OpenBlue

OpenBlue Bridge

Hardening Guide

GPS0023-CE-EN

Version 3.0

Rev A

Revised 2023-11-13

Johnson Controls

Introduction

Our solution provides peace of mind to our customers with a holistic cyber mindset beginning at initial design concept, continues through product development, and is supported through deployment. Johnson Controls also includes a rapid incident response process to meet the comprehensive and evolving cybersecurity environments.

The Hardening Guide intends to provide cybersecurity guidance used in planning, deployment, and maintenance periods.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation.

This guide provides hardening guidance specifically for the OpenBlue Bridge application, including software, configuration, hardware, permissions, roles, backup, restore, and patch management. While we do provide the supported platforms, hardening of the client / server operating system, and SQL is out of scope for this document.

This Johnson Controls **OpenBlue Bridge Hardening guide** is broken down into three main sections depicting the overall process for hardening:

1. Planning	2. Deployment	3. Maintain
Provides an introduction, general knowledge, and overall guidance for you to prepare your system for security and hardening	Guides you through the execution and hardening steps based on the products and security features of the target system components	Provides a checklist for future checkpoints to keep your system safe and secure

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of, any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur because of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Table of Contents

1 Planning

This section helps plan for the implementation of security requirement for the OpenBlue Bridge installation.

1.1.0 OpenBlue Bridge overview

The OpenBlue Bridge platform is designed to integrate devices, cloud Security as a Service (SaaS) offerings, legacy on premise platforms, and web applications.

The OpenBlue Bridge (OBB) product release is the next generation of OpenBlue Bridge software. OpenBlue Bridge brings a new dimension to the Industrial Internet of Things (IIoT) by embedding built-in edge intelligence and computing directly into a broad range of small-footprint edge devices. By hosting the processing, analytics, and applications as close as possible to the physical sensor infrastructure, OpenBlue Bridge minimizes latency, improves performance and response times, and enables more effective maintenance and operational strategies. The installation includes the Tempered Airwall technology which provides a secure network infrastructure based on a zero-trust model.

1.1.1 Deployment Architecture

The OpenBlue Bridge system is comprised of hardware and software components working closely together to provide performance monitoring over a site's meters, HVAC, and other building systems.

Figure 1.1.1.1: Typical OpenBlue Bridge deployment architecture diagram using Ethernet

