VERASYS®

SBH300 Hardening Guide

GPS0048-CE-EN
Version 5.1
Rev A
Revised 2023-11-16

Johnson Controls

Introduction

Our practices provide peace of mind to our customers with a holistic cyber mind set beginning at initial project design concept, and is supported through deployment, including a rapid incident response to meet comprehensive and evolving cybersecurity environments.

This hardening document intends to provide cybersecurity requirements used in planning, deployment, and maintenance periods for the Verasys solution.

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 Johnson Controls **Verasys Smart Building Hub (SBH300) 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

Appendixes are included at the end for additional literature, and acronyms used within this document.

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, expressed or implied, as to the efficacy of the cybersecurity practices or recommendations described within. 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 and connecting a Smart Building Hub (SBH300) to your network. The SBH300 uses communication protocols, security methods, and other technologies that you must consider carefully.

1.1.0 Verasys SBH300 Solution overview

The Smart Building Hub (SBH300) is the base controller for the Verasys™ Building Automation System (BAS) that provides wired and wireless connection between all Smart Equipment, Verasys and supported third-party controllers.

The Verasys system provides bundled equipment and controls solutions that are well-proven. The Verasys system features both simple, configurable controllers and HVACR equipment from the factory or installed in the field. You can use Verasys to configure many HVACR controls applications for one building or an entire enterprise comprised of multiple buildings, without using special programming tools or control engineering.

1.1.1 Deployment architecture

The Verasys solution is comprised of several components to provide options for wired and wireless communications within the building and to cloud services which provide analytics, secure remote access for monitoring, and management across the enterprise.

1. Wi-Fi / 4G
2. Customer Internet
3. Temp troubleshooting - Mobile hotspot

MS/TP BACnet Devices

Over the next pages, we will cover the common use cases for Verasys Solutions.

Devices	Approved Wireless Modem	Customer managed gateway
MS/TP BACnet	Use Case 1	Use Case 2

Figure 1.1.1.1: SBH300 architecture with a cellular modem

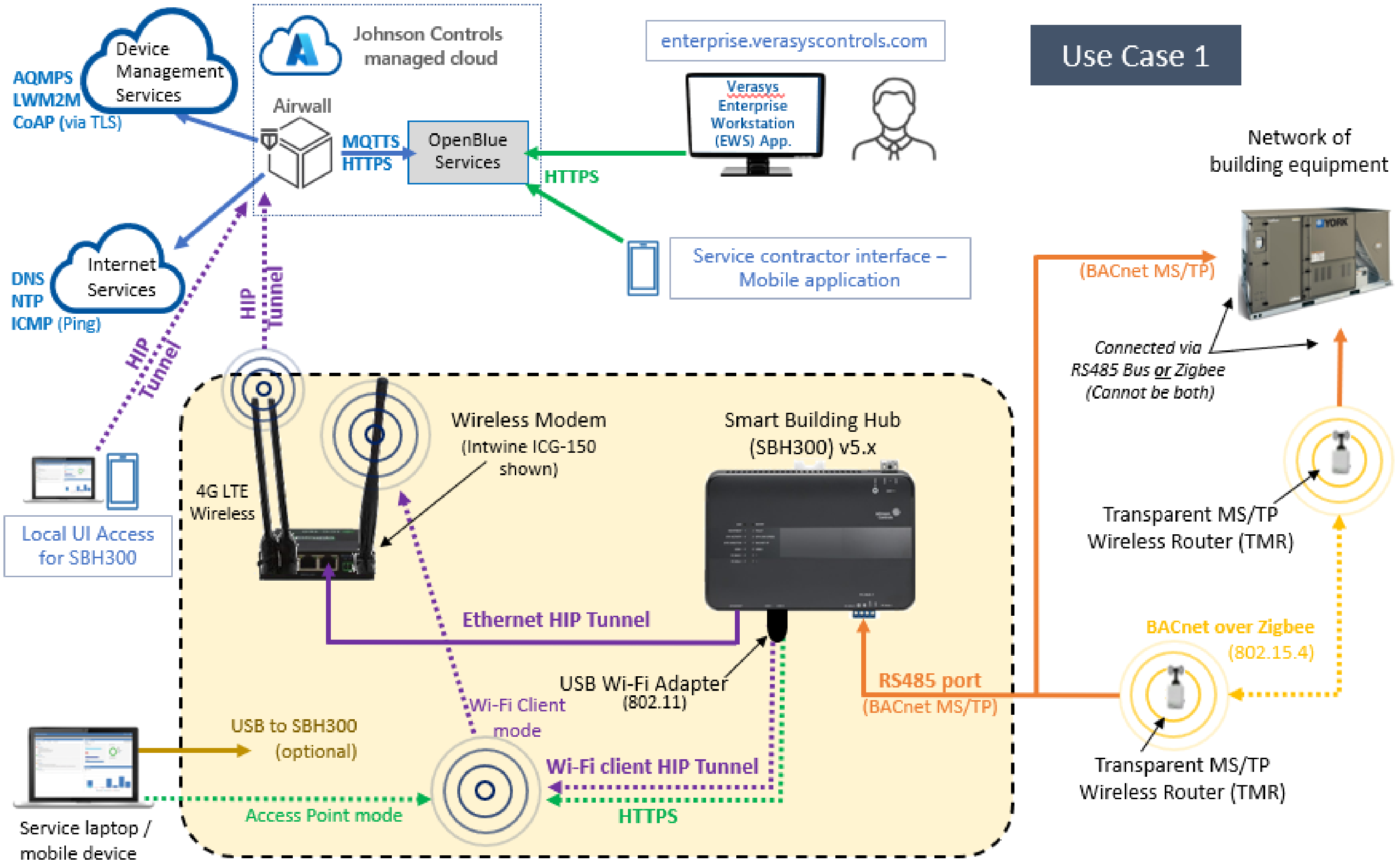
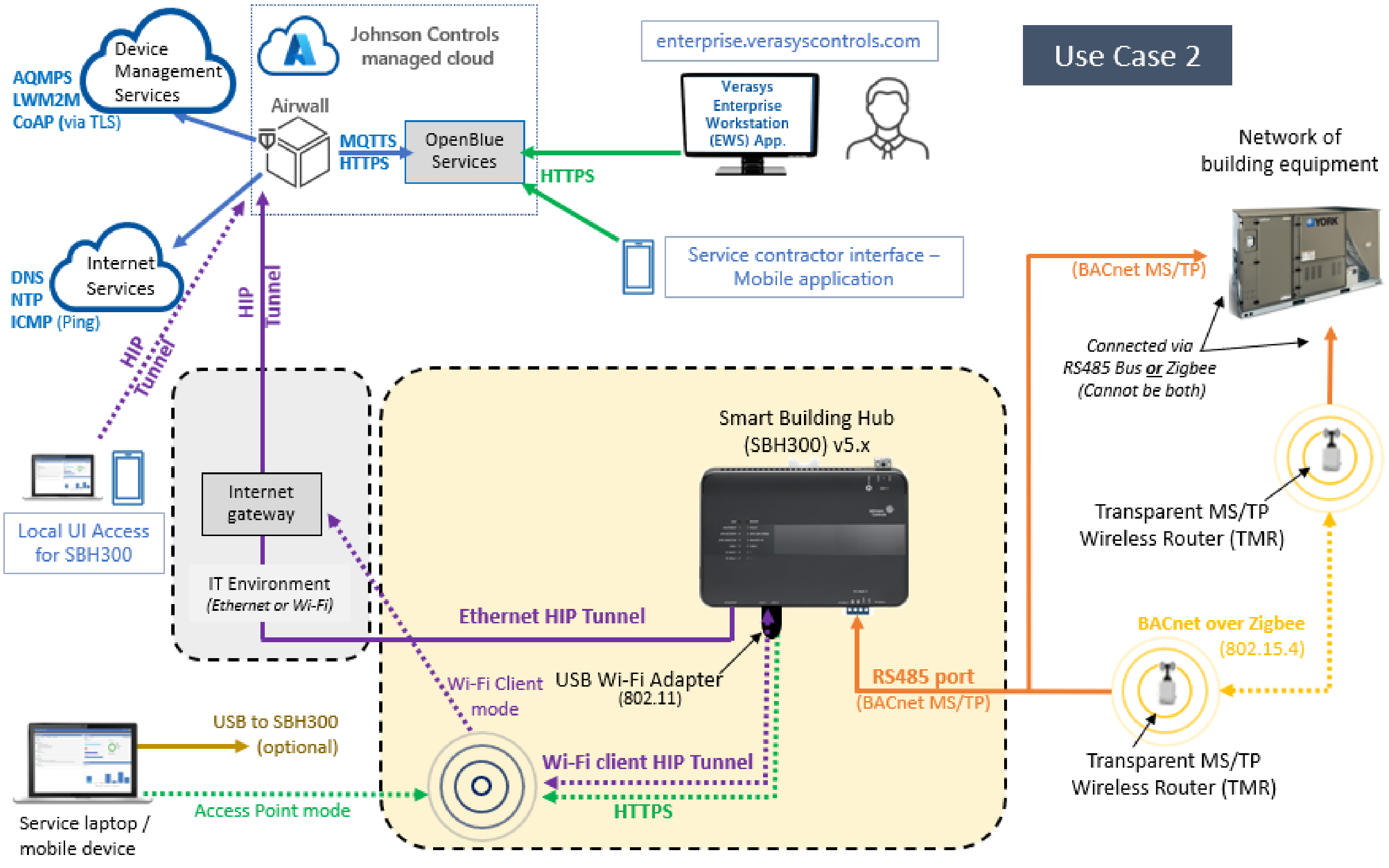

