Customer Technical Bulletin

CTB-00957 Rev 003

Date: April 11, 2022

Authors: Kevin Clarkson, Venkateswara Vaddineni

Product: Unifi™ Connect Platform

Subject: Updated Guidance for Unifi Connect Platform on Hologic's Breast and Skeletal (BSH) Systems

Revision History

Rev 002 – Updated Technology Description and IT Requirement sections to include new URLs and port number requirements.

Purpose

The purpose of this Customer Technical Bulletin (CTB) is to provide updated technical information regarding the use of Unifi Connect platform for remote diagnostics and support of Hologic BSH Systems.

Scope

This CTB is provided upon customer request.

What is Affected

All BSH systems that use Windows 7 and higher provide a new method of remote product support. Unifi Connect (which consists of Microsoft® Azure® and SecureLink™) has been adopted as the primary remote support platform to allow remote troubleshooting of all applicable BSH Systems. See Reference Table below for details.

Executive Summary

The Unifi Connect platform provides a secure connection between our Customer Support Center and customer sites to identify hardware and software problems and to send software upgrades, often without scheduling an on-site service call. It is available for most Hologic products* and minimizes equipment downtime and avoids unnecessary interruptions for on-site service.

Technical Bulletin (cont.)

The Unifi Connect platform provides rapid, high-speed connection between your Hologic products and our Customer Support staff, directly accessing the system through a safe, secure, private communications channel. The platform is also used by the Hologic Clinical Applications team for remote training.

With the continued promise to provide optimal remote performance for our customers, we have decided to create new fault tolerant and redundant geo-specific servers in lieu of one central serve. **To maximize our remote service capabilities, we request to open port 22 and port 443 for several new URLs, which avoids latencies in secure communication.** Thank you.

Reference: Hologic Products that are eligible for Unifi Connect Platform

- 3Dimensions™ Mammography System
- Selenia® Dimensions® Mammography System
- Selenia® Full-Field Digital Mammography System (on Windows OS)
- SecurView® Workstations
- Cenova™ Image Analytics Server
- Affirm® Prone Biopsy System
- Brevera® Breast Biopsy System
- Trident® HD Specimen Radiography System
- Aegis® MultiView™ Software
- RosettaDC™ Tomosynthesis data converter
- Horizon® DXA System
- Discovery® DXA System
- SecurXchange® Workflow Solutions
- Unifi™ Workspace
- Dicom 6000 software

Technology Description

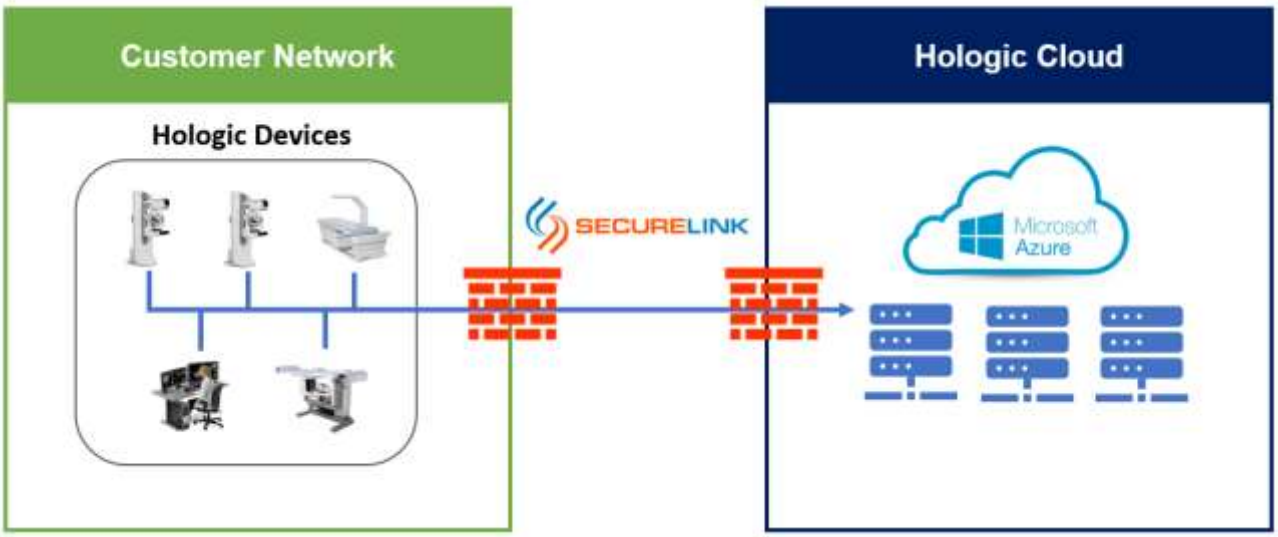

Figure 1 - Network Diagram

The Unifi Connect remote support platform is an on-demand service that can be installed once customer approval has been received by Hologic. Upon approval, a Hologic Technical Support representative will install the Unifi Connect service on each BSH System residing at the customer site. For systems that are currently using Hologic Connect, the Unifi Connect platform can be installed remotely. By default, Unifi Connect will be installed as a Windows Service and will have the service Startup Type set to auto. When the service is not running, a remote support connection to the BSH System is not available. In addition, customers are required to configure the Firewall to whitelist the URL provided at the bottom of the document and open the specified ports