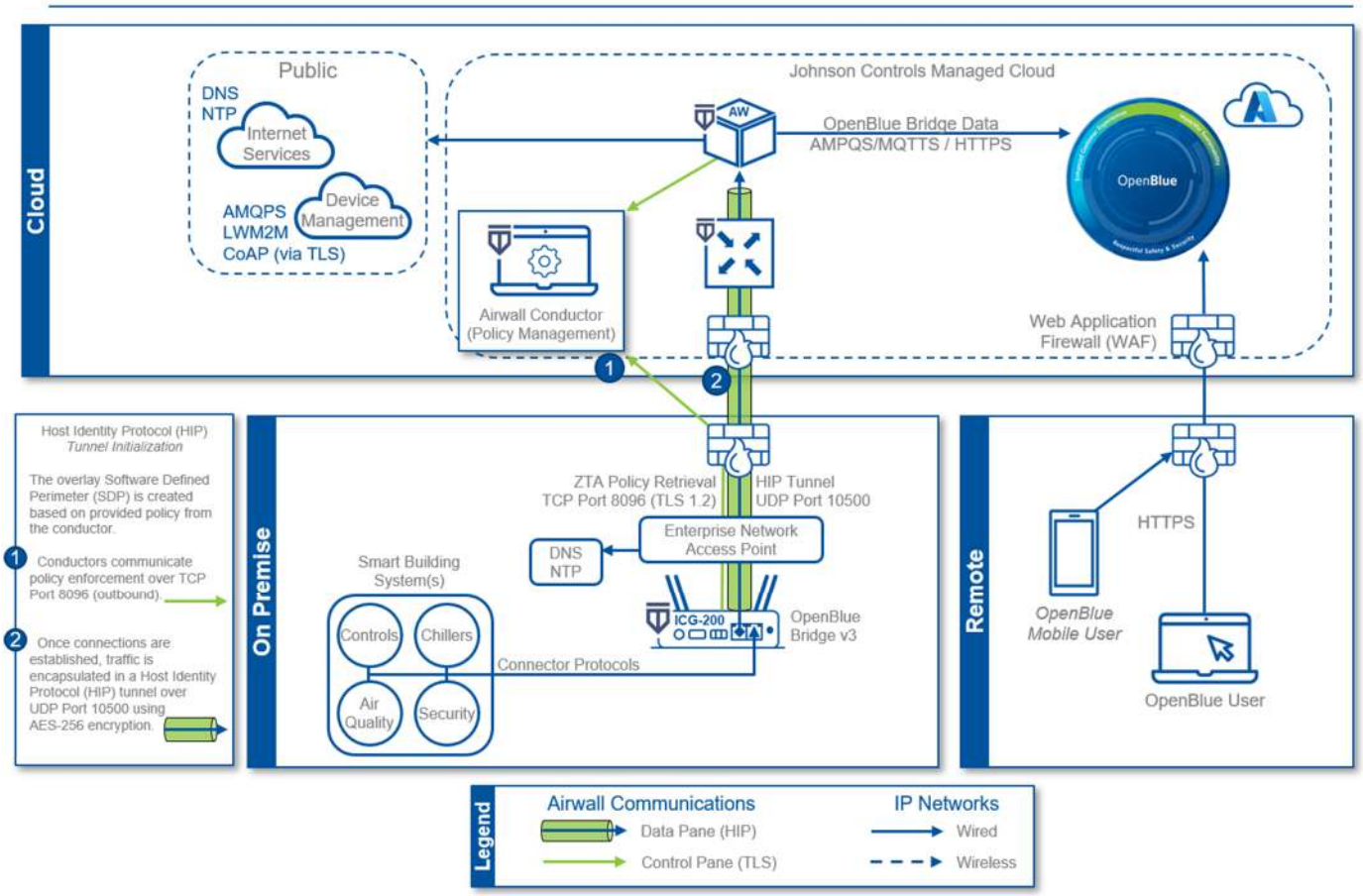
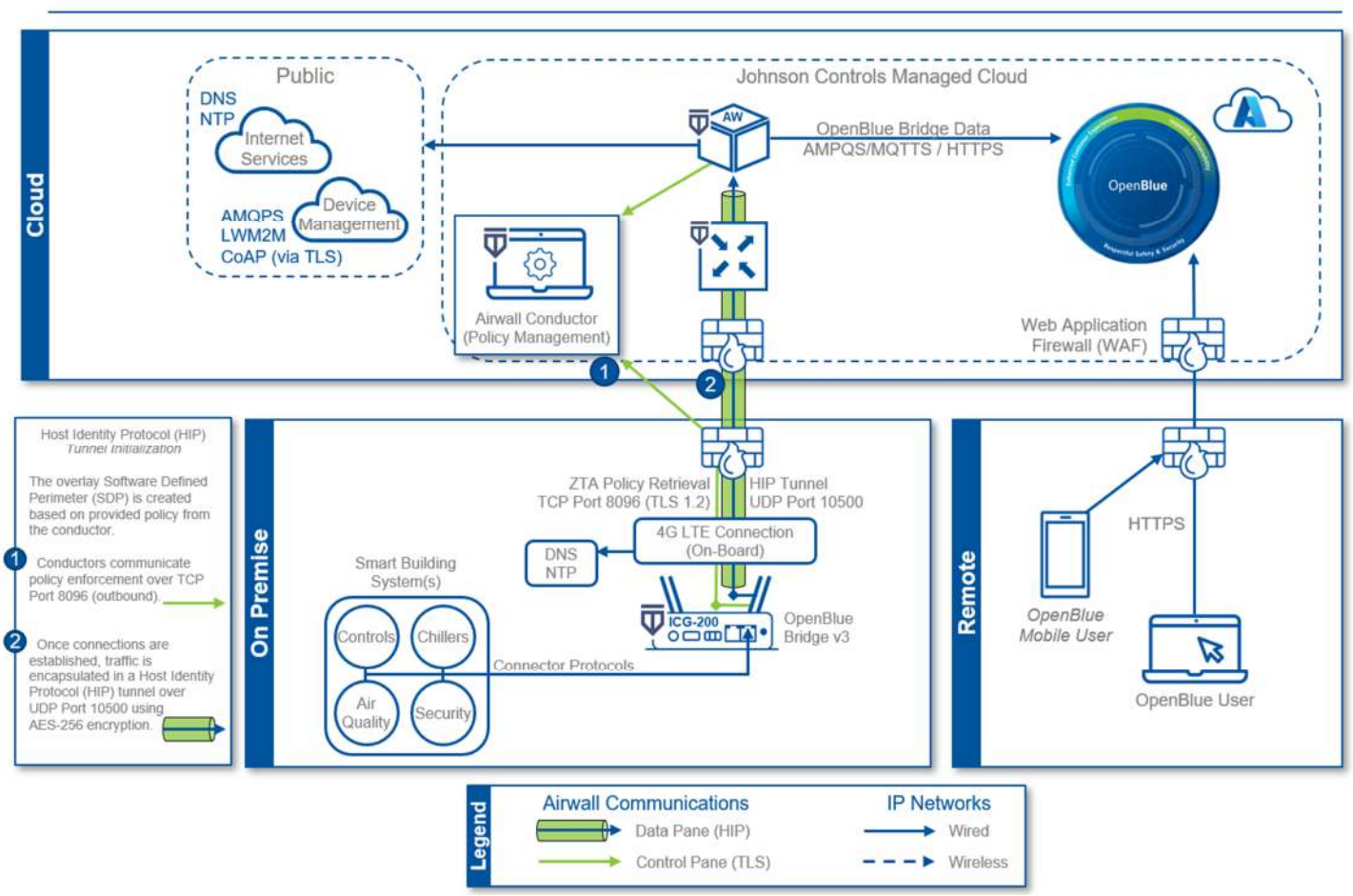


