Introduction

1.1 Purpose

To provide guidance for installation of antivirus software on the Brevera® breast biopsy system running on Windows® 10.

1.2 Scope

This document applies to all Brevera breast biopsy system products with software version 1.1 and later.

1.3 Estimated Time

Installation of antivirus software, including configuration, takes approximately 30 minutes to complete.

1.4 Approved Antivirus Software

Hologic® has verified only the products and versions that are in the following list. These products and versions do not interfere with the operation of the system. Hologic does not recommend installation of any other products or versions. Hologic cannot guarantee the effectiveness of these products in the prevention of malicious software.

This document provides instructions for installing and configuring the following antivirus products:

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

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

1.5 Definitions

- **LiveUpdate –** A feature that allows servers and clients to retrieve updates from an internal server or Symantec's official LiveUpdate server.
- **Managed –** The client's system is configured to send virus alerts and retrieve virus updates from an internal parent Symantec server.
- **Real-Time –** Real-time scanning of each file that is loaded in RAM.
- **SmartScan –** A scanning technique that scans the header of each file to determine its true file extension and identifies possible malicious code.
- **Unmanaged –** The clients do not connect to the network and do not have a parent server with which they communicate. These clients must download their own virus definition updates.

1.6 Customer Preparation

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.

1.7 Preinstallation Checklist

Before the installation, review the following:

- Ensure that you have access as a service-level (administrator) user on the system. Contact Hologic Technical Support (877.371.4372) for assistance with creating a service-level user.
- Ensure that there is no existing antivirus software loaded onto the workstation prior to installation.
- Ensure that the installer has the proper serial keys and associated licenses for the product to be installed.

1.8 Antivirus Installation Guide

1.8.1 Overview

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

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:

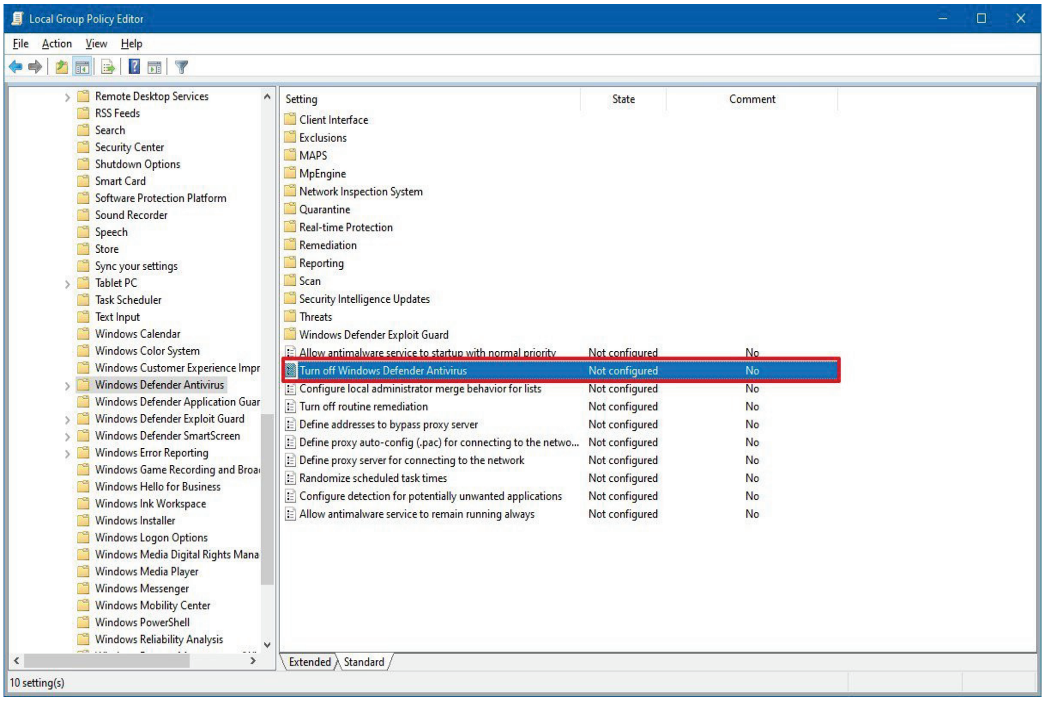
- Has the infrastructure already running.
- Has personnel who have the expertise to deploy and manage the antivirus product.
- Needs only general guidance, such as recommended features and files or directories on Hologic systems to exclude from scanning.

