

IN-FACILITY INSTRUCTIONS FOR USE

MAY 2023

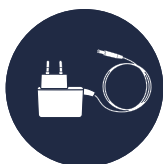
Table of Contents

- Device Overview
- Indications for Use
- Warnings and Precautions
- Installation and Setup
- Network and Firewall Settings
- Maintenance
- Support
- Safety and Regulatory Information
- Technical Specifications
- Appendices A and B

PACKAGE CONTENTS



Device unit



Power adapter



Info card

Device Overview

The BioHub™ Wi-Fi® device is a gateway that allows for seamless and secure data transmission with the BioButton® medical grade, multi-parameter wearable device.

Indications for Use

The BioHub Wi-Fi is a radio communications unit. The BioHub Wi-Fi wirelessly, via Bluetooth, collects data from authorized devices. The BioHub Wi-Fi device seamlessly and securely transmits the data via wireless or ethernet connection to the BioCloud™ data platform.

FRONT VIEW



Indicator light

BACK VIEW



Power input

Ethernet input

Warnings and Precautions

CAUTION!

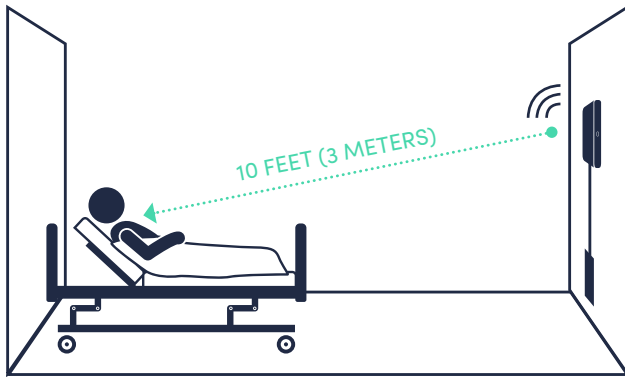
To prevent fire and electric shock, do not expose the BioHub Wi-Fi device to water or moisture. To avoid any possible risk of electric shock, never attempt to open the device. If the device is not working, contact BioIntelliSense customer care. Repair of the unit should be carried out by qualified technicians. No part of this device should be repaired by users.

WARNING!

- Place the device in a well-ventilated location to prevent accumulation of internal heat.
- Protect the receiver from high temperatures, humidity, water and dust.
- Do not place any objects that might damage the device near it (e.g., liquid filled objects).



Installation and Setup



INSTALLATION GUIDELINES FOR THE BIOHUB WI-FI GATEWAY DEVICE

- Install one (1) BioHub Wi-Fi device per patient room.
- Place the BioHub Wi-Fi <10 feet (3 meters) from the patient. Maintain an unobstructed, clear line of sight between the BioHub Wi-Fi device and patient.
- Orient the BioHub Wi-Fi with the top of the device facing towards the patient.
- Follow standard facility protocols for mounting devices within patient rooms. Optionally, apply industrial strength Velcro® adhesive strips to the back side of the BioHub Wi-Fi device. Do not cover the label with the device model and serial number information.
- Mount firmly to the patient room wall.

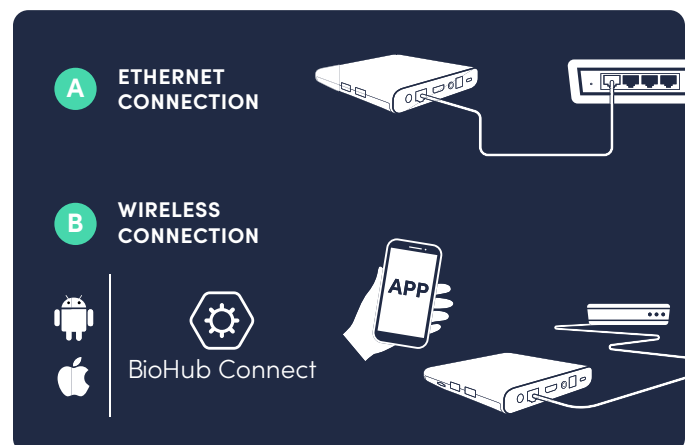
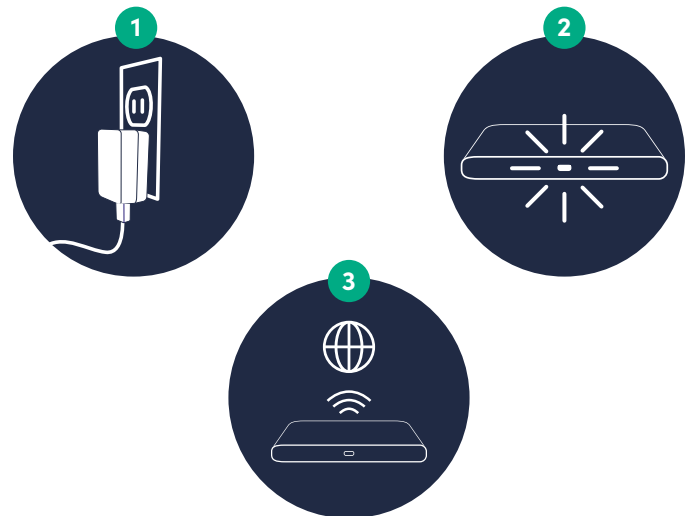
COMPLETE THE SETUP PROCESS FOR THE BIOHUB WI-FI GATEWAY DEVICE

