



Cybersecurity Product Report

MAN-06328 Revision 001

Unifi™ Workspace

Diagnostic Breast Imaging Solution

Cybersecurity Product Report

Part Number MAN-06328

Revision 001

July 2019

Technical Support

USA:	+1.877.371.4372	Asia:	+852 37487700
Europe:	+32 2 711 4690	Australia:	+1 800 264 073
All Other:	+1 781 999 7750	Email:	BreastHealth.Support@hologic.com

© 2019 Hologic, Inc. Printed in the USA. This manual was originally written in English.

Hologic, Unifi, and associated logos are trademarks and/or registered trademarks of Hologic, Inc., and/or its subsidiaries in the United States and/or other countries. All other trademarks, registered trademarks, and product names are the property of their respective owners.

This product may be protected by one or more U.S. or foreign patents as identified at www.Hologic.com/patents.



Hologic Inc.
36 Apple Ridge Road
Danbury, CT 06810 USA
1.800.447.1856
www.hologic.com

Asia Pacific Hologic Hong Kong, Inc.
7th Floor, Biotech Centre 2
No. 11 Science Park West Avenue
Hong Kong Science Park
Shatin, New Territories
Hong Kong

Australia / Hologic (Australia) Pty Ltd.
New Zealand Suite 402, Level 3
2 Lyon Park Road
Macquarie Park NSW 2113
Australia

HOLOGIC®

Table of Contents

1: Introduction

1.1 Audience

1

2: Cybersecurity

2.1 Manufacturer Disclosure Statement for Medical Device Security

2.2 Windows Domain and Active Directory

2.2.1 Third Party Software Packages

2.2.2 Intrusion Detection

2.2.3 Encryption

2.2.4 Operating System Patching

1

Introduction

Hologic is a leading developer, manufacturer and supplier of premium diagnostics, medical imaging systems and surgical products dedicated to serving the healthcare needs of women. Ensuring the integrity of our systems and the business continuity of our customers is a top concern for Hologic. This document is to be used in conjunction with Hologic's Enterprise Cybersecurity Best Practices Guide to assist an IT staff in securing their systems and infrastructure where Unifi™ Workspace is deployed.

1.1 Audience

The intended audience includes the systems administrator, network administrator, and/or security personnel. The reader of this document should be familiar with operating systems, networking, and security of computer systems.

Cybersecurity

Readers should be familiar with the Hologic Enterprise Cybersecurity Best Practices Guide available in the Unifi Workspace Support section of the Hologic website. The following sections of this document outline security features and guidelines specific to Unifi Workspace. For additional guidance or assistance in implementing security features on Unifi Workspace systems, consult Hologic Technical Support.

2.1 Manufacturer Disclosure Statement for Medical Device Security

For many products, Hologic uses the Manufacturer Disclosure Statement for Medical Device Security (MDS2) to provide HIPAA-related security information about its products. The latest version of the Unifi Workspace MDS2 is located in the Unifi Workspace Support section of the Hologic website.

2.2 Windows Domain and Active Directory

Unifi Workspace supports the use of Active Directory as a mechanism for user authentication.

2.2.1 Third Party Software Packages

Antivirus

The use of antivirus software is recommended for Unifi Workspace. Installation instructions provided with the antivirus software product should be used for installation and configuration.

If antivirus software is installed, the following directories¹ should be excluded from real-time scanning as not doing so may affect product performance:

- Unifi Workspace Application:
 - E:\Unifi Workspace (by default)
- Unifi Data Partition:
 - F:\Data (by default)
- Unifi database, settings, and log folder:
 - C:\ProgramData\Hologic
LogViewer
Unifi Workspace

2.2.2 Intrusion Detection

It is not recommended to run real-time intrusion detection monitoring software when Unifi Workspace is active as it may affect performance of the application. Intrusion detection could be run on the system when the Unifi Workspace application is idle.

2.2.3 Encryption

All Unifi Workspace hardware implements FIPS 140-2 encryption, consisting of AES 256 self-encrypting drives. Unifi Workspace also uses Bitlocker on all drives as a second means of data protection.

2.2.4 Operating System Patching

Unifi Workspace software runs on Windows 10. Microsoft frequently creates patches, service packs, and critical security updates to address potential vulnerabilities in these operating systems.

Due to the fact that vulnerabilities and updates may occur on a more frequent basis and the risk due to vulnerabilities is generally greater than the impact of a fix, customers may implement Automatic Updates for Microsoft Windows. For additional guidance on implementing Automatic Updates, consult Hologic Technical Support.

Patch release reports of approved patches are available on the Hologic website. It is recommended that you have a rollback strategy when applying patches not included in the Hologic patch release reports.

¹ The paths for these directories may be different for Unifi Workspace software-only installation.