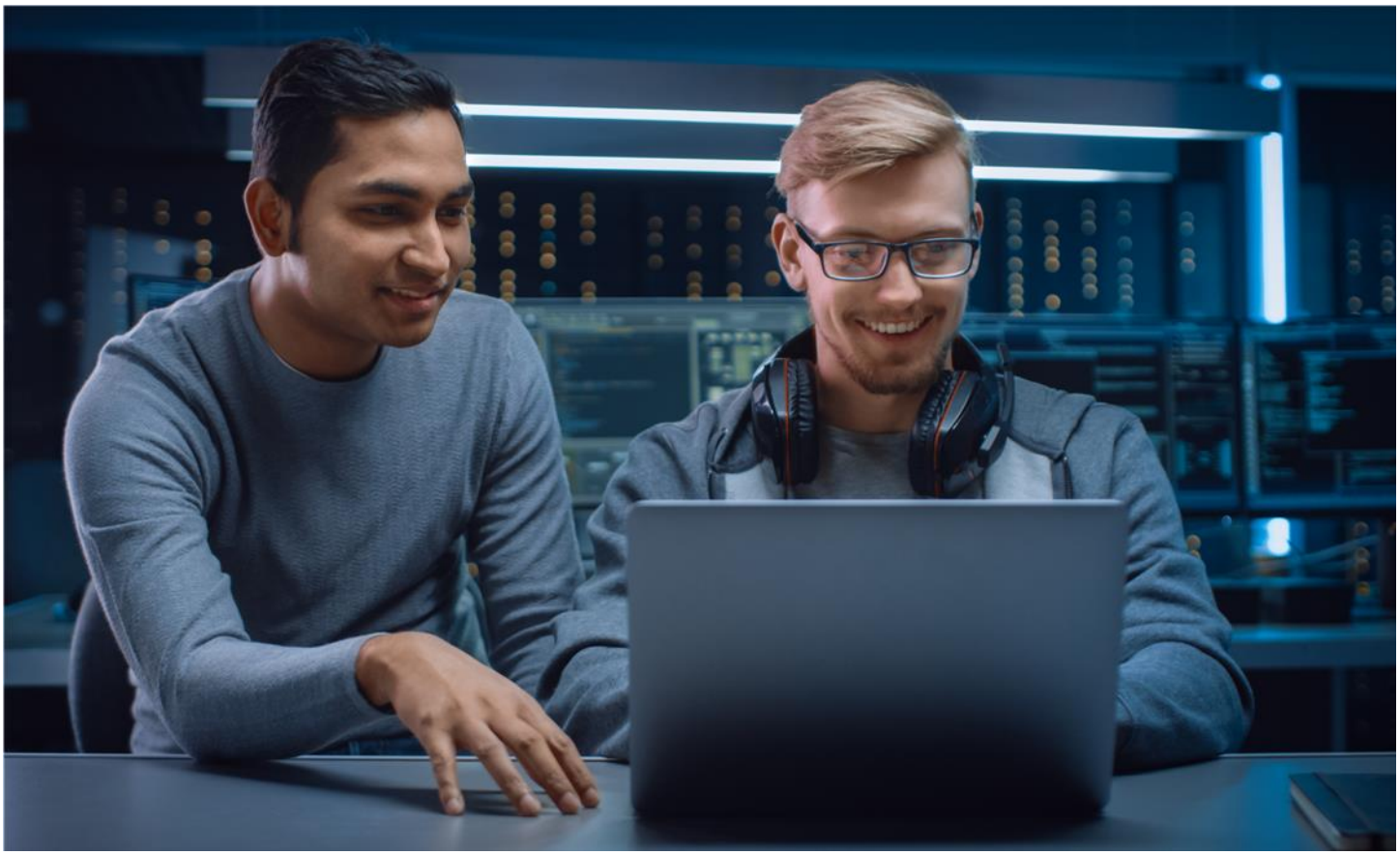
OpenBlue

OpenBlue Bridge

Hardening Guide



GPS0023-CE-EN

Version 2.12

Rev B

Revised 2024-18-07

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 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

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.

