DXA Products Cybersecurity Best Practices Guide

MAN-07193 Revision 002

HOLOGIC®

DXA Products

Bone Densitometry Systems

Cybersecurity Best Practices Guide

Part Number MAN-07193

Revision 002

November 2023

Product Support

USA: +1.877.371.4372

Europe: +32 2 711 4690

Asia: +852 37487700

Australia: +1 800 264 073

All Other: +1 781 999 7750

Email: BreastHealth.Support@hologic.com

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

Australia
Hologic (Australia & New Zealand) Pty Ltd
Level 3, Suite 302
2 Lyon Park Road
Macquarie Park, NSW 2113
Australia
1.800.264.073

1.0 Overview

Hologic, Inc. develops and markets a full line of Bone products. Ensuring the integrity of our systems is a top priority for Hologic. This document provides a guide for user "best practices" to ensure the integrity of Hologic products through their lifecycle. Additionally, this document outlines the most common cybersecurity vulnerabilities and the appropriate methods for securing our products.

Hologic uses Microsoft Windows® 7 and Windows 10 operating systems in its Dual-energy X-ray absorptiometry (DXA) medical products. Although Hologic performs extensive testing prior to the deployment of our computer systems, ongoing computer security threats may pose a significant threat to the security of these systems daily.

These Cybersecurity Best Practice recommendations have been performed in a laboratory environment and have undergone extensive testing. Adherence to these security recommendations will minimize the risk of cybersecurity threats. An experienced IT professional should be able to follow these instructions with minimal difficulty.

2.0 Introduction

Hologic continually monitors the current state of computer and network security to assess potential threats to our systems. Once the concern has been identified and properly classified, Hologic performs a risk analysis to determine the potential consequences of cyber-attacks. Additionally, the risk analysis will assess the potential consequences for actively mitigating the threat by inducing a product change.

Hologic also has an on-going maintenance program for the entire life cycle of our products. The on-going maintenance program consists of:

- Periodic vulnerability Assessments
- Laboratory evaluation of Anti-virus products
- Critical security updates validation
- Creation of a Cybersecurity team

Hologic is committed to delivering and maintaining our products in the rapidly changing environment of cybersecurity threats. By following the Cybersecurity Best Practices below and incorporating them into your facilities security policies and protocols, your cybersecurity risk and vulnerabilities will be minimized.

2.1. Audience

This document contains information related to the Hologic DXA systems. It is intended to aid in securing the customer's network infrastructure and network environment that incorporates Hologic products.

The reader of this document should be familiar with the OSI model, networking, and network security.

2.2. Remarks

It is recommended that the customer implement and maintain a set of facility security policies and procedures. These security policies and procedures should address the following:

- Discretionary access control
- Methods of auditing
- Disaster Recovery Plans / Business Continuity Plans
- Password reset policy
- Perimeter security (for example, firewalls, IDS, proxy servers)
- Internal security (for example, network topology monitors, log file review, weekly vulnerability scans)
- Physical Security (for example, biometrics, locks, cameras)
- Security Awareness

It is the customer's responsibility to ensure the confidentiality, integrity and availability of the information technology resources in its organization.

2.3. Definitions, Terms and Abbreviations

802.1q: The IEEE standard for VLAN tagging

ACL: Access control list

CBAC: Content Based Access Control

CLOC: Cyber level of concern

DAC: Discretionary Access Control

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized zone

Egress: Traffic destined outbound

FTP: File Transfer Protocol

IP: Internet Protocol

ISL: Inter-switch link protocol

LAN: Local Area Network

Layer 3: Any device that utilizes the 3rd layer of the OSI model (AppleTalk ®, IP, etc.)

