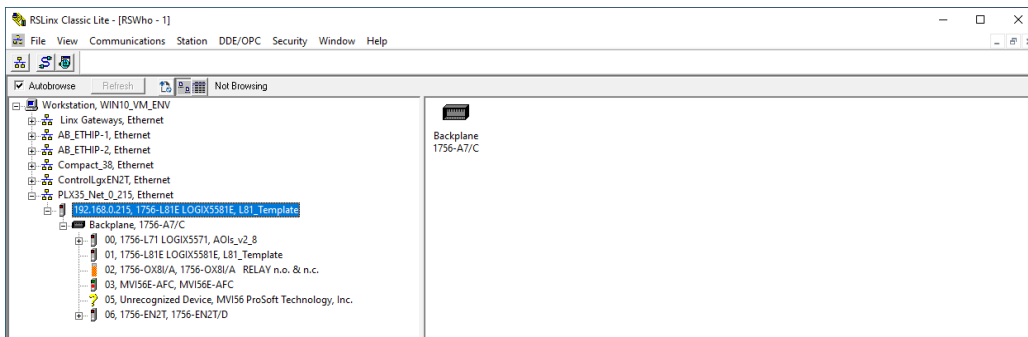
- 4 In the *Add New RSLinx Driver* dialog, assign a unique name.



- 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.

