Ranger Pro ISA100 Wireless Gateway

User Guide

Bently Nevada Machinery Condition Monitoring

158M1430 Rev. -

Bently Nevada
a Baker Hughes business

Baker Hughes

1631 Bently Parkway South, Minden, Nevada USA 89423
Phone: 1.775.782.3611 (US) or Bently.com/support
Bently.com

Contents

1. General Safety

1.1 Receiving Inspection

Visually inspect the device for obvious shipping damage. If you detect shipping damage, file a claim with the carrier and submit a copy to Bently Nevada. Include all model numbers and serial numbers with the claim.

1.2 Handling and Storing Considerations

To prolong the service life of the system, handle components carefully, use best practices during installation, and practice diligent inspection procedures. Follow prescribed maintenance procedures and dispose of obsolete components in compliance with applicable electronic waste regulations.

CAUTION

EQUIPMENT DAMAGE

Do not use a device with a damaged enclosure or Lithium battery. Using a damaged device may further damage the device, cause it to fail, or in hazardous locations cause other unintended consequences.

Devices

The Ranger Pro ISA100 Wireless Gateway is shipped in a foam-filled package and may be shipped with test data. **DO NOT DISCARD THIS TEST DATA!**

1.3 Personal Safety Warnings

Labels and markings are provided on the Data Hub to guide the system integrator in the processes of choosing appropriate interface equipment, determining safe use conditions, and identifying recommended installation procedures. The format of these markings are governed by the standards that dictate safe use and environmental compliance in a variety of regions and regulated settings.

Potential Interference

WARNING

Potential Interference

This equipment is compliant with Class A of CISPR 32 / EN 55032. In a residential environment this equipment may cause interference.

Antennas

WARNING

AUTHORIZED ANTENNAS ONLY

Do not use unauthorized antennas with this equipment. Only the specified antennas as outlined are permitted. Approval to operate the equipment is conditional upon use of authorized antennas and correct installation.

WARNING

PROFESSIONAL ANTENNA INSTALLATION ONLY

The equipment and antenna must be professionally installed in accordance with the requirements specified in this document. See the compliance section for a list of authorized antennas.

Potential Electrostatic Charging Hazard

WARNING

ELECTROSTATIC CHARGING HAZARD

RISK OF PERSONAL INJURY OR EQUIPMENT DAMAGE.

Potential for electrostatic charging hazard.

Do not separate when energized.

Remove power before service.

Connect grounding before power.

Installations and maintenance tasks performed in potentially hazardous areas must be performed only after the area has been verified to be free of hazardous materials, atmospheres, and conditions.

- Do not discharge static electricity onto the circuit board. Avoid tools or procedures that would subject the circuit board to static damage. Some possible causes of static damage include ungrounded soldering irons, non-conductive plastics, and similar materials.
- Use a suitable grounding strap before handling or performing maintenance on a printed circuit board.
- Transport and store circuit boards in electrically conductive bags or foil.
- Use extra caution during dry weather. Relative humidity less than 30% tends to multiply the accumulation of static charges on any surface.

The following situations could cause a spark sufficient to cause an explosion:

- Potential of electrostatic discharge on plastic components, or
- Removal or placement of an energized connection.

Hazardous Environment

WARNING

HAZARDOUS ENVIRONMENT

Risk of explosive atmosphere.

Avoid electrostatic potential, especially on plastic components. Adapters, isolation valves, or sealing rings that are not compatible with process gasses will corrode and fail. This failure may result in gas leaks, fire, explosion, or projectiles.

De-energize all devices before placement or removal. To prevent corrosion and failure, verify that all components are compatible. Verify that hazardous materials, atmospheres, and conditions have been removed or that relevant risk mitigation measures have been implemented.

Installations and maintenance tasks performed in potentially hazardous areas must be performed only after the area has been verified to be free of hazardous materials, atmospheres, and conditions.

The following situations could cause a spark enough to ignite an explosion:

- Potential of electrostatic discharge on plastic components, or
- Removal or placement of an energized connection.

WARNING

WARNING HAZARDOUS ENVIRONMENT

RISK OF EXPLOSIVE ATMOSPHERE

The power over ethernet function may not be utilized in a hazardous atmosphere. Only a suitable DC power supply may be utilized to power the equipment in a hazardous area.

WARNING

WARNING HAZARDOUS ENVIRONMENT

RISK OF EXPLOSIVE ATMOSPHERE

A static hazard may exist on the equipment as a result of the non-metallic coating. The equipment shall only be cleaned with a damp cloth when deployed in a hazardous area.

Hazardous Voltage

WARNING

HIGH ENERGY DISCHARGE HAZARD

RISK OF PERSONAL INJURY OR EQUIPMENT DAMAGE

Selection and installation of surge protectors as per these standards does not completely eliminate the possibility of personal injury or equipment damage due to lightning or similar surges, but it does sufficiently protect persons and equipment from the majority of these hazards.

1.4 Safe Disposal

Replacing Device and Failure Analysis

To return parts under warranty and request failure analysis, visit **Baker Hughes**.

Hazardous Materials

This device does not use hazardous materials outlined by RoHS or battery directive statutes. These regulations confirm that lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ether, and battery-related materials such as lithium are limited to no more than trace amounts within the system.

Recycling Facilities

Decommissioning of instrumentation should endeavor to minimize the impact of the waste created by disposal of system material. Refer to local or regional waste removal administration to collect information on proper material collection, reuse, and recycling.

Product Disposal Statement

Customers or third parties who are not member states of the European Union and who are in control of the product at the end of its life or at the end of its use, are solely responsible for diligent product disposal at the end of its useful life. No person, firm, corporation, association, or agency shall dispose of the product in a way that is in violation of any applicable international, federal, state, or local regulations. Visit www.weeerohsinfo.com for recycling information.

2. Overview

2.1 Description

Bently Nevada's Ranger Pro Gateway is a wireless network access device that is engineered for quick installation and setup to communicate with Ranger Pro ISA100 sensors. The Ranger Pro Gateway complies with the ISA100 international, industrial standard.

The Ranger Pro Gateway is an integrated RF access point and gateway that manages all aspects of ISA 100 network and provides the conversion between wireless and Ethernet networks. It hosts the relevant routing, system management, security management and gateway functions in a compact rugged enclosure suitable for outdoors and harsh environments with effortless deployment.

If a Ranger Pro Gateway cannot communicate with Ranger Pro ISA100 sensors that are out of range, you can use Ranger Pro ISA100 repeaters to extend your ISA100 network.

Ranger Pro 70M320 Gateway devices are intended for monitoring purposes only and should not be used in control or safety systems. The gateway is only intended for use with Bently Nevada Ranger Pro devices.

2.2 Compliance Information

This device complies with part 15 of the FCC Rules and contains license-exempt transmitter (s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to these conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

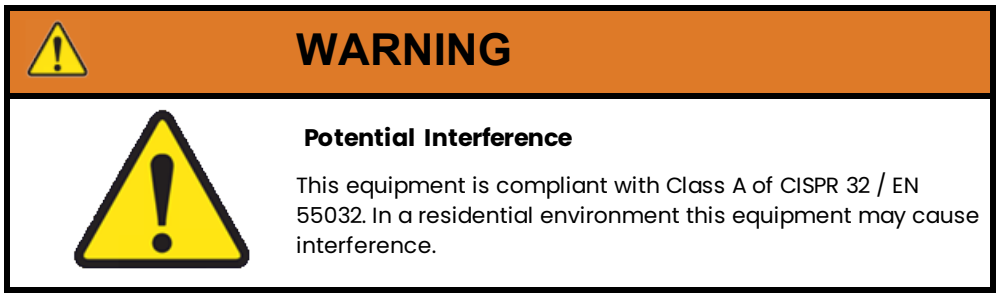
Changes or modifications not approved by the responsible party could void the user's authority to operate the equipment.

This radio transmitter (ISED: 8349A-154M74A) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Table 2 - 1: Ranger Pro Wireless Gateway Antennas

Antenna Part Number	Type and Gain (dBi)
147M0794	Omnidirectional 2dBi
147M0795	Omnidirectional 6dBi

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.



For complete compliance and hazardous location approval information, see the Ranger Pro Gateway Datasheet (157M8584) and Ranger Pro Gateway Warnings, Special Conditions and Additional Information (158M1429) available from Bently Nevada.

2.3 Informations de conformité

Cet appareil est conforme aux dispositions de la section 15 des règles de la FCC et contient des émetteurs / récepteurs exempts de licence conformes aux CNR d'Innovation, Sciences et Développement économique du Canada (ISDE Canada) applicables aux appareils radio exempts de licence.

- Cet appareil ne doit pas produire de brouillage, et
- Cet appareil doit tolérer tout type de brouillage subi, y compris ceux susceptibles de perturber le fonctionnement normal de l'appareil.

Les changements ou modifications non expressément approuvés par la partie responsable de la conformité pourrait annuler le droit accordé à l'utilisateur d'exploiter cet équipement.

Le présent émetteur radio (ISDE: 8349A-154M74A) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessus et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Pour obtenir des informations complementaires à propos de la conformité et de l'approbation de cet appareil en zone dangereuse, veuillez consultez Ranger Pro Gateway Datasheet (157M8584) et Ranger Pro Gateway Warnings, Special Conditions and Additional Information (158M1429) disponibles auprès du Bently Nevada.

3. Installation

3.1 Network Requirements

The following requirements apply to the PC/laptop used to configure the Gateway.

Ethernet:

- a Cat-5e (or higher) cable from any hub/switch capable of at least Ethernet 10/100 mbps

Compatible Web Browser applications:

We recommend using the most current version of the compatible web browser list below.

- Chrome
- Mozilla Firefox®
- Microsoft Edge

Microsoft® Internet Explorer® is not supported

These gateway ports need to be accessible from the host system through any network firewalls that may be in place:

- Port 80 (HTTP)
- Port 502 (MODBUS)
- Port 4901 (GCI)

All other ports are inaccessible on the gateway.