Device Management Services
AQMPS
LWM2M
CoAP (via TLS)
Johnson Controls managed cloud
Airwall
MQTTS
HTTPS
OpenBlue Services
HTTPS
enterprise.verasyscontrols.com
Verasys Enterprise Workstation (EWS) App.
Use Case 1
Network of building equipment
Service contractor interface – Mobile application
Internet Services
DNS
NTP
ICMP (Ping)
HIP Tunnel
HIP Tunnel
(BACnet MS/TP)
Connected via RS485 Bus or Zigbee (Cannot be both)
Local UI Access for SBH300
4G LTE Wireless
Wireless Modem (Intwine ICG-150 shown)
Smart Building Hub (SBH300) v5.x
Transparent MS/TP Wireless Router (TMR)
Ethernet HIP Tunnel
BACnet over Zigbee (802.15.4)
USB Wi-Fi Adapter (802.11)
Wi-Fi Client mode
RS485 port (BACnet MS/TP)
USB to SBH300 (optional)
Wi-Fi client HIP Tunnel
Transparent MS/TP Wireless Router (TMR)
Service laptop / mobile device
Access Point mode
HTTPS

Figure 1.1.1.2: SBH300 architecture with a customer managed gateway


Device Management Services
AQMPS
LWM2M
CoAP (via TLS)
Johnson Controls managed cloud
Airwall
MQTTS
HTTPS
OpenBlue Services
enterprise.verasyscontrols.com
Verasys Enterprise Workstation (EWS) App.
HTTPS
Use Case 2
Network of building equipment
Internet Services
DNS
NTP
ICMP (Ping)
HIP Tunnel
HIP Tunnel
Service contractor interface – Mobile application
(BACnet MS/TP)
Connected via RS485 Bus or Zigbee (Cannot be both)
Smart Building Hub (SBH300) v5.x
Internet gateway
IT Environment (Ethernet or Wi-Fi)
Local UI Access for SBH300
Transparent MS/TP Wireless Router (TMR)
Ethernet HIP Tunnel
BACnet over Zigbee (802.15.4)
Wi-Fi Client mode
USB Wi-Fi Adapter (802.11)
RS485 port (BACnet MS/TP)
USB to SBH300 (optional)
Wi-Fi client HIP Tunnel
Transparent MS/TP Wireless Router (TMR)
Access Point mode
HTTPS
Service laptop / mobile device

1.1.2 Components

The Verasys solution consists of the following components which require hardening on premises:

SBH300

The SBH300 streams data from BACnet® MS/TP compatible equipment to the modem via a wired Ethernet or wireless Wi-Fi connection. The SBH300 is compatible with Johnson Controls® and third party manufactured chillers, roof top units, input output modules, and air handling units. The SBH300 supports selecting up to one hundred BACnet MS/TP devices to monitor and manage from a single gateway, via wired or wireless BACnet network. Wireless equipment connects to the SBH300 using one or more Transparent MS/TP Wireless Router (TMR). Equipment connected to the SBH300 is self-discovered. The SBH300 includes a local user interface (UI) for monitoring and managing the Verasys system.

Zero-Trust. The SBH300 includes Airwall Gateway zero-trust architecture (ZTA) technology. The Airwall Gateway is a virtual air-gap solution that ensures that your device traffic is invisible from the internet and enforces a policy so that the devices can only talk to allowed endpoints through the zero-trust network. It eliminates lateral movement from bad actors across your network using software defined networks called overlay networks, that are built upon zero-trust policies. Airwall uses Host Identity Protocol (HIP) to secure network communication between devices, enabling micro-segmentation and remote access at scale on any network.

USB Wi-Fi adapter (optional)

The Wi-Fi Access Point (AP) adapter connects to one of the SBH300 USB ports and can serve as either an access point, a Wi-Fi client or both:

- **Access Point mode*** – Mobile devices and laptops can connect to the SBH300
- **Wi-Fi Client mode*** – Connects the SBH300 to a wireless modem using a zero-trust HIP tunnel to protect communications

** Connectivity to the access point relies on a clear wireless signal path. Connection distances will vary by environmental conditions.*

The USB Wi-Fi adapter is either included as part of the SBH300 panel kit or sold separately (product code ACC-WFUSB-LM808).

Transparent MS/TP Wireless Router (TMR) (optional)

The SBH300 can communicate to controllers via the TMR Wireless Field Bus System. This is an option for locations that cannot easily connect via wired MS/TP cabling. The adapter uses low power 802.15.4 mesh technology to connect HVAC equipment using the BACnet over Zigbee protocol. The wireless system creates a wireless mesh network and provides a reliable, resilient, self-healing network by automatically updating transmission paths for the data.

When the TMR is plugged into one of the SBH300's RS-485 ports, the SBH300 can communicate to other controllers connected using TMRs that are within signal range and share a common Personal Area Network (PAN) identifier.

Modem (optional)

Several approved 4G LTE modems are available from Johnson Controls which support this application. The modem establishes internet connectivity for transmission of SBH300 data to the Johnson Controls Cloud which host services for Verasys Enterprise customer applications.

Standard modem offering:

- Intwine ICG-150 – 4G LTE wireless with local Wi-Fi

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:

Service laptops / mobile devices

Service personnel can connect laptops or mobile devices to the SBH300 when the SBH300 has a Wi-Fi adapter installed and configured to run in Access Point mode.

Verasys Enterprise Workstation (EWS) Cloud Services

The Johnson Controls OpenBlue Cloud is hosted in a Microsoft Azure environment which receives data from the Building Automation system via the SBH300 connected through the internet. The Johnson Controls OpenBlue Cloud also hosts the Verasys Enterprise Customer Application and the Service Contractor Mobile

Application which users can access remotely via the internet. All connections to the cloud are secured using TLS communications overlayed with the Airwall Gateway HIP tunnel encryption.

Internet gateway

Utilized only with use case 2, an internet gateway is used for external communication instead of a modem. This internet gateway is to be supplied separately if required.

1.2.0 Security feature set

Johnson Controls products are designed with built-in cybersecurity features out of the box. Some features are included and set by default while other features need the reader to go through steps for advanced hardening.

Here are the features specific to the Verasys solution

- Protected site-to-cloud communications **–**
  - Encrypted communications – Equipment data is sent encrypted from the SBH300 to the cloud using TLS to protect messaging
  - Zero-trust connections – All messages sent to cloud services using the Airwall Zero-trust solution which further encapsulates all traffic from the site using Host Identity Protocol (HIP) using AES256 encryption, including messages already protected by TLS.
  - Zero-trust policy-managed authorizations – Only paths established within the Airwall Zero-trust Conducted will be permitted for each connection and user.
  - Zero-trust micro- segmentation support – Granular control over how data can flow within and across network segments
  - Hidden IP addresses – IP addresses are not exposed to internet
  - Outboard communications only **–** Only two outbound ports are required for site-to-cloud data exchange.
- Remote updates – Security updates and patches are pushed to the SBH300
- Forced password change – Default user account passwords must be changed on first logon
- Forced Wi-Fi setting change – Default Wi-Fi IDs and pass phrases must be changed during initial configuration

1.3.0 Intended environment

Physical access and installation of devices can greatly impact cybersecurity. Components are designed to be operated in an indoor, dry environment. However, components at each level will possess varying degrees of access. Here is some general guidance based on typical environments per component type:

Most components are designed to be installed within a user supplied panel or enclosure usually in an upright orientation. Install in areas free of corrosive vapors and where the ambient temperature stays below 122 degrees F (50 degrees C).

Please refer to the SBH300 Installation Guide for additional details. https://docs.johnsoncontrols.com/bas/r/Verasys/en-US/Verasys-Smart-Building-Hub-SBH300-Installation-Guide/5.0. Additional guides and documentation can be found in Appendix A.

