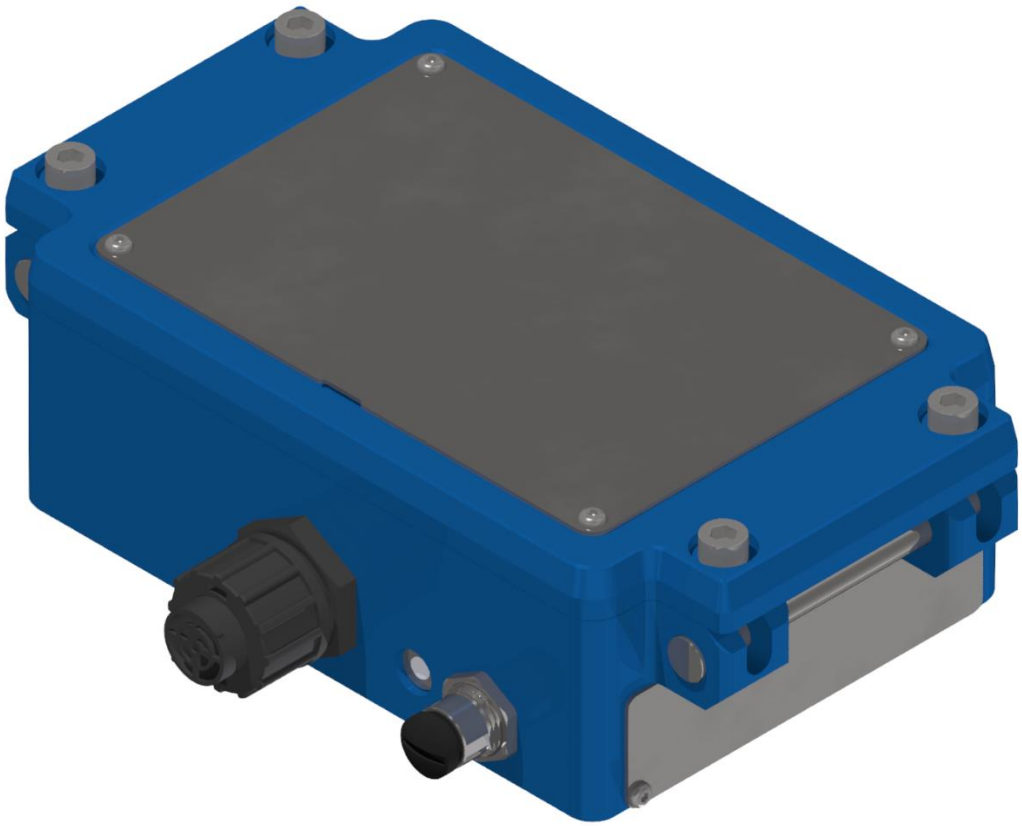
DIVIGRAPH

NG Series Industrial Wireless Gateway User Guide



Doc No. 20DD1980
Revision 4

Contact Information

When it is not possible to contact your local representative, use the following contact information:

Address	Prosperity Park, Computer Road, Milnerton, Cape Town, 7441, South Africa
Telephone	+27 (21) 065-0344
Email	info@divigraph.com
Internet	www.divigraph.com

Contents

General Safety

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 Divigraph. Include all model numbers and serial numbers with the claim.

Handling and Storing Considerations

Proper handling of components, best practices for system installation, and diligent inspection procedures will prolong the service life of the system. Additionally, procedures for dealing with system components that have been replaced are detailed below, to allow compliance with regulations relating to electronic waste.

Personal Safety Warnings

Labels and markings are provided on the product to guide the system integrator in the processes of choosing appropriate interface equipment, determining safe use conditions, and identifying recommended installation procedures. The formats of these markings are governed by the standards that dictate safe use and environmental compliance in a variety of regions and regulated settings. More specific product safety warnings are described in the document **NG Series Industrial Wireless Gateway Warnings, Special Conditions and Additional Information** (document 20DD2011).