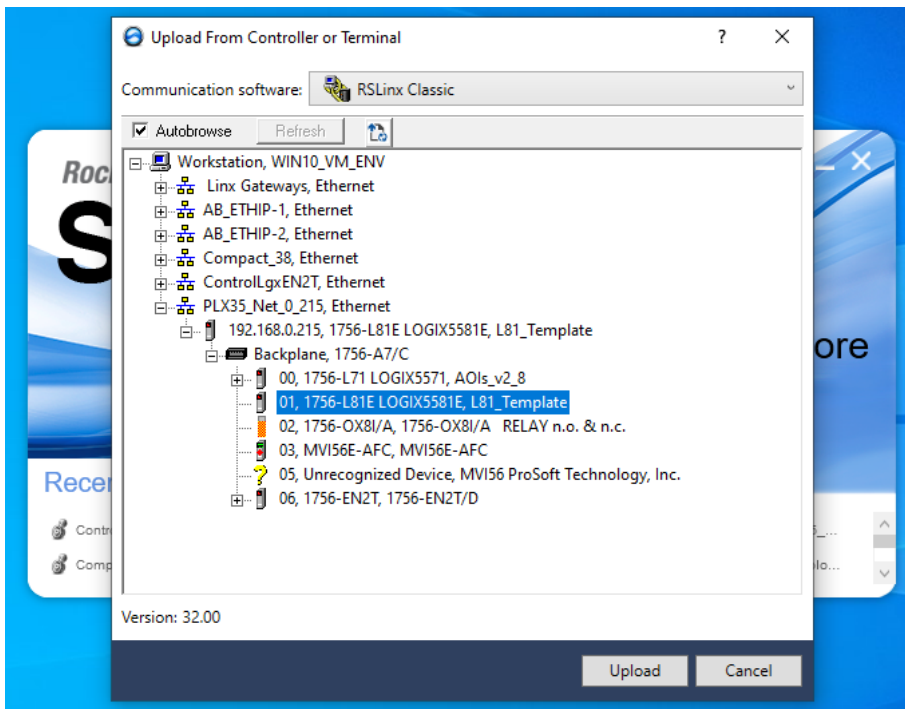


6.3 Uploading .ACD Project File

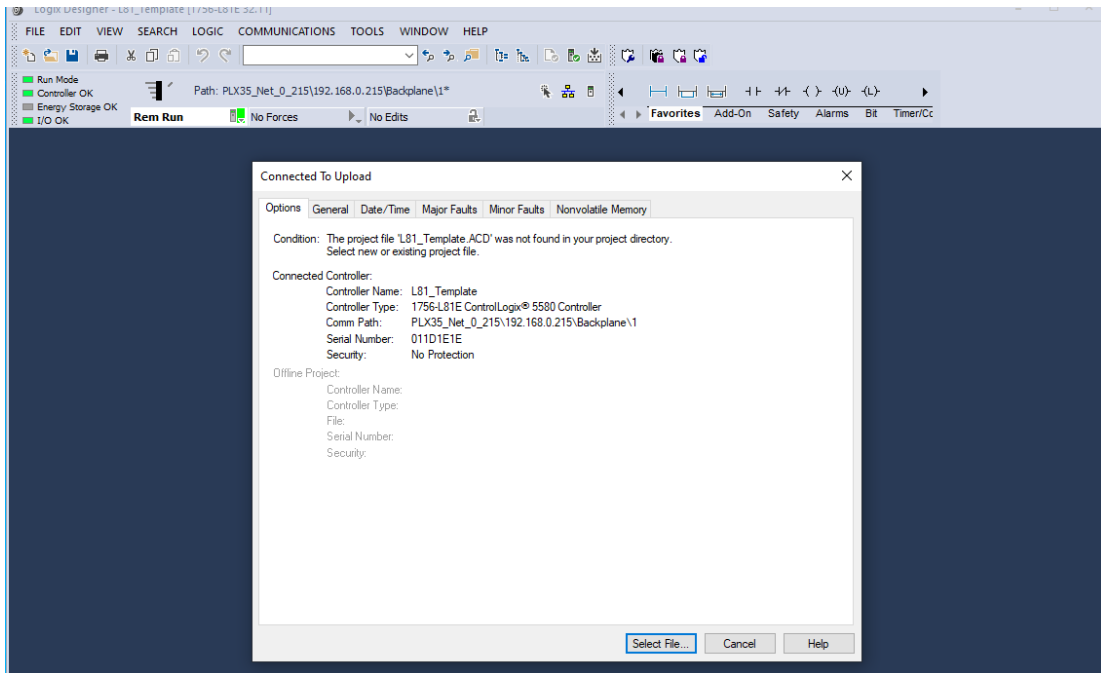
- 1 Open Studio/RSLogix 5000 and select the option to open **FROM UPLOAD**.



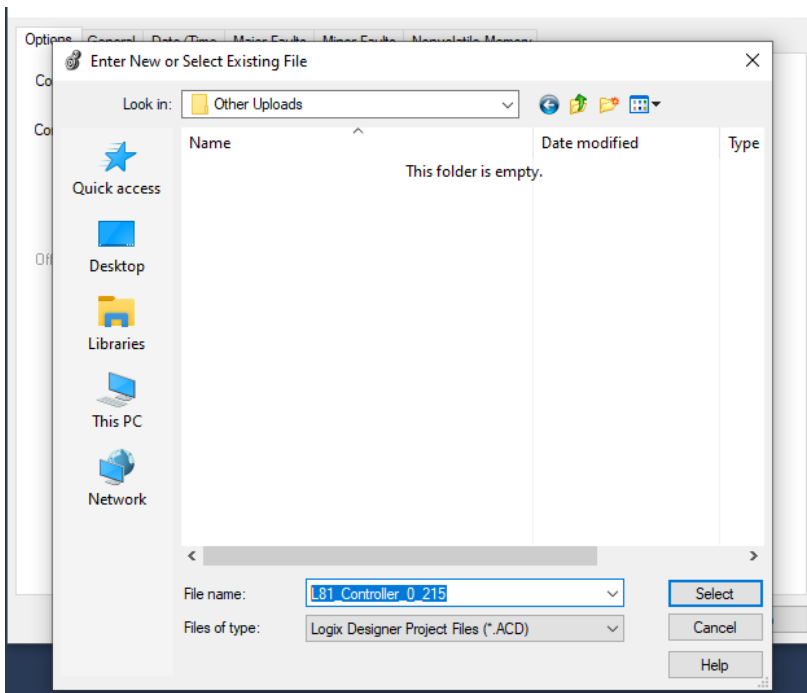
- 2 In the *Upload From Controller or Terminal* dialog, select the Controller to upload its .ACD project file from. Click the **UPLOAD** button.



