



**APEX™ Cybersecurity Best Practices**  
MAN-00462 Revision 009

### Table of Contents

---

<b>1.0 OVERVIEW</b> .....	<b>4</b>
<b>2.0 INTRODUCTION</b> .....	<b>5</b>
2.1. AUDIENCE .....	5
2.2. REMARKS.....	5
2.3. DEFINITIONS, TERMS AND ABBREVIATIONS.....	6
2.4. REFERENCES .....	6
<b>3.0 NETWORK SECURITY</b> .....	<b>7</b>
3.1. ACTIVE DIRECTORY .....	7
3.2. SEGMENTATION.....	7
3.3.1 VLANs.....	7
3.3.2 Firewall segmentation.....	7
3.3. EGRESS FILTERING.....	7
3.4. NETWORK MONITORING .....	8
3.5. REMOTE ADMINISTRATION.....	8
<b>4.0 HOST BASED SECURITY</b> .....	<b>9</b>
4.1. ANTI-VIRUS PRODUCTS.....	9
4.2. HOST-BASED FIREWALLS .....	9
4.3. SYSTEM-LEVEL AUDITING.....	9
4.4. INTERNET USAGE .....	9
4.5. AUDITING .....	10
4.6. SYSTEM PATCHING.....	10
<b>5.0 PHYSICAL SECURITY</b> .....	<b>10</b>
5.1. DESKTOP SECURITY .....	11
5.2. ONSITE VENDORS.....	11
<b>6.0 SECURING WINDOWS®</b> .....	<b>11</b>
6.1. CPU HIBERNATION.....	11
6.2. NULL SESSIONS .....	11
6.3. DISABLING SERVICES.....	12
6.4. PASSWORD SECURITY .....	12
6.5. ACCOUNT LOCKOUT POLICY.....	12
<b>7.0 FURTHER ASSISTANCE</b> .....	<b>13</b>

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

Hologic, APEX™, 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](http://www.Hologic.com/patents).

## **1.0 Overview**

Hologic, Inc. develops and markets a full line of Bone products including the APEX™ system. 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 Hologic 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 on a daily basis.

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 system. 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 (e.g., firewalls, IDS, proxy servers)
- Internal security (e.g., network topology monitors, log file review, weekly vulnerability scans)
- Physical Security (e.g., 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 3<sup>rd</sup> 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 APEX 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 APEX 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.

#### 3.3.1 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 (i.e.: 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 of a firewall.*

#### 3.3.2 Firewall segmentation

Many hardware firewalls are equipped with a 3<sup>rd</sup> interface. This interface is typically used as a DMZ in small to mid-size network. However, this 3<sup>rd</sup> 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 APEX™ 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 can't 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 3<sup>rd</sup> party host based firewalls on our systems. Some 3<sup>rd</sup> 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 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 depend 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. Click START > run, 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.

Browse to Control panel > Administrative Tools. Double click "Event Viewer." Expand "Event viewer (Local)" > "Windows Logs" in the tree in left pane. Right click "Security" and select properties. Ensure that auditing is set to overwrite as needed. Maximum log size should not be smaller than 1000Kb. Failure to ensure this setting is enabled may prevent access to the machine should the hard drive become full.

*NOTE: It is important 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 (i.e., faulty network drop).

## 6.0 Securing Windows®

### 6.1. CPU Hibernation

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

### 6.2. 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 isn't 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 up 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. Perform the same for "Network Access: Do Not Allow Anonymous Enumeration of Sam accounts and shares."

Additionally, disabling NetBIOS over TCP/IP and Unbinding File and Print Sharing will remove all SMB based protocols in the Hologic DXA system. This will effectively thwart all SMB based password attacks.

### 6.3. Disabling Services

Browse to Control Panel>Administrative Tools>Services

Locate the following services. Set the services to a “stopped” and “disabled” state.

- Remote Registry

### 6.4. 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 (i.e., @ % & ).
- 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 below).

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

### 6.5. Account Lockout Policy

Defining an “Account Lockout Policy” ensures a user account will be locked out after a pre-defined amount 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>