Figure 1.1.1.2: Typical OpenBlue Bridge deployment architecture diagram using Cellular



1.1.2 Components

Typical OpenBlue Bridge system core components include the following items:

OpenBlue Bridge Device

The OpenBlue Bridge Device, also known as the OpenBlue Bridge gateway, is a hardware device based on the Intwine Connected Gateway (ICG-200). It functions as both a physical layer gateway and an upper-level application gateway. OpenBlue Bridge serves as an edge computing and IoT hub, providing connectivity for end devices.

OpenBlue Bridge Connectors

OpenBlue Bridge Connectors offer connectivity to specific protocols for smart buildings and IoT systems. These connectors are enabled as needed to support each on-premises protocol OpenBlue Bridge will communicate with.

Airwall gateway

OpenBlue Bridge includes an Airwall Gateway as part of the OpenBlue zero-trust architecture (ZTA). The Airwall Gateway creates a virtual air-gap solution to make device network traffic invisible, preventing lateral

movement of malicious actors across your network. It uses the Host Identity Protocol (HIP) to secure network communication between devices, enabling micro-segmentation and remote access at scale on any network. OpenBlue Bridge also utilizes HIP to secure data transport for site to OpenBlue Cloud connectivity protecting it from discovery and attacks.

Device Manager

Device Manager is part of OpenBlue Bridge and acts as the central hub for all your Edge devices and applications. You can use this browser-based software to remotely manage data input and processing.

1.1.3 Supporting Components

Supporting components are those which are necessary for system operations but are not within the targeted scope of this document. This solution is supported by the following components:

Smart building systems and devices

OpenBlue Bridge interfaces and communicates with various smart building systems and devices. These systems include a wide range of control devices such as thermostats, lights, cameras, card readers, chillers, and more.

Firewall

The firewall acts as a protective barrier, ensuring that only authorized communication is allowed between the OpenBlue Bridge and external cloud services.

Local NTP server

The OpenBlue Bridge may be configured to utilize a local Network Time Protocol (NTP) server. This configuration allows the Bridge to synchronize its time with the local NTP server, instead of the default public NTP server, ensuring accurate and consistent timekeeping for all on premises components that synchronize time with the same local server.

Local DNS Server

The OpenBlue Bridge supports the configuration of a local Domain Name System (DNS) server. A local DNS server can be useful in scenarios where custom DNS settings or domain name resolution are required for specific applications or devices within the network.

1.2.0 Security feature set

This section describes the security features within OpenBlue Bridge.

- **Encrypted communications:** Collected data is sent encrypted from the OpenBlue Bridge (OBB) to the cloud using Transport Layer Security (TLS) encapsulated with HIP tunnel.
- **Zero-trust connection:** All messages are sent to cloud services using the tempered zero-trust solution which further encapsulates all traffic from the site using Host Identity Protocol (HIP).
- **Hidden IP addresses**: The IP address for the OpenBlue Bridge is not exposed to the internet.
- **Outbound communications only**: Only two outbound ports are required to initiate site-to- cloud data exchange.
- **Remote updates**: OpenBlue Bridge gateway device automatic pulls in security updates and through the embedded ZTA HIP tunnel Bridge.
- **Zero-trust policy-managed authorizations**: Only defined paths are permitted between the OpenBlue Bridge and remote services.
- **Secure remote Management**: Technicians access to protected resources can be scheduled for specific dates and times based on authorizations.
- **Event logging**: The OpenBlue Bridge maintains a log of system events which may be exported for review.

1.3.0 Intended environment

The OpenBlue Bridge device should be installed within an equipment rack or enclosure with restricted physical access.

1.3.1 Internet Connectivity

This platform will require internet access for operation.