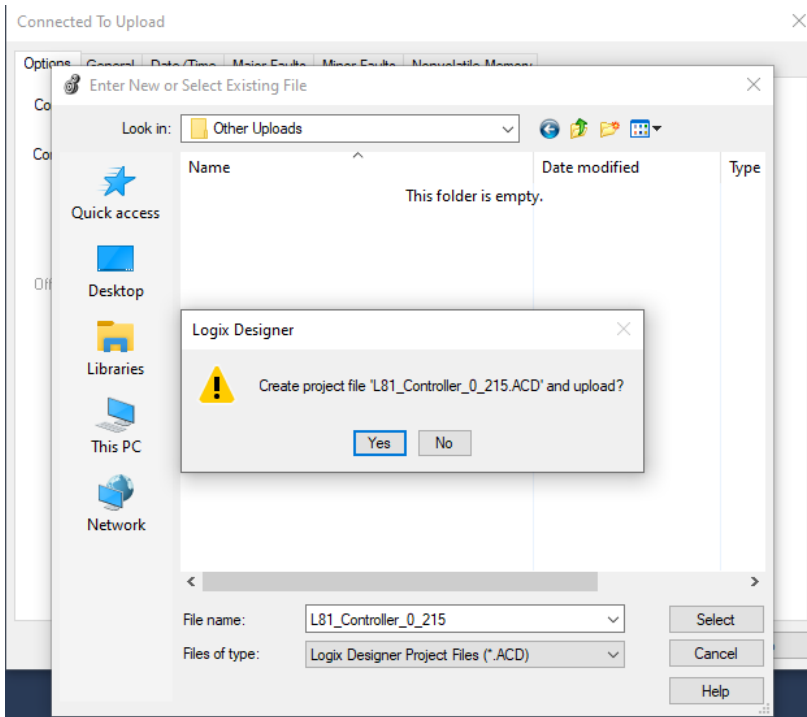
- 3 In the *Connected to Upload* dialog, click the **SELECT FILE...** button.



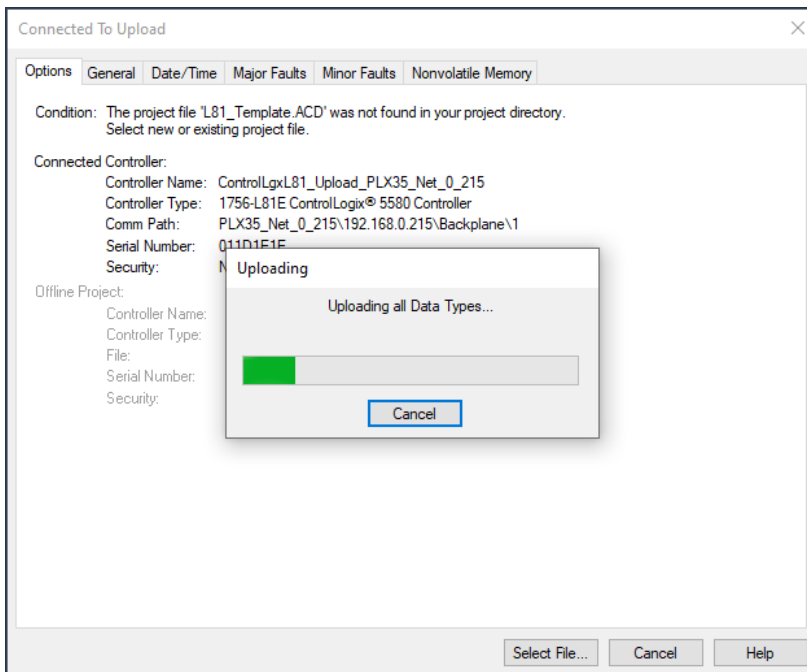
- 4 This opens the *Enter New or Select Existing File* dialog. Enter a new file name or select an existing .ACD file, then click the **SELECT** button.



