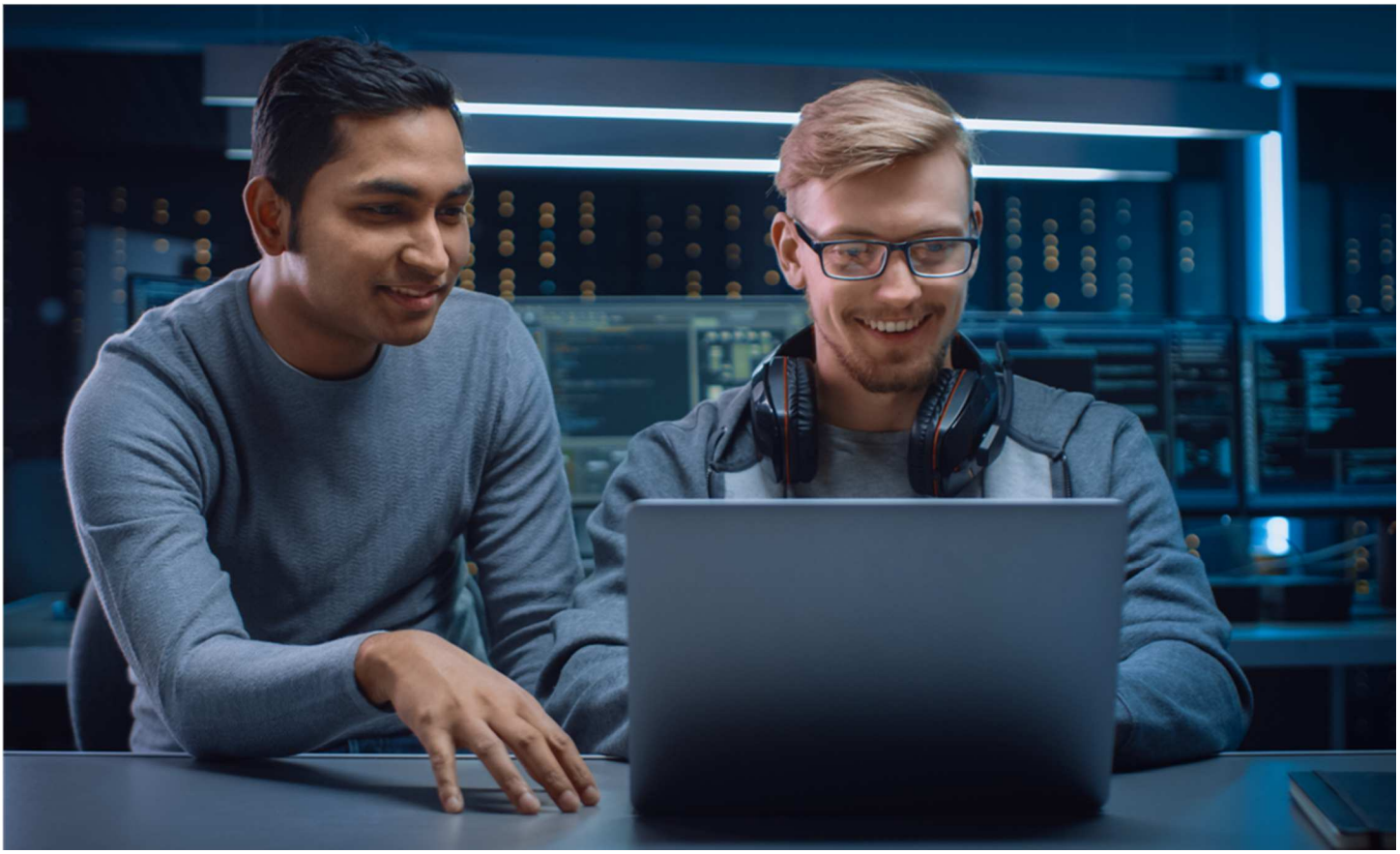
OpenBlue

# OpenBlue Bridge v1.1

## Hardening Quick Start Guide



GPS0019-CE-20210701-EN

Rev B

Johnson Controls

# Contents

## Introduction

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

The OpenBlue Bridge Hardening Quick Start Guide provides cybersecurity guidance used in planning, deployment, and maintenance periods.

Because cybersecurity threats have become a risk impacting 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 configuration and maintenance, including the operating system, user accounts, permissions and roles, and patch management.

## 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 guaranty 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 as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

# 1 OpenBlue Bridge overview

The OpenBlue Platform is a flexible, scalable, cloud-based platform that reaches across silos to gather data from disparate sources, stores it securely and standardizes the data. It enables you to have a streamlined, more productive day-to-day experience. As a result, applications that use the platform also help building professionals extend the life of their HVAC equipment, proactively manage security risks 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.

OpenBlue Bridge is an Internet of Things (IoT) connectivity platform designed to connect Operational technology (OT) and Information technology (IT) systems into the OpenBlue Cloud, while managing those connections throughout the device lifecycle. OpenBlue Bridge can leverage cloud resources.