1.4.0 Hardening methodology

While most building automation products provide onboard security safeguards, including many secure-by-default settings, we recommend that the device is hardened according to the guidance outlined in section 2, deployment.

Generally, you should aim for a defense-in-depth strategy employing standard IT hardening methods and compensating controls as needed to compliment the base security features of each component.

1.5.0 Data flow diagram

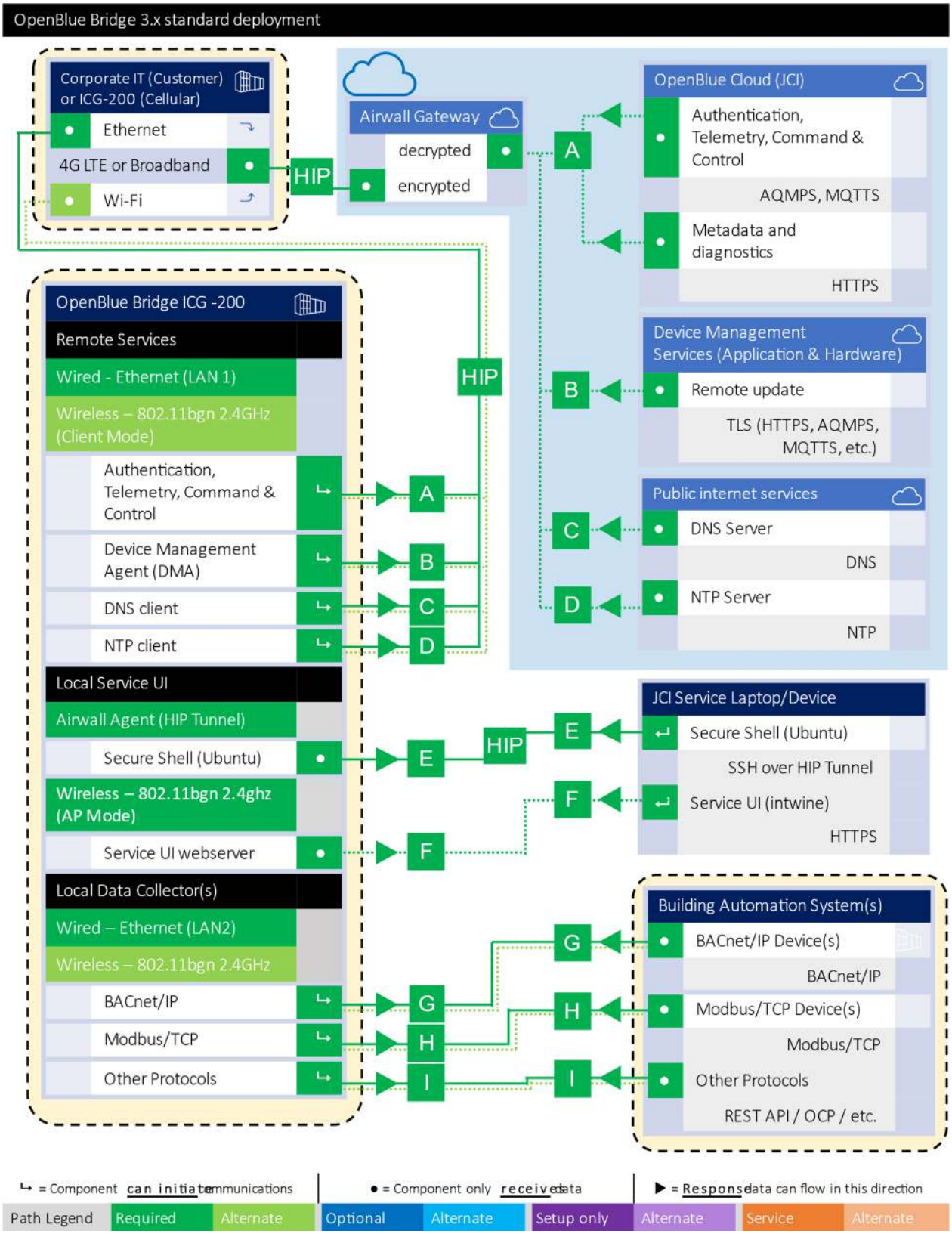
A data flow diagram (DFD) is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls, and zero-trust architectures.

The use requirements of each path should be identified as:

- Required – this path must be established for the solution to function for all supported applications
- Optional – this path is optionally required depending on the functions that will be enabled (e.g., webserver, email)
- Setup only – this path is only needed during the setup and configuration and disabling during normal operations is recommended
- Service – this path is only needed for service. A service path is typically a temporary remote service connection which is disabled during non-service periods

It is useful for someone who is not as familiar with the process to break down the communication paths to understand the processes for the basic to the more complex applications. It is helpful to group paths by function. Communication paths should be labelled so they can be referenced within the document.

