application notes

hp OpenView storage management appliance software

using antivirus software

Product Version: 2.1

Second Edition (October 2003)

Part Number: AA-RTD3B-TE

This document describes how to install and use optional antivirus applications on the HP OpenView Storage Management Appliance running software v2.1.

Additional information and HP OpenView documentation are available at http://h18006.www1.hp.com/products/sanworks/managementappliance/index.html.

Printed in the U.S.A.

Storage Management Appliance Software
Using Antivirus Software Application Notes
Second Edition (October 2003)
Part Number: AA-RTD3B-TE

Application Notes Contents

These Application Notes explain how to install and use supported versions of the following antivirus software products with the Storage Management Appliance software v2.1:

Intended Audience

This document is intended for customers running the HP OpenView Storage Management Appliance software v2.1. It has been developed for storage and system administrators who are experienced with the following:

- Managing storage area networks (SANs)
- Operating a Storage Management Appliance

Related Documentation

Refer to the following documentation for more information about the Storage Management Appliance software:

- *HP OpenView Storage Management Appliance Software Update Installation Card*
- *HP OpenView Storage Management Appliance Software User Guide*
- *HP OpenView Storage Management Appliance Software Release Notes*
- HP OpenView Storage Management Appliance Software Online Help

Additional information, including white papers and best-practices documents, is available from the HP website at http://h18006.www1.hp.com/products/sanworks/managementappliance/documentation.html.

Introduction

After installing the HP OpenView Storage Management Appliance (SMA) software v2.1, you can optionally install and use select antivirus applications on the SMA.

HP supports only the following qualified applications with the SMA software v2.1:

- Symantec Norton AntiVirus v7.6 and v8.0—Corporate Edition
- McAfee NetShield v4.5
- McAfee VirusScan Enterprise v7.0
- Trend Micro ServerProtect v5.31 and v5.5
- eTrust InoculateIT v6.0

This document provides instructions for using the above applications.

Instructions for using antivirus software with version 2.0 of the Storage Management Appliance software are contained in *HP OpenView Storage Management Appliance Software Installing Antivirus and Backup Software Application Notes*, available at http://h18006.www1.hp.com/products/sanworks/managementappliance/documentation.html.

The next section contains general procedures that you can use with most of the antivirus products. See the product sections in "Supported Antivirus Applications" beginning on page 7 for specific instructions on installing and running each application on the SMA.

Common Operations for Installing and Using Antivirus Applications

This section describes several of the common operations you will perform when installing most of the supported antivirus applications.

Getting Started

You can install most of the applications described in this document directly on the Storage Management Appliance using Microsoft Terminal Services. You can also install some of the applications remotely from a workstation. Whether you install the applications directly or remotely, you must first install the Terminal Services client on your workstation. By default, the SMA has Terminal Services turned on. See the Microsoft website, http://www.microsoft.com/windows2000/technologies/terminal, for more information on installing and using the Terminal Services client.

To run the application's setup program directly on the Storage Management Appliance, either insert the CD with the setup program in the SMA's CD-ROM drive, or specify the path to the setup program. If you are using a mapped network drive, you must specify the complete uniform naming convention (UNC) path for the setup program. If you do not, you might receive the error noted below during the installation.

Note: If you run the setup program from a mapped network drive, you might receive the following error: **Internal Error 2755.3,** *path \filename.msi*.
Microsoft documents this as a known bug in Knowledge Base article Q255582. See http://support.microsoft.com/default.aspx?scid=kb;en-us;Q255582 for more details.

For further instructions on direct and remote installations, see the appropriate product sections in this document.

Enabling File and Printer Sharing

Most of the antivirus application installation instructions require that file and printer sharing be enabled on the Storage Management Appliance.

Note: Symantec Norton AntiVirus is a standalone product and does not require file and printer sharing to be enabled.

File and Printer Sharing

To enable file and printer sharing using the SMA v2.1 software:

1. On the SMA software primary navigation bar, click **Settings**.
2. Click **Network**, and then click **File and Printer Sharing**.