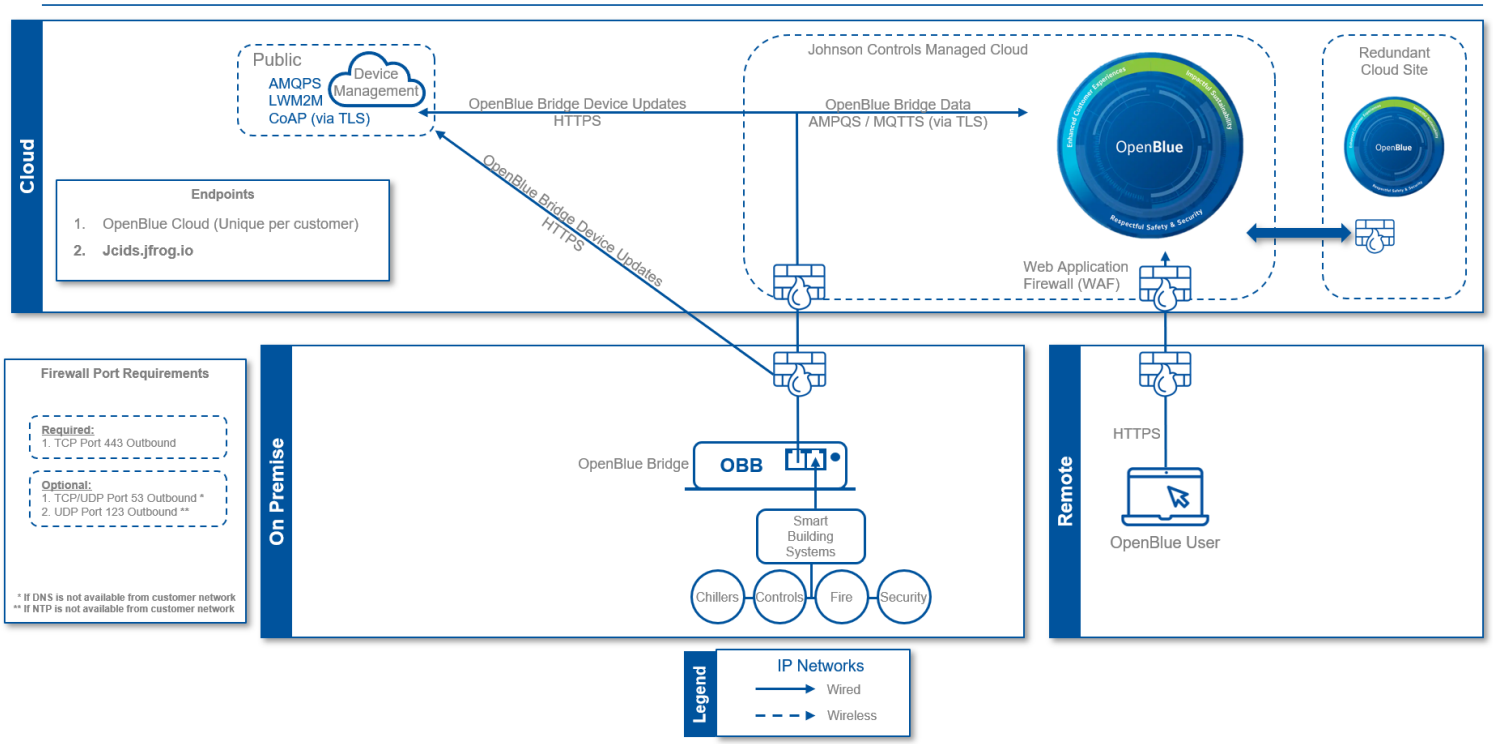
1.1.0 OpenBlue Bridge overview

OpenBlue Bridge is a software gateway that provides edge-to-cloud data communication. OpenBlue Bridge collects data from building systems and assets that are required for use in OpenBlue Cloud applications. The Bridge has a library of API and protocol connectors to support integration to the building systems and assets.

