HOLOGIC®

Unifi™ Connect Platform Security White Paper

Overview

The Unifi™ Connect platform includes a suite of products that allows our highly trained service & support staff to exclusively and securely access your Breast Health system remotely. This connection allows us to monitor your devices and provide you with efficient service, without the need to schedule an on-site visit, thus increasing your uptime and operational continuity.

The Unifi Connect platform utilizes the same technology that is used today in highly secure environments such as government, banking, health care, data centers, and several other manufacturing environments. This technology, built on remote services leader Microsoft® Azure IoT Platform and SecureLink, has been fully certified by Microsoft security authority and SecureLink security authority. Unifi Connect platform uses SSL certificates for all internet communication and Coalfire for Pen testing.

- Application-Level Assessment – detailed testing for known security vulnerabilities in Web-based applications

The Unifi Connect platform is comprised of the following components that address the strictest of security and privacy requirements.

- Unifi Connect Agent
- Unifi Connect Enterprise

Unifi Connect Agent

The Unifi Connect Agent is built on Microsoft Azure IoT platform technology, that allows your system to exchange information securely with our Enterprise servers, even when protected behind firewalls and proxy servers.

The Unifi Connect Agent achieves this by initiating all communications with our Enterprise servers, thus eliminating the need for firewall or proxy changes. These communications are based on standard Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) standards and JSON data structure. This method of communication:

- Leverages existing security infrastructure at the device location. The device receives the same network security coverage as all other computers within your facility.
- Simplifies device deployment. Your local IT staff does not need to change their existing security configuration. Once connected to the local network, the device is ready to communicate.
- Secures the device from attack. Since the device initiates all communication, and only with our Enterprise servers, it does not have a public IP address and is therefore not publicly accessible or subject to exploitation.

The Unifi Connect Agent encrypts all communications between your devices and our secure Enterprise servers by using Secure Sockets Layer (SSL) technology to provide secure transmission of data. All communications are initiated via HTTP POST commands and transmitted exclusively on port 443 and port 22. SSL provides a protocol for transmitting private data via the Internet by encrypting data and provides authentication to ensure that both the sender and receiver of data are known to each other. SSL supports key length up to 256 bits and mutual authentication using certificates. This protects all operational device data from being susceptible to unauthorized access while it is in transit.

The Unifi Connect Agent has satisfied most major Security and Privacy requirements via the VeriSign Audit. This audit is based on: ISO 17799 Security Standard, Sarbanes Oxley Section 404, Gramm-Leach-Bliley Act, HIPAA Security Standard, NERC Urgent Action Standard 1200, CA Notice of Security Breach, 21 CFR Part 11, Information Security Forum Standard of Good Practice, IT Control Standards for Sarbanes Oxley (ITGI/ISACA), and Payment Card Industry (PCI) Data Security Standards.

The Unifi Connect Agent supports Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) thus easy setup and secure communications from within your environment.

Unifi Connect Enterprise

The Unifi Connect Enterprise encompasses the full set of tools that our service and support staff have to monitor and maintain your devices for maximum uptime and operational availability. These applications reside in a highly secure environment and are only accessible to our employees following industry standard security measures.

Access to Unifi Connect Enterprise applications are limited exclusively to our highly trained service and support staff and require username and password authentication. User access security is addressed in two ways: activity-based access control and device-based access control. Activity-based access control limits our staff to access only the application functions that are required to complete their specific roles. Device-based access control limits our staff to access only the Hologic devices that they are required to support. These methods are combined to provide a maximum level of security and auditing. User access privileges are managed using the Okta SAML/Lightweight Directory Access Protocol (LDAP) standard. User login credentials are authenticated directly against this directory and no passwords are stored within the Hologic Unifi Connect Enterprise application.

The Unifi Connect Enterprise encrypts all communications between its servers and our service and support staff by using Secure Sockets Layer (SSL) technology to provide secure transmission of data. SSL provides a protocol for transmitting private data via the Internet by encrypting data and provides authentication to ensure that both the sender and receiver of data are known to each other. SSL supports key length up to 256 bits and mutual authentication using certificates. This protects all operational device data from being susceptible to unauthorized access while it is in transit and creates a complete end-to-end secure communication path.

The Unifi Connect Enterprise requires our Service and Support staff to log in again after ten minutes of inactivity. This forced inactivity period logout ensures greater confidentiality of secure device information.

The Unifi Connect Enterprise maintains extensive audit logs of all user access requests and all application functions performed on your devices. These audit logs provide extensive reporting capabilities and allow us to ensure complete accountability for staff activities. A few examples of audited functions include user logins, trigger creation or modification, remote access sessions, etc.

The Unifi Connect Enterprise has chosen Microsoft Azure Cloud services what are audited by reputed vendors and all services satisfied most major Security and Privacy. All services used in Unifi Connect application audits are based: Sarbanes Oxley, HITRUST, HIPAA Security Standard, 21 CFR Part 11, Information Security Forum Standard of Good Practice, IT Control Standards for Sarbanes Oxley (ITGI/ISACA), and Payment Card Industry (PCI) Data Security Standards.

Unifi Connect Deployment Utility

The Unifi Connect Deployment Utility provides you, our customer, with an added level of security and control over how devices within your environment are configured to securely communicate with our servers.

Summary

The Unifi Connect platform has been designed to leverage the power of the Internet while ensuring that the data handled by the system is protected. As new security standards and practices continue to evolve, we will incorporate them into the Unifi Connect platform.

CE **EC REP** Hologic BV, Da Vincilaan 5, 1930 Zaventem, Belgium

HOLOGIC BV
Da Vincilaan 5,
1935 Zaventem
Tel: +32.2.711.4680
info@hologic.com
www.hologic.com