Potential Electrostatic Charge Hazard

! WARNING
ELECTROSTATIC CHARGE HAZARD
 **RISK OF PERSONAL INJURY OR EQUIPMENT DAMAGE.** Potential for electrostatic charging hazard.

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.

Circuit boards contain devices that are susceptible to damage when exposed to electrostatic charges. Damage caused by obvious mishandling of the board will void the warranty. To avoid damage, observe the following precautions in the order given.

- 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, nonconductive 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.

Hazardous Environment

! WARNING
HAZARDOUS ENVIRONMENT
 **RISK OF EXPLOSIVE ATMOSPHERE.** De-energize all relays and connections before placement or removal. Take precautionary measures to avoid electrostatic potential, especially on plastic components.

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.

Lithium Batteries

! WARNING
LITHIUM BATTERY CHEMICAL HAZARD
 Do not use a device with a damaged battery. Using a damaged battery may further damage the device, cause it to fail, or in hazardous locations cause other unintended consequences.

Lithium batteries are volatile. When handling and storing lithium metal batteries, follow these precautions:

- Store and handle lithium metal batteries to avoid contact with other lithium batteries.
- Do not place lithium metal batteries on metal work surfaces.
- Avoid exposing lithium metal batteries to extreme temperatures.
- If you store an inactive device, remove the battery.
- Dispose of used or defective batteries in accordance with the applicable statutes and regulations, as well as site-specific safety requirements.

The lithium batteries will typically last up to five years. Use the Ranger Pro software or your network vendor's application to monitor battery performance and replace batteries as needed.

Safe Disposal

Replacing Device and Failure Analysis

Contact Divigraph for information on returning parts under warranty and/or requesting failure analysis.

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 endeavour 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. Divigraph is not responsible for product disposal at the end of its useful life. Visit www.weeerohsinfo.com for recycling information.

Introduction

Description

The NG Series Industrial Wireless Gateway provides ISA100 gateway and back bone router (BBR) functionality to communicate with VP Series 2000 ISA100 field devices. To enhance security, the devices use 128-bit AES encrypted packets.

If a gateway cannot communicate with ISA100 VP Series 2000 sensors that are out of range, you can use VP Series 2000 ISA100 repeaters to extend your ISA100 network.

NG Series Industrial Wireless Gateways are intended for monitoring purposes only and should not be used in control or safety systems.

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 the following 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: **23417-NG01**) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below (Table 1), 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 1: NG Series Industrial Wireless Gateway Authorized Antennas

Antenna Part Number	Type and Gain (dBi)
100A1001	Omnidirectional 2dBi
100A1002	Omnidirectional 6dBi

Note: 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.

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

For complete compliance and hazardous location approval information, see the **NG Series Industrial Wireless Gateway Datasheet** (document 20DD1979) and **NG Series Industrial Wireless Gateway Warnings, Special Conditions and Additional Information** (document 20DD2011) available from Divigraph.

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: **23417-NG01**) a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessus (Table 1) 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 complémentaires à propos de la conformité et de l'approbation de cet appareil en zone dangereuse, veuillez consultez **NG Series Industrial Wireless Gateway Datasheet** (document 20DD1979) et **NG Series Industrial Wireless Gateway Warnings, Special Conditions and Additional Information** (document 20DD2011) disponibles auprès du Divigraph.

Installation and Configuration

This section describes how to connect to the NG Series Industrial Wireless Gateway (gateway) for the first time and which settings should be configured before placing it on a live control network. It is important to note that some gateways do not reside on a network. In these cases, it is still important to configure the items outlined in this section.