Figure 1.5.0.1 OpenBlue Bridge DFD



1.5.1 Communication paths table

This table is useful to IT security groups and those configuring network devices such as switches, routers, firewalls, etc. When monitoring network traffic, the paths below illustrate the expected behavior in the system.

Figure 1.5.1.1. Communication Paths Table

OpenBlue Bridge 3.x standard deployment

Path	OpenBlue Bridge (OBB)					Direction / use requiement[2]	Connecting Component			Notes
	Function	Interface	Default Port	Default Port State[3]	Port Activity (if enabled)		Default Port [3,4]	Protocol	Internet access[1,4]	
HIP	Host Identity Protocol (HIP) Tunnel - Airwall Gateway					*Required	Device Management services			
	Control Plane (Initiate/Underlay)	Ethernet or USB Wi-Fi	8096	Enabled	On demand	↳ ▶ ◀	-	TCP TLS 1.2	Yes	
	Data Plane (Overlay)	Ethernet or USB Wi-Fi	10500	Enabled	On demand	↳ ▶ ◀	-	UDP HIP Tunnel	Yes	
A	OpenBlue Cloud (Authentication, Telemetry, Command & Control)					Required	OpenBlue Cloud			
	Data to Cloud	Ethernet or USB Wi-Fi	443	Enabled	∞	↳ ▶ ◀	443	HTTPS, AQMPS, MQTTS	*Yes	1,4
B	OpenBlue Bridge Device Updates					Required	OpenBlue Bridge Device Manager			
	Firmware update (FOTA)	Ethernet or USB Wi-Fi	443	Enabled	On demand	↳ ▶ ◀	443	TCP HTTPS	*Yes	1,4
C	DNS Client					Required	Public Internet – DNS Server			
	Host name resolution	Ethernet or USB Wi-Fi	53	Enabled	On demand	↳ ▶ ◀	53	DNS	*Yes	1,4
D	NTP Client					Required	Public Internet - NTP Server			
	Time syncronization	Ethernet or USB Wi-Fi	123	Enabled	On demand	↳ ▶ ◀	123	NTP	*Yes	1,4
E	Local Service Console (OS Maintenance)					Required	Service laptop / device (Airwall Agent)			
	Local Service Console	Ethernet or Wi-Fi	22	Enabled	∞	▶ ◀ ↵	22	SSH	*Yes	1,4
F	Local Service UI (ICG-200)					Required	Service laptop / device			
	Service UI webserver	Ethernet or Wi-Fi	443	Enabled	∞	▶ ◀ ↵	443	N/A	No	
G	Local Data Collection BACnet/IP					Optional	BACnet/IP Devices			
	BACnet/IP	Ethernet or Wi-Fi	47808	Enabled	∞	↳ ▶ ◀ ↵	-	BACnet/IP	No	
H	Local Data Collection Modbus/TCP					Optional	Modbus/TCP Devices			
	BACnet read property	Ethernet or Wi-Fi	502	Enabled	∞	↳ ▶ ◀ ↵	-	Modbus/TCP	No	
I	Local Data Collection "Others"					Optional	Other Protocols			
	BACnet read property	Ethernet or Wi-Fi	*	Enabled	∞	↳ ▶ ◀ ↵	*	*	No	

[1] Encrypted via Host Identity Protocol (HIP) tunnel in addition to Transport Layer Security (TLS) for secure communications, only outbound ports TCP 8096 and UDP 10500 are transmitted outside of the network to the cloud evironment.

[2] Application requirements are represented by the following color codes and symbols:

- ■ Green = required path
- ■ Blue = optional path
- ■ Purple = Commissioning-only path
- ■ Orange = Service path
- ↳ or ↵ These arrows indicate that the component can initiate communication in the direction of the arrow
- ▶ or ◀ These arrows indicate that the component can send response data in this direction of the arrow
- ⊙ This symbol indicates that the component only consumes data from this path.

[3] Typical default setting for connecting components

[4] Any Internet access, if used should be indirect and managed through Airwall Technology (default) and/or a Firewall

2 Deployment

This section is designed to help execute the deployment phase of your system. The contents within this section address how to initiate secure deployment for new installations, how to harden your attack surface and additional steps after commissioning required before the new or upgraded system is turned over to runtime operations.

2.1.0 Deployment overview

Security hardening begins prior to deployment with careful planning as outlined in section 1 of this guide. It is a good practice to review sections prior to deployment to fully understand the security feature set, its architecture, data flow and requirements before physically installing and making application specific configuration changes.

