OpenBlue

Hardening Guide

GPS0023-CE-EN

Rev A

Revised 2024-07-22

Introduction

Our solutions provide peace of mind to our customers with a holistic cyber mindset beginning at the initial design concept, which continues throughout product development, and even into deployment at our customers' local premises. 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 for the components used exclusively to support the OpenBlue Platform solutions (e.g. OpenBlue Bridge). For the hardening of the systems and devices which connect to the OpenBlue Bridge, please refer to their respective hardening guide or the Universal Hardening Guide as applicable.

This guide covers the following applications of OpenBlue:

- OpenBlue Enterprise Manager

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

1. Planning	2. Deployment
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

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

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.

Contents

1 Planning

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

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

1.1.0 OpenBlue Platform overview

The OpenBlue Platform is a flexible, scalable platform that reaches across silos to gather data of all kinds from disparate sources, stores it securely and standardizes the data into reportable formats. As a result, applications that use the platform also help building professionals extend the life of their HVAC equipment, proactively manage security risk, and efficiently maintain a comfortable environment for building occupants. The platform provides engineering efficiencies through reuse, addressing common concerns through shared components. More importantly the platform enables integration and interoperability.

The OpenBlue Platform has an edge component called OpenBlue Bridge and a cloud component called the OpenBlue Cloud Platform.

NOTE: The OpenBlue Cloud Platform is managed and hardened entirely by Johnson Controls. Therefore, there are no hardening steps included in this guide for that cloud component.

OpenBlue Bridge

OpenBlue Bridge (OBB) is the on-premises edge component of the OpenBlue Platform and acts as a secure gateway to gather data and send commands to the on-premises sub-systems. OBB includes a library of standard protocol connectors that enable integration with many sub-systems such as HVAC, lighting, and occupancy sensor systems. The OBB also features an SDK for custom system integration and development.

In addition to the southbound integrations to on-premises data sources, the OBB communicates via secure HIP tunnel with OpenBlue Cloud.

OpenBlue Cloud Platform

OpenBlue Cloud Platform is the cloud side of the platform that acts as a secure landing point for your OBB connection. The OpenBlue Cloud Platform provides various services to enable OpenBlue applications such as OpenBlue Enterprise Manager (OBEM).

1.1.1 OpenBlue Applications Overview

OpenBlue Enterprise Manager

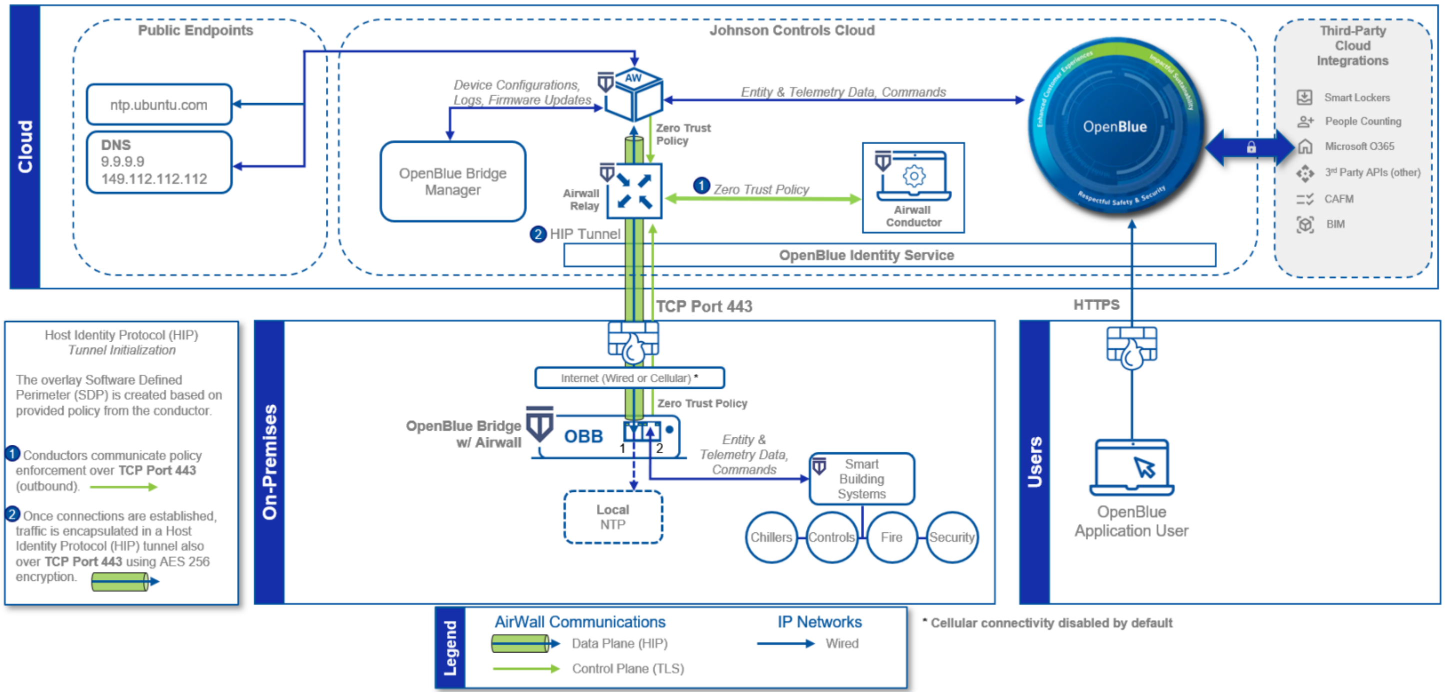
OpenBlue Enterprise Manager (OBEM) is a building data analytics application running on the OpenBlue cloud that pro-actively monitors and analyzes building energy, equipment, and space data to identify issues, faults, and opportunities for improved energy performance, operational savings, and tenant experience. OBEM includes a comprehensive suite of apps delivered through a single pane of glass, empowering customers to drive ESG attributes that improve property value and tenant revenue, while driving sustainability goals.