1.3.1 Internet connectivity

The SBH300 is designed to require internet access. There are currently two options (see figures 1.1.1.1 and 1.1.1.2):

- Use case 1 – Johnson Controls provided wireless 4G internet connectivity
- Use case 2 – Customer provided internet connectivity

Internet access increases your cybersecurity footprint and attack area which requires additional hardening steps. The hardening steps in section 2 must be taken to limit external access.

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

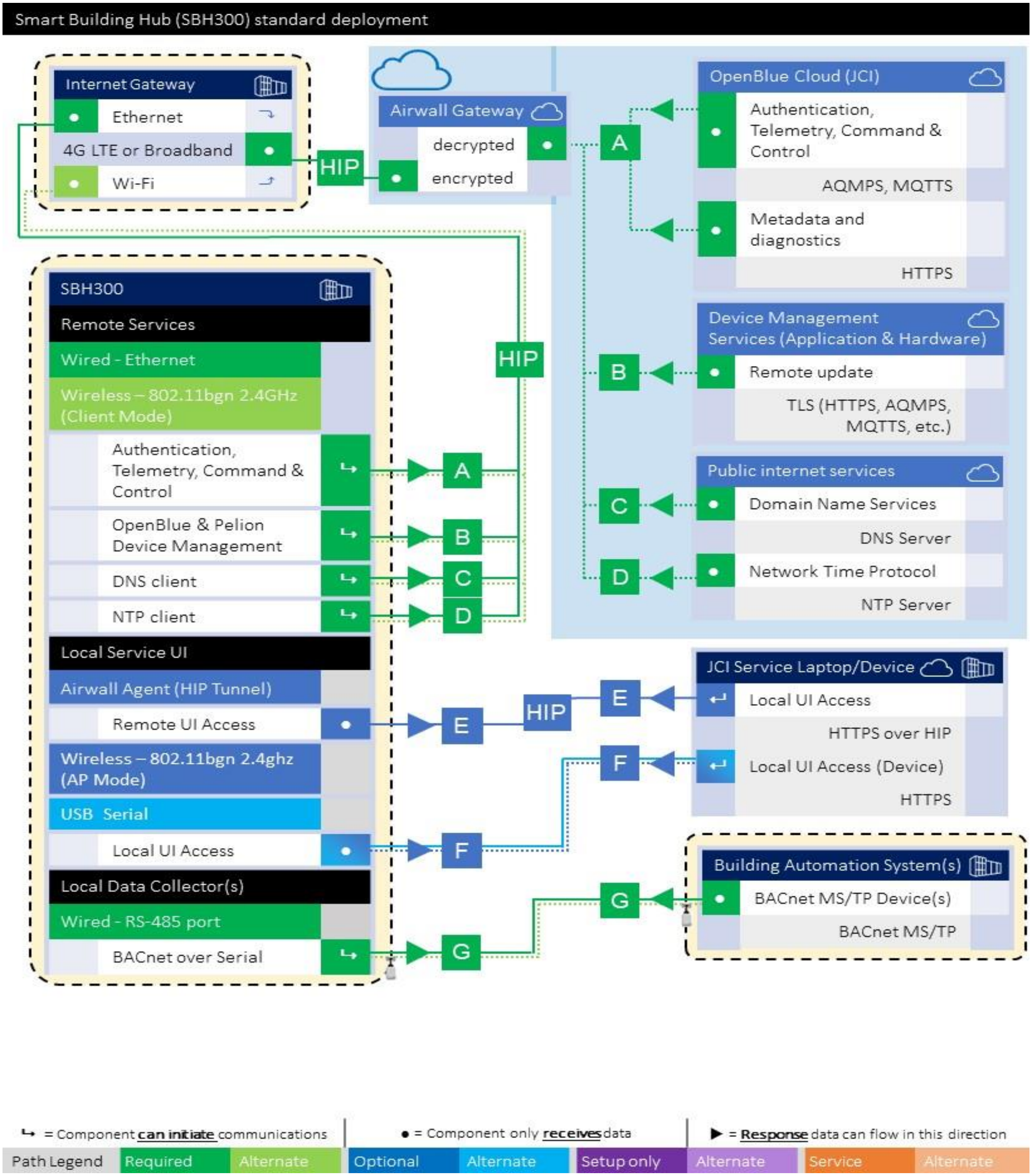
A data flow diagram (DFD) is a detailed view of the architecture which will show each communication path and flow direction. This resource will be used to aid in the configuration of network security settings (rules) within routers, firewalls and zero-trust architectures.

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 Use Cases 1 and 2 Data Flow Diagram



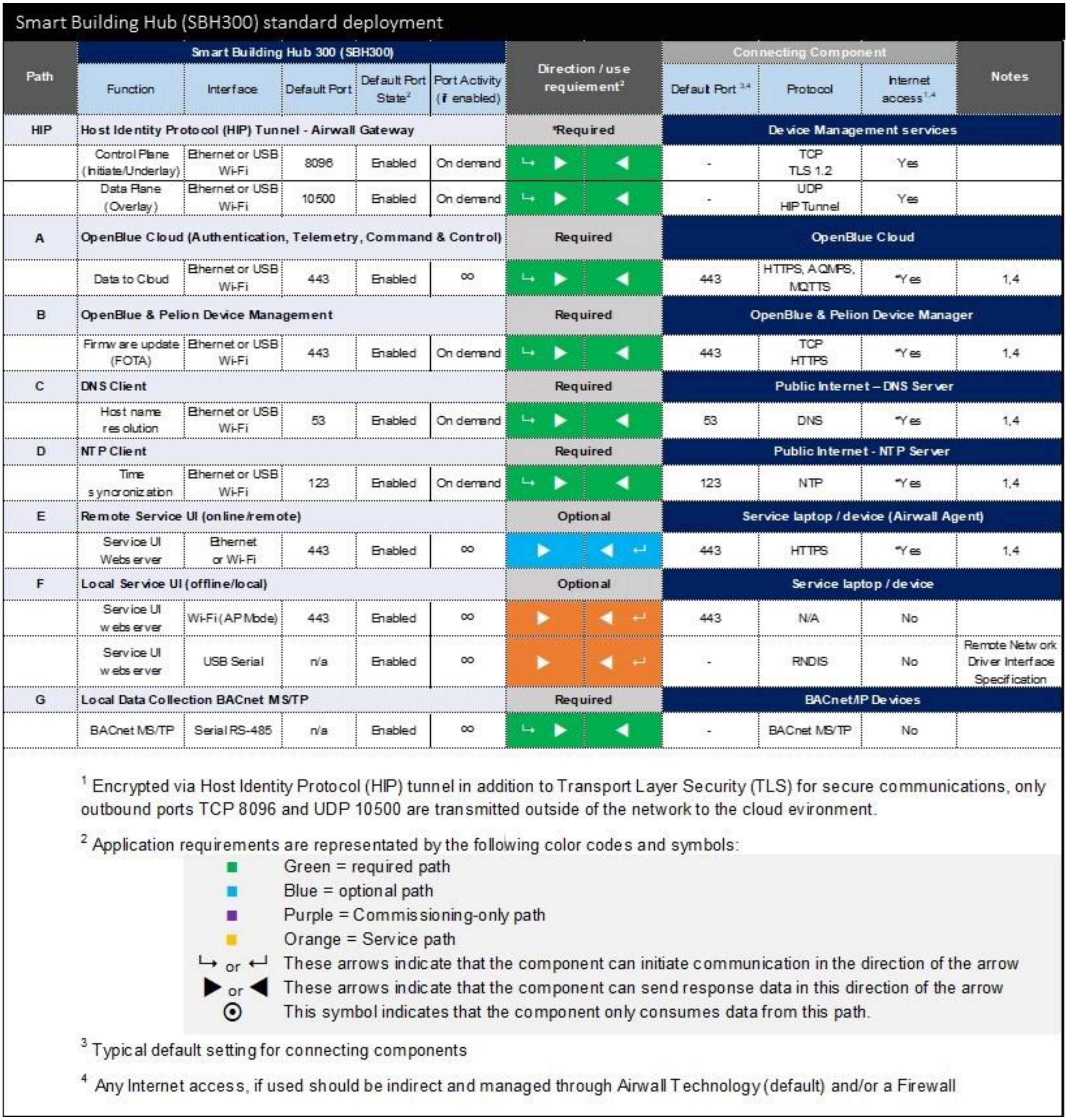
[1] Wi-Fi support limited to modems with capability.