Before the gateway is permanently mounted and connected to a live control network, it should be configured with an IP address. This is done by forming a private network between the gateway and a PC/laptop. The following items are needed to complete this section:

- NG Series Industrial Wireless Gateway
- Mounting hardware (plus adapters, if needed)
- Power supply (PoE injector or external PSU or both)
- Antenna
- Antenna cable (optional)
- Surge arrester(s) (required for outdoor or cabled antenna connections)
- RJ45 (8 pin) network cable (shielded Cat-5e or higher) with the supplied RJ45 gland
- A-coded M12 (4 pin) power cable or field connector (optional)
- VP Series 2000 field device(s)

Gateway Components

The device kit is composed of these parts:

- Gateway
    - Enclosure base (anodised, powder-coated aluminium)
    - Enclosure lid (anodised, powder-coated aluminium)
    - RJ45 connector protection cap (required when RJ45 connector is not in use)
    - M12 connector protection cap (required when M12 connector is not in use)
- RJ45 cable gland
- Mounting accessories
    - Mounting flanges (for surface and pole mount)
    - Mounting main bracket (for surface and pole mount)
    - Mounting support bracket (for pole mount only)
    - Mounting fasteners
- Self-amalgamating tape (for antenna installation)

The device has optional accessories:

- 2dBi Omnidirectional Antenna
- 6dBi Omnidirectional Antenna
- Surge Arrester
- Field Connector (M12 4-pin A-Coded)
- PoE Injector

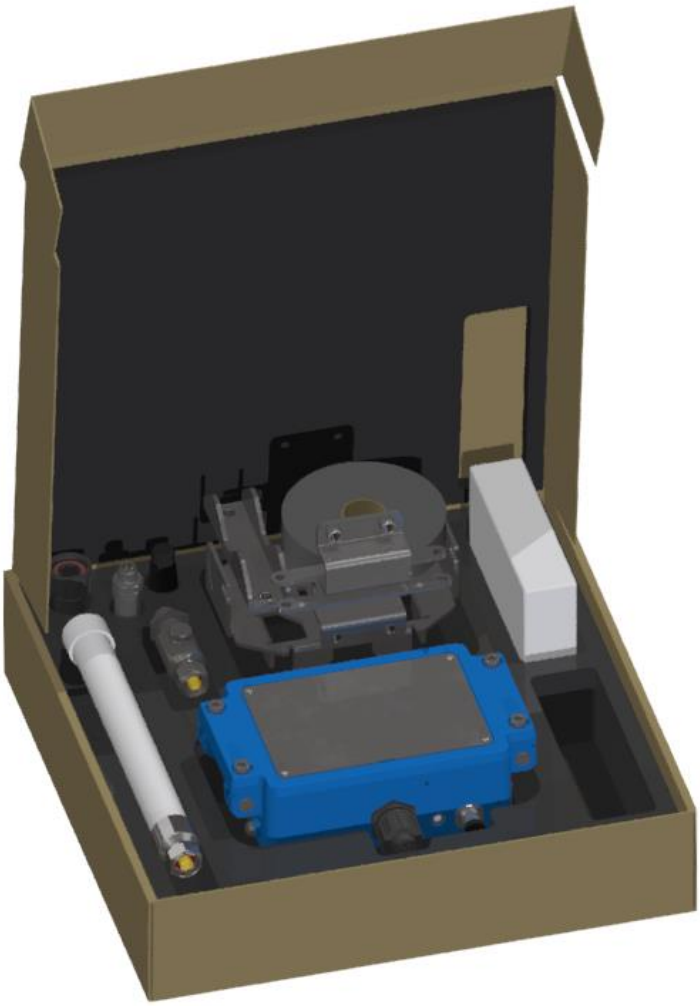


*Image shows gateway kit and optional accessories.

Figure 1: Packaged NG Series Industrial Wireless Gateway & Accessories

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:

- Chrome
- Mozilla Firefox®

Note: Microsoft® Internet Explorer® is not supported.

We recommend you use the most current version the compatible browser used.

These ports on the gateway 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 a NG Series Industrial Wireless Gateway to your network:

1. Survey your installation location.
2. Decide where to install the gateways and identify mounting points.
3. Install and configure gateways.
4. Provision VP Series 2000 ISA100 field devices.
5. Test and verify your installation.
6. Monitor and maintain your network.