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

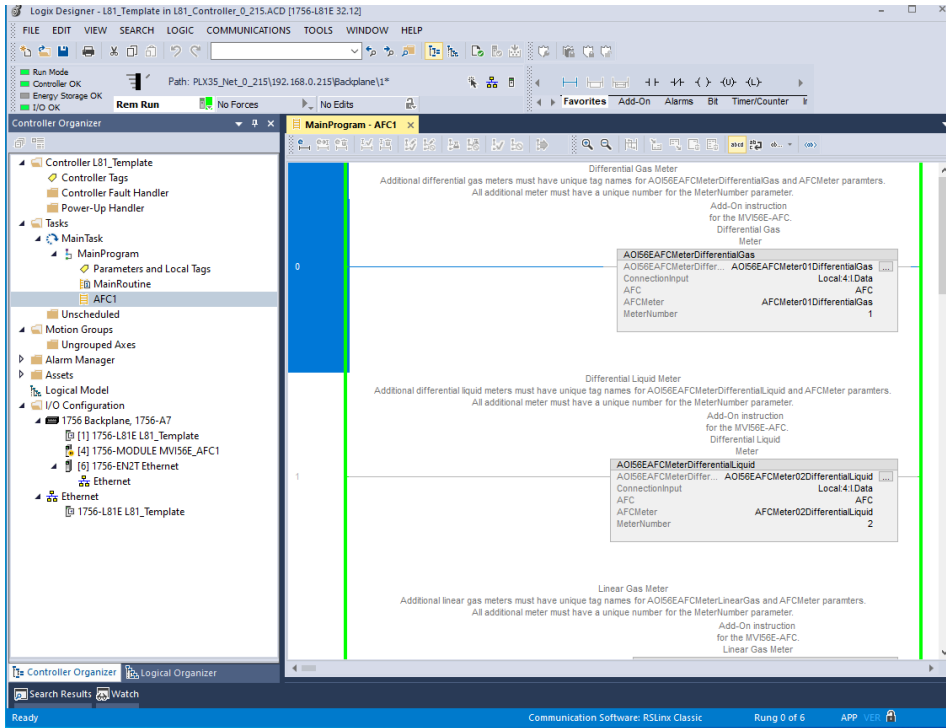


6 The upload process will initiate and complete.

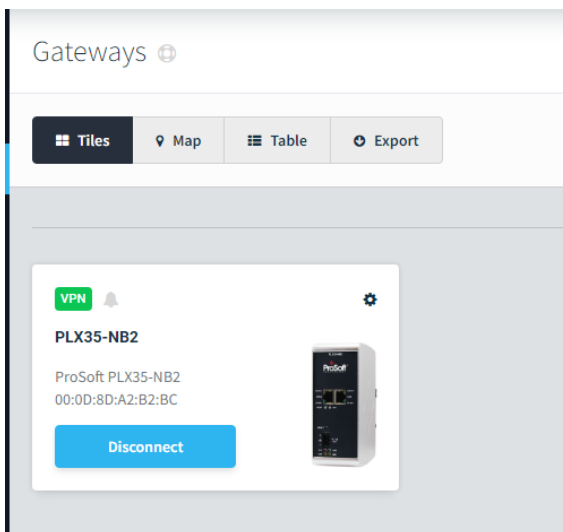


6.4 Ending the Tunnel Connection

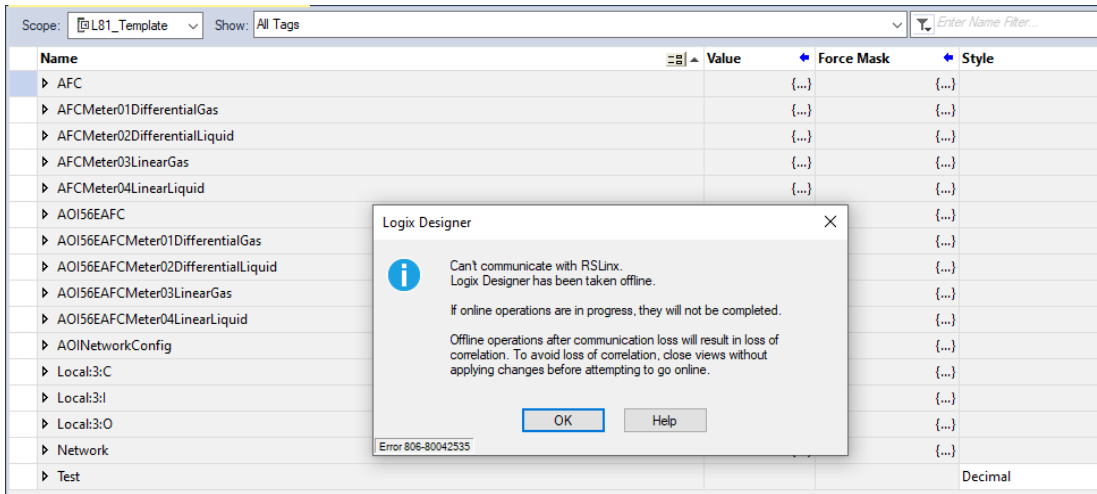
- 1 In Logix, connect to the Controller and set it to **Remote Run** mode to confirm the VPN Tunnel connectivity.



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



3 When the VPN tunnel connection terminates, the Controller displays a 'lost communications' message.



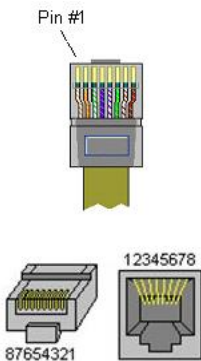
7 Ethernet Cable Specifications

ProSoft recommends using a category 5 (or better) Ethernet cable with the PLX35-NB2. A category 5 cable has four twisted pairs of wire that are color-coded and cannot be swapped. The gateway only uses two of the four pairs when running at 10 MBit or 100 MBit speeds.