- Intwine ICG-150 - supports Wi-Fi
- Digi WR11 - does not support Wi-Fi

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



Smart Building Hub (SBH300) standard deployment

Path	Smart Building Hub 300 (SBH300)					Direction / use requiement[2]		Connecting Component			Notes
	Function	Interface	Default Port	Default Port State[2]	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 & Pelion Device Management					Required		OpenBlue & Pelion 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	Remote Service UI (online/remote)					Optional		Service laptop / device (Airwall Agent)			
	Service UI Webserver	Ethernet or Wi-Fi	443	Enabled	∞	🟦 ▶	🟦 ◀ ↵	443	HTTPS	*Yes	1,4
F	Local Service UI (offline/local)					Optional		Service laptop / device			
	Service UI webserver	Wi-Fi (AP Mode)	443	Enabled	∞	🟧 ▶	🟧 ◀ ↵	443	N/A	No	
	Service UI webserver	USB Serial	n/a	Enabled	∞	🟧 ▶	🟧 ◀ ↵	-	RNDIS	No	Remote Network Driver Interface Specification
G	Local Data Collection BACnet MS/TP					Required		BACnet/IP Devices			
	BACnet MS/TP	Serial RS-485	n/a	Enabled	∞	🟩 ↳ ▶	🟩 ◀	-	BACnet MS/TP	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 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.

[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 products 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.

The SBH300 is packaged and sold with power supply, Wi-Fi adapter, optional cellular modem, and optional wireless TMR.

2.1.2 Default security behavior

On the initial startup, certain functions will be enabled to facilitate the most common commissioning tasks. Examples may include:

- User account settings (example: changing password on first login)
- Enhanced password validation
- A configuration webpage

2.1.3 Considerations for commission

In some applications the default settings may not be sufficient to fully commission the system. Functions that will not be used during the commissioning process should be disabled.

In the commissioning phase, a less secure configuration may be used before the full infrastructure is available to speed up the deployment process (for example, using wireless). Once the commissioning phase is complete, be sure to remove the temporary infrastructure and harden the system further before turning over to full runtime operations.

2.1.4 Recommended knowledge level

The person confirming that the proper hardening steps are executed should be experienced in your product’s administration and networking technologies. If training for your product(s) exist, completion of the basic installation course is required, and any advanced installation course is recommended.

Note: It is helpful to review the Verasys Smart Building Hub (SBH300) Network and IT Guidance Technical Bulletin before completing the following section. Link - https://cgproducts.johnsoncontrols.com/MET_PDF/12012324.pdf

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

While Verasys components have several secure-by-default safeguards, we recommend additional hardening to meet the security requirements of the target environment. This checklist provides an example list of hardening steps you may select to go through. The actual steps you will take is based upon the features included within your specific environment as gathered in Section 1.3.0.

- For steps that are not applicable to your instance, check off the “N/A” column
- As you complete the remaining steps, check off or include the date these were completed

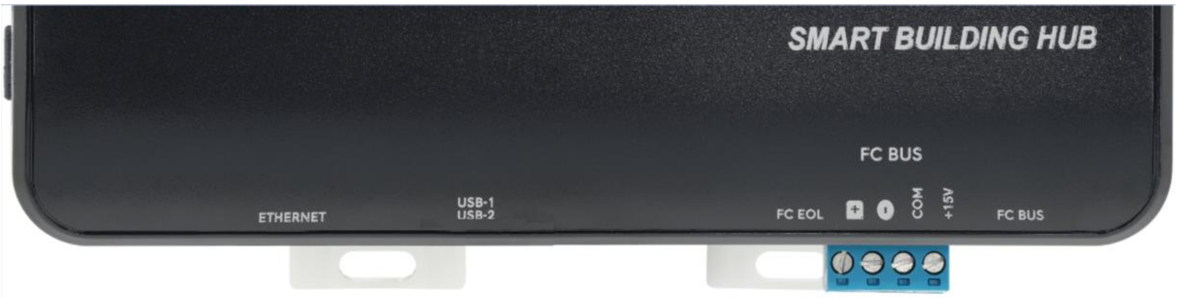
Hardening Step	Status	
	Complete	N/A
1. SBH300 Hardening	-	-
1.1: Remove USB Wi-Fi adapter if wireless is not permitted (conditional)	□	□
1.2: Change connection defaults (admin user / wireless)	□	-
1.2.1 Changing Wi-Fi Access Point settings after initial logon (optional)	□	□
1.3: Add additional users (optional)		
1.4: Configure modem communication mode (wired or wireless)	□	-

1.5: Update SBH300 Operating System (manual only if required)	□	-
1.6: Review supporting functions	-	-
1.6.1 - Audit Logs	□	-
1.6.2 - Reset Functions	□	-
2. Document Deployment Details		
2.1: Security documentation	□	-

SBH300 hardening

To harden the SBH300, it is necessary to log on through its User Interface, the SBH300 UI. The technician uses the SBH300 UI to make the necessary configuration changes which strengthen the security of the SBH300's IP enabled interfaces. These interfaces are used for local administration and internet-facing cloud services. It is important to minimize the attack surface and ensure that the remaining active interfaces have the appropriate level of protection.

Figure 2.2.1.1 – SBH300 ports



2.2.2 Determine internal communication types

The SBH300 can be configured for wired or wireless communications for service and modem connections as described in this table:

Table 2.2.2.1 – SBH300 Connections

SBH300 **Connection**	**Wireless path**	**Wired path**	**Preferred path**
Service laptop/mobile device	USB Wi-Fi adapter (access point mode)	micro-USB port	Wireless
Modem	USB Wi-Fi adapter (client mode)[1]	Ethernet	Wired

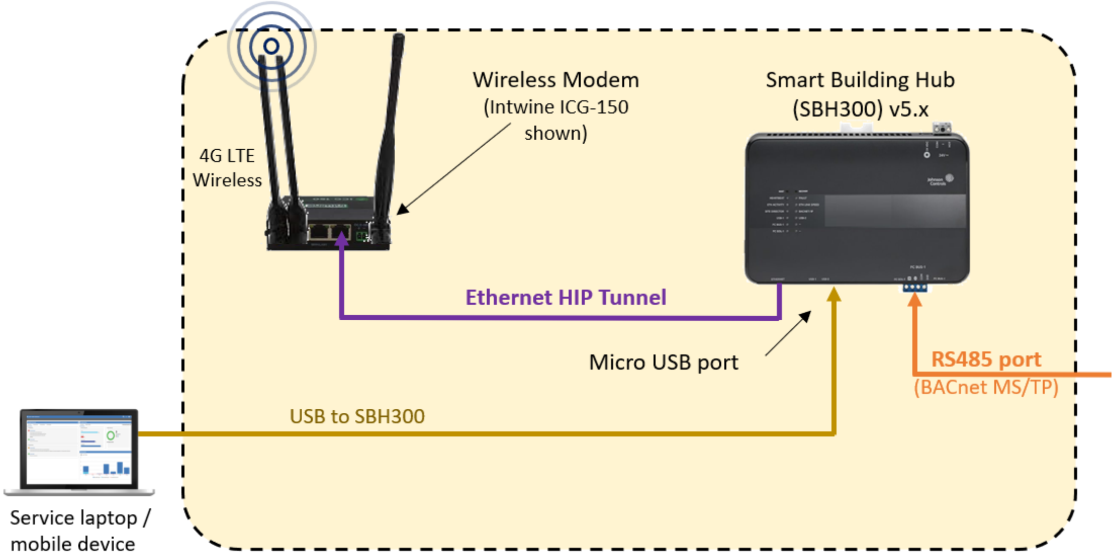
[1] Wi-Fi client mode requires use of modem with Wi-Fi capability (e.g., Intwine ICG-150)

Both forms of Wi-Fi communication are enabled by plugging the USB Wi-Fi adapter into the SBH300 USB port.

Step 1.1 – Remove USB Wi-Fi adapter if wireless is not permitted (conditional)

If the customer does not permit wireless in the environment, wired connections must be established for each path and the USB Wi-Fi adapter should be removed from the SBH300.

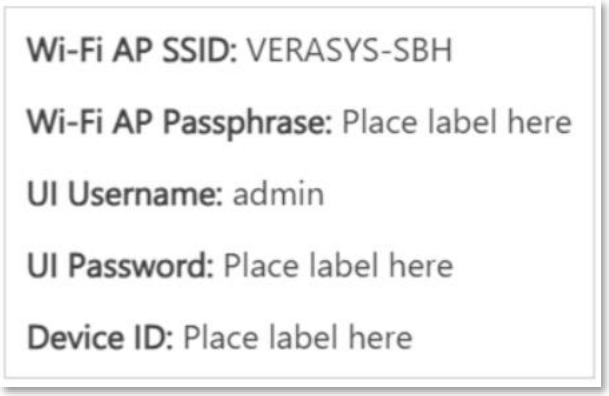
Figure 2.2.2.1 – Service laptop / Mobile device connection



2.2.3 Changing connection defaults (admin user / wireless)

Before you begin, locate the factory printed default Wi-Fi parameters label within the SBH300 Quick Start Guide. This document comes with the SBH300 and will be used for reference throughout this procedure. See Appendix A for a table with additional documentation.

