HOLOGIC®
The Women's Health Company

R2 Cenova™ 1.3 Antivirus Software Installation Instructions

Introduction

This document provides instructions for installing the following antivirus software on the R2 Cenova 1.3 server:

- Symantec™ AntiVirus™ Corporate Edition 10.0
- Symantec™ Endpoint Protection 12.1
- McAfee® VirusScan® Enterprise 8.5i

The antivirus software application must be supplied by the customer. Only the client of the corporate edition may be loaded on our products.

Installation of antivirus products requires approximately 30 minutes to complete.

Technical Support

If you have questions, contact the Technical Assistance Center:

Telephone: +1.866.CHECKED (+1.866.243.2533)

Email: r2support@hologic.com Website: www.hologic.com

For Europe/South America/Asia, contact your local distributor.

Definitions

Live Update – A feature that allows servers and clients to retrieve updates from an internal server or Symantec's official Live Update server.

Managed – The client system is configured to send virus alerts, as well as retrieve virus updates from an internal parent Symantec server.

Real-time – Real-time scanning of each file loaded in RAM. Real-time protection can be used with SmartScan.

SmartScan – A Symantec 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.

Preinstallation Checklist

Before beginning the installation, review the following:

- Ensure the customer has purchased and procured the software of choice. Hologic does not supply the customer with this software. It is the customer's responsibility to purchase the software and associated licenses.
- Ensure no existing antivirus software is loaded on the server prior to installation.
- Ensure you have the proper serial keys and licenses for the product to be installed.

Installing Symantec AntiVirus 10.0 or Symantec Endpoint 12.1 as an Unmanaged Client

Customers with Symantec AntiVirus Corporate Edition or Symantec Endpoint must provide their own Symantec server within their networked environment. Load only client software on R2 Cenova. The clients retrieve updates from their existing Symantec server, should they choose to install the client software in a 'managed' state. For customers who want their installations to interface with their existing Symantec server, choose 'Managed' setup.

▶ **To install Symantec AntiVirus 10.0 or Symantec Endpoint 12.1:**

1 **Log into Windows** on the server as 'Administrator'.

2 **Install Symantec software.**

- **a** Insert the Symantec CD into the CD-ROM drive. Autoplay should start the installation. If not, browse to the drive and launch the software with the setup icon.
- **b** When the InstallShield wizard appears, click Next.
- **c** Select 'I accept the terms in the license agreement', then click Next.
- **d** Select 'Client install', then click Next.
- **e** Select 'Complete', then click Next.
- **f** Select 'Unmanaged', then click Next.
- **g** Ensure 'Auto-Protect' and 'Run-LiveUpdate' are checked, then click Next.
- **h** Click Install. Wait for the installation to complete.
- **i** If the virus definitions are older than 30 days, run LiveUpdate.
- **j** When done, click Finish.

3 **Load license file** (if necessary).

⚠ ***Note:*** *If your package includes the license file then you may not need to do this step.*

- **a** Start up Symantec software. If your package does not include the license file, 'License not found' should appear.
- **b** Click the hyperlink **http://licensing.symantec.com/**.
- **c** Enter the serial number, then click Next. Follow the instructions to receive a license file (.sfl) via email. If there are problems, contact Symantec Technical Support.
- **d** From the e-mail application, copy the license file to the server's C: drive.
- **e** From the Symantec main screen, select 'Browse'. Locate and select the license file on the C: drive. Then click Next.

4 **Configure File System Auto-Protect**

- **a** Start up Symantec software and go to Configure > File System Auto-Protect.
- **b** Under 'File Types', change the setting to 'Selected.'

⚠ ***Note:*** *'Selected' scanning with SmartScan scans the header of each file to determine the file type. By default it scans for 57 predetermined extensions, but is fully configurable. To scan all files entering and leaving the server, leave 'All types' checked. (This may degrade server performance.)*

5 Exclude Cenova folders.

a Under Options, check 'Exclude selected files and folders', then click Exclusions.

b Click Files/Folders, then browse to the following folders and place a check in the box next to the folder names:

☑ C:\CasesFolders ☑ C:\Program Files\Hologic

c Click OK (twice), then close Symantec software.

Installing McAfee 8.5i

1 Log into Windows on the server as 'Administrator'.

2 Install McAfee software.

a Insert the McAfee 8.5i CD. When the McAfee VirusScan Enterprise Setup screen appears, click Next to begin installation.

b Select 'I accept the terms in the license agreement', then click Next.

c Select 'Typical install', then click Next.

d Select 'Standard Protection', then click Next.

e At the Ready to Install screen, click Install.

f When installation is complete, uncheck 'Run On-Demand Scan', check 'Update Now', then click Finish. The McAfee software will update the virus definitions.

g When done, click 'Finish'.

h If prompted, reboot the system.

3 Configure McAfee 8.5i.

a Launch the McAfee VirusScan Console.

b Ensure the following are **enabled**:

- Access Protection
- Buffer Overflow Protection
- On-Access Scanner

c Double-click '**Access Protection**'. A new window should appear.

d At bottom left, ensure 'Prevent McAfee services from being stopped' is checked.

e Click on '**Anti-virus Standard Protection**' and configure as follows:

Block	Report	
☑	☑	Prevent registry editor and task manager from being disabled
☑	☑	Prevent user rights policies from being altered
☑	☑	Prevent remote creation of autorun files
☑	☑	Prevent hijacking of .EXE and other executable extensions
☑	☑	Prevent Windows Process spoofing
☑	☑	Prevent mass mailing worms from sending mail
☑	☑	Prevent IRC communication
☑	☑	Prevent use of tftp.exe

f Click on '**Anti-virus Maximum Protection**' and configure as follows:

Block	Report	
☑	☑	Prevent svchost executing non-Windows executables
☑	☑	Protect cached files from password and email address stealers

g Click on '**Common Standard Protection**' and configure as follows:

Block	Report	
☑	☑	Prevent modification of McAfee files and settings
☐	☑	Prevent modification of McAfee Common Management
☐	☑	Prevent modification of McAfee Scan Engine files
☑	☑	Prevent common programs from running files from the Temp folder
☑	☑	Prevent termination of McAfee processes

h Click on '**Common Maximum Protection**' and configure as follows:

Block	Report	
☐	☑	Prevent programs registering to autorun
☐	☑	Prevent programs registering as a service
☐	☑	Prevent creation of new exe files in the windows folder
☐	☑	Prevent creation of new exe files in the program files

i When done, click Apply, then Close.

4 Exclude Cenova folders.

a On the VirusScan Console, double-click 'On-Access Scanner'.

b Highlight 'All Processes', select the Detection tab, then click Exclusions….

c Click Add…, Browse…, navigate to C:\CasesFolders, then highlight the folder name and click OK twice.

d Click Add…, Browse…, navigate to C:\Program Files\Hologic, then highlight the folder name and click OK twice.

e Click OK again to return to the Detection tab.

f Click OK to return to the VirusScan Console.

g Close the VirusScan Console.

Running the Self Test

After installing and configuring the software, run the R2 Cenova server's Self-Test. For more information, see the server's service manual.

Hologic Inc.
35 Crosby Drive
Bedford, MA 01730-1401 USA
Tel: +1.781.999.7300
Sales: +1.781.999.7453
Fax: +1.781.280.0668

Hologic N.V.
Authorized Representative
Leuvensesteenweg 250A
1800 Vilvoorde, Belgium
Tel: +32.2.711.4680
Fax: +32.2.725.2087