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

1.1.2 Deployment Architecture

The OpenBlue Bridge is comprised of hardware and software components working closely together to collect the data from and pass commands to on-site systems and sub-systems.

Figure 1.1.2.1: Typical OpenBlue Bridge deployment architecture diagram



The overlay Software Defined Perimeter (SDP) is created based on provided policy from the conductor.

1 Conductors communicate policy enforcement over **TCP Port 443** (outbound).

2 Once connections are established, traffic is encapsulated in a Host Identity Protocol (HIP) tunnel also over **TCP Port 443** using AES 256 encryption.

* Cellular connectivity disabled by default

1.1.3 Components

Typical OpenBlue Bridge core components include the following items:

OpenBlue Bridge device

The OpenBlue Bridge device, known as the OpenBlue Bridge (OBB), is an edge gateway built on the Intwine Connected Gateway (ICG-200). It functions as both a physical layer gateway and an upper-level application gateway. It allows edge computing and provides connectivity for on-premises systems and sub-systems. The following subcomponents are a part of the OpenBlue Bridge:

1. *OpenBlue Bridge Connectors*

   OpenBlue Bridge Connectors offer connectivity to IoT systems and sub-systems.
2. *Airwall Gateway*

   OpenBlue Bridge includes an Airwall Gateway as part of the OpenBlue zero-trust architecture (ZTA). The Airwall Gateway is a virtual air-gap solution that makes 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.

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

3. *Bridge Manager*

   The Bridge Manager is the OpenBlue Bridge configuration tool. It is a browser-based interface used to configure the OBB for initial installation. It is also used for firmware updates, ongoing diagnostics, and maintenance of the OBB.

For more information on the OpenBlue Bridge, please visit the OpenBlue Bridge Datasheet

1.1.4 Supporting Components

Supporting components are those which are necessary for system operations but are not within the targeted scope of this document. In some cases, it may not be feasible for Johnson Controls to provide the following components because they are intrinsically related to the environment the OpenBlue Bridge gateway is installed to. This solution is supported by the following components:

- *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.

- *Local 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 optionally 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 a public NTP server, ensuring accurate and consistent timekeeping for all on-premises components that synchronize time with the same local server.

- *Airwall Conductor*

  Part of Johnson Controls Zero Trust OpenBlue Airwall offering – the Airwall Conductor is a cloud-based software that acts as a broker for the Airwall overlay network. No network activity is permitted unless explicitly verified by the Airwall Conductor. Thus, the connection from on-premises OpenBlue Bridge to the Johnson Controls-hosted OpenBlue Cloud Platform is protected by a permanent zero trust identity management system.

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

1.2.0 Security feature set

This section describes the security features within OpenBlue Bridge:

Section	Type	Feature name
1.2.1	Secure Communications	AES 256 encrypted HIP site to cloud
		Hidden IP Addresses
		Outbound Initiation
		Zero-trust policies
1.2.2	Remote Management	Over the Air firmware/software updates
		Granular remote access for technicians
1.2.3	Event Logging	System events
1.2.4	Device Enhancements	Custom built OS
		Secure Boot
		Disk Encryption
		Trusted Execution Environment (TEE)
		Ongoing Kernel updates
		Local Web User Interface for configuration

1.2.1 Secure Communications

AES 256 encrypted HIP site to cloud: Collected data is encrypted at the OpenBlue Bridge (OBB) and is sent to the cloud using Transport Layer Security (TLS) encapsulated within an AES 256 encrypted HIP tunnel.