For more information regarding ISA100 network design, refer to the **VP Series 2000 User Guide** (document EVR-VPXDOC-0036).

User Interface

The NG Series Industrial Wireless Gateway provides a web-based user interface to configure and monitor all the 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 can be used for performing the following tasks.

- Network maintenance
- Device configuration and maintenance
- Operator activities

Login

You must login to be able to access the gateway functions.

Network

When the Network section is selected, a device tree, tab control and property list is displayed.

The device tree displays the System Manager, Access Point and VP Series 2000 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 Manager 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.

Network Health

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

GCI Stats

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

Provision

The Provision settings allow configuration of the Network ID, Join Key, local area network (LAN) settings as well as the Tag for the NG Series Industrial Wireless Gateway.

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, configuration of 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 max number of layers (hops) is also configurable. More routers result in higher consumption. The recommend maximum number of routers is no more than 30% of all field devices.

Setting	Description	Default Value
Max Layers	The number of routing layers between the back bone router and the last child device in the network chain after network optimisation.	3
IO devices per BBR	The maximum number of IO only devices that can connect directly to the back bone router.	50
Routing Devices per BBR	The maximum number of routing enabled devices (including IO routers) that can connect directly to the back bone router. 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.

Network Health

As per System Manager Network Health.

GCI Stats

As per System Manager GCI Stats.

Signal Strength

As per System Manager Signal Strength.

Event History

As per System Manager Event History.

General Settings

The General Settings show non configurable details of the access point such as the serial number and allow configuration of the access point Tag name.

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.

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 displays 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 VP Series 2000 field device. The Device Tag name can also be set here.

Device Restart

The Device Restart settings allow a VP Series 2000 field device radio (soft restart), or application processor (restart as provisioned) to be rebooted from the User Interface.

Device Role

The Device Role settings allow a VP Series 2000 ISA100 field device to be configured to join as a router, routerIO or IO device.

Firmware

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

Firmware

The Firmware tab is used to upload two different kinds of firmware for Over the Air (OTA) upgrading of VP Series 2000 field device radios and application processors.

Devices to Upgrade

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

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 NG Series Industrial Wireless Gateway time to be set manually or to the host time and date.

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, care must be taken to ensure that all related system times are adjusted to reflect the same UTC offset.

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.

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

1. Modify the NG Series Industrial Wireless Gateway Modbus settings:
    a. Create a new Modbus configuration file to upload 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*			
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)

2. Navigate to the "***Maintenance***" section and select the "***Modbus***" tab.
3. Select "***Upload Modbus File***" and browse to the relevant Modbus configuration file.

4. Click on "***OK***" to upload the file.
5. 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, Index 2 values, see the **VP Series 2000 User Guide** (document EVR-VPXDOC-0036).

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

Change Password

The Change Password function allows the user to change the NG Series Industrial Wireless Gateway password.

Currently the NG Series Industrial Wireless Gateway only supports one user (the admin user) with access to all operations on the NG Series Industrial Wireless 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 NG Series Industrial Wireless Gateway, they should use the Logout function to prevent unauthorized changes to the system.

Configuration

Configure Gateways

We recommend performing basic configuration of NG Series Industrial Wireless Gateways in an indoors 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:

- Use a PoE cable to connect the NG Series Industrial Wireless Gateway to a PoE adapter or network switch – refer to the *Plant Network Connection* section for additional information.
- (Optional) Connect an external supply using the auxiliary power cable. For details see ***Power Connection***.
- Connect to the NG Series Industrial Wireless Gateway web interface using a host PC connected to the PoE adapter or network switch.
- Set the host PC IPv4 address to a value within the NG Series Industrial Wireless Gateway default IP address range and subnet.
- Use a web browser to access the gateway user interface - http://Device_TCP_IPv4_Address.

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 NG Series Industrial Wireless Gateway web interface.