In this section more details are provided to help the installer prepare for deployment:

- Physical installation considerations
- Default security behavior
- Resetting factory defaults
- Considerations for commissioning
- Recommended knowledge level

Before you start the installation of your solution, consider the guidance in the following sections.

2.1.1 Physical installation considerations

Install hardware using the instructions provided in the installation guide. Keep in mind that the physical access to the device and physical installation of the device can impact the cybersecurity.

Physical access to certain devices enable actions that cannot be authenticated and logged electronically through the capabilities of this product. To prevent unauthorized access, be sure to place the device in a room, cabinet or enclosure that can restrict access (for example, mechanical lock or physical access control).

Some enclosures where the OpenBlue Bridge is installed are equipped with an optical tamper switch that you can use to send and log electronic alerts regarding physical tampering of the installation. Consider using protective electric wire conduits when communication wires with paths through areas of lower trust.

2.2.0 Hardening

While many products include secure-by-default safeguards, additional hardening is usually required to meet the security requirements of the target environment. It is important to apply to the correct level of protection as warranted by the customer policies and government regulations that may govern the application security settings for this deployment.

2.2.1 Hardening Checklist

- ☐ Hardening Step 1: Logging into the OpenBlue Bridge device
- ☐ Hardening Step 2: Update the Network Configuration
- ☐ Hardening Step 3: Change the Username and Password
    - ☐ Hardening Step 3.1: Change the NTP and Timezone
- ☐ Hardening Step 4: Configure the Security Settings
- ☐ Hardening Step 5: Review Audit Logs
- ☐ Hardening Step 6: Setup Airwall Configuration

2.2.2 Local Configuration App

The ICG-200 local configuration app, within the OpenBlue Bridge, is a web tool that allows users to customize the network configuration settings on their Bridge hardware. The tool is useful for kitting, initial installation, and ongoing diagnostics/maintenance.

Step 1: Logging into the OpenBlue Bridge device

To access the app and configure your OpenBlue Bridge simply connect to the OpenBlue Bridge's WiFi SSID or Ethernet port from any Internet enabled device (e.g., phone, tablet, or PC).

1) Locate the network: Using a WiFi enabled device, open the window that shows available Wi- Fi networks. The ICG-200 WiFi network will appear on the list. Select the network (SSID) shown on the label.

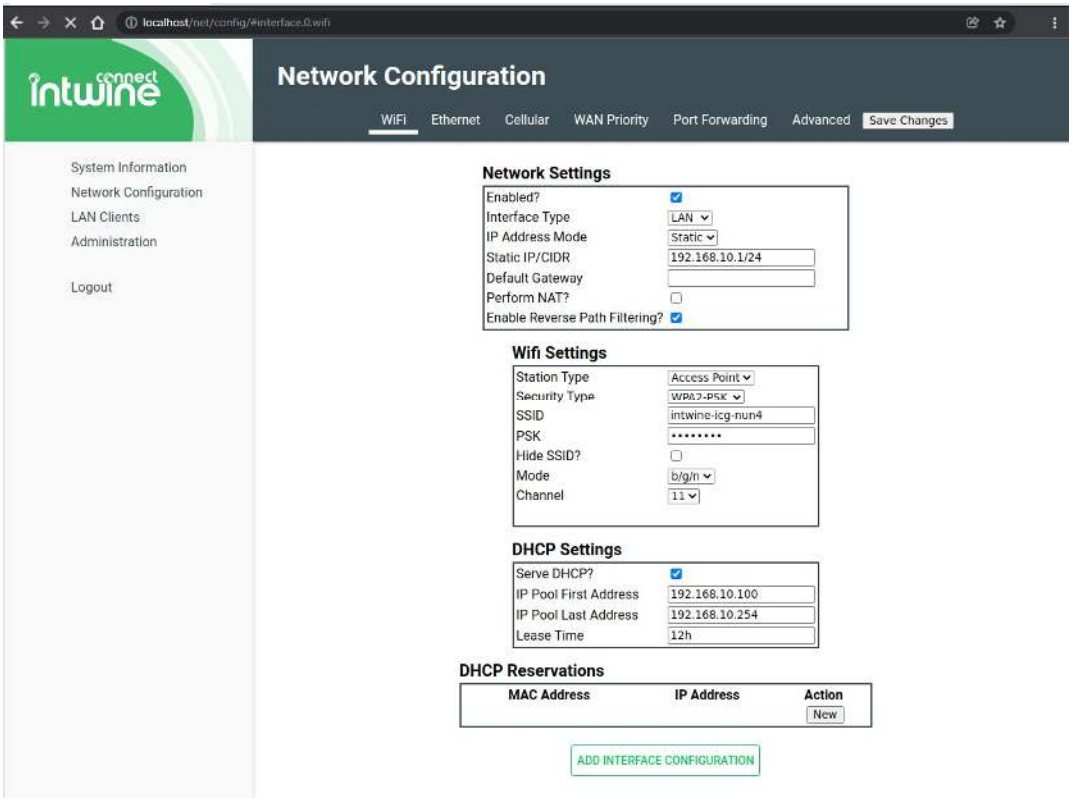
2) Connect to WiFi: After selecting the ICG-200 WiFi network, you will need to input the default WiFi password shown on the label.