   The **File and Printer Sharing** page opens.
3. Click the check box to enable file and printer sharing.
4. Click **OK**.

   File and printer sharing is enabled.

Caution: When file and printer sharing is enabled, the Storage Management Appliance can be vulnerable to improper copying or deleting of files. Therefore, after enabling file and printer sharing on the SMA, maintain security by:

- Setting appropriate security policies on shared files or printers
- Turning file and printer sharing off when the supported tasks are complete

Recommendations for Using Antivirus Applications

HP recommends that you configure your antivirus application as follows:

- Enable on-access or real-time scanning, if available.
- Run file scans during off hours to minimize the impact on system performance.
- Do not add any file types to the default list of types excluded from virus checking.
- Customize the virus update interval to accommodate the desired level in your organization.
- Do not use pager notification for alerts. The SMA does not support use of pager notifications.

Supported Antivirus Applications

The sections that follow provide specific instructions for installing and using the supported antivirus products on the Storage Management Appliance. These instructions assume you are familiar with the procedures described in "Common Operations for Installing and Using Antivirus Applications" on page 5 and with general operations for your antivirus application. Refer to the application's documentation for more information.

Symantec Norton AntiVirus—Corporate Edition

The SMA software lets you install, operate, and uninstall Symantec Norton AntiVirus v7.6 or v8.0. This section describes how to install the Symantec AntiVirus application and use it to scan files on the SMA.

Installing Symantec AntiVirus

To install the Symantec AntiVirus software:

1. Log on to the SMA using Terminal Services.
2. Run the Symantec AntiVirus setup program.
3. Follow the installation wizard and accept default values for all options. The following items explain selected options.
   - **Email Snap-In**—Do not install an email Snap-In because you are not installing other products such as Microsoft Exchange or Lotus Notes on the SMA.
   - **Network Setup Type**—Select **Un-managed** for Network Setup Type because the SMA is standalone.
   - **File System Realtime Protection**—Select this option to ensure maximum protection.
4. Select the option to run LiveUpdate. LiveUpdate requires Internet connectivity and installs the latest virus definitions from the Symantec website. HP recommends that you select this option.

When the installation is complete, you can configure Symantec AntiVirus to meet your needs.

Scanning

You can use features of Symantec AntiVirus to start a manual scan of files or schedule a scan at regular intervals. If you use Terminal Services to initiate scans, you must stop the Symantec AntiVirus Client services (see the note below).

Note: You must stop the Symantec AntiVirus Client service before performing either a manual scan or creating a scheduled scan while using Terminal Services. If you do not stop the Client service, an error occurs with the following message: "Could not start scan. Scan engine returned error 0x20000046." For more information about this error, go to the Symantec support website at: http://www.symantec.com/techsupp/enterprise/products/nav/nav_76_ce/search.html

---

Starting a Manual Scan

1. Log on to the SMA using Terminal Services.
2. Stop the Symantec AntiVirus Client service.
3. Start the manual scan.
4. Restart the Symantec AntiVirus Client service.

Creating a Scheduled Scan

1. Log on to the SMA using Terminal Services.
2. Stop the Symantec AntiVirus Client service.
3. Create a new scheduled scan using the Symantec AnitVirus console.
4. Restart the Symantec AntiVirus Client service.

Recommendations for using Symantec AntiVirus

- You must run LiveUpdate at regular intervals to update virus definitions. To run LiveUpdate, the SMA must have Internet access. If the SMA is running behind a firewall with access through a proxy server, you must configure LiveUpdate to identify the proxy server name.
- Be sure to set up the Symantec AntiVirus server to report any viruses encountered. Refer to the Symantec documentation on how to set up a Symantec AntiVirus server for virus reporting.

McAfee NetShield

The Storage Management Appliance lets you install, operate, and uninstall McAfee NetShield v4.5. You can install NetShield directly on the SMA or use McAfee ePolicy Orchestrator to install and control NetShield from a remote system.

Installing NetShield Directly on the Storage Management Appliance

To install the McAfee NetShield v4.5 virus scanning software directly on the SMA:

1. Log on to the SMA using Terminal Services.
2. Run the NetShield setup program, selecting the **Use System Account** option.