Hidden IP Addresses: The IP address for the OpenBlue Bridge is not exposed to the internet.

Outbound Initiation: Only one outbound port is required to initiate the site-to- cloud data exchange.

Zero-trust policies: Only explicitly defined communication paths are permitted between the OpenBlue Bridge and remote services.

1.2.2 Johnson Controls Remote Monitoring and Diagnostic Service

Over the Air firmware/software updates: The OpenBlue Bridge is designed to receive over-the-air updates, enabling seamless firmware and software updates. This ensures that your embedded gateway device is always up to date with the latest security patches and improvements, without disrupting your operations.

Granular remote access for technicians: Johnson Control technicians' access to protected, remote resources can be granularly assigned and scheduled for specific dates and times based on authorizations.

1.2.3 Event Logging

System events: The OpenBlue Bridge maintains a log of system events which may be exported for review.

1.2.4 Device Enhancements

Custom built OS: The OpenBlue Bridge operates on a custom-built, minimal base image Linux operating system, specifically tailored to meet the requirements of our platform. This specialized OS includes only the necessary drivers and packages for optimal performance and security.

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

Secure Boot: To prevent unauthorized modifications, the OpenBlue Bridge is equipped with secure boot functionality. This ensures that the device will only boot with signed firmware provided by Johnson Controls, maintaining the integrity of the system.

Disk Encryption: OpenBlue Bridge employs AES-256 disk encryption, safeguarding your data even in the event of physical theft. This encryption ensures that your information remains secure and inaccessible to unauthorized individuals.

Trusted Execution Environment (TEE): The OpenBlue Bridge incorporates a trusted execution environment, allowing certain sensitive workloads to run in a logically isolated portion of the CPU and memory. This TEE utilizes run-time encryption, enhancing the confidentiality of your data and protecting against potential breaches.

Ongoing Kernel updates: We have a dedicated team of security developers who work tirelessly to update the kernel of our device images. By remaining close to the leading edge of the active branch, we ensure that your OpenBlue Bridge benefits from the latest security enhancements.

Bridge Web User Interface for configuration: Web user interface available for initial configuration and hardening of the OpenBlue Bridge device.

1.3.0 Intended environment

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

For more information on the OpenBlue Bridge Gateway, please visit the OpenBlue Bridge Datasheet

1.3.1 Internet and Network connectivity

The OpenBlue Bridge will also require connectivity to public cloud endpoints so that it can establish a secure connection to the OpenBlue Cloud Platform via Airwall. Because of this consideration, Johnson Controls recommends deploying your OpenBlue Bridge behind a suitable network perimeter defense solution with internet access.

Airwall is a cloud-based, software-defined networking solution built upon Zero Trust principles. The Airwall cloud solution is hosted and managed by Johnson Controls to provide secure connectivity between OpenBlue customer sites and OpenBlue Cloud.

For the OpenBlue Bridge to initiate connectivity with our Airwall Zero Trust relays, the end-user must first allow the following rules in their network perimeter defense solution:

Please see **1.5.1 Port Assignments** later in the document for port details.

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

1.4.0 Hardening methodology

While most building automation products provide onboard security safeguards, including many secure-by-default settings, we recommend that the gateway 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

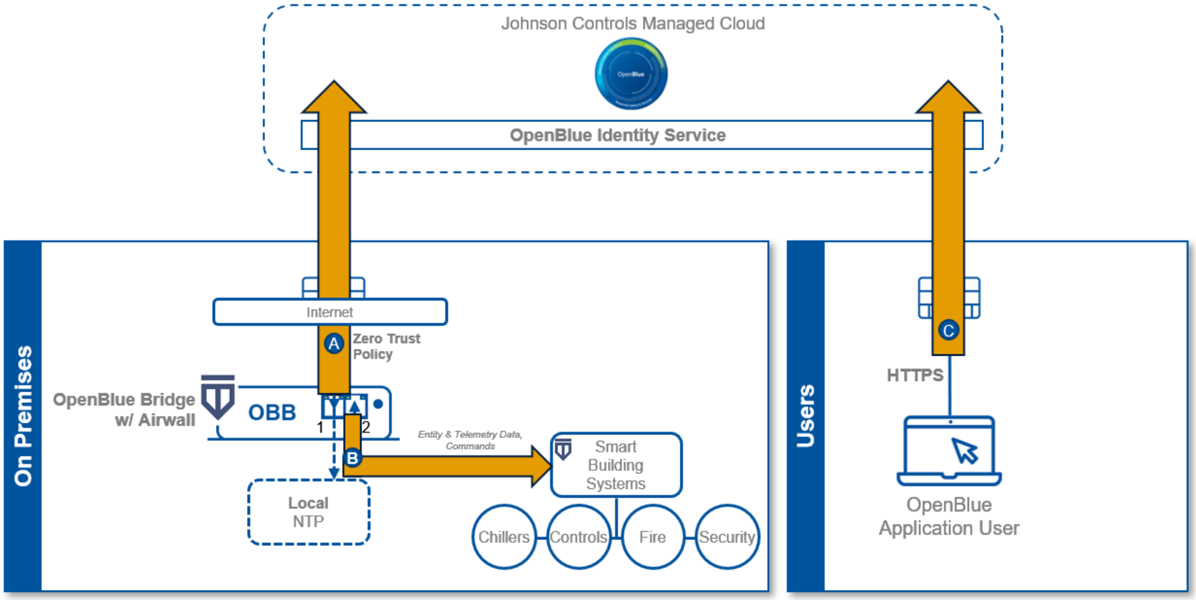
A data flow diagram (DFD) is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls, and zero-trust architectures.