Setup Overview

To add Ranger Pro Gateways to your network:

1. Survey your installation location.
2. Decide where to install Ranger Pro Gateways and identify mounting points.
3. Install and configure Ranger Pro Gateways.
4. Provision Ranger Pro ISA100 field devices.
5. Test and verify your installation.
6. Monitor and maintain your network.

For more information regarding wireless network design, refer to the **Ranger Pro User Guide** (125M6113).

3.2 Deploy Gateway

Ranger Pro Gateways must be installed in accordance with relevant site standards and regulations.

- All hazardous location installations **must** be performed by a suitably qualified person.
- RF antenna installations and replacements must be completed by an authorized, qualified person.

WARNING

HAZARDOUS ENVIRONMENT

Risk of explosive atmosphere.

Avoid electrostatic potential, especially on plastic components. Adapters, isolation valves, or sealing rings that are not compatible with process gasses will corrode and fail. This failure may result in gas leaks, fire, explosion, or projectiles.

De-energize all devices before placement or removal. To prevent corrosion and failure, verify that all components are compatible. Verify that hazardous materials, atmospheres, and conditions have been removed or that relevant risk mitigation measures have been implemented.

The connectors to the equipment cannot be connected or disconnected when energized.

Ranger Pro Gateway Mounting

Mounting accessories allow for limited adjustments for either pole or surface mounted installations. For ease of installation, the gateway with attached mounting flanges can be mounted after the main bracket has been installed. Remember to provide enough clearance around the main bracket to allow for the gateway to be attached and cables connected.

Pole Mounting

Mount Ranger Pro Gateways to either a vertical or horizontal pole using the supplied mounting accessories. The mounting main bracket is attached to the pole using the supplied mounting support bracket and the two M8x120 fasteners and washers as shown in the following figure.

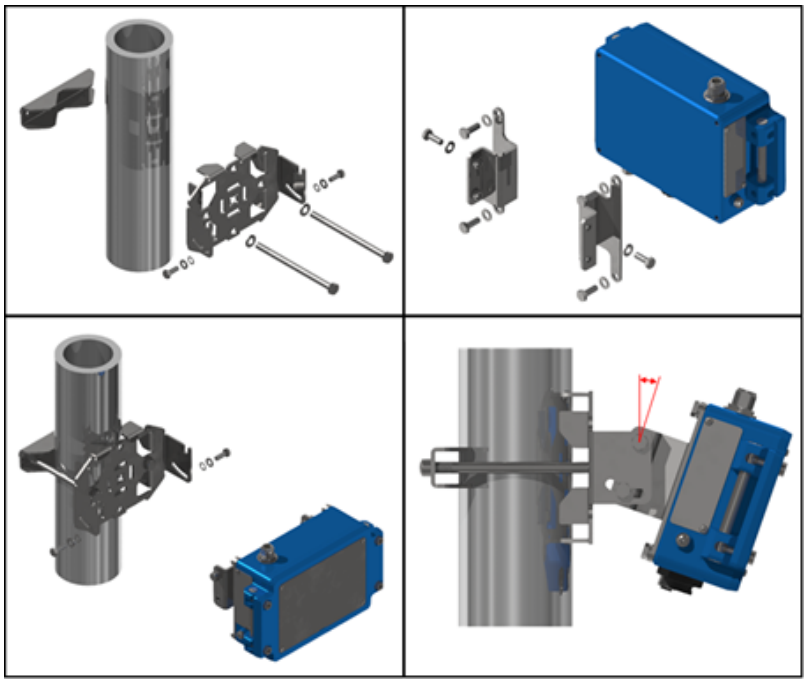


Figure 3 - 1: Pole mounting

Surface Mounting

For surface mounting, the customer can use an M8 or 5/16" fastener and washer (not supplied) with a minimum length of > 36 mm depending on the surface (see figure above). Ensure that the mounting surface is able to support the weight of the gateway as well as any additional strain applied by the cables connected to the gateway.

Ranger Pro Gateways can also be mounted directly into instrument panels or enclosures using the supplied mounting accessories.

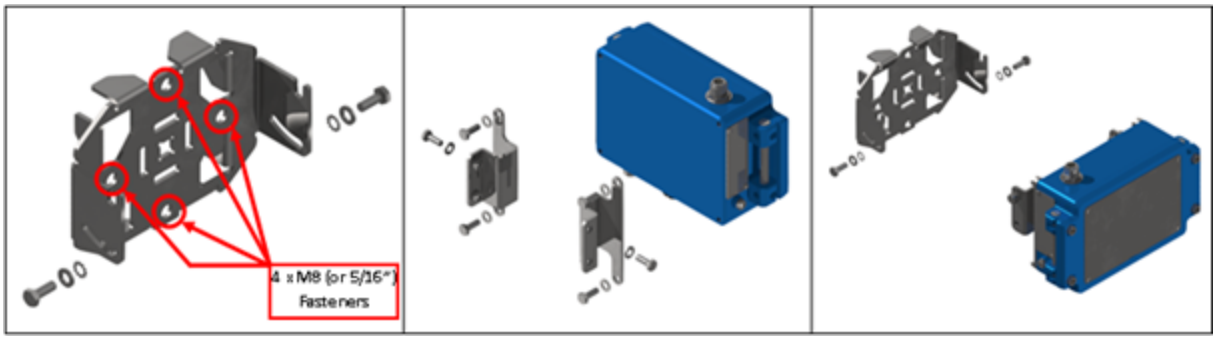


Figure 3 - 2: Surface mounting

Outdoor Mounting

When installing outdoors, the gateway should be mounted upright, and the supplied connector guard must be installed to protect against UV exposure as shown in Figure 4.

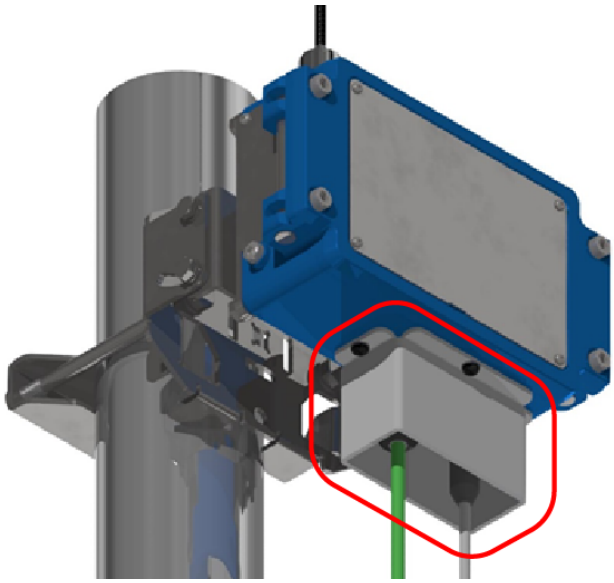


Figure 3 - 3: Connector guard installed for protection against UV exposure

Ground Connection

Ranger Pro Gateways must be grounded using a suitably gauged grounding wire connected to the grounding lug attachment point on the enclosure.

Surge Protection

The following information is intended only as guidelines and does not replace the need for surge protection assessment and installation by a suitably qualified person. General guidelines for surge arrester selection and application principles are given in standards such as:

- **IEC 61643-12:** Low-voltage surge protective devices - Part 12: Surge protective devices connected to low-voltage power systems - Selection and application principles.
- **IEC 61643-22:** Low-Voltage Surge Protective Devices - Part 22: Surge Protective Devices Connected To Telecommunications And Signalling Networks - Selection And Application Principles.

Refer to your site-specific requirements for selection and installation of surge arresters.

WARNING

HIGH ENERGY DISCHARGE HAZARD

RISK OF PERSONAL INJURY OR EQUIPMENT DAMAGE

Selection and installation of surge protectors as per these standards does not completely eliminate the possibility of personal injury or equipment damage due to lightning or similar surges, but it does sufficiently protect persons and equipment from the majority of these hazards.

Cabling and equipment are susceptible to induced surges from lightning as well as power generation equipment. The risk related to each source is different based on installation location.

The purpose of a surge arrester is to protect persons and equipment from electrical surges induced by lightning, static discharge, or other high-voltage electrical faults.

Surge arresters must be appropriately grounded using dedicated conductors connected directly to earth ground instead of locally available grounding points as these could be at a higher potential than a direct earth connection.

Indoor Connection

When equipment and cabling is installed within an enclosed environment, the risk related to lightning is less since enclosures such as buildings would typically have lightning protection features incorporated by design. However, there are still risks to persons and equipment from sources of surges within the enclosed environment. Where surges over 1 kV can occur, additional surge suppressors should be installed on the relevant equipment ports to protect from supply-side surges.

Partial Indoor / Outdoor Installation

The same consideration for supply-side surges as in indoor installation are relevant when the equipment is installed within a lightning-protected, enclosed environment and cabling to associated equipment extends into an area with no direct lightning risk.

Lightning-induced EMP can result in very high current and voltage levels in the system. Where cabling and associated equipment may be exposed to lightning induced EMP, appropriate surge arresters should be selected and installed at the point where the cabling or associated equipment enters the protected environment.

Outdoor Installation

When equipment is installed in an area outside of a lightning-protected, enclosed environment with no direct lightning risk, appropriate surge arresters should be selected and installed between the equipment and further connected equipment within the protected area and between the equipment and any associated equipment outside of the protected area.

WARNING

AUTHORIZED ANTENNAS ONLY

Do not use unauthorized antennas with this equipment. Only the specified antennas as outlined are permitted. Approval to operate the equipment is conditional upon use of authorized antennas and correct installation.

Antenna Installation

WARNING

PROFESSIONAL ANTENNA INSTALLATION ONLY

The equipment and antenna must be professionally installed in accordance with the requirements specified in this document. See the compliance section for a list of authorized antennas.

When the equipment is mounted outdoors it must be fixed and mounted on outdoor permanent structures and the antennas must not be co-located with any other antenna or transmitter device and have a separation distance of at least 20 cm from all persons.

Depending on the type used, antennae can be connected directly to Ranger Pro Gateways or can be mounted remotely. Remote antennae can be connected to Ranger Pro Gateways using the optionally supplied antenna cables. If the antenna or equipment is mounted outside, a surge arrester or multiple surge arresters should be used as appropriate and according to local regulations.