Figure 2.2.3.1 SBH300 Factory Printed Label



Wi-Fi AP SSID: VERASYS-SBH

Wi-Fi AP Passphrase: Place label here

UI Username: admin

UI Password: Place label here

Device ID: Place label here

Step 1.2 - Change connection defaults (admin user / wireless)

For the initial access to the SBH300 UI, execute the following steps:

1. Establish the respective connection between the Laptop/Service Device and the SBH300 (see wireless and wired instruction within table:

Wi-Fi service connections	USB service connections
A. Plug the Wi-Fi adapter into the USB port.	**A.** Ensure the SBH300 is powered off
B. Verify that the Wi-Fi AP LED is flashing.	**B.** Connect a laptop to the SBH300 using a USB cable between the device and SBH300 USB port
C. Access the Wi-Fi settings on your Wi-Fi connected mobile phone, tablet, or computer.	**C.** Power up the SBH300
D. Click the default Wi-Fi SSID and enter the Wi-Fi Passphrase (see factory label figure 2.2.3.1).	**D.** The Remote Network Driver Interface Specification (RNDIS) driver should be installed automatically. If it does not, then the RNDIS will need to be manually installed
	E. Verify static IP connection configuration by viewing your network setting properties (i.e., 192.168.142.2)

2. Open a web browser and enter **192.168.142.1** as the browser address.

   Note: Ignore the “***Your connection is not private***” warning and proceed.

3. Use the factory default UI Username and UI Password.

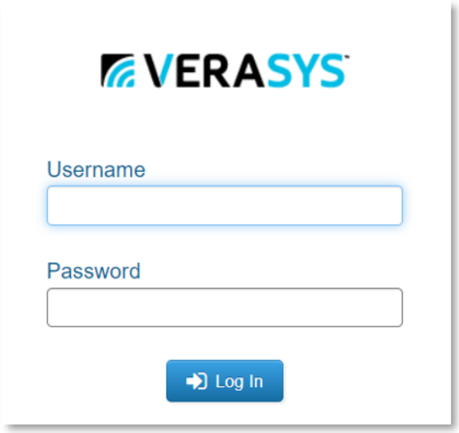
4. Read and accept the SBH300 license agreement.

   The first time you log on to the SBH300, you must change the following:

   - SBH300 UI Admin password
   - USB Access Point Wi-Fi SSID
   - USB Access Point Wi-Fi passphrase

   NOTE: It is still necessary to configure Wi-Fi parameters for installations not utilizing Wi-Fi as part of the initialization process.

Figure 2.2.3.1 – SBH300 Logon screen



See figure 2.2.3.2 for guidance:

Figure 2.2.3.2 – SBH300 field formation rules

	UI Admin password	Wi-Fi SSID	Wi-Fi Passphrase
Length (permitted)	8-32 characters	2-32 characters	8-63 characters
Minimum	8	To accommodate non-guessable values	8
Recommended	15+		15+
Supported character types	printable characters plus the space (ASCII 0x20), @, ?, ", $, [, \,], and +	printable characters plus the space (ASCII 0x20)	printable characters plus the space (ASCII 0x20)
Unsupported character types	N/A	?, ", $, [, \,], and +	?, ", $, [, \,], and +
Case-sensitive	Yes	Yes	Yes
Formation guidance	Avoid guessable values – Use a mix of case, alpha, numeric and special characters, and randomness to make entries harder to guess		
Formation rules	Yes	Not enforced	Not enforced
Mixed case	At least one upper and lower case		
Numbers	At least one number		
Blocked	Common passwords		

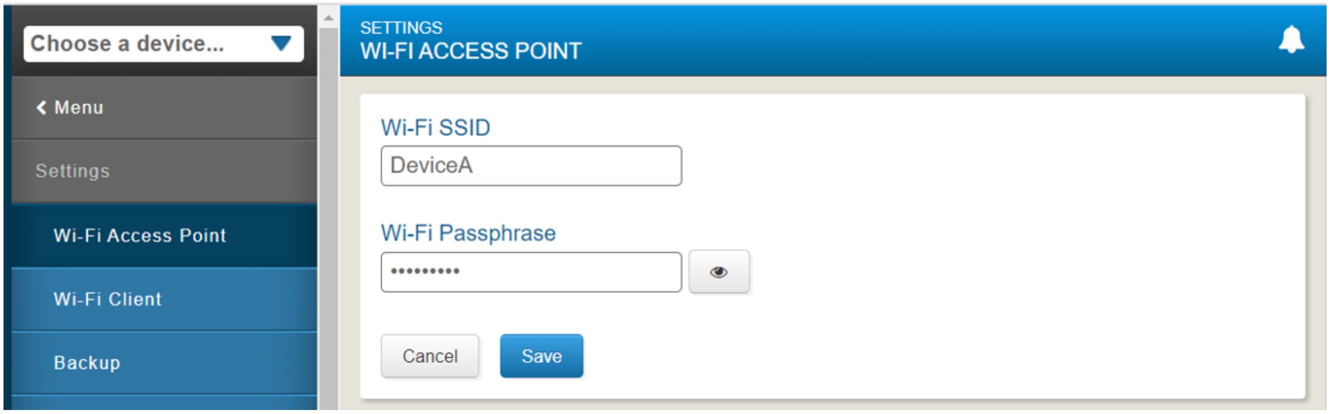
Important for Wi-Fi connections: After you change the Wi-Fi passphrase and SSID, the web server restarts, and you need to re-establish connection to the SBH300. If using Wi-Fi be sure to use the new SSID and passphrase. On some computers and mobile devices, click on the original Wi-Fi network before you rejoin the network with the new passphrase.

Step 1.2.1 – Changing Wi-Fi Access Point settings after initial logon (optional)

To change the Wi-Fi Access Point settings after the first logon, select **Settings> Wi-Fi Access Point** from the SBH300 UI menu.

The Wi-Fi SSID and Passphrase may be modified from this menu by users assigned the “Admin” or “Tech” roles.

Figure 2.2.3.3 – Wi-Fi Access Point screen



Wi-Fi SSID: DeviceA

Wi-Fi Passphrase: •••••••••

2.2.4 SBH300 User Management

Configuring multiple users helps distinguish who makes adjustments to the systems and when they access the system. When you assign a role to a user's account, apply the principal of least privilege.

The principal of least privilege means the following:

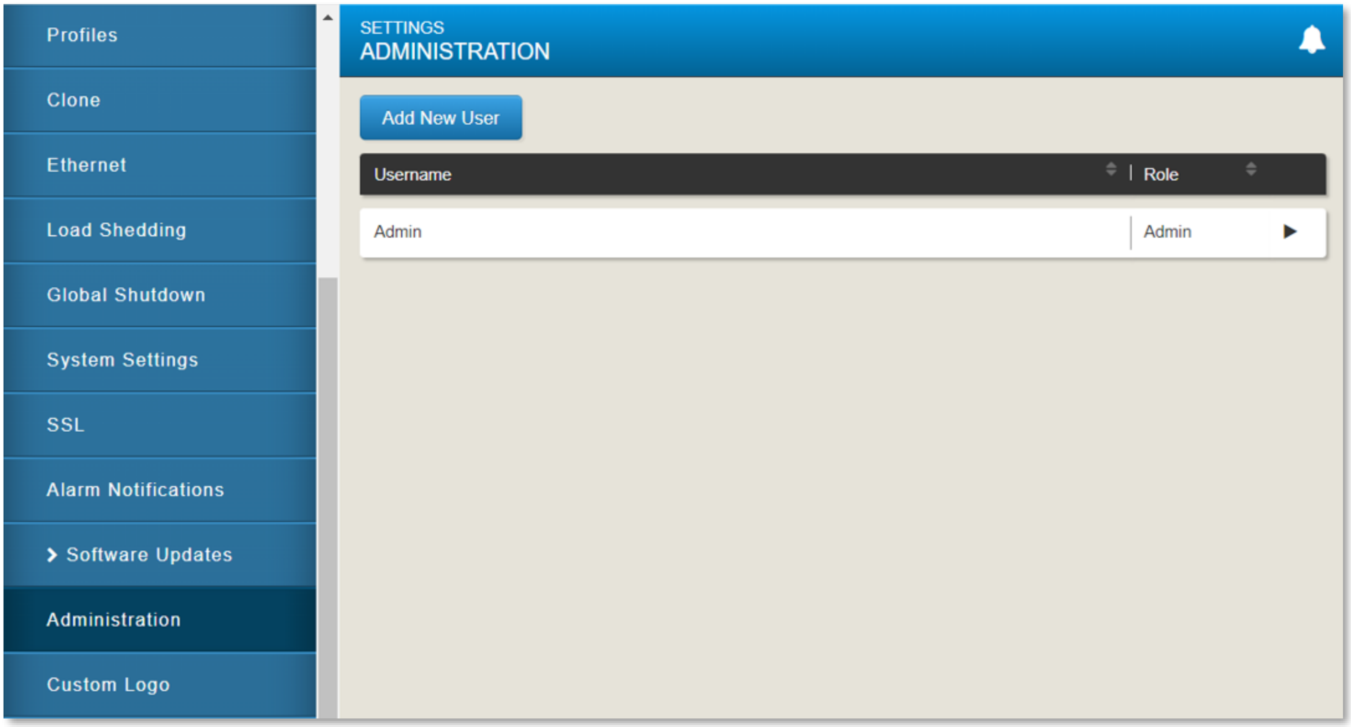
- Only the minimum necessary rights should be assigned to a user that requests access
- Access rights should be in effect for the shortest duration necessary to do their job. Some systems have this automated while other systems it is a manual process to expire their account after work is performed.

Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain or change information in unwanted ways. The best practice when assigning SBH300 access rights is to only give an individual user the necessary role to their job and nothing more.

Step 1.3 – Add additional users (optional)

You can configure users and user permissions from the **Administration** tab. The **Administration** tab is located on the **Settings** tab. By default, the system creates an Admin user role. For first-time log on information, see Connecting to the SBH within the Verasys Smart Building Hub (SBH) Quick Start Guide SBH300 (Part No. A16381V57K).

Figure 2.2.4.1 – SBH300 Add User screen



Username	Role
Admin	Admin

After you have logged on, you can configure the Admin user, or add more users to the system. See the following table.

Table 2.2.4.1 – New User

Field	Description
Name	Identifies the individual obtaining an account.
Username	Identifies the user. This unique identifier cannot contain spaces.
Password/Verify Password	The password must contain 12 or more characters (15 or more recommended), 1 lower case letter, 1 uppercase letter, 1 number and 1 special character.
Roles	**Tenant**: This role provides access to devices, facility, and schedules. Tenant permissions include device homepage, alarm notifications, and password settings. Refer to *Verasys Tenant User Guide LIT-12013613.* **Tech**: This role is similar to the admin role. Tech permissions provide access to the **Settings** tab. • Facility: Viewable and adjustable • Wi-Fi Access Point: Viewable and adjustable • Ethernet: Viewable and adjustable • Load Shedding: Viewable and adjustable • Global Shutdown: Viewable and adjustable • Alarm Notification: Viewable, not adjustable • Software Updates: Able to install updates • System Settings: Viewable and adjustable **Admin**: This role provides access to all settings and adjustments within the Verasys System.
Alarm Notification Level	Sets the user alarm notification levels. The four options include: **Disable**: User does not receive notifications via email or text message. **Service**: User receives all alarms (service, service priority, and critical). **Service Priority**: User receives only service priority and critical alarms. **Critical Alarms:** User only receives critical alarms.
Email address and SMS message notifications	You can enter the email address and SMS notifications into the following fields: • **Email Address 1** field • **Email Address 2** field

2.2.5 SBH300 – Configure Modem Communication Mode

The SBH300 uses an internet connection to communicate to the cloud. The SBH300 is connected to the internet through an Ethernet or Wi-Fi connected modem.

You will need to determine how the SBH300 will communicate with the Modem. To reduce security risk, modem communications should be set as wired or wireless but not both.

NOTE: Wired Ethernet connections are more secure than Wi-Fi connections as a physical connection to the network is required.

Step 1.4 – Configure modem communication mode (wired or wireless)

Option 1 – Ethernet (preferred)

- To enable wired Ethernet communications to the modem:
    a. Log on to the SBH300 local UI using the SBH300 Wi-Fi connection
    b. To configure a wired Ethernet connection, select **Settings > Ethernet**, and enter the necessary data as outlined in the following table:

Field	Setting[1]
Ethernet	On (default)
Auto DNS Configure	Off (default)
Primary DNS Server	9.9.9.9 (Need for Airwall protection)
Secondary DNS Server	149.112.112.112 (Need for Airwall protection)

[1] Settings are for North America

Option 2 – To enable wireless Wi-Fi Client Mode communications to the modem:

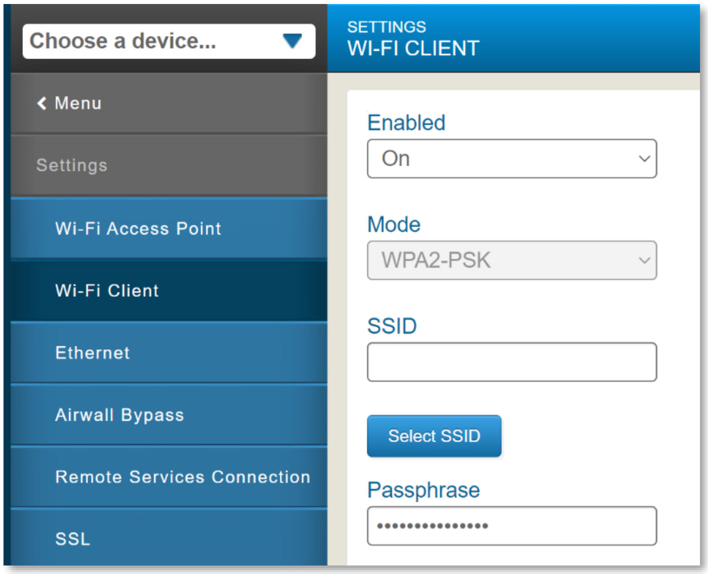
1) Disable Ethernet communications first to prevent a dual path between the modem and SBH300 –
    a. Log on to the SBH300 local UI using the SBH300 Wi-Fi connection
    b. To configure an Ethernet cable connection, select **Settings > Ethernet**, and set the “Ethernet” field to “Off”:

Field	Setting
Ethernet	Off

2) To enable wireless Wi-Fi communications to the modem via Wi-Fi Client mode:
    a. Ensure the SBH300 Wi-Fi adapter is connected to a USB port on the SBH300
    Note: In Step 1.1, the USB Wi-Fi adapter may have been removed from your system, causing the need to re-add the adapter.
    b. Select **Settings > Wi-Fi Client** from the SBH300 UI.
    c. At the top of the “Wi-Fi Client” page, use the dropdown menu to set the “Wi-Fi Client” field to “On”.

Field	Setting
Wi-Fi client	On

Figure 2.2.5.1 – SBH300 Wi-Fi Client screen



SETTINGS
WI-FI CLIENT

Enabled: On

Mode: WPA2-PSK

SSID:

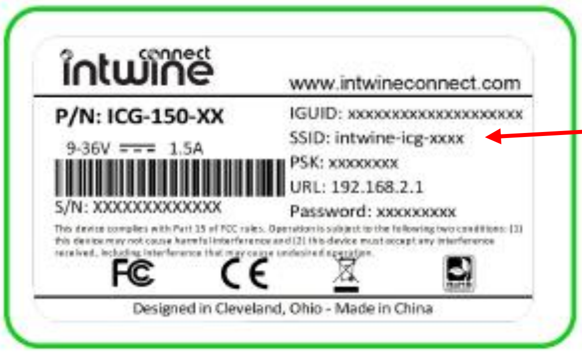
Passphrase: •••••••••••••••

d. In the field “Client SSID”, enter the SSID of the wireless network that the SBH300 will be connecting to. In the field “Passphrase”, enter the passphrase for the wireless network the SBH300 will be connecting to.

Field	Setting
Client SSID	As configured in the modem
Passphrase	As configured in the modem

As an example, if a site is using the Intwine ICG-150 modem, the default SSID is located on the device label.