To change the password:

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

Set IPv4 TCP/IP Address

To prevent plant network conflicts, we recommend you change the NG Series Industrial Wireless Gateway IPv4 TCP/IP address.

To change the TCP/IP address:

- Select "***Network***" > "***System Manager***".
- Expand 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 NG Series Industrial Wireless Gateway network ID.

To change the device network ID:

- Select "***Network***" > "***System Manager***".
- Expand System Manager "***Provision***".
- 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 NG Series Industrial Wireless Gateway join key.

To change the join key:

- Select "***Network***" > "***System Manager***".
- Expand System Manager "***Provision***".
- Change the "***Join Key***" as required.

Provision Field Devices (ISA100)

The NG Series Industrial Wireless Gateway does not currently support OTA provisioning. Refer to the **VP Series 2000 User Guide** (document EVR-VPXDOC-0036) to manually provision compatible VP Series 2000 ISA100 field devices.

Before deploying VP Series 2000 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.

Configure Field Devices

Once VP Series 2000 field devices have joined the network, they can be configured using the NG Series Industrial Wireless Gateway web interface.

You can configure these options:

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

To configure the device **Tag**:

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

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

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

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

Deploy Gateway

The NG Series Industrial Wireless Gateways must be installed in accordance with relevant site standards and regulations.

- All hazardous location installations ***MUST*** be performed by a suitably qualified competent person.
- RF antenna installations should be completed by a suitably qualified competent person.

! WARNING
HAZARDOUS ENVIRONMENT
 **RISK OF EXPLOSIVE ATMOSPHERE.** The connectors to the equipment may not be connected or disconnected when energized.

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. Provide enough clearance around the main bracket to allow for the gateway to be attached and cables connected.

Pole Mounting

Mount NG Series Industrial Wireless 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 fasteners (see Figure 2).

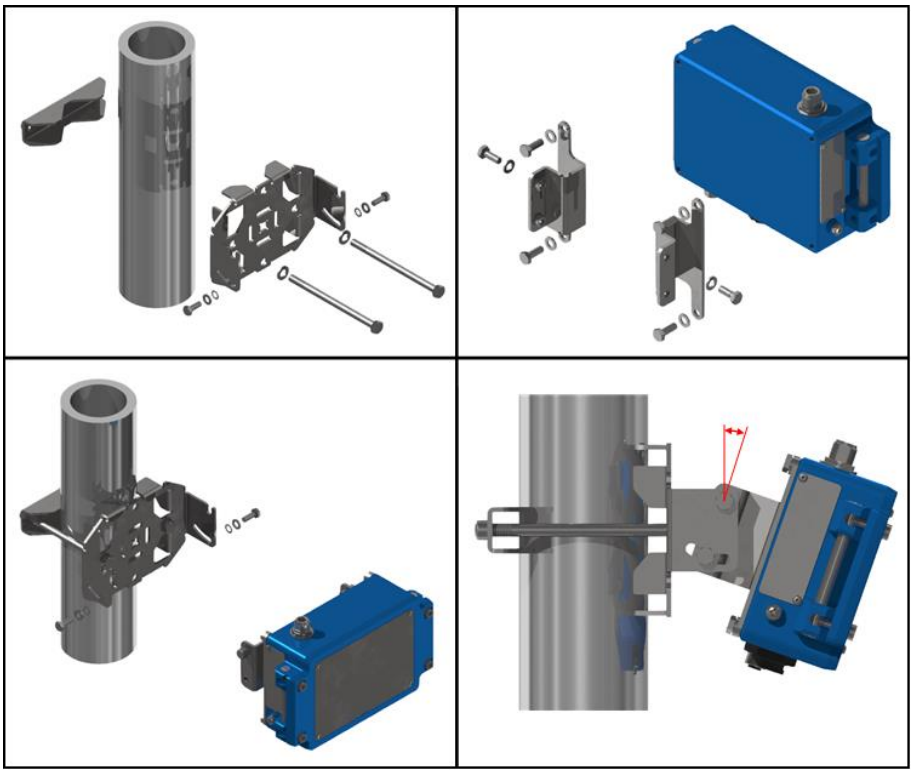


Figure 2: Pole mounting

Surface Mounting

The mounting main bracket can be attached directly to a suitable surface such as a wall or bulkhead using four appropriate M8 (or 5/16") fasteners (see Figure 3). 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.