Self-amalgamating tape must be used to seal the connections between gateways, surge arresters, and antennae.

Plant Network Connection

Ranger Pro Gateways can be connected to the plant network using an appropriate ethernet cable with the supplied RJ45 cable connector housing or the optional accessory cable supplied by Bently Nevada. The gateway can be connected to a PoE switch, PoE adapter, or standard network switch. When connecting to a standard switch, the device must be powered from an external power supply.

The RJ45 Ethernet connection uses industry standard wiring connections. Either a standard or cross-over cable may be used when connecting the device.

You must use only compliant (IEEE 802.3at Type 1) power supply equipment that support Mode B (or midspan) and injects power on the Ethernet cable spare wire pairs and not on the data wire pairs.

When installing the gateway outdoors, you need to provide adequate UV protection for the network cable connector. This can be done using a suitable enclosure or by mounting the gateway upright and using the optional network and power cable connection guard.

Power Connection

When connected to a standard Ethernet connection, Ranger Pro Gateways require an external power supply connection using the supplied A-coded M12 field-wireable connector or optional M12 power-cable accesory.

WARNING

WARNING HAZARDOUS ENVIRONMENT

RISK OF EXPLOSIVE ATMOSPHERE

The power over ethernet function may not be utilized in a hazardous atmosphere. Only a suitable DC power supply may be utilized to power the equipment in a hazardous area.

The power connection also serves as an optional secondary power supply connection when using a PoE plant network connection. If needed, use the supplied A-coded M12 field-wireable or optional M12 power cable accessory to connect to an external power supply to establish a redundant power-supply connection.

A secondary power supply allows for continued operation. Switching between power supplies causes the gateway to reboot and results in temporary loss of wireless connectivity.

The A-coded M12 connection uses these wiring connections.

Table 3 - 1: Power and Reset Connector Wire Color Guide

M12 Pin	Wire Colour	Description
1	Brown	IO – Reset 1
2	White	V+ (20-57 Vdc, 4 W)
3	Blue	IO – Reset 2
4	Black	V-

The power cable and connector can be used as an alternative to the magnetic interface to reset the gateway TCP/IP IPv4 address or restore the gateway to factory default settings.

Using an appropriate tool, the M12 power connector must be tightened to a torque of 0.6 Nm.

4. Configuration

4.1 User Interface

The Ranger Pro Gateway provides a web-based user interface to configure and monitor all devices connected to a network. To start managing the wireless field device network, you first need to configure the gateway.

In addition, the user interface performs the following tasks.

- Network maintenance
- Device configuration and maintenance
- Operator activities

Login

You must login to access the gateway functions.

Network

Selecting the Network section displays a device tree, tab control, and property list.

The device tree displays the System Manager, Access Point, and Ranger Pro Field Devices (Sensors and Repeaters).

Depending on the tree entry selected, the tab control and property list displays different information.

System Manager

When the System Manger is selected, the tab control displays the Network Health, GCI Stats, Signal Strength and Event History. The property list displays the Provision, Logging, and Operational Settings.

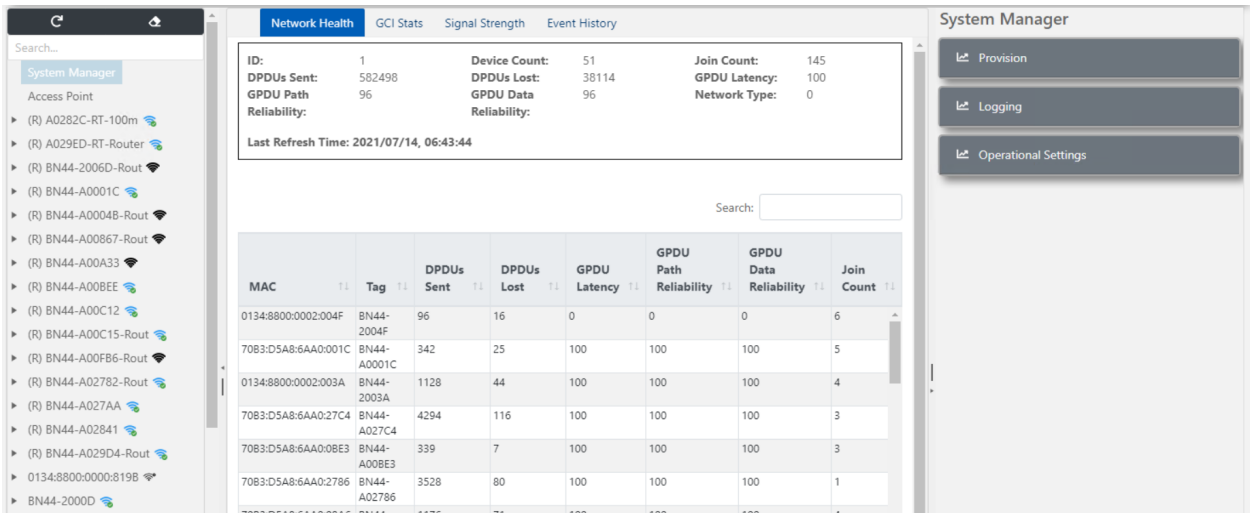


Figure 4 - 1: System Manager

Network Health

The Network Health tab displays joined Routers, Router + IOs, and IO devices packet transmitted and lost, reliability of its published process values, and the join count of each device.

GCI Stats

The GCI Stats tab displays external GCI client connections, their respective start times, data transmitted and received, and number of leases used. GCI client connections are limited to 2 concurrent connections.

Signal Strength

The Signal Strength tab displays all Level one Routers, RouterIOs, and IO devices, as well as their respective transmitted and received success and fail count. The respective signal strength and quality are also displayed.

Event History

The Event History tab displays a log of internal events, such as gateway restarts, logins, firmware updates, and other general events.

Provision

The Provision settings allow configuration of the Network ID, Join Key, local area network (LAN) settings, and the Tag for the Ranger Pro Gateway device.

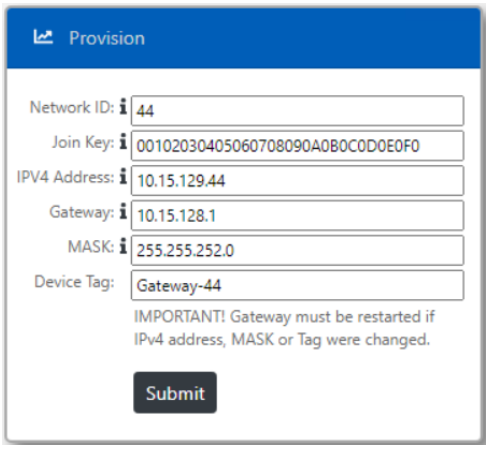


Figure 4 - 2: Provision Settings

Logging

The Logging settings change the System Manager level of detail which is recorded in logs for debugging purposes.

Operational Settings

The Operational Settings contain channel enabling/disabling and the configuration of the number of router and IO nodes allowed to join the 1st layer of the mesh (i.e. the 1st hop from the access point). The number of Routers and IOs allowed to connect to routers in further hop layers is also configurable. The maximum number of layers (hops) is also configurable. More routers result in higher consumption. The recommended maximum number of routers is no more than 30% of all field devices.

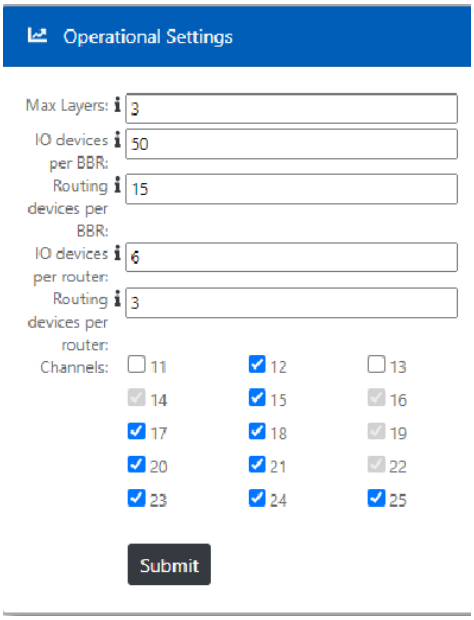


Figure 4 - 3: Operational Settings

Table 4 - 1: Operational Settings Inputs

Setting	Description	Default Value
Maximum Layers	The number of routing layers between the Back Bone Router (BBR) and the last child device in the network chain after network optimization	3
IO devices per BBR	The maximum number of IO-only devices that can connect directly to the BBR	50
Routing Devices per BBR	The maximum number of routing enabled devices (including IO routers) that can connect directly to the BBR. We recommend not exceeding 20 routers per 50 devices.	15
IO devices per router	The maximum number of IO only devices that can connect directly to the parent router	6
Routing devices per router	The maximum number of routing enabled devices (including IO routers) that can connect directly to the parent router	3
Channels	The communication channels used by the network Channels 14, 19, and 22 are set. Channels 11 and 13 are optional. Remaining channels can be de-selected as required.	

Access Point

When the Access Point is selected, the tab control displays the Network Health, GCI Stats, Signal Strength, and Event History. The property list displays the Logging and General Settings.