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

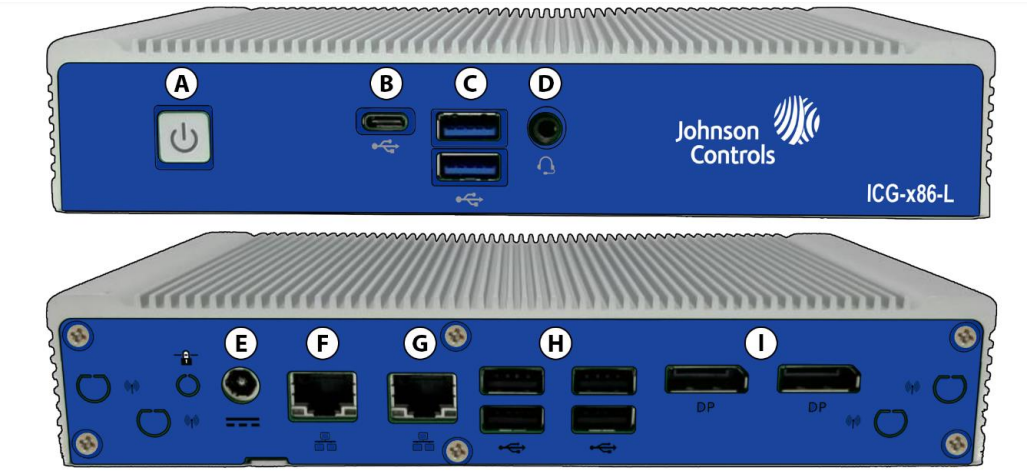


1.1.2 Components

Typical OpenBlue Bridge system core components include the following items:

OpenBlue Bridge Device

This is the OpenBlue Bridge platform Ubuntu server which is installed on dedicated x86 hardware (ICG-x86-L) with operating system version 2.0.



Callout	Description
A	Power on and power off
B	USB Type C
C	USB 3.2 (2 ports)
D	Headphones
E	Power connector
F	Gb Ethernet for WAN connection
G	Gb Ethernet for LAN connection
H	USB 2.0 (4 ports)
I	Ports for DisplayPort cable to computer monitor (2 ports)

OBB Connectors

OBB Connectors offer connectivity using various protocols for smart buildings and IoT systems. These connectors are enabled as needed to support bridge connections.

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 inclusion of a local Network Time Protocol (NTP) server is configurable within the OpenBlue Bridge. This configuration allows the Bridge to synchronize its time with the local NTP server, ensuring accurate and consistent timekeeping.

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.

1.2.1 Secure Shell (SSH) Hardening (Version 2.0)

The secure Shell is hardened as follows:

- SSH port has been configured to 8922
- No root login is permitted
- The default user account “obb” is the only user permitted to login via SSH
- SSH Protocol 2 is utilized with SSH Protocol 1 disabled
- X11 Forwarding is disabled
- Login grace period is set to 2 minutes
- Terminal timeout for no user interaction is 10 minutes (3 warnings given)

1.3.0 Intended environment

The OBB 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

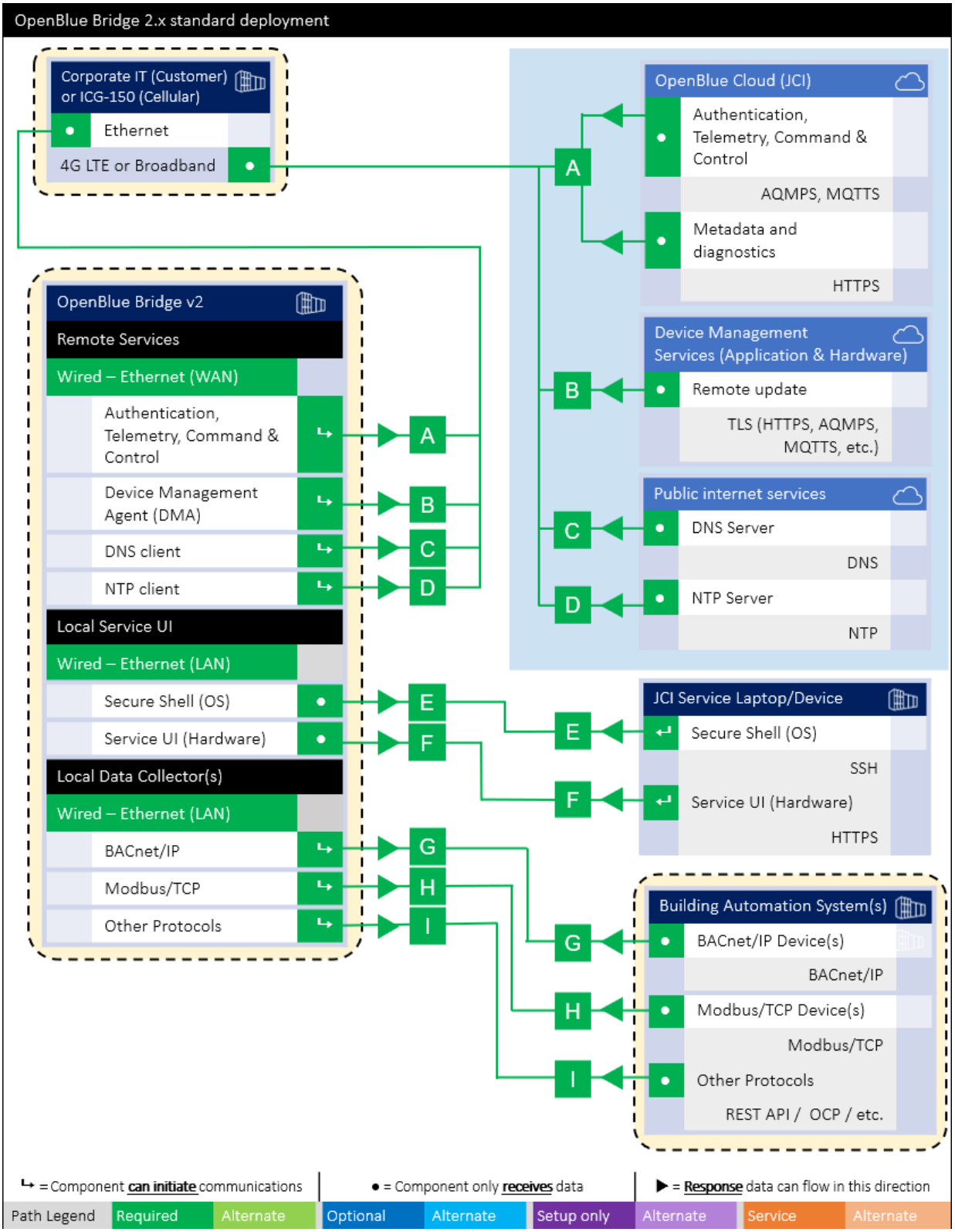
A data flow diagram (DFD) is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls, and zero-trust architectures.