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 Data Flow Diagram


Johnson Controls Managed Cloud
OpenBlue
OpenBlue Identity Service
On Premises
Internet
A
Zero Trust Policy
OpenBlue Bridge w/ Airwall
OBB
1
2
B
Entity & Telemetry Data, Commands
Smart Building Systems
Local NTP
Chillers
Controls
Fire
Security
Users
C
HTTPS
OpenBlue Application User

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

1.5.1 Port Assignments

Path A – LAN1/WAN: Outbound to Internet

All traffic outbound from the OpenBlue Bridge is encapsulated in a Host Identity Protocol tunnel and encrypted from edge device to the cloud.

Direction	Port	Transport Protocol	Protocol	Required	End Point	Purpose
Outbound	443	TCP	WSS	Yes	to all regional Airwall Relays (contact Johnson Controls for list)	Zero Trust – Control and Data
Outbound	53	UDP	DNS	Yes	9.9.9.9 and 149.112.112.112	DNS
Outbound	67, 68	UDP	DHCP	Optional	DHCP Server	DHCP IP assignment*
Outbound	123	UDP	NTP	Yes	ntp.ubuntu.com	Network Time sync
Outbound			ICMP	Optional	8.8.8.8	

*Static IP address can be provided per deployment, contact your Johnson Controls Account or Branch Representative for more information

Path B – LAN2: to Building Systems and local IT

These inbound connections can be configured from sources trusted by the end-user. Certain inbound connections to various endpoints are required to initialize the OpenBlue Bridge, while others may simply improve functionality of the device.

Standard Port	Transport Protocol	Protocol	Required	End Point	Purpose
47808	UDP	BACnet	Optional	BACnet Connector	BACnet protocol communications
1883	TCP	MQTT	Optional	MQTT Connector	MQTT protocol communications
4840	TCP	OPC UA	Optional	OPC Agent	OPC UA protocol communications
502	TCP	Modbus	Optional	Modbus	Modbus protocol communications

Path C: Client Connections to OpenBlue

This is a typical HTTPS connection up to the OpenBlue Enterprise Manager application hosted in the Johnson Controls cloud. This endpoint is the URL that the OBEM users will navigate to via their browsers.

Direction	Port	Transport Protocol	Protocol	Required	Browser End Point	Purpose
Outbound	443	TCP	HTTPS	Yes	jemprod-ui.myenterprisemanagement.com	OpenBlue Enterprise Manager – Browser Experience

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

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 OpenBlue Bridge per instructions in the official installation guide: OpenBlue Bridge Installation Guide

Please 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 can 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.