2.2.3 Network Configuration

Step 2: Update the Network Configuration

For those users that require more complex configurations, the below section show the advanced settings of the OpenBlue Bridge device and best practices to ensure appropriate configuration.

All headings refer to a specific tab in the **Network Configuration** page and explain its function in detail.



1) If not using Wi-Fi, deselect the "Enable Wi-Fi" checkbox.
2) If using Wi-Fi, change the SSID and PSK.

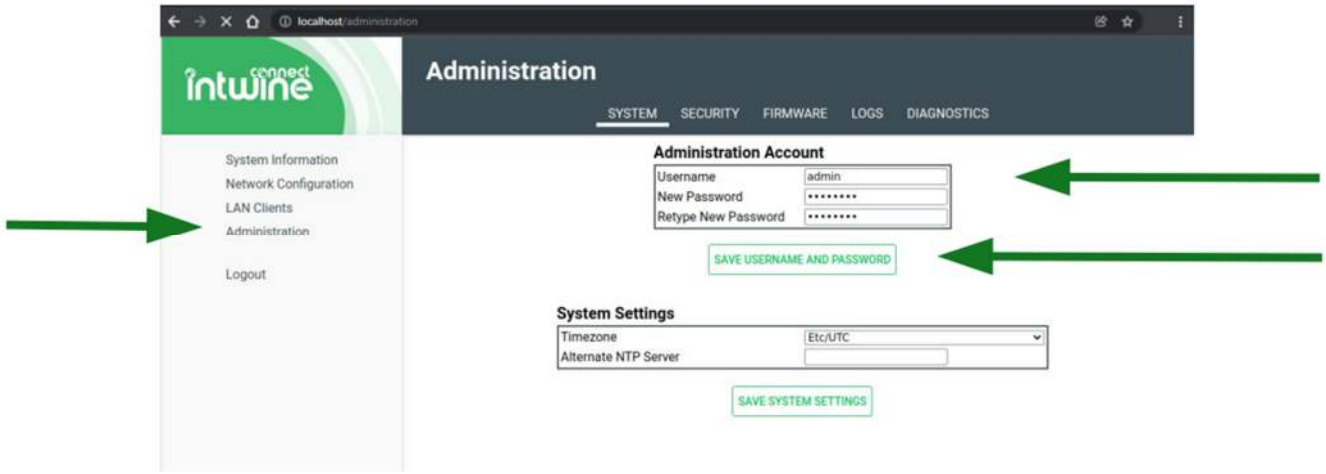
2.2.4 Changing Passwords

To change existing passwords and/or usernames, follow the below instructions.

NOTE: Changing usernames/passwords will replace the information on the label. Be sure to WRITE IT DOWN and store in a SECURE LOCATION

Hardening Step 3: Change the Username and Password

To change the administration username and password, click on the **Administration** tab on the left-hand side of your browser. Change the username and password using the text boxes provided.



NOTE: Changes to the admin username and password will keep you logged in but will change upon logging out.