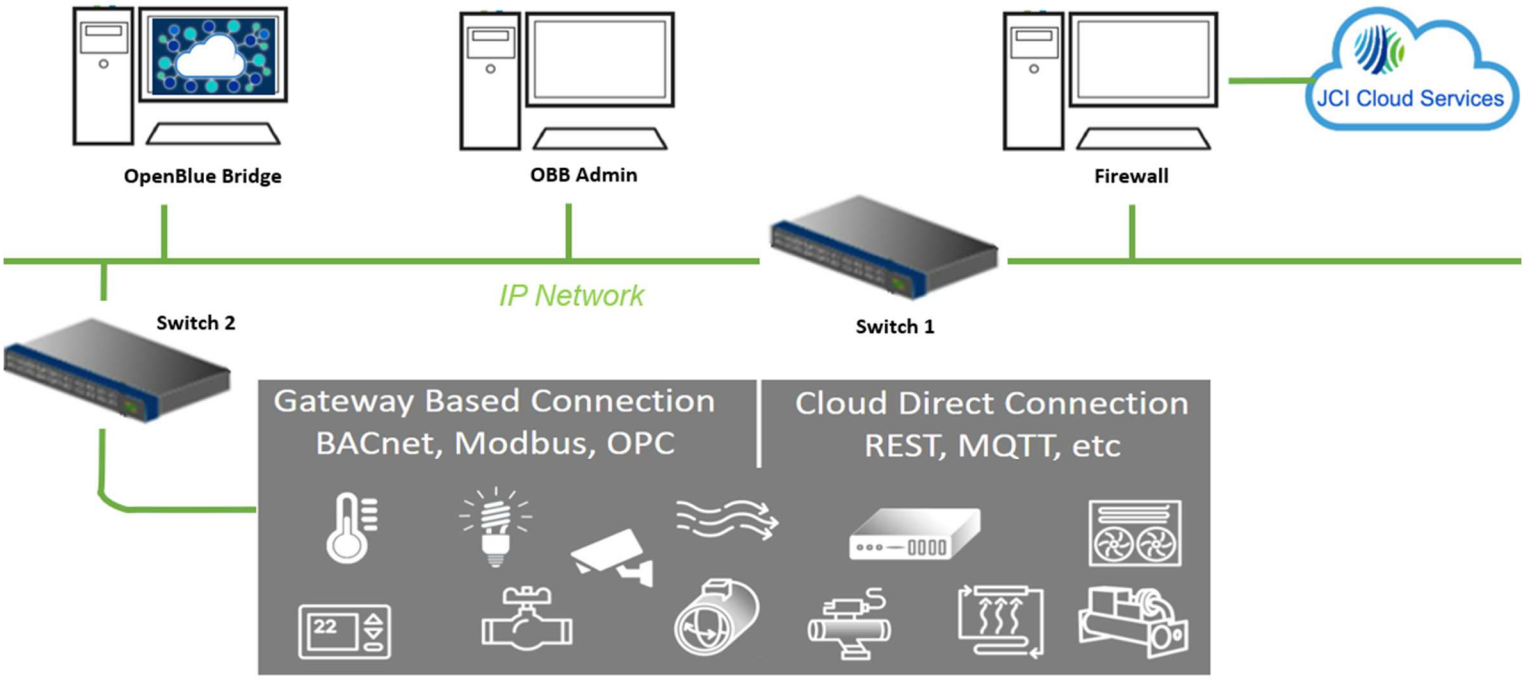
The OpenBlue Bridge platform is a micro-services-based platform designed to integrate devices, cloud Security as a Service (SaaS) offerings, legacy on premise platforms, and web applications.

OpenBlue Bridge, Twin and Cloud form the core of the technology stack with several differentiated technologies underlying each. Please see the respective resources for additional support of OpenBlue products such as Twin and Cloud are not supported in this Hardening Quick Start guide.

## 1.1.0 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: Typical OpenBlue Bridge deployment architecture diagram



### 1.2.0 Components

Typical OpenBlue Bridge system core components include the following items:

*OpenBlue Bridge*

This is the OpenBlue Bridge platform Ubuntu server which can be installed on dedicated hardware or a supported virtual machine.

*OpenBlue Bridge Administration*

The OpenBlue Bridge Administration portal is used to create and configure functions within OpenBlue Bridge, such as connector installation, connector configurations, connection status, etc.

*Network Switch*

A network switch allows data to flow across your network to and from OpenBlue Bridge. A switch with routing to an external facing connection is required for JCI Cloud services. One or several segregated switches are then required to faciliate edge device communications to OpenBlue Bridge.

*Firewall*

A firewall is an appliance which provides security when you are connected to the internet by disguising addresses and/or establishing a barrier between trusted and untrusted (Internet) networks.

*Devices*

OpenBlue bridge supports a multitude of connected control devices. Some common devices are thermostats, lights, cameras, card readers, chillers, etc.

## 2 Deployment

OpenBlue Bridge is intended to be operated by a professional with experience in deploying and administering micro-services-based platforms or similar systems. Use this section to initiate secure deployment for new installations, harden the solution, and complete additional steps after commissioning.

### 2.1.0 Intended Environment

OpenBlue Bridge platform should be installed on premise within a data center equipment rack with restricted access. For example, deploy on a corporate network, use a firewall to block unused ports, use TLS encrypt communication, and user credentials for access.

Internet connectivity - This product will require Internet access for installation and operation.

A machine running Ubuntu 20.04 Server LTS (Focal Fossa) is required. Do not install the desktop version of Ubuntu.

### 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
- Apply fixes for LOW and MEDIUM vulnerabilities within one of the next two available releases 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. Updates can be found at https://ubuntu.com/ .

##### 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 default user credentials of the OpenBlue Bridge messaging and reporting services account.

### 2.3.3 User management best practices

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.

#### *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. 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. To import self-signed certificates onto a client machine's certificate store, see section 2.2.1.2.1 Importing a self-signed certificate into a Windows client or section 2.2.1.2.2 Importing a self-signed certificate into a Mac client.

##### 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 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.