IDS: Intrusion Detection System

OSI model: Open Systems Interconnection Reference Model

VLAN: Virtual LAN

TCP/IP: Transmission Control Protocol/Internet Protocol suite

TFTP: Trivial File Transfer Protocol

2.4. References

- FDA Guidance for Off-The-Shelf Software Use in Medical Devices, 2016
- FDA General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002
- NEMA Patching Off-the-Shelf Software Used in Medical Information Systems, 2004

3.0 Network Security

3.1. Active Directory

Hologic DXA systems are compatible with Active Directory however connecting them to network domains may cause undesirable behavior because of transfer of domain policies and other configurations to Hologic systems Since domain controllers override Hologic DXA system's factory settings, Hologic cannot support issues caused by domain policies and recommends you remove the system from network domain should unexpected behavior occur.

3.2. Segmentation

Properly segmenting Hologic's products from the rest of your network can further increase the security of the systems. The goal with segmentation is to prevent unauthorized access to the system(s) by utilizing ACLs.

3.2.1 VLANs

VLANs (or Virtual LAN) are a way to create several different broadcast domains on a single switch. VLAN capability is available on most modern switches.

Utilizing VLANs allows you to apply some level of security (access control lists and CBAC) to protect certain extensions of your network. If implemented correctly, this creates a "virtual" DMZ.

Resources needed:

- VLAN capable switch
- Layer 3 switch OR existing router capable of recognizing different VLAN tagging (that is, 802.1q, ISL)
- Knowledge of networking and Cisco products

Note
VLANs were designed for management purposes and not for security. There are specific cybersecurity threats (attacks) where a user can "jump" VLANs. A more effective way of segmenting a LAN would be using a physical interface off a firewall.

3.2.2 Firewall segmentation

Many hardware firewalls are equipped with a 3rd interface. This interface is typically used as a DMZ in small to mid-size network. However, this 3rd interface may also be utilized to create a dwelling for machines that need increased security.

3.3. Egress Filtering

It is recommended that you employ egress filtering on your network. This will reduce the chances of external data theft and/or loss. In the beginning stages of a system compromise, one of the first things an attacker will do is TFTP or FTP to a remote server that stores privilege escalation tools. Implementing proper egress filtering will reduce the chances of this occurring.

3.4. Network Monitoring

Effective monitoring of your network may detect the initial reconnaissance stages of a potential attack. This is vital information to capture, as it may indicate how and when a system may be compromised. Network monitoring can be accomplished by utilizing an Intrusion Detection System (IDS).

3.5. Remote Administration

Hologic does not allow the installation of remote monitoring programs like LogMeIn or VNC on the Hologic DXA System. Any administration that needs to be accomplished should be done physically at the PC or using Hologic Connect™. Alternatively, you can contact your local service representative for assistance.

4.0 Host Based Security

4.1. Anti-virus Products

It is recommended that you employ anti-virus software to protect your DXA system. While there are several “All in one” anti-virus products available on the market, Hologic does not recommend using these as they may compromise system stability. These “All in one” anti-virus products usually include: an Antivirus engine, Anti-spy ware and stateful firewall. These can significantly raise CPU usage and memory usage during regular usage, which may result in:

- CPU Deprivation
- System hangs
- Performance degradation
- Potential data corruption

Hologic recommends that anti-virus products be configured for "on-demand" scanning and not "real-time protection." Real-time protection can significantly raise CPU usage and memory usage which may result in problems during image acquisition.

In the event that real time protection or auto scans cannot be disabled, it is recommended to create exceptions for Hologic specific folders to exclude them from anti-virus scans.

4.2. Host-based Firewalls

Hologic does not allow the installation of 3rd party host-based firewalls on our systems. Some 3rd party host-based firewalls are vulnerable to denial of service attacks and if improperly configured, may let an intruder gain system level access to the system. The APEX™ system comes shipped with Windows built in firewall enabled.

4.3. System-level Auditing

Hologic's products are shipped with auditing enabled to track security events. This is to provide accountability and to help diagnose potential problems that may arise. Please do not attempt to disable auditing. It is recommended a daily review of the logs be completed to ensure the integrity of the system.