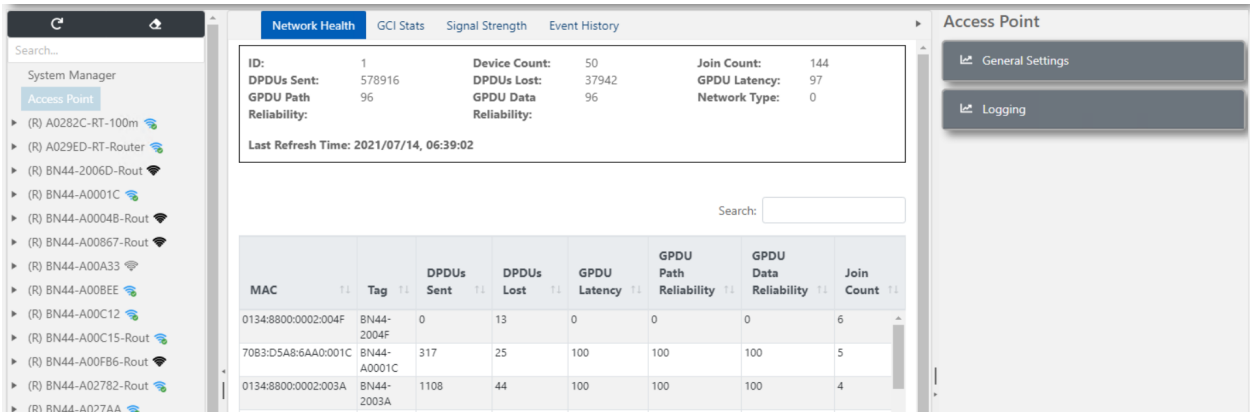


Figure 4 - 4: Access Point Property Panel Display (right)

Network Health

The Network Health tab displays joined Routers, Router + IOs, and IO data packets transmitted and lost, reliability of its published process values, and the join count of each device.

GCI Stats

The GCI Stats tab displays external GCI client connections, their respective start times, data transmitted and received, and number of leases used. GCI client connections are limited to 2 concurrent connections.

Signal Strength

The Signal Strength tab displays all Level one Routers, RouterIOs, and IO devices, as well as their respective transmitted and received success and fail count. The respective signal strength and quality is also displayed.

Event History

The Event History tab displays a log of internal events, such as gateway restarts, logins, firmware updates, and other general events.

General Settings

The General Settings show read-only details of the access point (shown below as gray fields with green outlines). The user can name the BBR tag as desired. The user must select the **Submit** button to rename the BBR Tag.

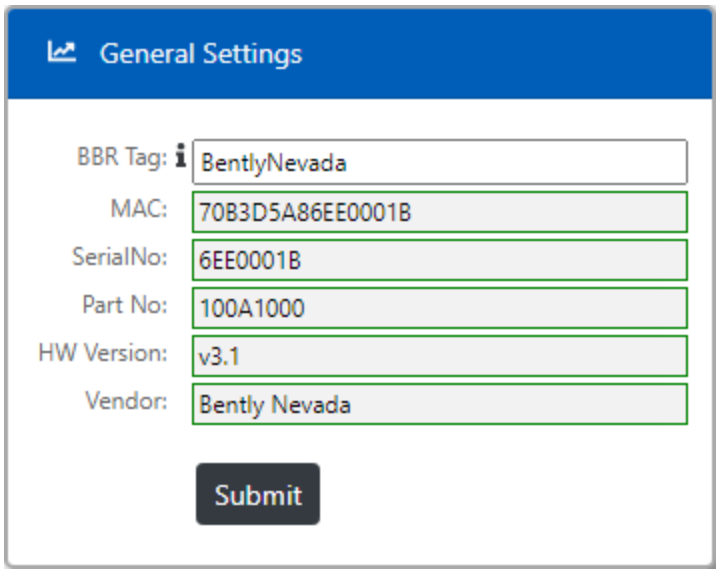


Figure 4 - 5: Access Point

Logging

The Logging settings change the access-point level of detail which is recorded in logs for debugging purposes.

Field Device

When a field device is selected, the tab control displays the data Trend, Device Join History, Readings, and Signal Strength. The property list displays the Device Information, Device Restart and Device Role settings.

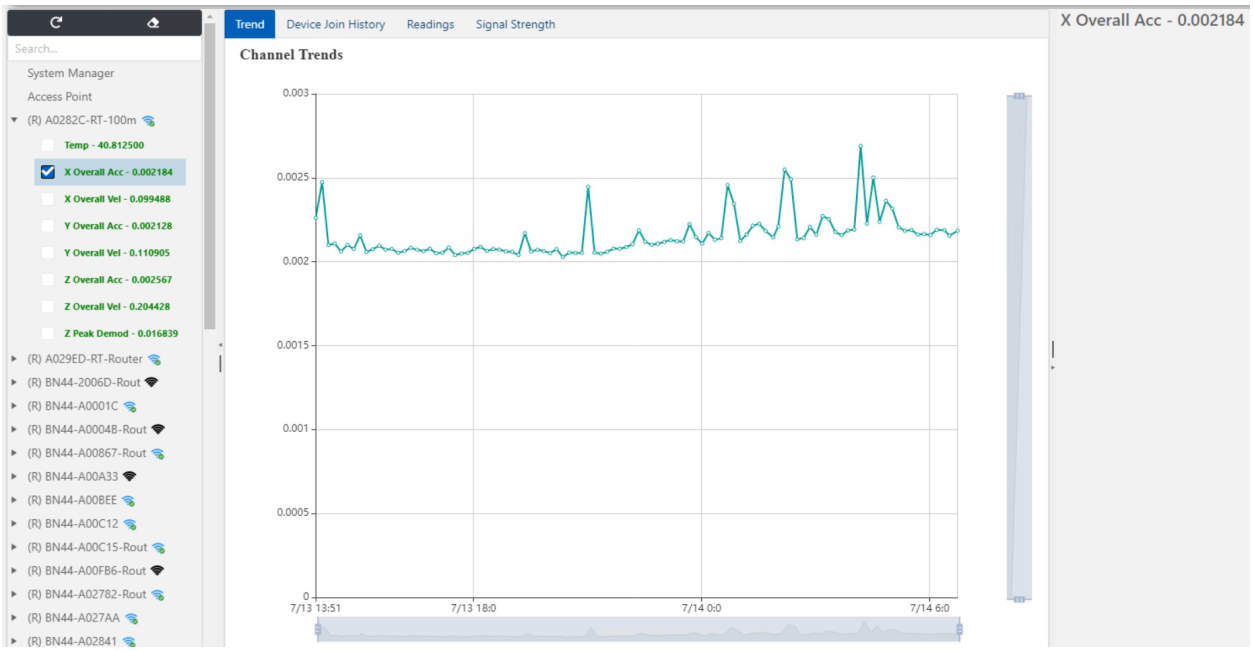


Figure 4 - 6: Trend Plot Example

Trend

The Trend tab is visible once a field device is selected and displays a plot of selected channels automatically scaled to the smallest and largest values.

Device Join History

The Device Join History tab display the join states and times of highlighted units.

Readings

The Readings tab displays process value data for each channel in a historical table format.

Signal Strength

The Signal Strength tab displays all connected children and parents of a router or just the parent of an IO.

Device Information

The Device Information settings show the device model, manufacturer, serial number, battery level, both radio and application firmware versions and address of the highlighted Ranger Pro field device. The Device Tag name can also be set here.

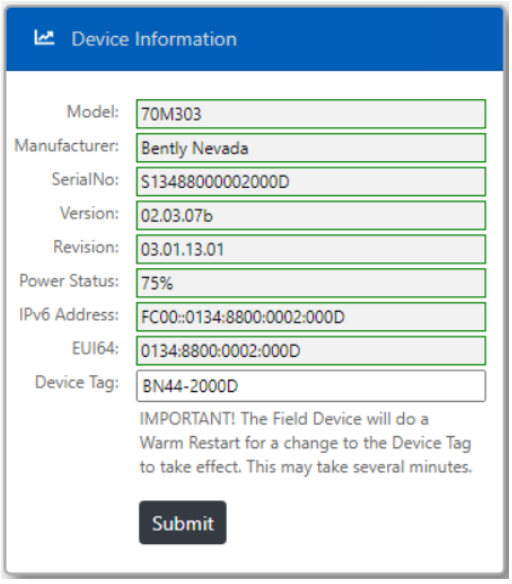


Figure 4 - 7: Device Information Panel

Device Restart

The Device Restart settings allow a Ranger Pro field device radio (soft restart) or application processor (restart as provisioned) to be rebooted from the User Interface.

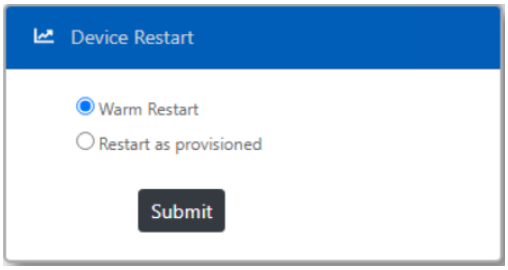


Figure 4 - 8: Device Restart Panel

Device Role

The Device Role settings allow a Ranger Pro ISA100 field device to be configured to join as a router, router + IO, or IO device.

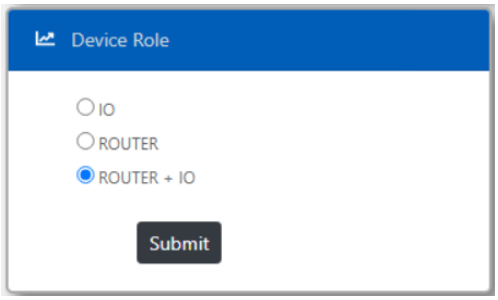


Figure 4 - 9: Device Role Panel

Firmware

When the Firmware section is selected, a tab control displays the Firmware, Devices to Upgrade, Queue, and Progress information.

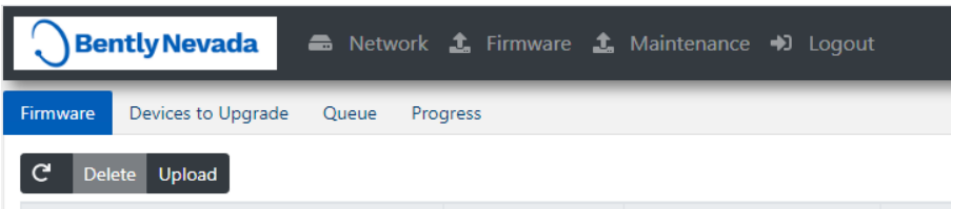


Figure 4 - 10: Firmware Tab

The Firmware tab is used to upload two different kinds of firmware for Over the Air (OTA) upgrading of Ranger Pro field device radios and application processors.