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

2.2.1 Hardening Checklist

□ Hardening Step 1: Update the Network Configuration

□ Hardening Step 2: Change the Username and Password

□ Hardening Step 3: Change the NTP and Time zone

□ Hardening Step 4: Configure the Security Settings

□ Hardening Step 5: Review Audit Logs

□ Hardening Step 6: Review Firewall Rules

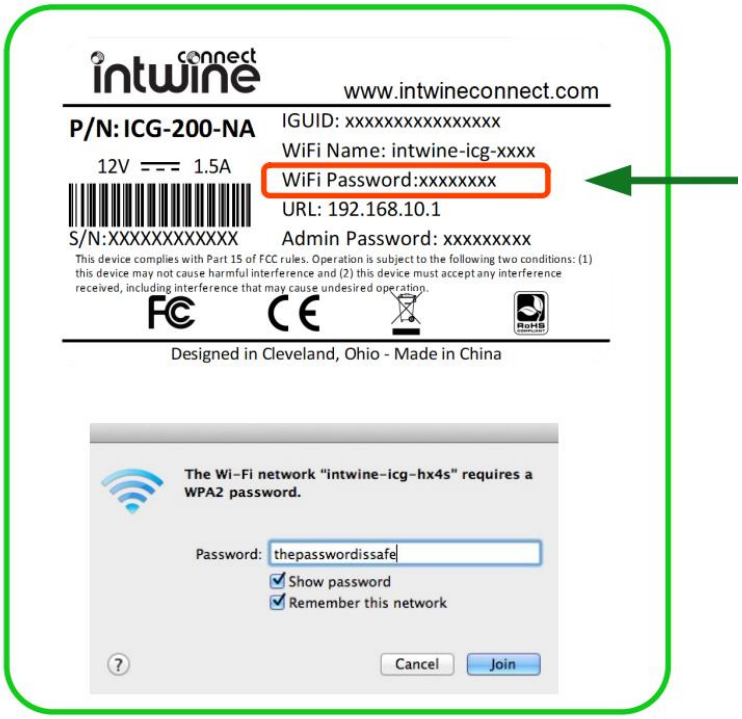
Logging into the OpenBlue Bridge Edge Manager:

To configure your OpenBlue Bridge for the first time, simply connect to the OpenBlue Bridge's Wi-Fi SSID or Ethernet port from any Internet enabled device (e.g., phone, tablet, or PC).

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

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

Figure 2.2.1.1



www.intwineconnect.com

P/N: ICG-200-NA

12V 1.5A

S/N:XXXXXXXXXXXX

IGUID: xxxxxxxxxxxxxxxx

WiFi Name: intwine-icg-xxxx

WiFi Password:xxxxxxxx

URL: 192.168.10.1

Admin Password: xxxxxxxxx

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Designed in Cleveland, Ohio - Made in China

The Wi-Fi network "intwine-icg-hx4s" requires a WPA2 password.

Password: thepasswordissafe

☑ Show password

☑ Remember this network

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

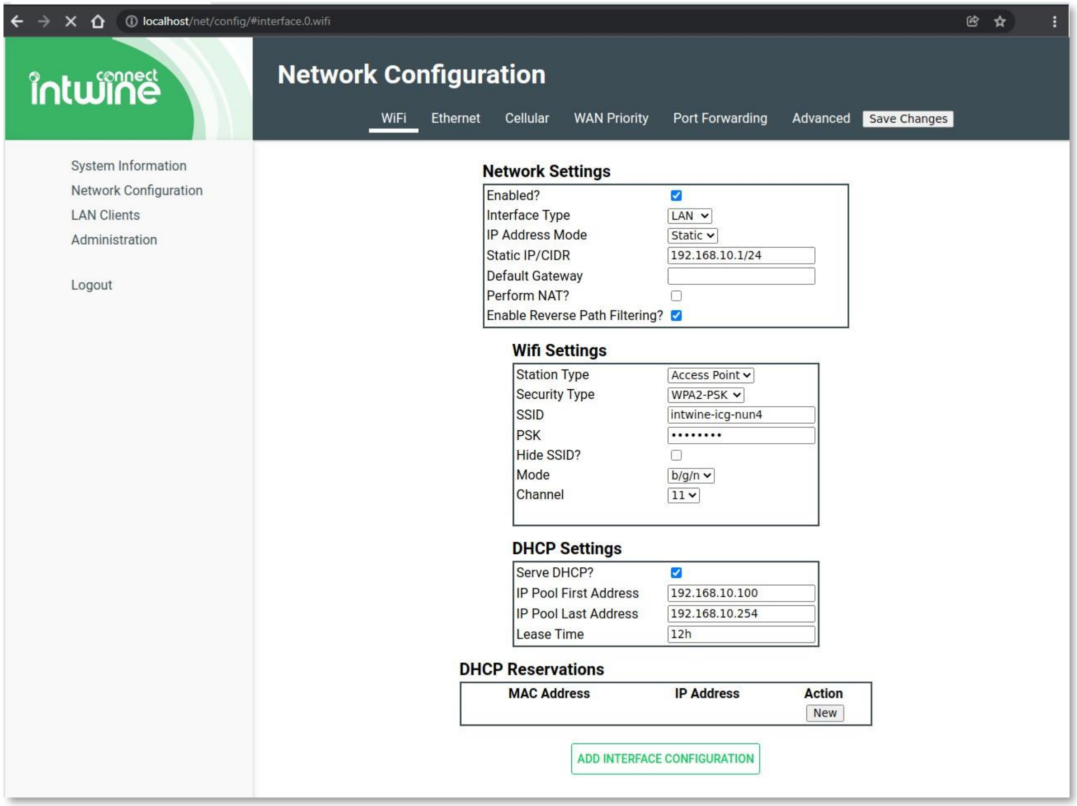
2.2.2 Network Configuration

Hardening Step 1: 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.