Although not required, NG Series Industrial Wireless Gateways can be mounted directly into instrument panels or enclosures using the supplied mounting accessories.

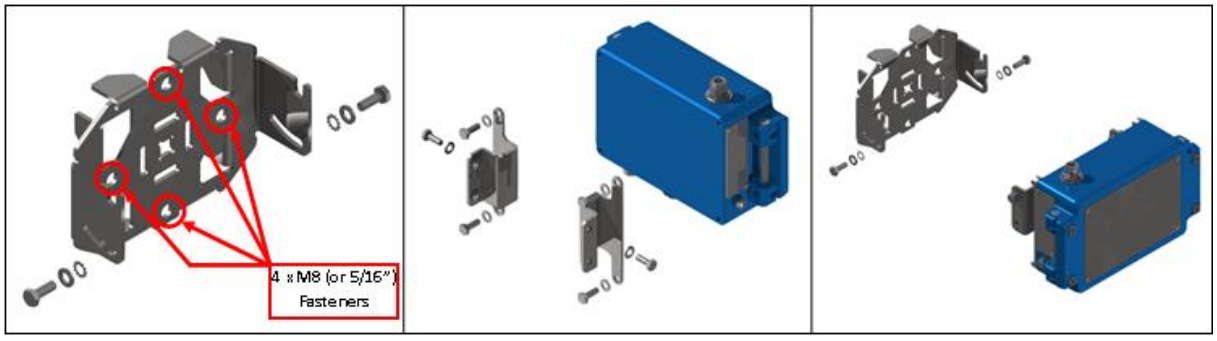


Figure 3: Surface mounting

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.

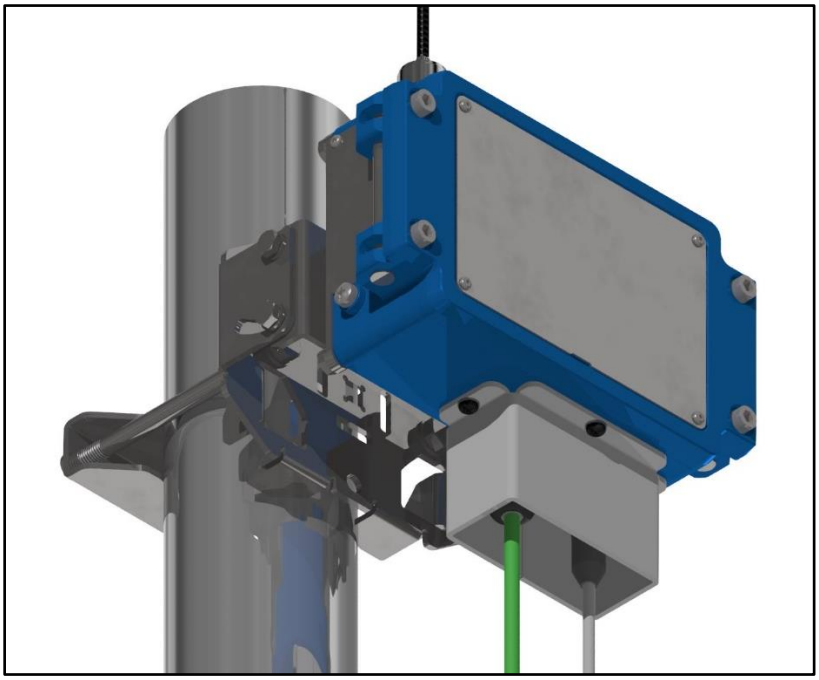


Figure 4: Connector guard installed for protection against UV exposure

Ground Connection

NG Series Industrial Wireless Gateways must be grounded using a suitable gauge grounding wire connected to the grounding lug attachment point on the enclosure.