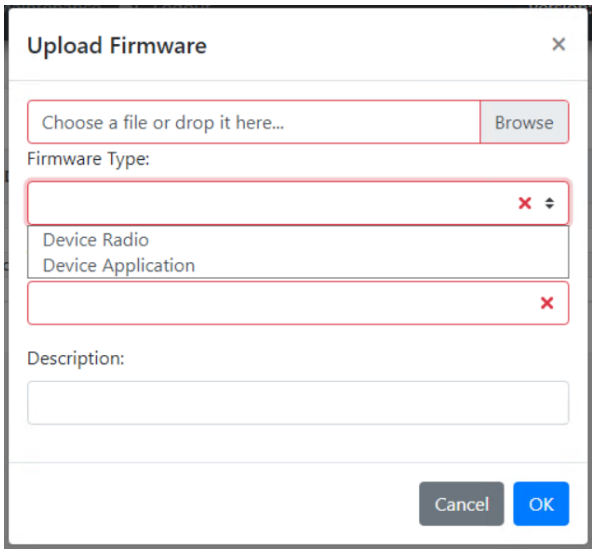
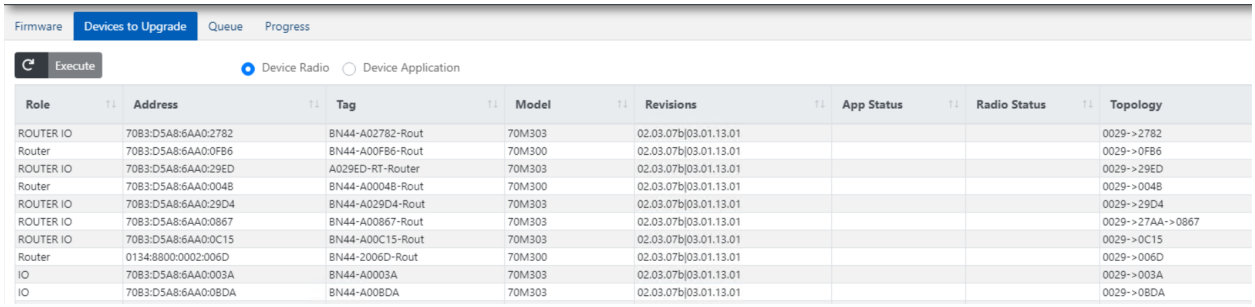


Figure 4 - 11: Firmware Upload Tab Pop Up

Devices to Upgrade

The Devices to Upgrade tab is used to initiate uploads to selected field devices.



Role	Address	Tag	Model	Revisions	App Status	Radio Status	Topology
ROUTER IO	70B3:D5A8:6AA0:2782	BN44-A02782-Rout	70M303	02.03.07b|03.01.13.01			0029->2782
Router	70B3:D5A8:6AA0:0FB6	BN44-A00FB6-Rout	70M300	02.03.07b|03.01.13.01			0029->0FB6
ROUTER IO	70B3:D5A8:6AA0:29ED	A029ED-RT-Router	70M303	02.03.07b|03.01.13.01			0029->29ED
Router	70B3:D5A8:6AA0:004B	BN44-A0004B-Rout	70M300	02.03.07b|03.01.13.01			0029->004B
ROUTER IO	70B3:D5A8:6AA0:29D4	BN44-A029D4-Rout	70M303	02.03.07b|03.01.13.01			0029->29D4
ROUTER IO	70B3:D5A8:6AA0:0867	BN44-A00867-Rout	70M303	02.03.07b|03.01.13.01			0029->27AA->0867
ROUTER IO	70B3:D5A8:6AA0:0C15	BN44-A00C15-Rout	70M303	02.03.07b|03.01.13.01			0029->0C15
Router	0134:8800:0002:006D	BN44-2006D-Rout	70M300	02.03.07b|03.01.13.01			0029->006D
IO	70B3:D5A8:6AA0:003A	BN44-A0003A	70M303	02.03.07b|03.01.13.01			0029->003A
IO	70B3:D5A8:6AA0:0BDA	BN44-A00BDA	70M303	02.03.07b|03.01.13.01			0029->0BDA

Figure 4 - 12: Devices to Upgrade Tab

Progress

The Progress tab is used to observe overall progression levels of upgrades.

Maintenance

When the Maintenance section is selected, a tab control displays the Export Logs, Save/Restore, Set Time, Software Upgrading, Modbus, Change Password, and Restart functions.

Export Logs

Use the Export Logs tab to archive and encrypt logs for debugging of problems when requested by support technicians. This takes a couple of minutes to complete.

Save / Restore

Save / Restore allows the backing up or restoration of the configuration of the device.

Set Time

The Set Time function allows the Ranger Pro Gateway time to be set manually or to the host time and date in the relevant UTC zone.

By setting the time to the host time and date, the time is adjusted to the host time without the UTC offset.

For example, if the host indicates a time of 14:30 (UTC+8), the gateway time will be set to 06:30 (UTC). The time must be manually adjusted to include the UTC offset for the gateway to reflect the host time.

We recommend using UTC time. When setting the time to include the UTC offset, ensure that all related system times are adjusted to reflect the same UTC offset.

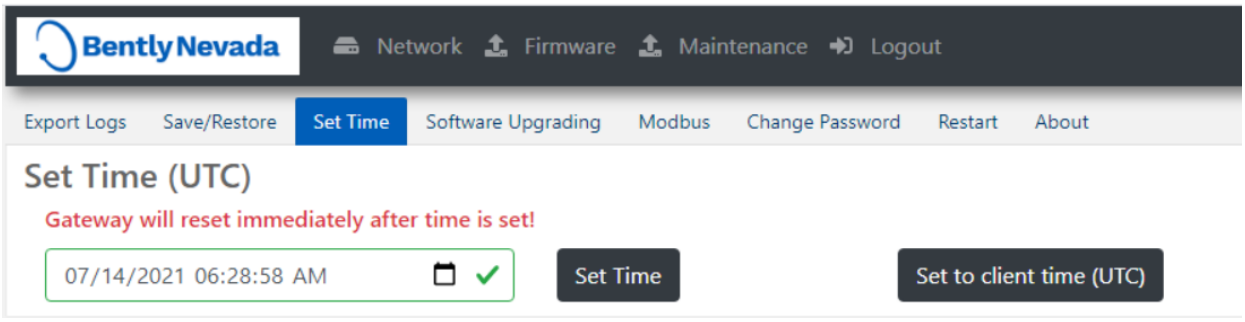


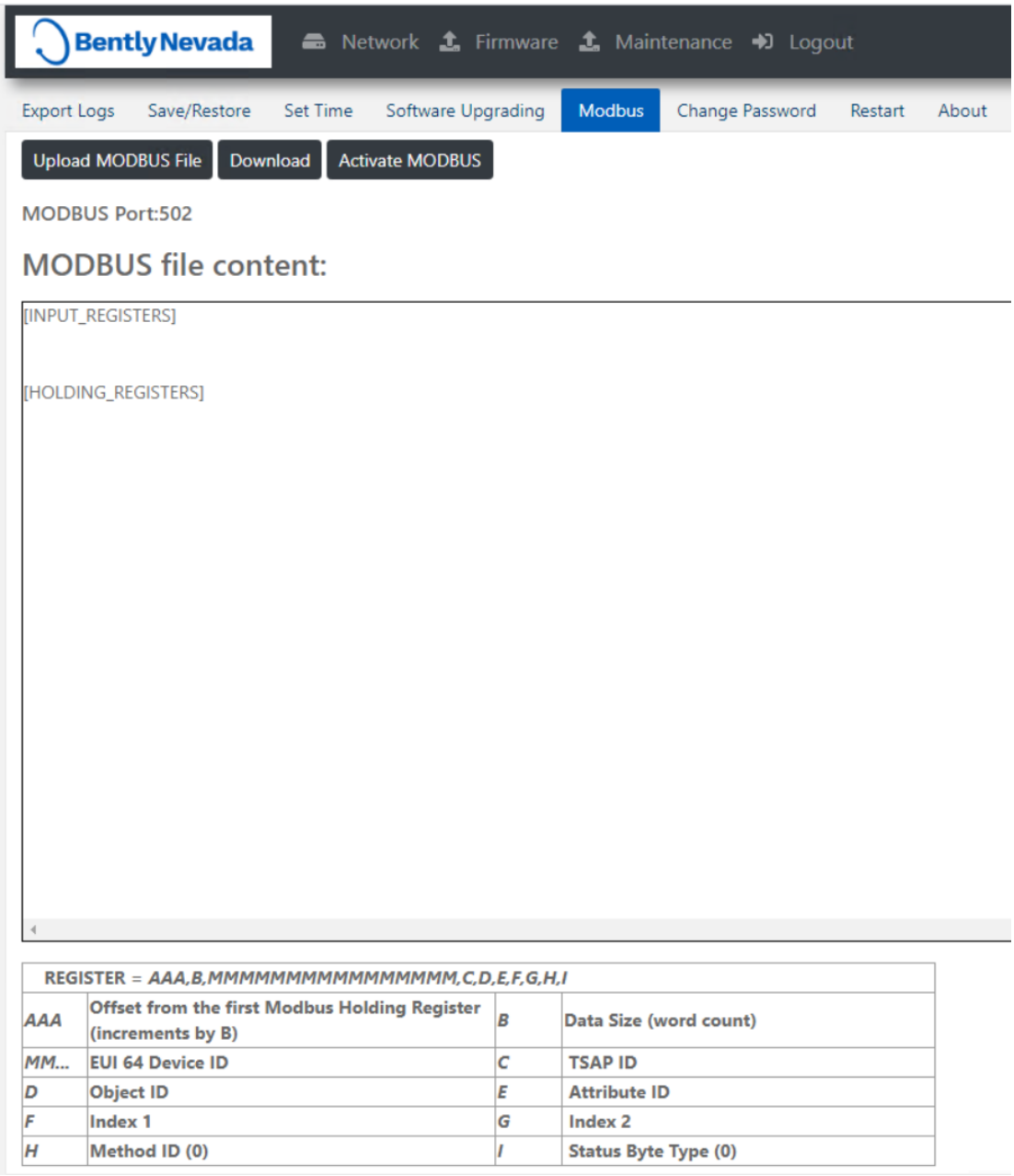
Figure 4 - 13: Set Time Tab

Software Upgrading

Software Upgrading allows the selection of a software file to upgrade the gateway. On selection, a dialog box will appear to allow selection of the software file. On submit, the file will be checked and a confirmation dialog box will appear.