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 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 OBB Data Flow Diagram



1.5.1 Communication paths table

This table is useful to IT security groups and those configuring network devices such as switches, router, 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 2.x standard deployment

Path	OpenBlue Bridge (OBB) v2					Direction / use requiement[2]	Connecting Component			Notes
	Function	Interface	Default Port	Default Port State[1]	Port Activity (if enabled)		Default Port [2,3]	Protocol	Internet access	
A	OpenBlue Cloud (Authentication, Telemetry, Command & Control)					Required	OpenBlue Cloud			
	Data to Cloud	Ethernet	443	Enabled	∞	↳ ▶ ◀	443	HTTPS, AQMPS, MQTTS	*Yes	3
B	OpenBlue Bridge Device Updates					Required	OpenBlue Bridge Device Manager			
	Firmware update (FOTA)	Ethernet	443	Enabled	On demand	↳ ▶ ◀	443	TCP HTTPS	*Yes	3
C	DNS Client					Required	Domain Name Services (DNS) Server			
	Host name resolution	Ethernet	53	Enabled	On demand	↳ ▶ ◀	53	DNS	*Yes	3
D	NTP Client					Required	Network Time Protocol (NTP) Server			
	Time syncronization	Ethernet	123	Enabled	On demand	↳ ▶ ◀	123	NTP	*Yes	3
E	Local Service Console (OS Maintenance)					Required	Service laptop / device			
	Local Service Console	Ethernet	8922	Enabled	∞	▶ ◀ ↵	8922	SSH	*Yes	3
F	Local Service UI					Required	Service laptop / device			
	Service UI webserver	Ethernet	443	Enabled	∞	▶ ◀ ↵	443	N/A	No	
G	Local Data Collection BACnet/IP					Optional	BACnet/IP Devices			
	BACnet/IP	Ethernet	47808	Enabled	∞	↳ ▶ ◀ ↵	-	BACnet/IP	No	
H	Local Data Collection Modbus/TCP					Optional	Modbus/TCP Devices			
	Modbus/TCP	Ethernet	502	Enabled	∞	↳ ▶ ◀ ↵	-	Modbus/TCP	No	
I	Local Data Collection "Others"					Optional	Other Protocols			
	REST API, OCP, etc.	Ethernet	*	Enabled	∞	↳ ▶ ◀ ↵	*	*	No	

[1] Application requirements are representated 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.

[2] Typical default setting for connecting components

[3] Any Internet access, if used should be indirect and managed through a Firewall and/or Johnson Controls Airwall technology

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 OBB 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 Patch Policy

The policy documented here sets forth the current internal operating guidelines and process regarding OpenBlue Bridge, which may change from time to time at the sole discretion of Johnson Controls. Johnson Controls employs commercially reasonable efforts to pursue the operating guidelines and process described herein. However, other mitigating factors may prevent complete adherence to this policy, as determined by Johnson Controls at its discretion. Regardless, Johnson Controls endeavours to address issues that arise within OpenBlue Bridge with the severity that they warrant.

