Introduction

1.1 Purpose

This document explains how to install and configure antivirus software on the Affirm® prone biopsy systems running on Windows® 10.

1.2 Scope

This document applies to all Affirm prone biopsy systems with software version 1.1 software and later.

1.3 Estimated Time

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

1.4 Approved Antivirus Software

Hologic® has verified only the products and versions in the following list. These products and versions do not interfere with the operation of the system. Hologic does not recommend installing any other product or version. 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 products. Load only the client/agent software and only one antivirus program per system.

36 Apple Ridge Road, Danbury, CT 06810 (800) 447-1856

1.5 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 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.

1.6 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.

1.7 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.

1.8 Antivirus Installation Guidance

1.8.1 Overview

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

1.8.2 Disabling Windows Defender

Windows Defender is the built-in antimalware software from Microsoft® that comes installed with the Windows operating system. It should be disabled before installing third-party antivirus software.

1. On the Acquisition Workstation, log in as a user with the 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** policy.

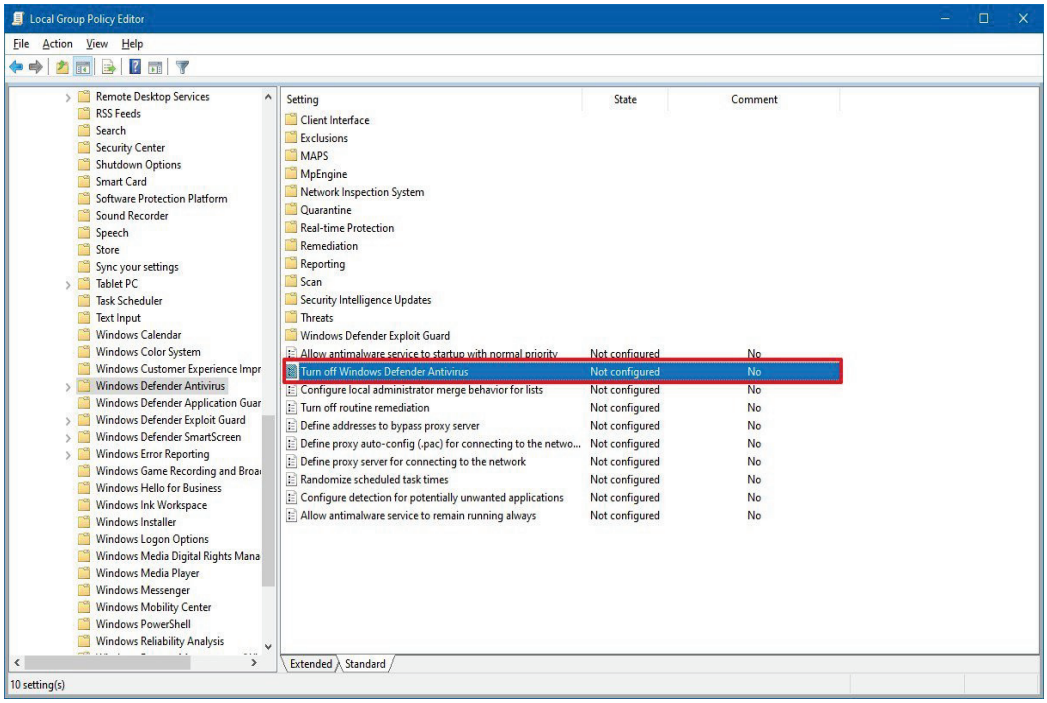

Figure 1: Turn Off Windows Defender Antivirus

6. Deselect **Enabled** to disable Windows Defender Antivirus.

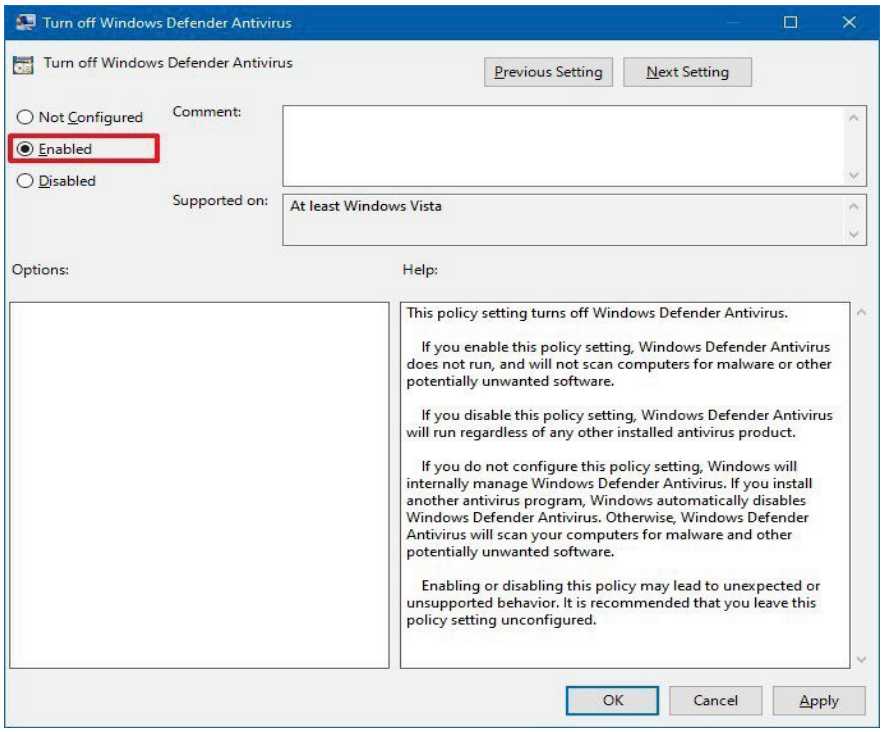

Figure 2: Disable Windows Defender Antivirus

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 should typically be installed as an administrator user. Customer IT 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 for the product device. To achieve this, we recommend adding Hologic product devices to their own antivirus policy group and configuring 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.

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, sub directories, and file types:

- Product Directory (including sub directories):

  C:\Aries

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

- DICOM File Type:

  .DCM

1.8.6 Additional Considerations

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 device, 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.

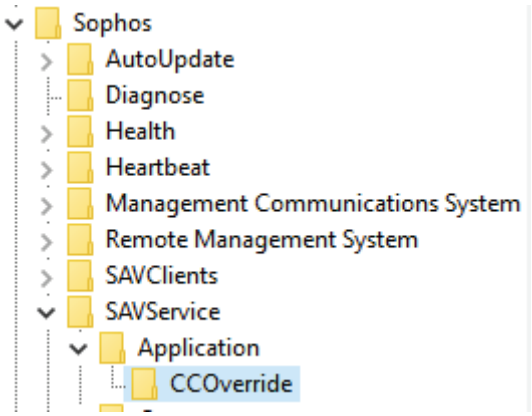

Figure 3: New Registry Key

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