1.8.2 Disabling Windows Defender Anti-Virus

Windows Defender is the built-in antimalware software from Microsoft® that is installed with the Windows operating system. Disable Windows Defender before installing any third-party antivirus software.

1. At the Acquisition Workstation, log in as a user who has a Hologic Service role (administrator).
2. Right-click **Windows Start** and select **Run**.
3. In the **Run** dialog box, type `gpedit.msc` and select **OK**.
4. In the **Local Group Policy Editor**, browse to the following path:

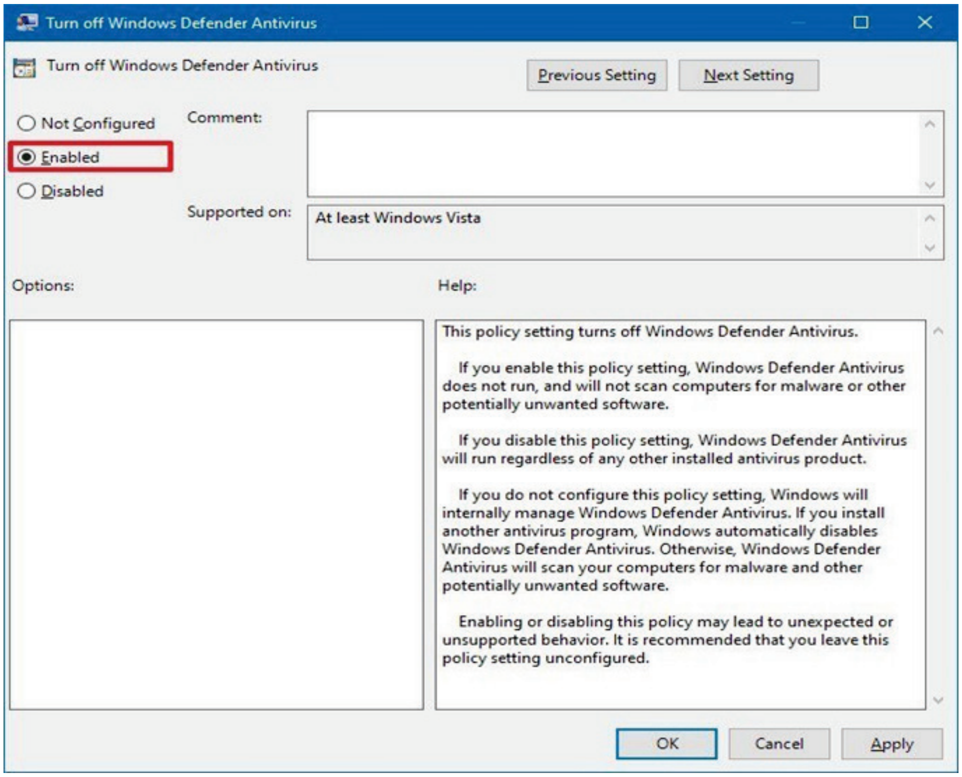
   Computer Configuration > **Administrative Templates** > **Windows Components** > **Windows Defender Antivirus**
5. Double-click the **Turn off Windows Defender Antivirus** option. (See following figure.)