When the installation is complete, you can configure NetShield to meet your needs. Refer to the NetShield documentation for details.

If you want to also use the ePolicy Orchestrator for additional security policy management and enforcement, proceed to the next section, "Using ePolicy Orchestrator to Deploy and Control NetShield."

Using ePolicy Orchestrator to Deploy and Control NetShield

You can use the McAfee ePolicy Orchestrator console to remotely deploy NetShield on the SMA or to control NetShield after directly installing it on the SMA. In either case, you must first install the ePolicy Orchestrator agent on the SMA.

Note: Before you can install the agent, you must have the ePolicy Orchestrator software installed and configured on a server system. HP does not support the installation of the ePolicy Orchestrator on the SMA.

Installing the Agent

Numerous methods are available for installing (or deploying) the ePolicy Orchestrator agent on the SMA. HP recommends you use the method of distributing the agent manually, which is documented in the McAfee *ePolicy Orchestrator Product Guide*. This section provides important additional information about installing the agent on the SMA.

File and printer sharing must be enabled before you install the ePolicy Orchestrator agent on the SMA. See "Enabling File and Printer Sharing" on page 6.

To install the ePolicy Orchestrator agent on the SMA:

1. Choose **Start > Programs > ePolicy Orchestrator** and log on to the ePolicy Orchestrator server.

   The ePolicy Orchestrator console window opens.
2. Add the SMA as a new computer in an appropriate level of the **Directory** portion of the console tree. See the ePolicy Orchestrator documentation for complete instructions.

3. Make the following entries and selections when adding the SMA:
   - Enter the name of the SMA.
   - Select **Deploy agent**.
   - Clear **Use ePO Server Credentials** at the bottom.
   - For the **User account**, enter *appliance name***administrator**. If your appliance name is not resolved by DNS, you can enter its IP address instead.
   - Enter the administrator password for the SMA.
4. Click **OK**.

   The ePolicy Orchestrator agent installs.

After the agent is installed, it reports system information in the ePolicy Orchestrator console window. To view this information, select the **Properties** tab for the SMA.

If you have already installed the NetShield software directly on the SMA, as described on page 9, the agent automatically connects to NetShield and communicates with the ePolicy Orchestrator. You can then use the ePolicy Orchestrator to perform tasks.

Deploying NetShield with the ePolicy Orchestrator

If the NetShield software has not been installed directly on the SMA, you can deploy it using the ePolicy Orchestrator. You need to first enable the ePolicy Orchestrator Repository.

Enabling the Repository

1. Right-click **Repository** in the ePolicy Orchestrator console tree.
2. Select **Configure Repository** to display the first window of a wizard series.
3. Follow the wizard instructions to enable the repository.

After enabling the Repository, you can deploy Netshield on the SMA.

Installing NetShield with the ePolicy Orchestrator

1. Select the SMA name in the console tree and then click the **Policies** tab on the left-hand side.
2. Select **NetShield V4.5 for Windows**.
3. In the lower window, clear **Inherit**, click **Force Install**, and then click **Select**.
4. Select the NetShield package in the **Software Package** pop-up window, and then click **Apply**.

   NetShield installs on the SMA.

Depending on how frequently the ePolicy Agent is set to communicate with the server, it may be necessary to send an "Agent Wakeup Call." Click the SMA name in the navigation tree and select **Agent Wakeup Call**.

Once the NetShield software has been installed, you can schedule updates of the virus definition files and file scans.

McAfee VirusScan Enterprise

The Storage Management Appliance lets you install, operate, and uninstall McAfee VirusScan Enterprise v7.0. You can install VirusScan directly on the SMA or use McAfee ePolicy Orchestrator to install and control VirusScan from a remote system.

Installing VirusScan Directly on the Storage Management Appliance

To install the McAfee VirusScan v7.0 software directly on the SMA:

1. Log on to the SMA using Terminal Services.
2. Run the VirusScan setup program.

When the installation is complete, you can configure and use the VirusScan software to perform antivirus activities on the SMA. Refer to the VirusScan documentation for details.