Figure 2.2.5.2 – Intwine ICG-150 product connection details label



P/N: ICG-150-XX
9-36V ⎓ 1.5A
S/N: XXXXXXXXXXXXX

IGUID: xxxxxxxxxxxxxxxxxxxx
SSID: intwine-icg-xxxx
PSK: xxxxxxxx
URL: 192.168.2.1
Password: xxxxxxxxx

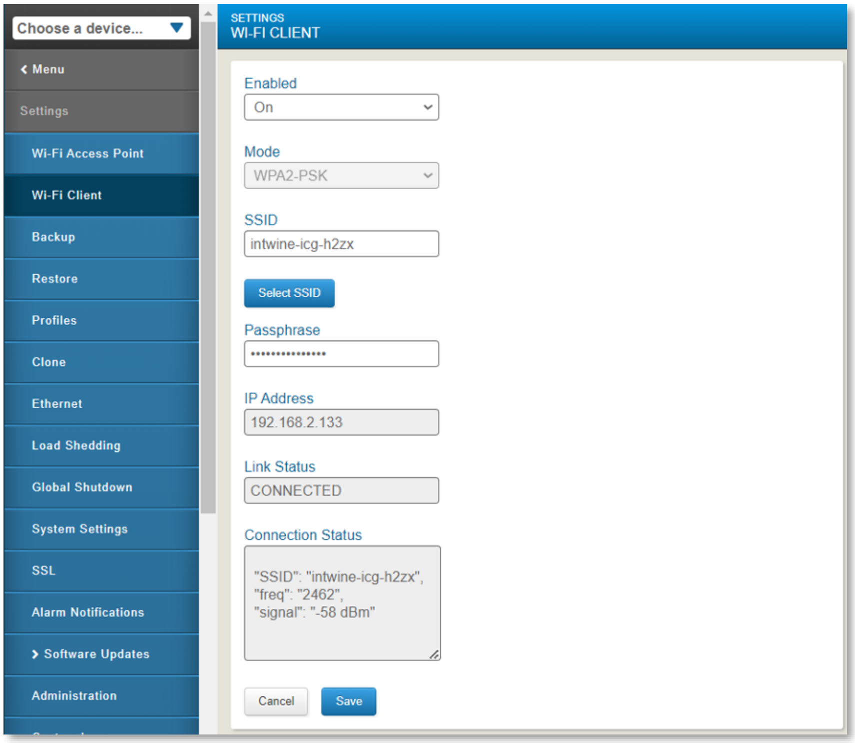
This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference and (2) this device must accept any interference received, including interference that may cause undesired operation.

Designed in Cleveland, Ohio - Made in China

Wireless Network	SSID

e. At the bottom of the screen, click “Save”. Once the changes have saved, the “Authentication Status” and “Connection Status” fields will indicate if the SBH300 has connected to the wireless network successfully.

Figure 2.2.5.3 – SBH300 Connection Status screen



Enabled: On

Mode: WPA2-PSK

SSID: intwine-icg-h2zx

Passphrase: •••••••••••••••

IP Address: 192.168.2.133

Link Status: CONNECTED

Connection Status:

```
"SSID": "intwine-icg-h2zx",
"freq": "2462",
"signal": "-58 dBm"
```

2.2.6 SBH300 – Software Updates

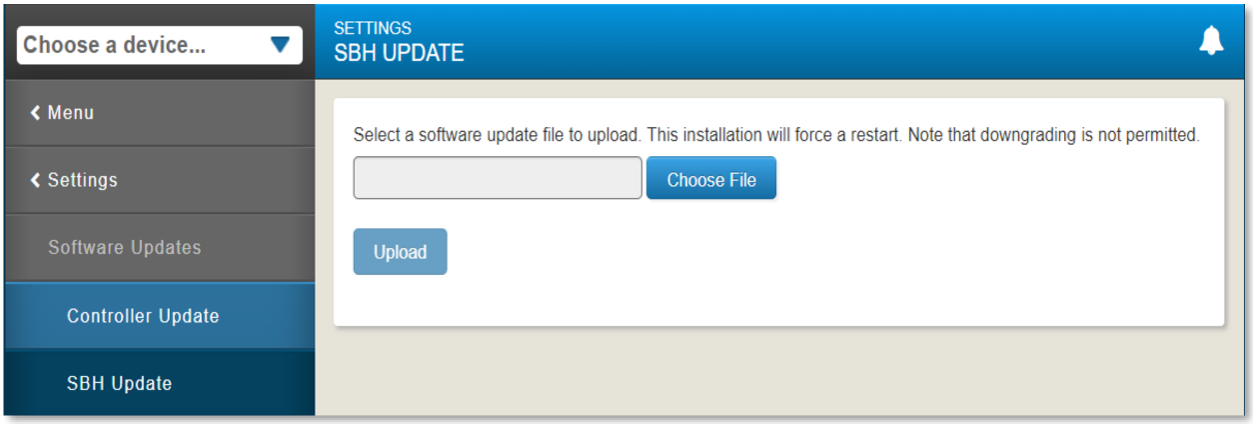
The SBH300 receives software upgrades automatically from the cloud when a new version of software is available via the **Remote Services Connection**. The SBH300 checks for software upgrade package during startup, when remote connection is re-established and periodically during an established connection.

Step 1.5 – Update SBH300 Operating System (manual only if required)

With the cloud service, local updates of the SBH300 are not required. However, it is possible to manually update the SBH300. This may be necessary if an update is required before a connection to the cloud can be established.

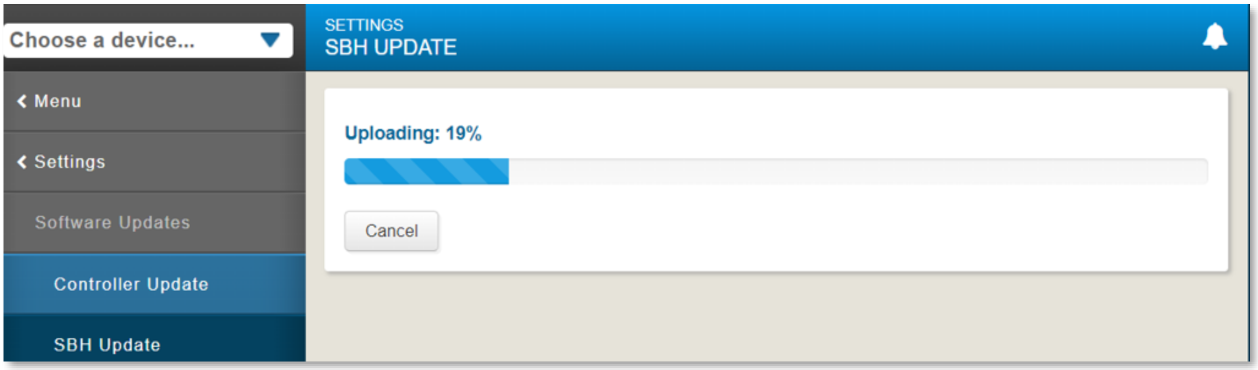
1) Log on to the SBH300 local UI using the SBH300 Wi-Fi connection
2) Select **Settings > Software Updates > SBH Update** and select **Choose File**
3) Select a file that is accessible from the laptop or mobile device connecting to the SBH300
4) Select **Upload** from the **Software Updates** screen to transfer the file to the SBH300

Figure 2.2.6.1 – SBH300 Software Updates screen



Select a software update file to upload. This installation will force a restart. Note that downgrading is not permitted.

Figure 2.2.6.2 – SBH300 Upload in progress screen



Uploading: 19%

5) After the upload has completed to 100%, you will see the **Install Button**.
   Click the **Install Button** to install the new operating system update
6) The SBH300 goes offline temporarily while the updates are applied, during which time you may see a **Connection Problem** message

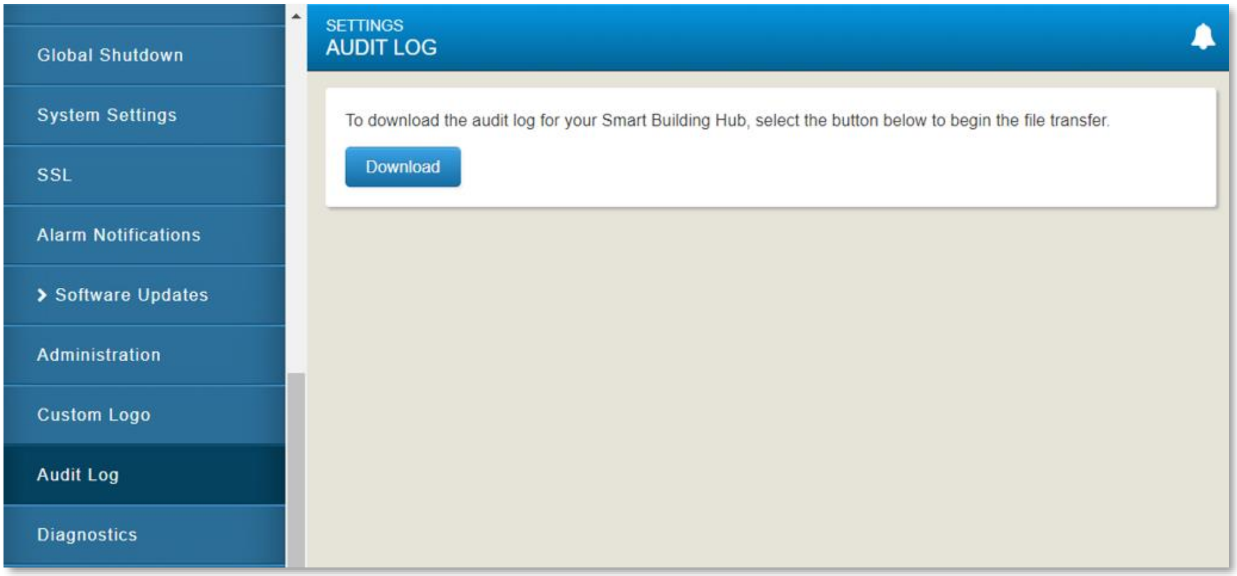
2.2.7 SBH300 – Audit Log

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

Step 1.6.1 – Audit Logs

The audit log provides a user readable text file that shows actions taken on the local SBH300 user interface.