To perform remote diagnostic operations or debugging an issue on the device, Hologic service team must first authenticate using Hologic MFA and then initiate a remote request using SecureLink application request, the SecureLink GateKeeper service establishes a secure end-to-end outbound connection from the BSH System to the SecureLink Application Server using SSL. The GateKeeper is locked from modification and only allows connection to the Hologic maintained SecureLink Application Server located at **.hologicsecurecare.com (See the table below)*. The TCP connection is established to port 443 and port 22 of the SecureLink Application Server. After this secure connection has been established, a Hologic support representative can remotely connect to view the GUI of the System, access important configuration files and equipment status logs or transfer files that may be needed for diagnosis of an error.

NOTE: Hologic does not support the usage of a customer's existing SecureLink infrastructure in the case this product is already in use within the organization.

Authentication into the SecureLink Application Server for Hologic support personnel is managed through Hologic Active Directory and authenticated using Okta with multi-factor authentication. Details of each remote support session (including a record of the employee ID) are archived indefinitely for audit purposes. The remote support connection activity can be made available upon request to BSH Technical Support.

Each SecureLink GateKeeper instance is uniquely identified by a registration code that is entered by a Hologic FSE during installation, allowing for granular control of GateKeeper systems that are authorized to connect to the SecureLink Application Server and unique certificate for communication

The SecureLink GateKeeper is capable of automatically updating itself to a new version to ensure vulnerabilities are addressed and allow product enhancements to be delivered without requiring a Hologic FSE visit. Once a connection has been established to the SecureLink Application Server, a version check will be performed. If a higher version is found, the GateKeeper will download the necessary components for the upgrade, perform the upgrade, and restart the service.

The SecureLink Application Server resides in Hologic's Enterprise Azure Infrastructure and is isolated onto its own network segment. The server instance Operating System is hardened to reduce attack vectors by disabling and removing unnecessary services and tools. All SecureLink session connections utilize the SSL protocol for data transport with AES-256 for bulk encryption, and RSA (2048-bit key length) for key exchange. Every key is uniquely generated per session and mutual authentication is enforced to mitigate Man-In-The-Middle attacks.

The appliance also utilizes Whitelisted shell access, a Stateful Packet Inspecting Firewall, a Web Application Firewall (WAF), an In-Line Intrusion Prevention System (IPS), an Intrusion Detection System (IDS), and an embedded anti-virus solution to mitigate unauthorized access to the appliance and increase its security posture. In addition, the Hologic Enterprise Azure Infrastructure implements an additional network firewall to mitigate unauthorized access over the network.

Workflow

1) The local instrument operator experiences an instrument error or requires further information regarding the operation of the BSH System.
2) The local system operator contacts Hologic Technical Support with their concern.
3) The Hologic support representative informs the local instrument operator they would like to establish a remote support session with the instrument and an outbound connection is established using SSL to the SecureLink Application server.
4) The Hologic support representative authenticates with the SecureLink Application Server and locates the applicable GateKeeper instance to launch either the remote desktop sharing or file transfer services.
5) Once the support session has concluded, the Hologic support representative will instruct the local system operator to stop the remote diagnostics service.

IT Requirements

It may be necessary to configure the customer's enterprise firewall to allow the BSH Systems to utilize SecureLink depending on the current Outbound Rule Set. No Inbound rules need to be added for a remote support connection to be established. The following connections must be allowed to enable a successful remote connection.

Application	URL	Protocol & Port	Connection Type
Unifi Connect	prod.unificonnect.com	TCP 443	Outbound
SecureLink	• connect.hologicsecurecare.com • connectus-west.hologicsecurecare.com • connectus-east.hologicsecurecare.com • connectus-cent.hologicsecurecare.com	TCP 22, 443	Outbound
Microsoft Azure IoT Service Bus	• proddevicefiles.blob.core.windows.net • hologiciothubprod.azure-devices.net • blob.blz21prdstr14a.store.core.windows.net • prod-ud-ns.servicebus.windows.net • iothub-ns-hologiciot-7940997-52cc229fc7.servicebus.windows.net	TCP 443	Outbound

OPTIONAL DNS PROVIDERS			
Primary DNS	OpenDNS	UDP/TCP 53	Outbound
Secondary DNS	Google	UDP/TCP 53	Outbound

If there are any questions or concerns regarding this communication, please contact your local Hologic support representative or Hologic Technical Support. Alternatively, country-specific telephone and email contact information for Technical Support can be found at www.hologic.com/support.