1. Plug in the BioHub Wi-Fi device to a standard wall outlet or power source that allows the device to remain powered 24/7.
2. Confirm the BioHub Wi-Fi device indicator light turns on.
3. Connect the BioHub Wi-Fi device to the internet by plugging in an ethernet cable or connecting the BioHub Wi-Fi device to a wireless network using the downloadable BioHub Connect application.
 - a. **Ethernet connection:** Plug one end of an ethernet cable (not included) to the BioHub Wi-Fi device's ethernet port and the other directly into a wall jack.

OR

 - b. **Wireless connection:** Download the BioHub Connect app for Android or iOS mobile devices ([download here](#)). Follow the app's on-screen instructions to connect the BioHub Wi-Fi device to a wireless network.

NOTE: Do not use both the ethernet and wireless connections.





Network and Firewall Settings

The BioHub Wi-Fi device does not require that the inbound ports are open on the network to function correctly. However, there are several outbound connections that IT administrators should be aware of when setting up their respective network environments.

The following known endpoints are required for the BioHub Wi-Fi device:

ANDROID ENTERPRISE NETWORK REQUIREMENTS

Google provides a list of domains that are recommended for whitelisting and are subject to change (see Appendix A). The use of wildcards, where appropriate, provides greater flexibility in managing potential domain changes without restricting access and requiring network reconfigurations.

BIO SYNC™ APPLICATION NETWORK REQUIREMENTS

The BioIntelliSense BioSync mobile application requires various network requests to support data transmission, application analytics, and content retrieval (see Appendix B). “biocloud.biointellisense.com” is the only host that is fully controlled by BioIntelliSense. As noted above, whitelisting with wildcards allows for third-party domains to change subdomains without restricting access and requiring network reconfigurations. In addition, the subdomain wildcards ensure that requests are made within the expected domains.

MAC ADDRESS DETAILS

COMPANY:	OUI:	TYPE:
BioIntelliSense, Inc.	C0:61:3D	IEEE MA-L

Maintenance

Maintain the power source and network configuration settings for the BioHub Wi-Fi gateway to ensure a stable connection and data transmission with the BioButton patient monitoring wearable device.

GENERAL CLEANING AND DISINFECTION PROCEDURE

1. Please follow your facility's standard operating procedures (SOP) for cleaning and disinfection of electronic devices in the patient environment.
2. Remove any visible debris or contaminants using a disposable soft, non-abrasive, lint-free damp cloth or wipe.
3. Never spray products directly on the BioHub Wi-Fi device.

CAUTION: WARNINGS AND PRECAUTIONS RELATED TO CLEANING AND DISINFECTION PROCEDURE

- The device is **NOT** waterproof or water resistant.
- Avoid any water accumulation or run-off on any surface of the device. Special attention should be paid on any device panel that has openings or ports.
- Do not use liquid or aerosol cleaner or disinfectant directly on device surfaces, panels or ports.

Support

Please contact BioIntelliSense Customer Care by email at support@biointellisense.com or call **1.888.908.8804** between 7:00am - 7:00pm MT.

If you contact support after standard business hours, please leave your name, phone number and reported issue for appropriate follow-up customer service.