Surge Protection

The following information is intended as guidelines only and does not replace the need for surge protection assessment and installation by a suitably qualified person according to local regulations. 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 their own conductors directly to earth ground instead of locally available grounding points as these could be at a higher potential than a direct earth connection.

Indoor Installation

When equipment and cabling is installed within an enclosed environment, the risk related to lightning is less as enclosures such as buildings would typically have lightning protection features incorporated by design. However, there are still risks to persons and the equipment from sources of surges within the enclosed environment. Where surges over 1kV 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 as well as 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! The equipment and antenna must be professionally Installed in accordance with the requirements specified in this document. See compliance section for 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 20cm from all persons.

Depending on the installation type used, the antenna can be connected directly to equipment or can be mounted remotely. The remote antenna can be connected to the equipment 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 antennas.

Plant Network Connection

NG Series Industrial Wireless 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 Divigraph. 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 supports 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 by making use of 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, NG Series Industrial Wireless Gateways require an external power supply connection using the supplied A-coded M12 field wireable connector or optional M12 power cable accessory.

! 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 wirable connector or optional M12 power cable accessory to connect to an external power supply to establish a redundant power supply connection.

The secondary supply allows for continued operation should the primary supply fail. Switching between the primary and secondary supply will cause the gateway to reboot and results in temporary loss of wireless connectivity.

The A-coded M12 connection uses these wiring connections:

Table 2: M12 connector pin descriptions & wire colours

M12 Pin	Wire Colour	Description
1	Brown	IO – Reset 1
2	White	V+ (20-57 Vdc, 4W)
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 0.6Nm.

Verification

Verify Network Connectivity

NG Series Industrial Wireless Gateways can send data or commands to and receive data from VP Series 2000 field devices in a wireless network. Commands or data can be sent from the user to the gateway or data sent from the gateway to the user through the General Client Interface (GCI) for ISA100. 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 the relevant versions of Bently Nevada System 1 and the Ranger Pro Core plugin installed. Furthermore, dynamic data is only sent to the user using GCI.

Refer to the **VP Series 2000 User Guide** (document EVR-VPXDOC-0036) for more information regarding configuring and verifying field device network connectivity.

Verify Network Joining

To verify that your devices have joined your network, use the NG Series Industrial Wireless Gateway web interface. It can take several hours for many 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 Device

- Reboot the field device. This increases the frequency that the device attempts to join the network.
- Verify that the device is correctly provisioned. ISA100 field devices must be in a provisioned state to join the network.
- Verify the device's network connection. Dismount the device from the machine and position it closer to the relevant NG Series Industrial Wireless Gateway.
- If possible, improve the device's radio frequency communication by relocating it or reorienting the device's axis or orientation relative to the gateway.

Add a Routing Device (ISA100)

- In areas that have weak RF coverage (for example, where RSSI < -78dB), configure a VP Series 2000 ISA100 field device to enable routing or, preferably, add a VP Series 2000 ISA100 repeater.
- Use the NG Series Industrial Wireless Gateway web interface to verify, and if necessary, enable the router function of each ISA100 field device.
- Verify that each VP Series 2000 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.

NG Series Industrial Wireless 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 NG Series Industrial Wireless Gateway and a VP Series 2000 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. OR
- Add gateways.

Verify Signal Strength

Check that the devices' signal strength are within guidelines. Use your NG Series Industrial Wireless 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 NG Series Industrial Wireless 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 tick 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 VP Series 2000 sensor in the device tree to view a history of the selected parameters.

Modbus Readings

The NG Series Industrial Wireless Gateway can output VP Series 2000 sensor static data (trended variables) using the Modbus TCP protocol.

Use any Modbus tool to connect with the NG Series Industrial Wireless Gateway through port 502. Check the Modbus register values as listed in the gateway user interface Modbus page.