Figure 2.2.2.1



Network Configuration

Network Settings

Enabled?	☑
Interface Type	LAN
IP Address Mode	Static
Static IP/CIDR	192.168.10.1/24
Default Gateway	
Perform NAT?	☐
Enable Reverse Path Filtering?	☑

Wifi Settings

Station Type	Access Point
Security Type	WPA2-PSK
SSID	intwine-icg-nun4
PSK	••••••••
Hide SSID?	☐
Mode	b/g/n
Channel	11

DHCP Settings

Serve DHCP?	☑
IP Pool First Address	192.168.10.100
IP Pool Last Address	192.168.10.254
Lease Time	12h

DHCP Reservations

MAC Address	IP Address	Action
		New

If not using Wi-Fi, deselect the "Enabled?” checkbox. Please keep in mind that you will be disconnected from the device if you are accessing the Edge Manager via WiFi.

If using Wi-Fi, change the SSID and PSK.
Explicit steps listed for any action we are prescribing through local bridge manager.

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

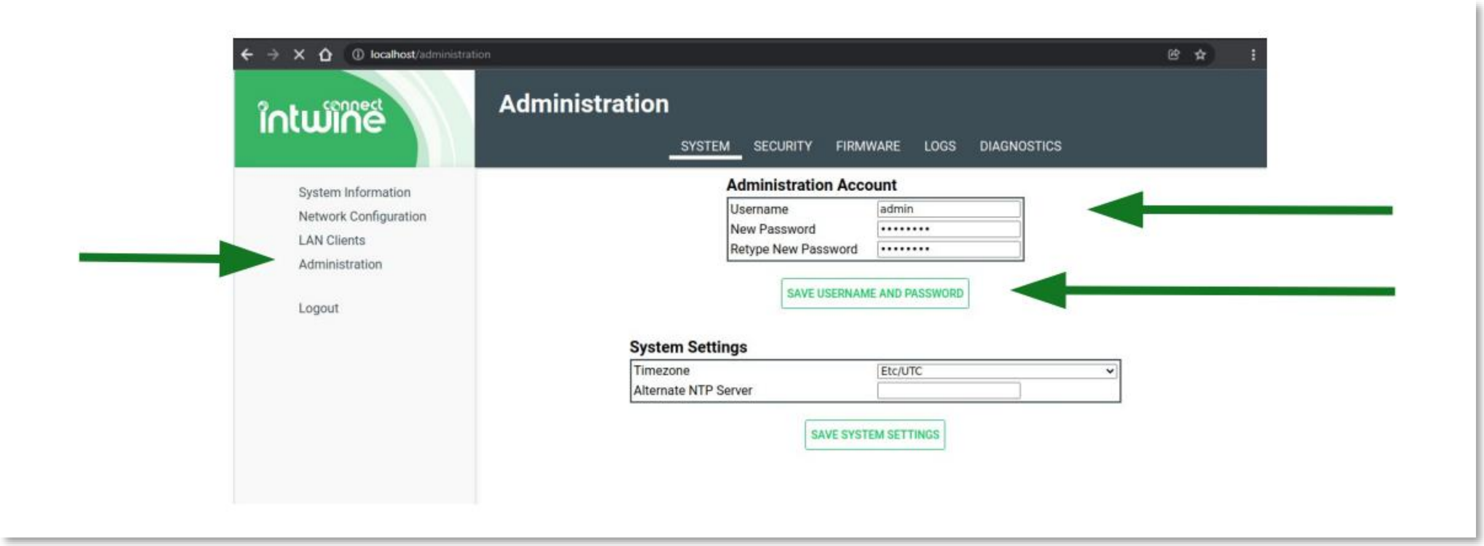
2.2.3 Changing Passwords

NOTE: Changing usernames/passwords will replace the information on the label. It is recommended to replace with a strong password, at least 15 characters, and storing it within a password manager or a secure place of the end-user’s choosing.

Hardening Step 2: 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.