2.2.4.1 Change NTP and Timezone

Step 3.1: Change the NTP and Timezone

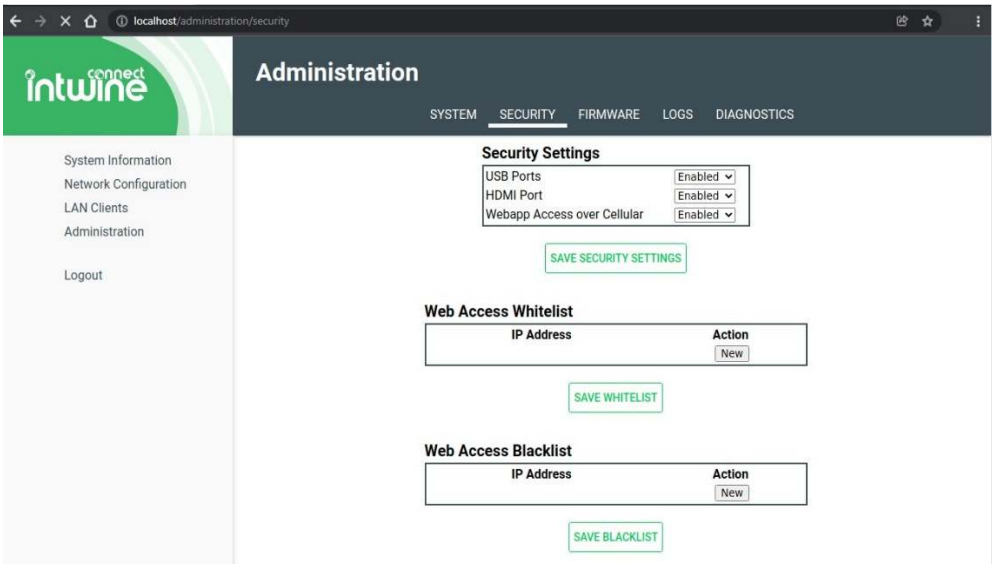
NTP allows synchronization of system time with a reliable server, ensuring accurate timekeeping. Adjusting the timezone sets the local time reference for the system. These settings are crucial for accurate timestamps, scheduling, and system functionality.

Note: NTP should be common for the systems this OpenBlue Bridge is communicating with to ensure a consistent timestamp for all components. Work with the local network administrators to determine the best NTP server to enter.

2.2.5 Security

Step 4: Configure the Security Settings

The Security tab allows you to customize additional security options on the OpenBlue Bridge device. You can disable the use of USB ports, the HDMI interface, or prevent the local configuration webapp from being accessed via the cellular network.



Ensure USB and HDMI tabs are disabled.

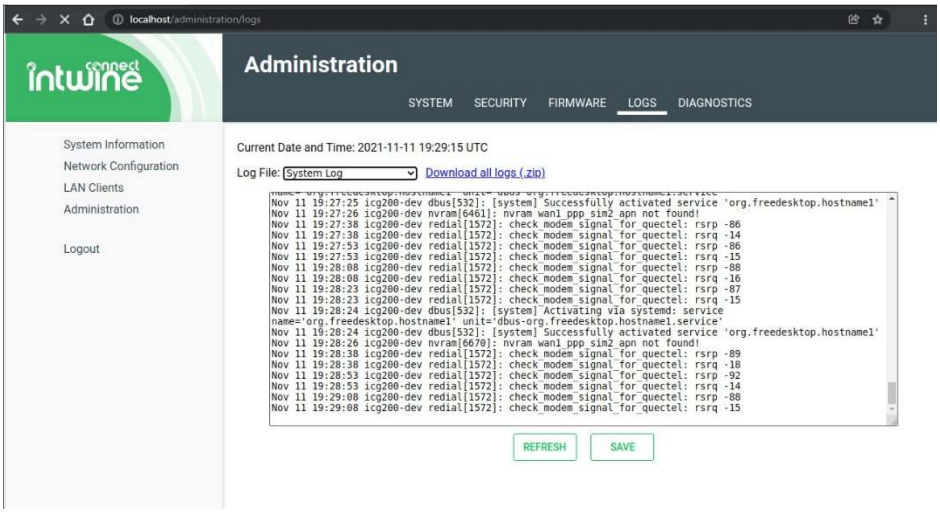
2.2.6 OpenBlue Bridge audit log:

The audit log provides valuable information that can be used for both functional troubleshooting and security investigations.

Step 5 Review Audit Logs

The audit log provides a user readable text file that shows actions taken on the local ICG user interface.

The audit log may be downloaded to the laptop or mobile device connecting to the ICG by selecting the **Download** button.



The Logs tab allows users to take a look at or download the logs. The available log files are –

System Log, Application Framework, Network Config daemon, ICG Log.

2.2.7 Airwall

Step 6: Setup Airwall Configuration

Step 1: Configure Customer Firewall

- Prepare to configure the customer's firewall to allow the necessary communication for the Airwall.

Step 2: Obtain Conductor URL and Relay IP Address

- Contact the Airwall Conductor administrator to obtain the Conductor URL and Relay IP address required for configuration.

Step 3: Configure Firewall Rules

- Configure outbound rules on the customer's firewall as follows:
    - Allow outbound traffic on TCP Port 8096 to the Conductor URL.
    - Allow outbound traffic on UDP Port 10500 to the Relay IP address.
    - Ensure that all other ports and addresses are closed for security purposes.

These steps ensure that the Airwall is commissioned and configured correctly to establish connections with the Conductor URL and Relay IP address while maintaining firewall security.