Setting	State	Comment
Client Interface		
Exclusions		
MAPS		
MpEngine		
Network Inspection System		
Quarantine		
Real-time Protection		
Remediation		
Reporting		
Scan		
Security Intelligence Updates		
Threats		
Windows Defender Exploit Guard		
Allow antimalware service to startup with normal priority	Not configured	No
Turn off Windows Defender Antivirus	Not configured	No
Configure local administrator merge behavior for lists	Not configured	No
Turn off routine remediation	Not configured	No
Define addresses to bypass proxy server	Not configured	No
Define proxy auto-config (.pac) for connecting to the netwo...	Not configured	No
Define proxy server for connecting to the network	Not configured	No
Randomize scheduled task times	Not configured	No
Configure detection for potentially unwanted applications	Not configured	No
Allow antimalware service to remain running always	Not configured	No

Figure 1: Turn Off Windows Defender Antivirus

6. Deselect the **Enabled** option to disable Windows Defender Antivirus. (See following figure.)


Turn off Windows Defender Antivirus
Turn off Windows Defender Antivirus
Previous Setting
Next Setting
Comment:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Supported on: At least Windows Vista

This policy setting turns off Windows Defender Antivirus.

If you enable this policy setting, Windows Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software.

If you disable this policy setting, Windows Defender Antivirus will run regardless of any other installed antivirus product.

If you do not configure this policy setting, Windows will internally manage Windows Defender Antivirus. If you install another antivirus program, Windows automatically disables Windows Defender Antivirus. Otherwise, Windows Defender Antivirus will scan your computers for malware and other potentially unwanted software.

Enabling or disabling this policy may lead to unexpected or unsupported behavior. It is recommended that you leave this policy setting unconfigured.

Figure 2: Disable Windows Defender Antivirus

7. Select **Apply**.
8. Select **OK**.
9. Restart the computer.

1.8.3 Installing Agent Software on the Product Device

It is recommended that only the endpoint antivirus agent software be installed on the product device. Agent software is typically installed as an Administrator user. The customer IT personnel provides or installs the agent software.

1.8.4 Recommended Features

It is recommended that only core antivirus monitoring and scanning features be installed or configured on the product device. To achieve this, add Hologic product devices to the customer antivirus policy group and configure 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 the features properly. These features must be disabled or configured by the customer if they have personnel who have the right skill set to configure and maintain them.

1.8.5 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:

- Product Directory (including subdirectories): C:\Orion

Note
If the drive letters do not apply to the configuration, substitute them with the appropriate drive letters.

- DICOM File Type: .DCM

1.8.6 Additional Considerations

Sophos Endpoint Security Resets Windows Security Settings

Sophos antivirus software resets certain Windows security settings to default values during detection of malware. One or more of these security settings has been modified from the default value so that the Hologic product operates as intended. This reset behavior should be disabled.

Details for Sophos resetting security settings during remediation are located at:
https://community.sophos.com/kb/en-us/118583

After the Sophos agent/client software has been installed onto the product device, perform the following steps to disable resetting of the Windows security settings 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. (See following figure.)

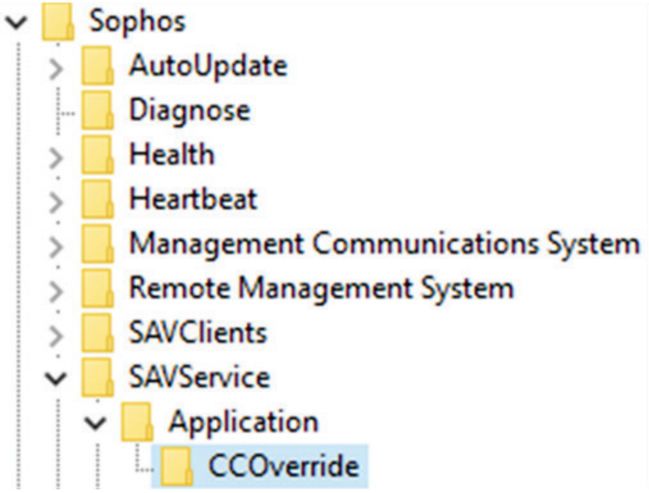


Figure 3: Create a New Registry Key

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