4.4. Internet Usage

Please do not allow any users or staff to access the Internet from any of the Hologic DXA systems. This exposes your systems to a plethora of vulnerabilities such as:

- Viruses
- Spyware
- Trojans
- Hostile code (embedded into webpages)

Hologic's products are considered medical devices; therefore, you are not permitted to install unauthorized software on your own. Peer to peer software can expose your entire hard drive to any individual running the same type of software.

4.5. Auditing

Hologic depends upon auditing to provide for accountability and to track system changes. It also assists us with diagnosing potential problems that may arise. Hologic has tested the Hologic DXA system with auditing enabled and determined that proper operation is not compromised.

To enable auditing:

1. Select **Start** > R**un**, and type **gpedit.msc**.
2. Browse to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policy** > **Audit Policy**.
3. Define every object for both "Success" and "Failure."
4. Browse to **Control Panel** > **Administrative Tools** > **Event Viewer**.
5. Right-click on **Security** and select **Properties**.
6. Browse to **Control panel** > **Administrative Tools**. Double-click **Event Viewer**.
7. Expand **Event viewer (Local)** > **Windows Logs** in the tree in the left pane.

8. Right-click **Security** and select **Properties**.
9. Ensure that auditing is set to overwrite as needed. Maximum log size should not be smaller than 1000Kb. Failure to ensure that this setting is enabled may prevent access to the machine should the hard drive become full.

Note
It is important that the clock on your system is set correctly. If the time is set incorrectly, it will not provide proper accountability in the event of a system compromise. Hologic recommends using an in-house NTP server to synchronize the clock on all your systems (including all network-based monitoring devices).

4.6. System Patching

Hologic's products are considered medical devices, therefore you are not permitted to upgrade the operating system or apply service packs that have not been validated by Hologic. Hologic periodically performs regression testing on critical patches and service packs.

5.0 Physical Security

It is recommended you employ some method of physical security when dealing with our systems. This ensures only authorized personnel have access to Hologic's products.

There are several vulnerabilities a malicious user could exploit locally. Some examples are:

- Theft of equipment
- Local password cracking
- Installation of hardware keyloggers

5.1. Desktop Security

It is of vital importance to ensure desktop security is addressed in your environment. Some examples of desktop security are:

- Log out of system when not in use
- Utilize a form of close captioned monitoring
- Physically segment the systems in a secure room

5.2. Onsite Vendors

If your organization uses vendors to assist in the administration of your network infrastructure, please make them aware of the recently added Hologic products. Ensure they do not make any configuration changes in any network devices. Doing so may adversely affect the performance of our products. It is also advised that you do not permit any outside vendors near our systems unless there is an absolute need (such as faulty network drop).

6.0 Securing Windows

The DXA Family of products, including Physicians Viewer, do not incorporate application level rights management but instead, rely on the Windows Operating System for rights management of users. Ensuring OS level of authentication is the responsibility of the customers IT departments.

6.1. Hard Drive Encryption

Windows 10 includes BitLocker, a hard drive encryption feature designed to protect data by providing encryption for entire volumes. BitLocker is not enabled in Windows by default but may be enabled if hard drive encryption is desired for your system.

Note
BitLocker requires you to back up your recovery key. A recovery key is used to access files and folders if you are having problems unlocking your PC. This back up key cannot be saved on an encrypted drive which would be your PC's hard drive. It is recommended to save to a USB drive and make multiple copies in the event one is damaged or lost.

To enable BitLocker:

1. Ensure APEX is not running (exit APEX without Shutdown).
2. Insert a USB drive with at least 5 MB of free space into a USB port on the computer for use as the recovery key (see note above).
3. Browse to **Control Panel** > **System and Security** > **BitLocker Drive Encryption**.
4. Select **Turn on BitLocker**.
5. At the **User Account Control** prompt enter the password for the Admin user. Select **YES**.
6. Select **Save to a file**.
7. Select the path for the recovery key USB drive and select **Save** (DO NOT change the file name or type).
8. Remove the USB drive.
9. Select **Next** on the **How do you want to back up your recovery key?** screen.
10. Select the option to **Encrypt entire drive** and then select **Next**.
11. Select the option for **New encryption mode** and then select **Next.**
12. Ensure the option to **Run BitLocker system check** is enabled and then select **Continue**.
13. Restart the computer.

14. Login as the **QDR** user and exit APEX without shutdown.
15. Browse to **Control Panel** > **System and Security** > **BitLocker Drive Encryption**.
16. The **Operating system drive** status will be shown as **C: BitLocker Encrypting** while the hard drive is being encrypted.
17. Do not use the computer until BitLocker is finished encrypting the hard drive (this process could take about an hour). When the **Operating system drive status** is shown as **C: BitLocker on** the hard drive has been successfully encrypted.

6.2. CPU Hibernation

APEX systems are configured from factory to never hibernate. This eliminates the possibility of scan being interrupted due to unexpected sleep timeouts.

6.3. Null Sessions

Null sessions are a built-in part of Microsoft's operating system. They allow systems and users to view available resources from other servers or domains. This can be useful if you manage a large enterprise. However, there are severe risks with null sessions. Null sessions do not require authentication and leave no trace if the proper auditing is not in place. Windows is protected against null sessions by default. However, improper configuration can resurrect this vulnerability. To ensure your machine is protected against Null Sessions, perform the following:

1. Open **Administrative tools** (via Control Panel).
2. Double-click **Local Security Policies**.
3. Expand **Local Security Policies** and highlight **Security Options**.
4. Locate the parameter titled "Network Access: Do Not Allow Anonymous Enumeration of Sam accounts."
5. Ensure this is set to **Enabled**.
6. Locate the parameter titled "Network Access: Do Not Allow Anonymous Enumeration of Sam accounts and shares."
7. Ensure this is set to **Enabled**.
8. If possible, disable NetBIOS over TCP/IP and Unbind File and Print Sharing which will remove all SMB based protocols in the Hologic DXA system and will effectively thwart all SMB based password attacks.

6.4. Disabling Services

Browse to **Control Panel>Administrative Tools>Services.**

Locate the following services:

- Remote Registry

Set the services to a **Stopped** and **Disabled** state.

6.5. Password Security

In today's world, passwords can be compromised in literally seconds by using a wide variety of tools and techniques. As new automated tools are invented each year, the more trivial it becomes to crack passwords (both remotely and locally). To lower the possibility of a compromised password, it is vital that a set of protocols be adhered to.

- Choose a password between 7-10 characters (choosing a password 15 characters or greater ensures the password is not stored as LmHash).
- Use special characters in the password (for example, @ % &).
- Do not share your password.
- Do not base your password on a pet, loved one or dictionary name.
- Do not write down your password.
- Make your password alphanumeric. This can trick a potential attacker (some tools only crack passwords upper-case).
- Examine the back of your host computer system for hardware keyloggers.
- Do not leave your account logged in.
- Routinely examine the event viewer logs. Under the **Security** tab, look for failed attempts. This may be a sign of an attack.
- Define an "Account Lockout Policy" (see next Section).

Furthermore, your Hologic DXA system is configured so any local passwords are not stored as LANMAN. This will thwart most locally based password attacks.

6.6. Account Lockout Policy

Defining an "Account Lockout Policy" ensures a user account will be locked out after a pre-defined number of failed attempts. This is important to define, as it will protect your user account from being "brute forced attacked."

7.0 Further Assistance

Hologic is here to help. If at any time you need further assistance or just have general questions regarding the security of Hologic products, please do not hesitate to contact us at 800.321.4659. You may also reference our Security Center at https://www.hologic.com/hologic-products/breast-skeletal/horizon-dxa-system