Figure 2.2.3.1



Administration

Administration Account

Username	admin
New Password	••••••••
Retype New Password	••••••••

System Settings

Timezone	Etc/UTC
Alternate NTP Server	

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

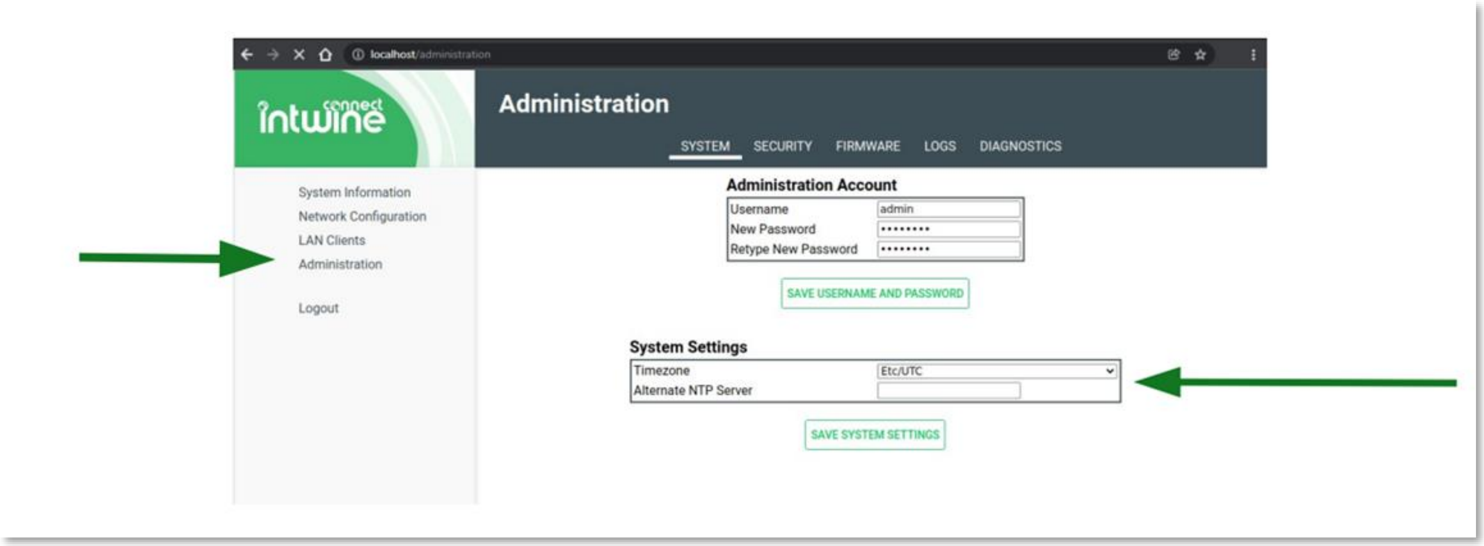
2.2.4 Configuring NTP and Clock settings

Hardening Step 3: Change the NTP and Time zone

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

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

Figure 2.2.4.1



Administration Account

Username	admin
New Password	••••••••
Retype New Password	••••••••

System Settings

Timezone	Etc/UTC
Alternate NTP Server	

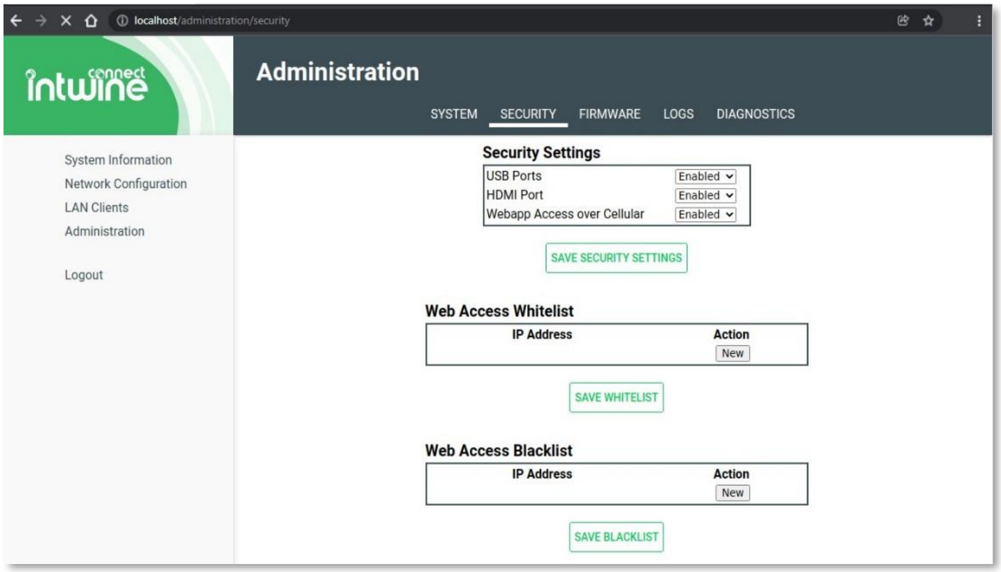
Note: NTP should be common for the systems this OpenBlue Bridge is communicating with to ensure a consistent timestamp for all components. Work with the local network administrators to determine the best NTP server to enter.