When CRITICAL security vulnerabilities are discovered within OpenBlue Bridge, Johnson Controls will use commercially reasonable efforts to issue a Critical Service Pack for the current version of OpenBlue Bridge as soon as is reasonably practicable.

When non-CRITICAL vulnerabilities are discovered within OpenBlue Bridge, Johnson Controls will use commercially reasonable efforts to:

- Apply fixes for HIGH severity vulnerabilities in the next immediate release of OpenBlue Bridge

Note: In line with industry recognized security best practices, backporting of OpenBlue Bridge enhancements and fixes to prior releases is not supported. Updates are only applied to latest version of the released product.

2.3.0 Hardening Checklist

- ☐ Hardening Step 1: Apply Operating System security patches
- ☐ Hardening Step 2: Configure Cloud service monitoring
- ☐ Hardening Step 3: Configure User Accounts
- ☐ Hardening Step 4: Configure TLS Certificates

2.3.1 Hardening the OpenBlue Bridge server platform

Hardening step 1: Apply Operating System security patches

OpenBlue Bridge Server and Web Client.

To maintain OpenBlue Bridge software functionality and support the latest security, regularly check for the latest version and upgrade accordingly.

Ubuntu 20.04 Server LTS

Practice patch management on the underlying Ubuntu host operating system to ensure the platform is hardened using the most up to date security patches.

Cloud service monitoring.

Hardening Step 2: Configure Cloud service monitoring

- When leveraging **OpenBlue** cloud services, perimeter controls must be applied independent to OpenBlue Bridge, in compliance to organizational guidelines and policies
- When you deploy OpenBlue Bridge change the default password of the built-in account.
- Each user must have their own unique set of credentials for OpenBlue Bridge account.
- Secure any edge devices and ensure they meet company network secure policies. Monitor and control devices accordingly. Devices should be configured to communicate via TLS when supported by the device to interact with OpenBlue Bridge services. For more information on TLS, see section 2.4.1.

For more information on deployment refer to the OpenBlue Bridge Platform Deployment and Installation guide.

2.3.2 Changing OpenBlue Bridge service accounts

Hardening Step 3: Configure User Accounts

Prior to installing OpenBlue Bridge, you must change the user credentials of the OpenBlue Bridge Administrative (messaging and reporting) services account. See section 2.3.3.4 for strong password criteria.

2.3.3 User management best practices

The OpenBlue Bridge Administrative account has the permission to create new user accounts. Following best practices for managing user accounts, account credentials and authorizations (permissions) can greatly improve the security for the system. Some guidance is presented in this section. For additional guidance, NIST standards such as SP 800-63 Digital Identity Guidelines may be consulted.

You should create unique user accounts for each administrator. The proper configuration of individual user accounts assures that security best practices are followed and that all user actions cannot be repudiated.

Best practices for account management include:

2.3.3.1 No shared accounts

Unique accounts should be used during all phases of operation. Installers, technicians, auditors, and other deployment phase users should never share common user accounts.

2.3.3.2 Remove or rename default user accounts (as permitted)

By removing or renaming default user accounts, the ability to gain unauthorized access to the system will be reduced as those attempting to do so will need to enter an unpublished username which is much harder to gain knowledge of.

2.3.3.3 Change default passwords

During installation, all default user accounts that have not been replaced must have their password changed.

2.3.3.4 Strong passwords

Strong passwords should be used to minimize the risk of password guessing. Automated forms of password guessing such as "dictionary attacks" and "rainbow tables" can run through commonly used passwords and can be successful if strong passwords are not used. You can strengthen a password with length and complexity. The length of a password has the biggest impact on making password guessing difficult.

Each OpenBlue Bridge password must meet the following criteria (at a minimum):

- 8 Total characters (For additional hardening, create passwords of at least 12-15 characters)
- 1 Special character (such as $, !, &, #, %, ^, etc.)
- 1 Upper case character
- 1 Lower case character
- 1 Number between 0-9
- Cannot be a common dictionary word

2.3.3.5 Password policy

It is important to have a password policy. Customers often have password policies that all systems must support.

2.4.0 Hardening OpenBlue Bridge web service and message communication

Harden OpenBlue Bridge Web Service and Message Communication on server and desktop platforms.

Hardening Step 4: Configure TLS Certificates

2.4.1 Enable TLS (HTTPS)

TLS connections require a user-specific certificate which must be manually configured to enable them. TLS is utilized in all web communication because it actively prevents reading and manipulation of communication between the client and the web service. OpenBlue Bridge supports TLS version 1.2 or 1.3. Versions 1.0 and 1.1 are not supported.