Modbus Settings

The Modbus tab allows process values to be published using the MODBUS protocol on port 502.



REGISTER = *AAA,B,MMMMMMMMMMMMMMMM,C,D,E,F,G,H,I*			
AAA	Offset from the first Modbus Holding Register (increments by B)	*B*	Data Size (word count)
MM...	EUI 64 Device ID	*C*	TSAP ID
D	Object ID	*E*	Attribute ID
F	Index 1	*G*	Index 2
H	Method ID (0)	*I*	Status Byte Type (0)

Figure 4 - 14: Modbus Tab

To use the Modbus TCP protocol to output sensor static data:

1. Modify the Ranger Pro Gateway Modbus settings:
   a. Create a new Modbus configuration file to upload the file to the gateway using a text editor.
   b. Save the file to be uploaded as **`modbus_gw.ini`**.

c. Edit the file:

```
[INPUT_REGISTERS]
 [HOLDING_REGISTERS]
 REGISTER = 200,2,0134880000010041,2,3,1,0,0,0,0
 REGISTER = 202,2,0134880000010041,2,4,1,0,0,0,0
 REGISTER = 204,2,0134880000010041,2,5,1,0,0,0,0
REGISTER = ….
```

Where REGISTER = AAA,B,MMMMMMMMMMMMMMMM,C,D,E,F,G,H,I :

a. Navigate to the **Maintenance** section and select the **Modbus** tab.
b. Select **Upload Modbus File** and browse to the relevant Modbus configuration file.
c. Click on **OK** to upload the file.
d. After the upload is complete, click on **Activate Modbus** to apply the configuration.

For more details about TSAP ID, Object ID, Attribute ID, Index 1, and Index 2 values, see the following table or Ranger Pro User Guide.

e. The current Modbus configuration file can be downloaded by clicking on **Download**.

Table 4 - 2: Modbus Definitions and Settings

Location	Description	Setting
AAA	Offset from the first Modbus Holding Register (increments by B)	Modbus initial register address is 200
B	Data Size (word count)	Reserved (2)
MM...	EUI 64 Device ID	
C	TSAP ID	TSAP is the device application processor object ID for accessing process values. TSAP (2) is the only supported application object.
D	Object ID	Object ID refers to internal AIO objects. ◦ **3**: temperature ◦ **4**: Z acceleration ◦ **5**: Z velocity ◦ **6**: peakdemod ◦ **7**: Y accleration

Location	Description	Setting
		◦ **8**: Y velocity ◦ **9**: X acceleration ◦ **10**: X velocity
E	Attribute ID	Attribute ID referes to the AIO attributes. Attribute ID (1) is the Process Variable (PV) and the only value supported.
F	Index 1	Reserved (0)
G	Index 2	Reserved (0)
H	Method ID	Reserved (0)
I	Status Byte Type	Status byte (0).

Change Password

The Change Password function allows the user to change the Ranger Pro Gateway password.

Currently the Ranger Pro Gateway only supports one user (the admin user) with access to all operations on the Ranger Pro Gateway.

Restart

The soft restart allows a software restart to be initiated on the gateway. It is a faster option for reinitialization of the gateway. The Power Cycle option will reinitialize the hardware of the gateway and will reliably restore the device to a well-initialized state.

Logout

Once a user has completed any configuration or validation of the network using the Ranger Pro Gateway, they should use the Logout function to prevent unauthorized changes to the system.

4.2 Configure Gateways

We recommend performing basic configuration of Ranger Pro Gateway in an indoor equipment room or a similar environment before installation in the field.

This includes:

- Device web interface password (recommended; default username = **admin**; default password = **Admin#1!**)
- TCP/IP IPv4 Address (default = **192.168.1.1**)
- ISA100 wireless Network ID (default = **5**)
- ISA100 wireless network Join Key (default = **00102030405060708090A0B0C0D0E0F0**)
- Device Tag (optional; default = **Gateway**)

To configure these settings:

1. Use a PoE cable to connect the Ranger Pro Gateway to a PoE adapter or network switch. Refer to the Plant Network Connection section for additional information.
2. (Optional) Connect an external supply using the auxiliary power cable. For details, see Configuration.
3. Connect to the Ranger Pro Gateway web interface using a host PC connected to the PoE adapter or network switch.
4. Set the host PC IPv4 address and subnet mask to a value within the Ranger Pro Gateway default IP address range and subnet.
5. Use a web browser and visit **http://192.168.1.1**.

Keep connector protection caps in place to prevent exposure to contaminants for connections not used during configuration or installation.

Set Password

For security purposes, we recommend you change the password for the Ranger Pro Gateway web interface.

To change the password:

- Select **Maintenance** > **Change Password** tab.

Set IPv4 TCP/IP Address

To prevent plant network conflicts, we recommend you change the Ranger Pro Gateway IPv4 TCP/IP address.

To change the TCP/IP address:

- Select **Network** > **System Manager**.
- Expand the System Manager **Provision**.
- Change the IPv4 Address, Gateway (Default Gateway) and Mask (Subnet Mask) values as required.

Have your plant network administrator allocate a dedicated static IPv4 plant network address or ensure that you assign an unused TCP/IP IPv4 address.

Set Network ID

To prevent wireless network conflicts, we recommend you change the Ranger Pro Gateway device network ID.

To change the device network ID:

1. Select **Network** > **System Manager**.
2. Expand the System Manager **Provision**.
3. Change the **Network ID** as required.

You must use an unused ISA100 network ID. Consult with your plant ISA100 wireless network administrator as needed.

Set Join Key (ISA100)

For security purposes, we recommend you change the Ranger Pro Gateway join key.

To change the join key:

1. Select **Network** > **System Manager**.
2. Expand the System Manager **Provision**.
3. Change the **Join Key** as required.

4.3 Provision Field Devices (ISA100)

The Ranger Pro Gateway does not currently support OTA provisioning. Ranger Pro configuration software is able to manually provision compatible Ranger Pro ISA100 field devices. Refer to the Ranger Pro User Guide (125M6113).

Before deploying Ranger Pro ISA100 field devices, we recommend you provision each device to join your network. Depending on the number of field devices and their current sleep state, provisioning can take up to several hours.

When you provision the device, you:

- Set the network ID to match the gateway network ID.
- Set the network join key to match the gateway network join key.

4.4 Configure Field Devices

Once Ranger Pro field devices have joined the network, they can be configured using the Ranger Pro Gateway web interface.

You can configure these options:

- **Tag** (up to 16 Characters)
- **Role** (IO (Default), Router and Router IO) (ISA100)

To configure device **Tag**:

- Select **Network** > relevant device in the device list.
- Expand the **Device Information**.
- Change the **Device Tag** as required.

To configure device **Role**(ISA100):

- Select **Network** > [device name].
- Expand the **Device Role**.
- Change the **Device Role** as required.

To implement changes, you must reboot the devices. For details, see Reboot Field Devices on page 46.

5. Verification

5.1 Verify Network Connectivity

Ranger Pro Gateways can send data or commands to, and receive data from, Ranger Pro field devices over a wireless network. Information such as Data on Demand (DoD), configuration change requests, and vibration and temperature data, is transfered between the gateway and the client through the ISA100 General Client Interface (GCI). Data received by the gateway can also be published by Modbus.

To send data or commands or collect data using the GCI, the user must have installed the relevant versions of Bently Nevada System 1 Software and the Ranger Pro Core plugin. Furthermore, dynamic data is only sent to the user using GCI.

Refer to the Ranger Pro User Guide (document 125M6113) for more information regarding configuring and verifying Ranger Pro field device network connectivity.

Verify Network Joining

To verify that your field devices have joined your network, use the Ranger Pro Gateway web interface. It can take several hours for many Ranger Pro field devices to join your network.

If a provisioned field device fails to join your network after several hours, try these options:

Verify / Reboot the Ranger Pro Device

- Reboot the Ranger Pro field device. This increases how often the device attempts to join the network. Refer to the Ranger Pro User Guide (document 125M6113) for more information.
- Verify that the device is correctly provisioned. ISA100 field devices must be in a provisioned state with the correct Network ID and join key to join the network.
- Verify the device's network connection. Dismount the device from the machine and position it closer to the relevant Ranger Pro Gateway.
- Improve the device's radio frequency communication by reorienting the device's axis relative to the gateway. Optimal RF communication occurs when the device's x-axis is in the horizontal plane." (See the Ranger Pro User Guide, 125M6113, for more details).

Add a Routing Device (ISA100)

- In areas that have weak RF coverage (for example, where RSSI < -78 dB), configure a Ranger Pro ISA100 field device to enable routing or, preferably, add a Ranger Pro ISA100 repeater.
- Use the Ranger Pro Gateway web interface to verify, and if necessary, enable the router function of each ISA100 field device.
- Verify that each Ranger Pro field device has a good network connection.
- Remember to stay within the recommended number of hops per device (4 hops).

Remember that using an ISA100 sensor as a router decreases its battery life.

Ranger Pro Gateway device managers limit the number of field devices connected to the gateway. This could be any combination of **IO**, **Router**, or **Router IO** devices up to a total of 50 devices. Up to 9 child devices may connect to each router enabled device. The maximum number of hops between the Ranger Pro Gateway and a Ranger Pro field device should be limited to 4.

Move the Device or Gateway

Relocating a field device or reorienting its axis or orientation relative to the gateway as little as 6 cm (2 1/3 inch), or one-half of a 2.4 GHz wavelength, may improve signal strength.

Change Gateway

Change the gateway deployment by using the authorized 6dBi higher gain antenna on the gateway. Verify that the resulting narrowly focused radio frequency distribution pattern meets your needs. You can also add additional gateways.