2.2.5 Security

Hardening 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.

Figure 2.2.5.1



Security Settings

USB Ports	Enabled
HDMI Port	Enabled
Webapp Access over Cellular	Enabled

Web Access Whitelist

IP Address	Action
	New

Web Access Blacklist

IP Address	Action
	New

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

Ensure USB and HDMI tabs are disabled.

2.2.6 OpenBlue Bridge device audit log:

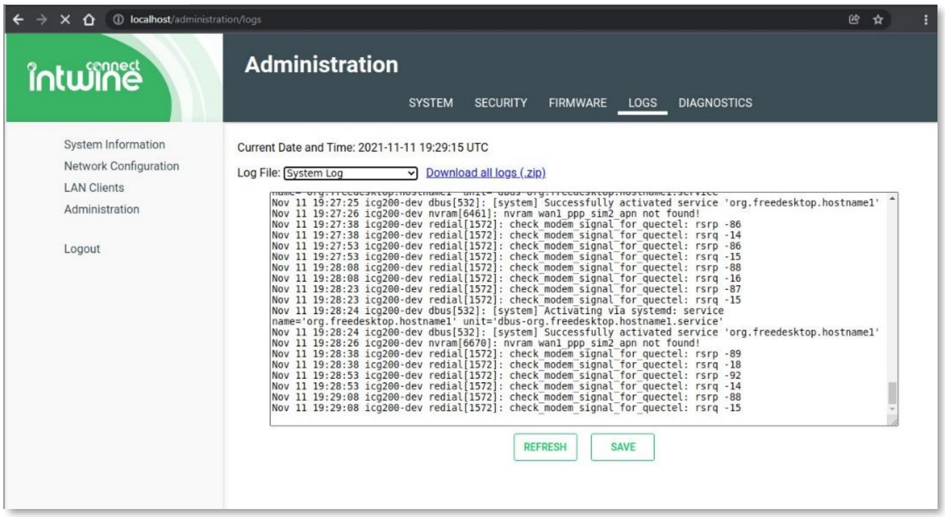
The audit log provides valuable information that can be used for both functional troubleshooting and security investigations.

Hardening 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.

Figure 2.2.6.1



Current Date and Time: 2021-11-11 19:29:15 UTC

Log File: System Log

```
Nov 11 19:27:25 icg200-dev dbus[532]: [system] Successfully activated service 'org.freedesktop.hostname1'
Nov 11 19:27:26 icg200-dev nvram[6461]: nvram wan1_ppp_sim2_apn not found!
Nov 11 19:27:38 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrp -86
Nov 11 19:27:38 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrq -14
Nov 11 19:27:53 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrp -86
Nov 11 19:27:53 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrq -15
Nov 11 19:28:08 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrp -88
Nov 11 19:28:08 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrq -16
Nov 11 19:28:23 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrp -87
Nov 11 19:28:23 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrq -15
Nov 11 19:28:24 icg200-dev dbus[532]: [system] Activating via systemd: service
name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Nov 11 19:28:24 icg200-dev dbus[532]: [system] Successfully activated service 'org.freedesktop.hostname1'
Nov 11 19:28:26 icg200-dev nvram[6670]: nvram wan1_ppp_sim2_apn not found!
Nov 11 19:28:38 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrp -89
Nov 11 19:28:38 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrq -18
Nov 11 19:28:53 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrp -92
Nov 11 19:28:53 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrq -14
Nov 11 19:29:08 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrp -88
Nov 11 19:29:08 icg200-dev redial[1572]: check_modem_signal_for_quectel: rsrq -15
```

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 Network Perimeter Security:

Because the OpenBlue Bridge is connecting to both on-premises equipment and the Johnson Controls cloud (through Airwall), it is highly recommended that you place the device behind suitable network perimeter security such as a firewall or proxy server.

In some cases, the end-user may also wish to place a firewall on both sides of the OpenBlue Bridge, to provide added assurance that only the expected data packets are able to flow through the system.

Hardening Step 6: Review Firewall Rules

Sections **1.3.1 (Internet and Network Connectivity)** and **1.5.0 (Data Flow Diagram)** provide the expected communications and firewall rules that will need to be permitted to establish connectivity holistically through the system.

It is recommended that you review the network security requirements of the end-user environment and use the

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.

details within the tables and diagrams in the mentioned sections to ensure that the necessary rules are in place in your network perimeter solutions. **The assumption is that a firewall would be set to deny by default, but then we must allow these minimal ports and endpoints to be permitted to establish normal functionality.**

© 2024 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice.