Antivirus Software Installation

For Breast & Skeletal Health Products

RD-04468 Revision 001

HOLOGIC®

Table of Contents

1. Purpose

This document provides guidance for approved antivirus software use on Breast & Skeletal Health product systems. It provides details on which antivirus solutions are supported, Hologic product versions tested and found to be compatible with those solutions, as well as any additional guidance for installation and configuration of the antivirus software.

2. Scope

This document applies to Breast & Skeletal Health products.

3. Estimated Time

Installation and configuration of antivirus products typically takes approximately 30 minutes to complete.

4. Definitions

- **LiveUpdate –** This is a feature that allows servers and clients to retrieve updates from an internal server or Symantec's official LiveUpdate server.
- **Managed –** The client system is configured to send virus alerts and to retrieve virus updates from an internal parent Symantec server.
- **Real-Time –** This term refers to real-time scanning of each file that is loaded in RAM.
- **SmartScan –** This is a scanning technique that scans the header of each file to determine its true file extension and to identify possible malicious code.
- **Unmanaged –** The clients do not connect to the network, nor do they have a parent server with which they communicate. These clients must download their own virus definition updates.

5. Hologic Products & Approved Antivirus Software

Hologic® has verified third party antivirus software for only the Breast and Skeletal Health products and versions listed below. These products and versions have been tested with the antivirus software listed and found to be compatible. Only Hologic products and antivirus software combinations tested should be configured to ensure optimal operation of the medical device.

Hologic does not recommend installing any other antivirus product or version. Hologic cannot guarantee the effectiveness of these products in the prevention of malicious software.

The following Hologic products have been tested.

Note
The customer must provide antivirus agent software. Load only the client/agent software and only one antivirus program per system.

5.1. Advanced Workflow Manager (AWM)

Advanced Workflow Manager (AWM) v1.11

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Server): 2022.2.2.1 (Core) / 2021.3.1.15 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

Advanced Workflow Manager (AWM) v1.10

- Symantec™ Endpoint Protection 14
- McAfee® Endpoint Security 10.6
- Sophos® Endpoint Security & Control 10.8 and Sophos Intercept X 2.0
- Trend Micro® OfficeScan® 12

Advanced Workflow Manager (AWM) v1.6 to v1.9

- Symantec™ Endpoint Protection 12
- McAfee® Enterprise VirusScan 8.8
- Sophos® Endpoint Security & Control 10
- Trend Micro® OfficeScan® 10.6

5.2. Affirm Prone Biopsy System

Affirm Prone Biopsy System v1.1

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

Affirm Prone Biopsy System v1.0

- Symantec™ Endpoint Protection 12
- McAfee® Enterprise VirusScan 8.8
- Sophos® Endpoint Security & Control 10
- Trend Micro® OfficeScan® 11

5.3. Brevera

Brevera v1.1

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

Brevera v1.0

- Symantec™ Endpoint Protection 12
- McAfee® Enterprise VirusScan 8.8
- Sophos® Endpoint Security & Control 10
- Trend Micro® OfficeScan® 11

5.4. Cenova

Cenova v4.0

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

Cenova (Legacy)

- Previously left up to end user's discretion. Recommend using one of the antivirus software now being validated.

5.5. Dimensions / 3Dimensions

Dimensions v1.11 / 3Dimensions v2.2

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

Dimensions v1.10 / 3Dimensions v2.1

- Symantec™ Endpoint Protection 14
- McAfee® Endpoint Security 10.6
- Sophos® Endpoint Security & Control 10.8 and Sophos Intercept X 2.0
- Trend Micro® OfficeScan® 12

Dimensions v1.6 to v1.9

- Symantec™ Endpoint Protection 12
- McAfee® Enterprise VirusScan 8.8
- Sophos® Endpoint Security & Control 10
- Trend Micro® OfficeScan® 11

5.6. Faxitron Specimen Radiography Systems

Products:

- Faxitron Core
- Faxitron Path
- Faxitron Path Plus
- Faxitron Pro
- Faxitron Pro Plus
- Faxitron OR
- Faxitron BioVision+
- Faxitron VersaVision
- Faxitron MultiFocus

Running Vision v3.1 Software

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

5.7. Horizon DXA

Horizon DXA v5.6

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

Horizon DXA (Legacy)

- Symantec™ Endpoint Protection 14

5.8. Insight / Insight FD

Insight / Insight FD v6.1

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

Insight / Insight FD (Legacy)

- Symantec™ Endpoint Protection 14

5.9. SecurView DX/RT Workstation and Manager

SecurView v11.1

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

SecurView (Legacy)

- Previously left up to end user's discretion. Recommend using one of the antivirus software now being validated.

5.10. Trident HD

Trident HD v1.0

- Symantec™ Endpoint Protection: 14.3.8268.5000
- McAfee® Endpoint Security: 5.7.7.378
- Sophos Intercept X (Endpoint): 2022.2.1.9 (Core) / 2022.1.1.22 (Intercept X)
- Trend Micro® Apex One: 14.0.11676
- CrowdStrike® Falcon®: 6.44.15803.0
- Blackberry® Cylance Protect: 3.0.1005.38

5.11. Trident (Legacy)

Trident v1.x

- Symantec Endpoint Protection 12
- McAfee Enterprise VirusScan 8.8
- Sophos Endpoint Security & Control 10
- Trend Micro OfficeScan 10.6

6. Customer Preparation Checklist

Before the installation, note the following:

- Hologic does not supply antivirus software. It is the responsibility of the customer to procure the software and associated licenses.
- Windows Defender (the built-in antivirus software) is enabled by default.

7. Preinstallation Checklist

Prior to the installation, review the following:

- Ensure that you have access to a Service-level (administrator) user on the system. Contact Hologic Technical Support (877.371.4372) if you need assistance creating a Service-level user.
- Ensure that no existing antivirus software is loaded on the workstation prior to installation.

8. Antivirus Installation Guidance

8.1. Overview

This section provides general guidance on installing and configuring the agent/client software on the product.

All antivirus software tested for compatibility by Hologic are IT-centric products that are geared toward an enterprise with IT support staff. Hologic assumes that the customer:

- has the infrastructure already running;
- has the personnel with expertise to deploy and manage the antivirus product; and
- only needs general guidance, such as recommended features and files or directories on Hologic systems to exclude from scanning.

8.2. Installing Agent Software on the Product

It is recommended that only the endpoint antivirus agent software be installed on the product. Agent software should typically be installed as an administrator user. Customer IT provides or installs the agent software.

8.3. Recommended Features

It is recommended that only core antivirus monitoring and scanning features be installed or configured for the product. To achieve this, we recommend adding Hologic products to their own antivirus policy group and configuring them with the following in mind.

Advanced features such as device firewall, encryption, application control, application behavior monitoring, and web control can increase the risk of reduced productivity due to the high maintenance required to care for them properly. These features should either be disabled or configured at your own risk if you have the local personnel with the skill set to configure and maintain them.

8.4. Product Scan Exclusions

For optimal product application performance, it is important that the antivirus agent software be configured to exclude monitoring of the following directories, **subdirectories**, and file types defined below per product supported.

8.4.1. Advanced Workflow Manager (AWM)

- Product Directories (including sub directories):
  - C:\Gemini
  - C:\Img
- DICOM File Type:
  - *.dcm

8.4.2. Affirm Prone Biopsy System

- Product Directories (including sub directories):
  - C:\Aries
  - C:\Img
- DICOM File Type:
  - *.dcm

8.4.3. Brevera

- Product Directories (including sub directories):
  - C:\Orion
  - C:\Img
- DICOM File Type:
  - *.dcm

8.4.4. Cenova

- Product Directories (including sub directories):
  - C:\Program Files\Hologic
  - C:\CasesFolders
- DICOM File Type:
  - *.dcm

8.4.5. Dimensions / 3Dimensions

- Product Directories (including sub directories):
  - C:\Gemini
  - C:\Img
- DICOM File Type:
  - *.dcm

8.4.6. Faxitron Specimen Radiography Systems

NOTE: Reference ***Hologic Products & Approved Antivirus Software*** section for the list of supported Faxitron Specimen Radiography System products.

- Product Directories (including sub directories):
  - C:\Faxitron
- DICOM File Type:
  - *.dcm

8.4.7. Horizon DXA

- Product Directories (including sub directories):
  - C:\QDR
- DICOM File Type:
  - *.dcm

8.4.8. Insight / Insight FD

- Product Directories (including sub directories):
  - C:\Program Files (x86)\Hologic
- DICOM File Type:
  - *.dcm

8.4.9. SecurView DX/RT Workstation and Manager

- Product Directories (including sub directories):
  - F:\ApplicationEventLog
  - F:\DICOM
  - F:\DICOMExport
  - F:\DICOMImport
  - F:\DICOMTemp
  - F:\DICOM_Annotation
  - F:\DICOM_Spool
  - F:\DICOM_SR
  - F:\Exports
  - F:\Images
  - F:\ImagesTemp
  - F:\IPCTemp
  - F:\Log
  - F:\MAPTEMP
  - F:\PrintSpool
  - F:\ScreenCaptureTmp
  - F:\ServiceLogfiles
  - F:\Temp
  - F:\Thumbnails
  - F:\TomoImages
  - F:\Workspace
  - C:\Program Files (x86)\PostgresPlus
  - C:\Program Files\PostgresPlus

    - E:\arcticdata
- DICOM File Type:
    - *.dcm

8.4.10. Trident HD

- Product Directories (including sub directories):
    - C:\Trident
    - C:\Img
- DICOM File Type:
    - *.dcm

8.4.11. Trident

- Product Directories (including sub directories):
    - C:\Gemini
    - C:\Trident
    - C:\Images
- DICOM File Type:
    - *.dcm

8.5. Additional Considerations

This section contains additional considerations and guidance related to installing, configuring, and operating approved antivirus software on Hologic products referenced in this document.

8.5.1. Sophos Endpoint Security Resets Windows Security Settings

When malware is detected, Sophos antivirus software resets certain Windows security settings to their default values. Some of these settings have been changed from their default values to facilitate the proper operation of the product. Therefore, this reset behavior is undesired for the product and should be disabled.

For details on Sophos resetting security settings during remediation, refer to the following website:

https://community.sophos.com/kb/en-us/118583

After Sophos agent software has been installed on the product, perform the following steps to disable resetting of Windows security settings to default during remediation:

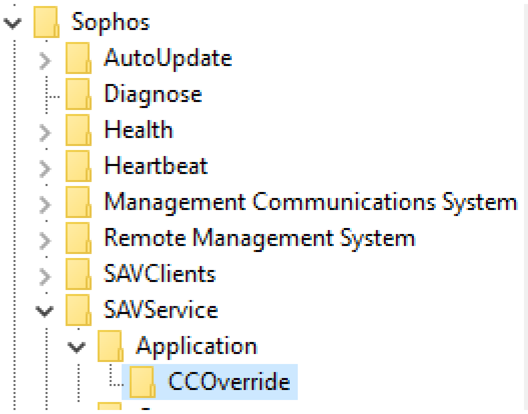
1. Log into the system as the Hologic Service role (administrator).
2. Disable Sophos software tamper protection temporarily.
3. Open the Registry Editor.
4. Navigate to the following registry key:

   HKLM\SOFTWARE\WOW6432Node\Sophos\SAVService\Application

5. Under the Application key, create a new registry key:

   CCOverride

6. Confirm that the registry key now exists and is spelled correctly:



Sophos
AutoUpdate
Diagnose
Health
Heartbeat
Management Communications System
Remote Management System
SAVClients
SAVService
Application
CCOverride

Figure 1: New Registry Key

7. Restart the computer.
8. Re-enable Sophos software tamper protection.