The Ethernet port on the gateway automatically detects the network speed and cable type and use the appropriate pins to send and receive Ethernet signals. Use either a standard Ethernet straight-through cable or a crossover cable when connecting the gateway to an Ethernet hub, a 10/100/1000 Base-T Ethernet switch, or directly to a PC.

7.1 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-

8 Appendix

8.1 PLX35-NB2 Network Requirements

The following port and transport protocol specifications are utilized by the PLX35-NB2 LAN and WAN ports.

8.1.1 PLX35-NB2 LAN Port

Port	Transport Protocol	Purpose
80	TCP	HTTP
123	UDP	NTP
53	UDP	DNS
443	TCP	HTTPS

IP Addresses

0.0.0.0/0 (all)

8.1.2 PLX35-NB2 WAN Port

Port	Transport Protocol	Purpose
68	UDP	DHCP Renewal
53	TCP	DNS
53	UDP	DNS
443	TCP	Tunnel Connection
500	UDP	Tunnel Connection
4500	UDP	Tunnel Connection

IP Addresses

0.0.0.0/0 (all)

DNS Addresses

*.belden.io

*.prosoft.io

8.2 PDN & SRA Tunnel Server IP/DNS Addresses

The following are the IP and DNS addresses of the Persistent Data Network (PDN) and Secure Remote Access (SRA) tunnel end points. Ensure that the required endpoints are accessible to the PLX35-NB2 WAN port to successfully establish a VPN connection to the PLX35-NB2.

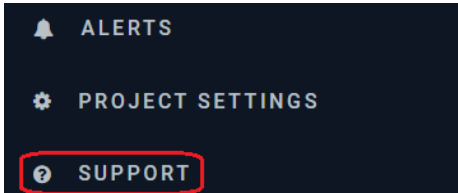
IP Address	SRA Tunnel Server	Region
54.148.164.142	us-west-tunnel-agent.prosoft.io	NA California / US West
18.192.94.16	eu-frankfurt-tunnel-agent.prosoft.io	EMEA/EU Frankfurt
54.169.94.228	apac-singapore-tunnel-agent.prosoft.io	APAC Singapore
52.65.129.24	apac-sydney-tunnel-agent.prosoft.io	APAC Sydney
13.127.196.149	apac-mumbai-tunnel-agent.prosoft.io	APAC Mumbai
18.178.158.9	apac-tokyo-tunnel-agent.prosoft.io	APAC Tokyo
177.71.185.249	sa-sao-paulo-tunnel-agent.prosoft.io	SA Sao Paolo
54.227.141.76	us-east-tunnel-agent.prosoft.io	US East
15.185.119.47	middle-east-tunnel-agent.prosoft.io	Middle East

IP Address	PDN Tunnel Server	Region
44.233.217.124	pdn-us-west-tunnel-agent.prosoft.io	NA California / US West
18.198.29.67	pdn-eu-frankfurt-tunnel-agent.prosoft.io	EU Frankfurt
18.139.132.236	pdn-apac-singapore-tunnel-agent.prosoft.io	APAC Singapore
54.153.176.80	pdn-apac-sydney-tunnel-agent.prosoft.io	APAC Sydney
15.206.59.157	pdn-apac-mumbai-tunnel-agent.prosoft.io	APAC Mumbai
3.115.215.189	pdn-apac-tokyo-tunnel-agent.prosoft.io	APAC Tokyo
34.196.232.179	pdn-us-east-tunnel-agent.prosoft.io	US East
157.175.22.109	pdn-middle-east-tunnel-agent.prosoft.io	Middle East

9 Support, Service & Warranty

9.1 Contacting Technical Support

With Belden Horizon, you can click on the **SUPPORT** link to initiate a chat with Support about issues in Belden Horizon, or gateways managed by Belden Horizon.



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 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) Phone: +1.661.716.5100 info@prosoft-technology.com Languages spoken: English, Spanish REGIONAL TECH SUPPORT support@prosoft-technology.com	Europe / Middle East / Africa Regional Office 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 Phone: +52.222.264.1814 latinam@prosoft-technology.com Languages spoken: Spanish, English REGIONAL TECH SUPPORT support.la@prosoft-technology.com	Asia Pacific Regional Office 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.

9.2 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.com/legal