Verify Signal Strength

Check that the devices' signal strength and packet error rate are within guidelines. Use your Ranger Pro Gateway web interface to monitor device signal strength and packet error rates. Signal strength (RSSI) should be above -85 dBm, and preferably above -78 dBm.

Validate Device Data

Using the Ranger Pro Gateway device-manager web-interface, verify the publication status and that the measurements are displayed in the **Readings** tab.

	Icon	Status	Description
	Wireless signal icon with a cross	Not Joined	Device is not visible to the network. It may be out of range, is restarting, or is off.
	Wireless Signal Icon	Joining	Device is busy negotiating to join the network.
	Bold Wireless Signal Icon	Joined	Device joined and configuring.
	Wireless Signal Icon with a check mark	Joined and Publishing	Device configured and publishing PV data.

Initial publication of measurements may take some time after devices have joined the network. After the initial period, during which the network is forming, measurements will be published at 1-minute intervals.

Use the data trend tab after selecting a Ranger Pro sensor in the device tree to view a history of the selected parameters.

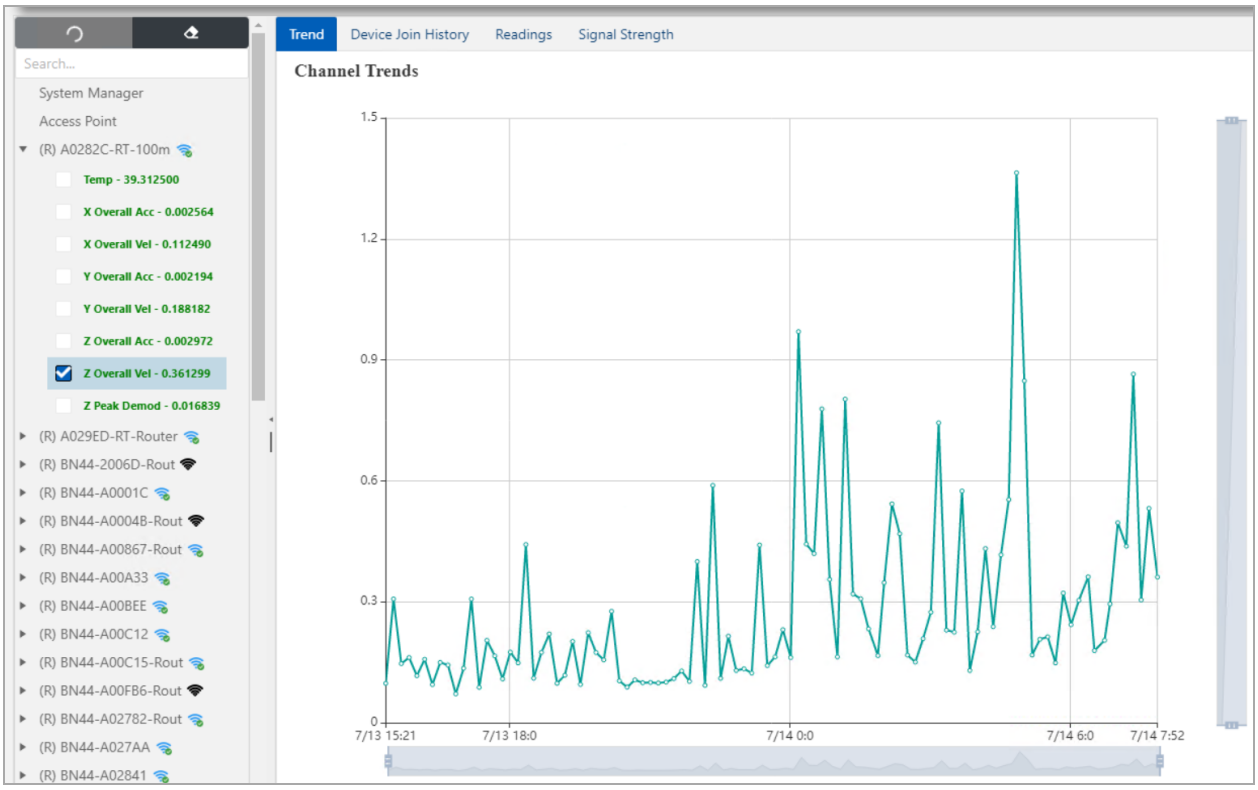


Figure 5 – 1: Ranger Pro Trend Data

5.2 Modbus Register Values

The Ranger Pro Gateway can output Ranger Pro sensor static data (trended variables) using the Modbus TCP protocol.

Use any Modbus tool to connect with the Ranger Pro Gateway through port 502. Check the Input Register Values as listed in the gateway user interface Modbus tab.

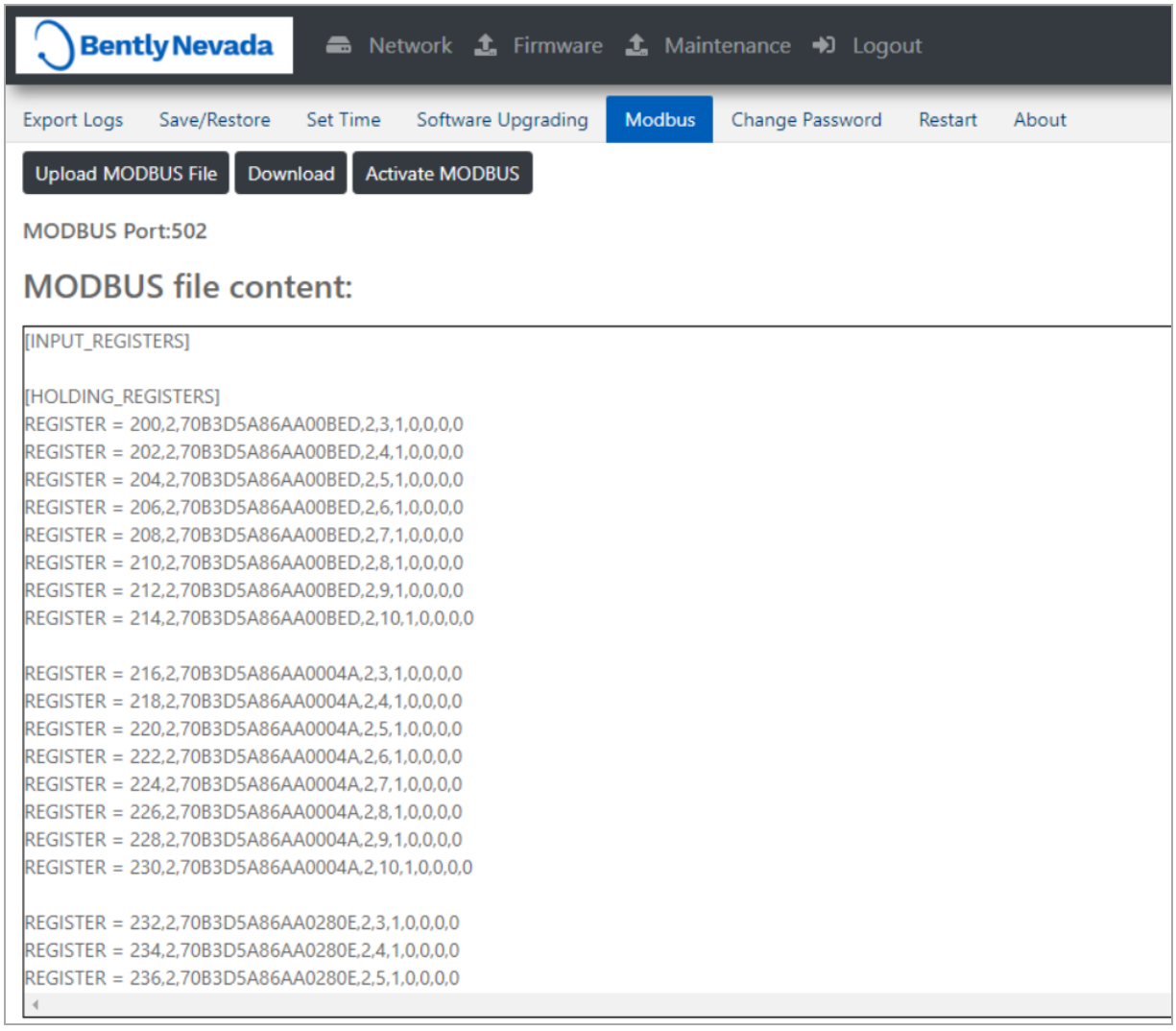


Figure 5 - 2: Modbus Input Register Values Example

6. Maintenance

Ranger Pro Gateways need minimal maintenance. If a device fails, it may be due to environmental damage, or even a blocked wireless connection.

6.1 System Time Backup Power Battery

Ranger Pro Gateways use a Lithium coin-sized batter to keep the real-time clock and radio oscillator running when the gateway does not have power from the PoE or external power connector.

The battery should be replaced if the Ranger Pro Gateway time keeps resetting to the same incorrect date and time after power loss.

Install only approved CR2032 Lithium batteries. For details and ordering information, see the Ranger Pro Gateway datasheet (document 157M8584).

6.2 Clean and Inspect Devices

Use a damp cloth to clean the exterior of the Ranger Pro Gateway in potentially hazardous environments.

WARNING

WARNING HAZARDOUS ENVIRONMENT

RISK OF EXPLOSIVE ATMOSPHERE

A static hazard may exist on the equipment as a result of the non-metallic coating. The equipment shall only be cleaned with a damp cloth when deployed in a hazardous area.

Before cleaning or inspecting Ranger Pro Gateways device in a potentially hazardous environment, verify that hazardous materials, atmospheres, and conditions have been removed.

Clean the Exterior

When cleaning a Ranger Pro Gateway in an equipment room or a similar environment:

- Use a clean, dry, non-abrasive, anti-static cloth to clean the exterior. Do not use solvents or solutions.
- To remove deposits from the exterior of the sensor, use an electronic contact or switch cleaner.