Safety and Regulatory Information

The BioHub Wi-Fi is a Medical Device Data System (MDDS) as defined in FDA regulation 21 CFR Section 880.6310. The BioHub Wi-Fi consists of software functions (Non-Device-MDDS) and hardware functions (Device-MDDS) that are intended to transfer, store, convert formats, and display medical device data and results.

The BioHub Wi-Fi performs all intended functions without controlling or altering the function or parameters of any connected medical devices. The BioHub Wi-Fi is not intended to be used in connection with active patient monitoring (any device that is intended to be relied upon in deciding to take immediate clinical action).

FCC STATEMENT

Model: BIOHBX1020800 (US); BIOHBX1020801 (UAE)
FCC ID: 2ASE7-BIOHBX10208

The BioHub Wi-Fi device complies with part 15 of the 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.

Radio frequency radiation exposure information:

The BioHub Wi-Fi device complies with the radiation exposure limits prescribed for an uncontrolled environment for fixed and mobile use conditions. The device should be installed and operated with a minimum distance of 20cm between the radiator and the body of the user or nearby persons. This transmitter must not be co-located or operating in conjunction with any other antenna except as authorized in the certification of the product.

The device has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. The device generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Increase the distance between the device and television or radio receiver.
- Consult the dealer, the manufacturer, or an experienced technician for help.

RESPONSIBLE PARTY

BioIntelliSense, Inc.
570 El Camino Real #200
Redwood City, CA 94063

TERMS OF USE

Use of the BioIntelliSense Product(s) is subject to BioIntelliSense Terms of Use and Privacy Policy at biointellisense.com/legal

By using the Product(s), you indicate you have read these terms and policies and that you agree to them, including the limitations and disclaimers of liability. In particular, you understand and consent that use of the Product(s) measures and records personal information about you, including vital sign and other physiologic measurements. That information may include respiratory rate, heart rate, temperature, activity level, sleep duration, body position, step count, gait analysis and other symptomatic or biometric data. You understand that the Product(s) do not render medical advice or diagnose or prevent any specific disease, including any communicable disease or virus. If you have any concerns about your health, including whether you have been exposed to or have contracted any disease or virus, immediately contact your healthcare provider.

SYMBOL LIBRARY



Bluetooth icon



HDMI icon



FCC icon



European conformance icon



Technical Specifications

DIMENSIONS

WIDTH:

4.33" / 110 mm

HEIGHT:

0.85" / 21.6 mm

LENGTH:

4.25" / 108 mm

PHYSICAL FEATURES

- **Operating Temperature**
0°C - 50°C, 32°F - 122°F
- **Storage Temperature**
-20°C - 70°C, -4°F - 158°F

LED INDICATOR COLORS

- **RED**
Standby
- **WHITE**
Active

NETWORK

- **Wi-Fi**
802.11 b/g/n/a/ac 2.4G/5G
- **Ethernet**
100 Mbps
- **Bluetooth**
Bluetooth 5.0

REGIONAL SUPPORT

- **Region Support**
North America, Middle East

HARDWARE PLATFORM

- **Chipset**
Amlogic S905X3-B
- **GPU**
ARM Mali - G31 MP2 850 MHz
- **RAM**
2GB LPDDR4
- **Flash**
eMMC 8GB