Web Service TLS connections are provided through two mechanisms:

- Let's Encrypt/ACME: A free service to provide TLS certificates with minor restrictions
- External: User-supplied certificates for TLS. Purchase certificates from a certificate authority, such as VeriSign, DigiCert, or Network Solutions.

2.4.1.1 Using your own certificate

If you don't provide your own certificate, the OpenBlue Bridge installer automatically generates a set of self-signed certificates to encrypt the platform's service and messaging communications. You can still provide your own certificates to encrypt platform's communication before the deployment. To use your own certificate, complete the following steps prior to deployment:

1. Navigate to the OpenBlue Bridge deployment script folder and open the `config.yml` file.
2. In the file locate the TLS section and modify tls.enabled flag to **True**.
3. Update the **<path-to-certificate>** section in path of certificate files to point to the correct certificate, key and CA files.

Note: Your certificate file name must be `certificate.pem` and your certificate authority file name must be `CA.pem`.

```
1.  tls:
2.    enabled: true
3.    SSLCertificateFile: /<path-to-certificate>/certificate.pem
4.    SSLCertificateKeyFile: /<path-to-certificate>/certificate.pem
5.    SSLTrustedCACertificateFile: /<path-to-certificate>/CA.pem
```

4. Click **Save.**
5. Deploy the OpenBlue Bridge platform using the OpenBlue Bridge - Deployment/Installation - Platform (OBB) - How To v1.0 guide.

2.4.1.2 Importing self-signed certificates

This section describes how to encrypt the TLS connection by importing self-signed certificates and certificate authority (CA) on client machines including Windows® and Mac®. Encryption is important for client

communicate with OpenBlue Bridge through messaging channels because self-signed certificates are not trusted by default.

2.4.1.2.1 Importing a self-signed certificate into a Windows client

To import a self-signed certificate into a Windows client, complete the following steps:

1. Navigate to the following folder in deployment `/docker.services.mayflower/scripts/certs`.
2. Locate the self-signed certificate `openblue-bridge.com.cer`.
3. In the Windows search bar type *`Manage computer certificates`*.
4. Right click **Trusted Root Certification Authorities**.
5. Click **All Tasks**.
6. Click **Import**.
7. The certificate wizard opens.
8. Select **Local Machine**, click **Next**.
9. Browse to the location of your certificate file.

   Note: You may have to change the file type to **All Files**.
10. Select your self-signed certificate.
11. Click **Next**.
12. If the certificate store is set to **Trusted Root Certification Authorities** click **Next**, then click **Finish**.
13. To verify that the certificate is successfully imported to **Trusted Root Certification Authorities** store, check openblue-bridge.com.

2.4.1.2.2 Importing a self-signed certificate into a Mac client

To import a self-signed certificate into a Mac client, complete the following steps:

1. Click the spotlight icon and type *`Keychain Access`*.
2. Double click **Keychain Access**.
3. In the **Keychains** menu click **System**.
4. In the **Category** menu click **Certificates**.
5. Drag your certificate into the pane.
6. Double click certificate.
7. Expand the **Trust** section.
8. For **When Using This Certificate:** select **Always Trust.**
9. Close **Keychain Access**.

2.5.0 Hardening OpenBlue Bridge Edge devices and network connectivity

Once the OpenBlue Bridge installation is complete, you will be prompted to ensure that edge devices have a certificate applied. Navigate to the prompted location to retrieve the certificate and apply to your device accordingly. Follow your device manufacture’s guidelines on how to apply a certificate.

This section provides guidance on how to further harden your OpenBlue Bridge network and devices:

- End device connections to OpenBlue Bridge and OpenBlue Bridge web clients must be on their own segregated networks that are also controlled and monitored following customer company policies.
- The flow of data between network segments should be managed to only enable flow from known sources and required ports to the intended target destination.
- When supported, Deep Packet Inspection (DPI) should be enabled to restrict commands which can transverse segments (trust boundaries) to those required for the desired interoperability. Consider disabling command that can “write” or “set” values for read-only data exchange.

2.6.0 Hardening the network ports

When you use a protocol, ensure that the corresponding port is open. Validate if any additional open ports are necessary to be open. Otherwise, it is strongly recommended that you close ports that are not mentioned below and unnecessarily open.

For additional information on ports and protocols which are specific to the OpenBlue Bridge device, see Figure 1.5.1.1