Maintenance

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

System Time Backup Power Battery

To keep the real-time clock (system time) and radio oscillator running while the gateway does not have power from the PoE or external power connector, NG Series Industrial Wireless Gateways use a Lithium coin-sized battery.

The battery should be replaced if the NG Series Industrial Wireless 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 **NG Series Industrial Wireless Gateway Datasheet** (document 20DD1979).

Clean and Inspect Devices

Use a damp cloth to clean the exterior of NG Series Gateways in potentially hazardous environments.

! 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 NG Series Industrial Wireless Gateways in a potentially hazardous environment, verify that hazardous materials, atmospheres, and conditions have been removed.

Clean the Exterior

When cleaning a NG Series Industrial Wireless 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 device, use an electronic contact or switch cleaner.

Diagnose Device Status

If a device fails, use the diagnostic LED to identify the fault.

LED State	Description
Amber (steady on)	Initialising
Green (steady on)	Ready
Amber (flashing)	Upgrade in progress
Green/Amber (alternate flashing)	IPv4 reset initiating – IPv4 will be reset after 5 seconds
Amber/Red (alternate flashing)	IPv4 reset in progress. Factory reset initiating – device will be set to factory default after 15 seconds.
Red (steady on)	Factory reset in progress.

Open the Device

Before opening the device, de-energise the cables and remove it 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 Aluminium and is epoxy powder coated. Inspect:

- Aluminium 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 NG Series Industrial Wireless Gateway batteries in an indoors equipment room or a similar environment. Do not replace batteries in a hazardous area. Use only approved battery types described in the relevant NG Series Industrial Wireless 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 NG Series Industrial Wireless 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 5Nm.

Update Gateway Software

You may on rare occasions need to update the NG Series Industrial Wireless Gateway software. Request or download software updates from Divigraph technical support. You can update NG Series Industrial Wireless Gateway software using the web-interface.

To update gateway firmware:

1. Use your web browser to navigate to the IP address of your NG Series Industrial Wireless Gateway and login
2. Select "***Maintenance***" > "***Software Upgrading***".
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!**"
6. Wait until the upgrade is completed.

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

Reset Gateway

The NG Series Industrial Wireless Gateway can be reset using the web-interface or using the power connector if in a non-hazardous environment.

To reset the NG Series Gateway:

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

IPv4 Address Reset

To reset the NG Series Industrial Wireless Gateway IPv4 address using a magnet:

1. Place a magnet against the magnet icon located on the NG Series Industrial Wireless 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 NG Series Industrial Wireless 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.

Restore Factory Defaults

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

1. Place a magnet against the magnet icon located on the NG Series Gateway until the status indicator starts flashing between green and amber.
2. Hold the magnet in place for 15 seconds while the status indicator flashes between amber and red to start the factory default restoration process. The status indicator will indicate steady red once the restore factory defaults process starts.
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.

Note!

The factory default restore cannot be undone.

Update Field Device Firmware

You may on rare occasions need to update VP Series 2000 field device firmware. Request or download firmware updates from Divigraph. You can update firmware using the NG Series 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.
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.

Reboot Field Devices

VP Series 2000 field devices can be rebooted by navigating to the "***Network***" section and selecting the device of interest, then opening the "***Device Reset***" accordion, then select from warm restart or restart as provisioned.

Troubleshoot NG Series Gateways

If the NG Series Gateway Wireless device fails, it may be due to environmental damage, or even a blocked wireless connection.

Refer to the *Diagnose Device Status* section to identify the status of the NG Series Industrial Wireless Gateway.

Harden the System

The security risk to your network when using NG Series Gateways is like that in 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 NG Series Gateways:

- Verify that the latest software is installed on all devices.
- Follow your site's standards or industry's best practices for strong passwords.
- Only install NG Series Gateway configuration software on computers dedicated to that purpose and maintain appropriate physical security of those computers.

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