Open the Device

Before opening the device, de-energise the cables and remove the device from the field and operating environment. Open the casing by loosening and partially removing the captive screws on one of the hinges and completely removing the captive screws on the other hinge.

Clean the Interior

Clean the interior using a clean, dry, anti-static cloth.

Inspect the Device Casing

The device casing is made of anodised Aluminum and is epoxy-powder coated. Inspect the:

- Aluminum device casing for damage or oxidation.
- Lithium battery and terminal springs. Look for chemical corrosion or deposits.
- Antenna N-Type connector for soiling or oxidation.
- Power M12 and network RJ45 connectors for soiling or damage to the seals.

Inspect the Lid Seal

The device uses a continuous seal to protect the unit against dust and moisture ingress. The seal maintains the device's dust and water-resistant IP rating.

Inspect the seal:

- Verify that the seal is free from dust and debris.
- To remove dust and dirt, use a clean, dry cloth.

Inspect the Battery

Inspect the battery before removing it. Look for:

- Swelling or deformation.
- Indentations or lifting of battery terminals.
- Moisture or liquid on the battery surface.
- Chemical corrosion or deposits on the battery terminals.

CAUTION

EQUIPMENT DAMAGE

Do not use a device with a damaged enclosure or Lithium battery. Using a damaged device may further damage the device, cause it to fail, or in hazardous locations cause other unintended consequences.

If a battery has leaked, do not touch the corrosive electrolyte.

If the battery is damaged or is leaking, follow your site's hazardous materials handling procedures.

Replace the battery

We recommend that you replace Ranger Pro Gateway batteries in an indoor equipment room or a similar environment. Do not replace batteries in a hazardous area. Use only approved battery types described in the relevant Ranger Pro Gateway datasheet.

To dispose of used or partially expended batteries, follow your on-site or locally accepted hazardous materials handling procedures.

Close the Device

To close the device:

1. Ensure that the Ranger Pro Gateway lid seal is clean before closing it.
2. Align and fasten the captive screws into the hinges using a cross-tightening technique (do not tighten both screws on one side while leaving both screws on the other side loose).

DO NOT over-tighten the captive screws as this may compromise the lid seal. Fasten captive screws to a torque of 6 Nm.

6.3 Update Gateway Software

You may on rare occasions need to update the Ranger Pro Gateway software. Request or download software updates from Bently Nevada technical support. You can update Ranger Pro Gateway software using the web-interface.

To update gateway firmware:

1. Use your browser to navigate to the IP address of your Ranger Pro Gateway and login.
2. Select **Maintenance** > **Software Upgrading** tab.
3. Click on the **Upload** file area to browse to and select the relevant gateway software file.
4. Wait for the upload to complete.
5. Click **Upgrade!** The upgrade is completed.

Click on **Remove Files** to remove all uploaded software files before uploading new files.

6.4 Reset Gateway

The Ranger Pro Gateway can be reset using the web-interface or using the power connector if in a non-hazardous environment.

To reset the gateway:

1. Navigate to **Maintenance**.
2. Select the **Restart** menu item.
3. Select **Soft Restart** or **Power Cycle**.

IPv4 Address Reset

To reset the Ranger Pro Gateway IPv4 address using a magnet:

1. Place a magnet against the magnet icon located on the Ranger Pro Gateway until the status indicator starts flashing between green and amber.
2. Hold the magnet in position for approximately 5 seconds.
3. The status indicator should start flashing between amber and red indicating that the IPv4 address has been reset to factory default (**192.168.1.1**).
4. Remove the magnet.

To reset the Ranger Pro Gateway IPv4 address by using the A-coded M12 auxiliary power connector:

1. If in a non-hazardous environment, connect pin 2 to pin 3 (white to blue wire) until the status indicator starts flashing between green and amber.
2. Maintain the connection for approximately 5 seconds.
3. The status indicator should start flashing between amber and red indicating that the IPv4 address has been reset to factory default (**192.168.1.1**).

Remove the magnet or auxiliary power reset connection within 10 seconds of starting the process to prevent the device from entering the factory default restore process.

6.5 Restore Factory Defaults

To use a magnet to restore the gateway to the factory default settings:

1. Place a magnet against the dot icon located on the front label of the Ranger Pro Gateway until the status indicator starts flashing between green and amber.
2. Hold the magnet in place for approximately 15 seconds while the status indicator starts flashing between amber and red and then changes to a steady red. This begins the factory default restoration process.
3. After a few minutes the TCP/IP IPv4 address will be reset to factory default (**192.168.1.1**), all user configurations will revert to the factory default and device software will be reverted to the factory installed version.

Alternatively, if in a non-hazardous environment, use the auxiliary power connection reset option by connecting pin 2 to pin 3 (white to blue wire) until the status indicator starts flashing between amber and red. Remove the connection after 15 seconds.

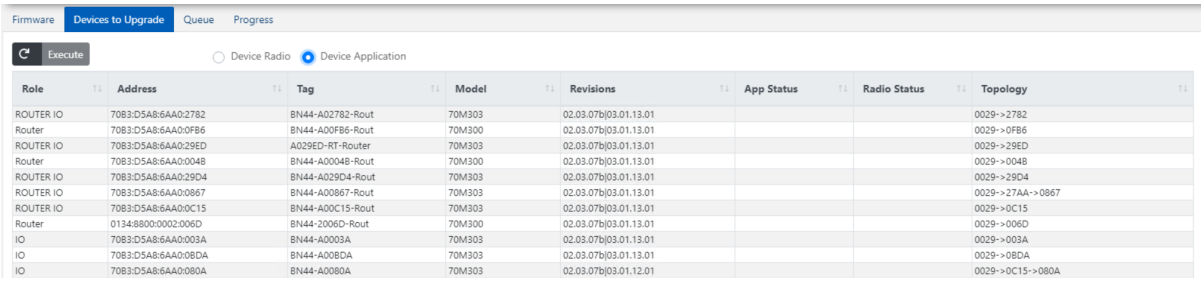
The factory default restore cannot be undone.

6.6 Update Field Device Firmware

You may on rare occasions need to update Ranger Pro field device firmware. Request or download firmware updates from Bently Nevada. You can update firmware using the Ranger Pro Gateway web-interface.

To update field device firmware:

1. Navigate to the **Firmware** section.
2. Click **Upload** to upload new device firmware to be uploaded OTA to devices.
3. Click **Browse** to select the firmware binary file, then choose **Device Radio** or **Device Application** from **Firmware Type**.
4. Enter the firmware Version and description.
5. Click **OK**.
6. Navigate to **Devices to Upgrade** and select **Device Radio** or **Device Application** for respective firmware updates. The **Topology** field shows the chain of the devices in the network and each 4 digit entry to the left of the 4 digits representing the device in the chain represents a parent of the device.



Role	Address	Tag	Model	Revisions	App Status	Radio Status	Topology
ROUTER IO	70B3:D5A8:6AA0:2782	BN44-A02782-Rout	70M303	02.03.07b|03.01.13.01			0029->2782
Router	70B3:D5A8:6AA0:0FB6	BN44-A00FB6-Rout	70M300	02.03.07b|03.01.13.01			0029->0FB6
ROUTER IO	70B3:D5A8:6AA0:29ED	A029ED-RT-Router	70M303	02.03.07b|03.01.13.01			0029->29ED
Router	70B3:D5A8:6AA0:004B	BN44-A0004B-Rout	70M300	02.03.07b|03.01.13.01			0029->004B
ROUTER IO	70B3:D5A8:6AA0:29D4	BN44-A029D4-Rout	70M303	02.03.07b|03.01.13.01			0029->29D4
ROUTER IO	70B3:D5A8:6AA0:0867	BN44-A00867-Rout	70M303	02.03.07b|03.01.13.01			0029->27AA->0867
ROUTER IO	70B3:D5A8:6AA0:0C15	BN44-A00C15-Rout	70M303	02.03.07b|03.01.13.01			0029->0C15
Router	0134:8800:0002:006D	BN44-2006D-Rout	70M300	02.03.07b|03.01.13.01			0029->006D
IO	70B3:D5A8:6AA0:003A	BN44-A0003A	70M303	02.03.07b|03.01.13.01			0029->003A
IO	70B3:D5A8:6AA0:0BDA	BN44-A00BDA	70M303	02.03.07b|03.01.13.01			0029->0BDA
IO	70B3:D5A8:6AA0:080A	BN44-A0080A	70M303	02.03.07b|03.01.12.01			0029->0C15->080A

Figure 6 - 1: Devices to Upgrade Tab

7. Select the device(s) to upgrade and click **Execute**. If multiple devices are selected, the device upgrades are optimised by an upgrade scheduler.
8. Select the appropriate **Firmware** and click **OK**.
9. The **Radio Status** field displays the upgrade status and is updated by the upgrade scheduler.
10. Navigate to **Queue** to view detailed upgrade status information.
    - **Pending**, awaiting the next retry.
    - **Active**, the active progress can be viewed on the **Progress** tab.
    - **Fail**, the maximum allowed number of retries has been reached.
    - **Success**, the upgrade has succeeded.
    - **Cancelling**, the scheduler is in the process of cancelling an upgrade.

- **Cancelled**, the user cancelled the upgrade.
- **Request Pending**, **Request Cancelled** are scheduler internal states and will automatically progress to **Pending** or **Cancelling**.

11. Navigate to **Progress** to observe active OTA upgrade attempts in progress.

6.7 Reboot Field Devices

Ranger Pro field devices can be rebooted by navigating to the **Network** section and selecting the device of interest, opening the **Device Reset** accordion, then select from warm restart or restart as provisioned.

6.8 Harden the System

The security risk to your network when using Ranger Pro Gateways is like that of any distributed control system or industrial control system. You need to take all reasonable steps to properly secure these devices.

At a minimum, to secure Ranger Pro Gateways:

- Install on secure networks due to unencrypted communications.
- Use unique, strong passwords for all devices.
- Provide adequate phyical security to prevent unathorized access.
- Verify that the latest software is installed on all devices.

The gateway only has one user role. To prevent unauthorized changes, limit access to systems connected to the gateway.