Figure 2.2.7.1 – SBH300 Audit Log screen



To download the audit log for your Smart Building Hub, select the button below to begin the file transfer.

The audit log may be downloaded to the laptop or mobile device connecting to the SBH300 by selecting the **Download** button.

2.2.8 SBH300 – Reset Functions

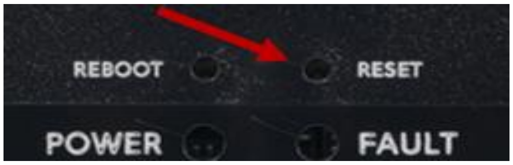
Use the following reset functions of the SBH300 if you are unable to communicate to the SBH300 or cannot logon due to lost credentials. There are two types of reset functions:

- **Network Reset** – only the network settings are reset
- **Factory Reset** – all settings are restored to factory defaults

Step 1.6.2 – Reset Functions

Use the instructions in the following sections according to the type of reset you require.
The following information applies for both types of resets (shown on the next page):

- The **RESET** button is on the front of the device and is pressed using a tiny screwdriver or similar tool



- When you press the **RESET** button, if the SBH300 is connected to the network it will disconnect
- If you press and hold the **RESET** button for more than nine seconds, the reset operation cancels
- the **RESET** button will not work if a fault condition exists

Network Reset

The Network Reset function resets Wi-Fi and Ethernet settings. Use this function if you forget your Wi-Fi connection information. To reset the Wi-Fi and Ethernet settings, complete the following steps:

1. Press and hold the **RESET** button for two seconds. The **FAULT LED** flickers slowly.

2. Release the **RESET** button within three seconds. The **FAULT LED** continues to flicker slowly.
3. Within five seconds, press the **RESET** button again, and then immediately release it to confirm that you want to reset the Wi-Fi and Ethernet settings. If you do not press the **RESET** button to confirm within five seconds, the reset operation is canceled.

The Wi-Fi SSID, passphrase, and Ethernet are set to factory defaults. The LEDs stop flickering for two seconds, then the LEDs return to normal operation based on the current state of the device.

Factory Reset

The Factory Reset function resets all device settings including user profiles to the factory defaults. The function also resets your SSL certificate to the Johnson Controls self-signed certificate that is included in the device. This function is for administrators who want to clear all user profiles from a device. The Factory Reset function does not change the version of the software. If you run a software upgrade, the SBH300 retains the upgraded software version and does not reset to the factory default version.

To reset to factory defaults, complete the following steps:

1. Press and hold the **RESET** button for six seconds. After two seconds, the **FAULT LED** flickers slowly. After an additional four seconds of holding the **RESET** button, the **FAULT LED** changes to a faster flicker.
2. Release the **RESET** button within three seconds of seeing a fast flicker. The **FAULT LED** continues to flicker quickly.
3. Within five seconds, press the **RESET** button again, and then immediately release it to confirm that you want to reset to factory defaults. If you do not press the **RESET** button to confirm within five seconds, the reset operation is canceled.

All device settings reset to factory defaults. The LEDs stop flashing for two seconds, and then the LEDs return to normal operation based on the current state of the device.

2.2.9 Security audits and documentation

A well-documented deployment of the solution will be useful in security audits, and a security audit can expose errors in the system documentation and identifying gaps in protection.

Hardening step 2.1: Security documentation

Document deployment once hardening is sufficient for run-time operations. When updates are released, or security advisories are published this documentation will be useful. The documentation will allow for quick assessment to determine if the deployment is impacted by the issues described in a security advisory and requires a configuration change, software update or patch.

Include the following details in creating as-built security documentation:

- As-built architecture drawing of system
- For all system components record:
  - Component identification
    - Name
    - Description
    - Device Type
    - Location
    - Vendor

    - Model
    - IP address
    - MAC address
- Support details
    - Software version
    - Hardware version
    - Licenses
    - Installation date
- Communication configuration details
    - Enabled Ports and protocols
    - Encryption settings

Appendix A - Additional Literature

Document title	Document number
TMR Series Wireless Best Practices	LIT-12013954
VEC100 Generic RTU Controller, Modulated Heating and Modulated Cooling Application Note	LIT-12013484
VEC100 Generic RTU Controller, Modulated Heating and Staged Cooling Application Note	LIT-12013361
VEC100 Generic RTU Controller, Staged Heating and Modulated Cooling Application Note	LIT-12013485
VEC100 Generic RTU Controller, Staged Heating and Staged Cooling Application Note	LIT-12013443
VEC100 Generic RTU Heat Pump Controller Application Note	LIT-12013452
Verasys 18 Point 24 VAC Application Controller Installation Guide	24-10143-01477
Verasys 18 Point 240 VAC Application Controller Installation Guide	24-10143-01507
Verasys 32 Point 24 VAC Application Controller Installation Guide	24-10143-01515
Verasys Airwall Agent for Android Application Note	LIT-12014322
Verasys Airwall Agent for iOS Application Note	LIT-12014323
Verasys Airwall Agent for macOS Application Note	LIT-12014321
Verasys Airwall Agent for Windows Application Note	LIT-12014307
Verasys Airwall Agent for Windows Application Note	LIT-12014307
Verasys Alarms Summary Technical Bulletin	LIT-12013648
Verasys BACnet MS/TP Communications Technical Bulletin	LIT-12012362
Verasys BACnet MS/TP Integration Technical Bulletin	LIT-12013606
Verasys Constant Volume Controller Application Note	LIT-12013067
Verasys Enterprise Configuration and User Guide	LIT-12012995
Verasys Enterprise Product Bulletin	LIT-12013647
Verasys Enterprise Security and IT Guide	LIT-12013026
Verasys Equipment Controller (VEC) Installation Guide	24-10143-1272
Verasys Input Output Module Application Note LC-VAC1002-0	LIT-12012992
Verasys Input/Output Module (IOM) Installation Guide	24-10143-1256
Verasys Input/Output Module Installation Guide	24-10143-01736
Verasys Lighting Controller Application Note	LIT-12012524
Verasys Sideloop Controller Application Note	LIT-12013364
Verasys Simple Boiler Controller Application Note	LIT-12014166
Verasys Smart Building Hub (SBH) Network and IT Guidance Technical Bulletin	LIT-12012324
Verasys Smart Building Hub (SBH300) Catalog Page	LIT-1901218
Verasys Smart Building Hub (SBH300) Installation Guide	LIT-12014293
Verasys Smart Building Hub (SBH300) Quick Start Guide	A16381V57K
Verasys System Changeover Bypass Zoning System Design Application Note	LIT-12012331
Verasys System Operation Overview Technical Bulletin	LIT-12012370
Verasys System User Guide	LIT-12012371
Verasys Tenant User Guide	LIT-12013613
Verasys TMR Series Wireless Router Installation Guide	LIT-12014167
Verasys ZEC310 Zone Damper and BYP200 Bypass Damper Controllers Installation Guide	24-10143-1248
Verasys ZEC510 VAV Controllers Installation Guide	24-10143-01485
Verasys Zone Coordinator (VZC) Installation Guide	24-10143-1280

The following table contains a list of the most important Verasys documents. For more documentation and resources, visit https://docs.johnsoncontrols.com/bas/home or http://www.verasyscontrols.com.

Appendix B - Acronyms

Acronym	Description
AP	Access Point
BAS	Building Automation System
DFD	Data Flow Diagram
DNS	Domain Name System / Service
HIP	Host Identity Protocol
HVAC	Heating, Ventilation, and Air Conditioning
HVACR	Heating, Ventilation, Air Conditioning, and Refrigeration
LAN	Local Area Network
MS/TP	Master-Slave Token-Passing
NTP	Network Time Protocol
SBH	Smart Building Hub (SBH300)
TMC	Transparent MS/TP Coordinator
TMR	Transparent MS/TP Router
VLAN	Virtual Local Area Network
ZTA	Zero-Trust Architecture