POWER

- **DC Input Range**
1x 12v 1.0 ADC Adapter
- **Power Consumption**
Maximum 12W



APPENDIX A

Android Enterprise Network Requirements

DESTINATION HOST	PORTS	PURPOSE
play.google.com android.com google-analytics.com googleusercontent.com *.gstatic.com *.gvt1.com *.ggpht.com dl.google.com dl-ssl.google.com android.clients.google.com *.gvt2.com *.gvt3.com	TCP/443 TCP, UDP/5228-5230	Google Play and updates gstatic.com , googleusercontent.com contains User-Generated Content (for example, app icons in the store) *.gvt1.com, *.ggpht, Google Chrome - Download the Fast Secure Browser from Google , Google Chrome - Download the Fast Secure Browser from Google , android.clients.google.com - Download apps and updates, Play Store APIs gvt2.com and gvt3.com are used for Play connectivity monitoring and diagnostics.
*.googleapis.com m.google.com	TCP/443	EMM/Google APIs/PlayStore APIs/Android Management APIs
accounts.google.com accounts.google.[country]	TCP/443	Authentication For accounts.google.[country], use your local top-level domain for [country]. For example, for United States use accounts.google.com.us , and for United Kingdom use accounts.google.co.uk .
gcm-http.googleapis.com gcm-xmpp.googleapis.com android.googleapis.com	TCP/443,5228-5230	Google Cloud Messaging (e.g. EMM Console <-> DPC communication, like pushing configs)
fcm.googleapis.com fcm-xmpp.googleapis.com firebaseinstallations.googleapis.com	TCP/443,5228-5230	Firebase Cloud Messaging (for example, Find My Device, EMM Console <-> DPC communication, like pushing configs). For the most up to date information on FCM, click https://firebase.google.com/docs/cloud-messaging/concept-options#messaging-ports-and-your-firewall
fcm-xmpp.googleapis.com gcm-xmpp.googleapis.com	TCP/5235,5236	When using persistent bidirectional XMPP connection to FCM and GCM servers
pki.google.com clients1.google.com	TCP/443	Certificate Revocation list checks for Google-issued certificates
clients2.google.com clients3.google.com clients4.google.com clients5.google.com clients6.google.com	TCP/443	Domains shared by various Google backend services such as crash reporting, Chrome Bookmark Sync, time sync (tlsdate), and many others
omahaproxy.appspot.com	TCP/443	Chrome updates
android.clients.google.com	TCP/443	CloudDPC download URL used in NFC provisioning
connectivitycheck.android.com connectivitycheck.gstatic.com www.google.com	TCP/443	Used by Android OS for connectivity check whenever the device connects to any WiFi/Mobile network. Android connectivity check, starting with N MR1, requires https://www.google.com/generate_204 to be reachable, or for the given Wi-Fi network to point to a reachable PAC file.
mtalk.google.com mtalk4.google.com mtalk-staging.google.com mtalk-dev.google.com alt1-mtalk.google.com alt2-mtalk.google.com alt3-mtalk.google.com alt4-mtalk.google.com alt5-mtalk.google.com alt6-mtalk.google.com alt7-mtalk.google.com alt8-mtalk.google.com android.clients.google.com device-provisioning.googleapis.com	TCP/443,5228-5230	Allows mobile devices to connect to FCM when an organization firewall is present on the network. (see details https://firebase.google.com/docs/cloud-messaging/concept-options#messaging-ports-and-your-firewall)



APPENDIX B

BioSync Network Requirements

DESTINATION HOST	PURPOSE
http://time.google.com/	BioSync: Network Time Protocol (NTP) Server used to set time on wearables
http://time1.google.com/	BioSync: Network Time Protocol (NTP) Server used to set time on wearables
https://biocloud.biointellisense.com	BioSync: Data transfer endpoint
http://storage.googleapis.com/	BioSync: Access to Google Cloud Storage to download firmware binaries for OTA
https://googletagmanager.com	BioSync: Support application analytics Reference: https://live.paloaltonetworks.com/t5/general-topics/how-to-configure-url-filtering-ssl-site/td-p/215854
https://tagmanager.google.com	BioSync: Support application analytics
*.launchdarkly.com <ul style="list-style-type: none">http://clientstream-ga.launchdarkly.comhttps://clientstream.launchdarkly.comhttps://stream.launchdarkly.comhttps://clientsdk.launchdarkly.comhttps://app.launchdarkly.comhttps://mobile.launchdarkly.comhttps://events.launchdarkly.com	BioSync: Application configuration management Reference: https://docs.launchdarkly.com/sdk/concepts/domain-list
https://app-measurement.com	BioSync: Support application analytics
*.crashlytics.com Alternatives: <ul style="list-style-type: none">crashlyticsreports-pa.googleapis.comfirebasecrashlyticsymbols.googleapis.com	BioSync: Support application analytics Reference: https://stackoverflow.com/questions/43605068/whitelisting-fabric-crashlytics-ip
http://connectivitycheck.gstatic.com	Google Server for Static Content Reference: https://www.google.com/search?q=what+is+connectivitycheck.gstatic.com&rlz=1CAOTWH_enUS825&oq=what+is+connectivitycheck.gstatic.com&aqs=chrome..69i57j0.3660j0j7&sourceid=chrome&ie=UTF-8
*.pool.ntp.org <ul style="list-style-type: none">http://2.android.pool.ntp.org	Network Time Protocol (NTP) Server used to set system time