If you want to also use the ePolicy Orchestrator for additional security policy management and enforcement, proceed to the next section, "Using ePolicy Orchestrator to Deploy and Control VirusScan."

Using ePolicy Orchestrator to Deploy and Control VirusScan

You can use the McAfee ePolicy Orchestrator console to remotely deploy VirusScan on the SMA or to control VirusScan after directly installing it on the SMA. In either case, you must first install the ePolicy Orchestrator agent on the SMA.

Note: Before you can install the agent, you must have the ePolicy Orchestrator software installed and configured on a server system. HP does not support the installation of the ePolicy Orchestrator on the SMA.

Installing the Agent

Numerous methods are available for installing (or deploying) the ePolicy Orchestrator agent on the SMA. HP recommends you use the method of distributing the agent manually, which is documented in the McAfee *ePolicy Orchestrator Product Guide*. This section provides important additional information about installing the agent on the SMA.

File and printer sharing must be enabled before you install the ePolicy Orchestrator agent on the SMA. See "Enabling File and Printer Sharing" on page 6.

To install the ePolicy Orchestrator agent on the SMA:

1. Copy *framepkg.exe* from the ePolicy Orchestrator server to a network share.
2. Log on to the SMA using Terminal Services.
3. Run *framepkg.exe* on the SMA.

   The ePolicy Orchestrator agent installs on the SMA.
4. Open a command prompt window and run the following commands on the SMA:

   ```
   cd C:\program file\network associates\common framework
   cmdagent /p /e /c
   ```

   Running **cmdagent** establishes communication between the ePolicy Orchestrator agent and the server.

5. Choose **Start > Programs > Network Associates > ePolicy Orchestrator** and log on to the server.

   The ePolicy Orchestrator console window opens.

6. If the SMA entry is listed in the **Lost&Found** groups of the ePolicy Orchestrator server, move the entry to another location in the Directory.

   When the ePolicy Orchestrator server cannot determine an appropriate location for a computer in the Directory, the server puts the computer in **Lost&Found** groups. You will not be able to manage antivirus activities on the SMA if it remains in **Lost&Found**.

After the agent is installed, it reports system information in the **ePolicy Orchestrator console** window. To view this information, select the **Properties** tab for the SMA.

If you have already installed the VirusScan software directly on the SMA, as described on page 11, the agent automatically connects to VirusScan and communicates with the ePolicy Orchestrator. You can then use the ePolicy Orchestrator to perform tasks.

Deploying VirusScan with the ePolicy Orchestrator

If the VirusScan software has not been installed directly on the SMA, you can deploy it using the ePolicy Orchestrator. To do so, you need to add VirusScan to the ePolicy Orchestrator Repository and then schedule deployment. Adding and deploying VirusScan are documented in the McAfee *VirusScan Enterprise Configuration Guide for ePolicy Orchestrator.*

Trend Micro ServerProtect

The Storage Management Appliance lets you install, operate, and uninstall Trend Micro ServerProtect v5.31 or v5.5 Normal Server software for local system antivirus protection.

You can install the Normal Server client software using Terminal Services or using the Management Console from the ServerProtect Information Server. Follow the appropriate installation instructions below.

Note: HP does not support the installation of the ServerProtect Management Console on the SMA.

Installing ServerProtect Normal Server Directly

File and printer sharing must be enabled on the ServerProtect Information Server before you install ServerProtect on the SMA.

Enabling File and Printer Sharing on the Information Server

Use the following procedure to enable file and printer sharing if your ServerProtect Information Server is a Windows system. For other platforms, consult the ServerProtect documentation.

1. Log on to the system that is dedicated as the Information Server.
2. Right-click **My Network Places** on the desktop and choose **Properties**.
3. Right-click the appropriate LAN connection in the **Network and Dialup Connections** window, and then choose **Properties**.
4. Select the **File and Printer Sharing for Microsoft Networks** in **Components checked are used by this connection**, and then click **OK**.

Installing the ServerProtect Normal Server

To install ServerProtect Normal Server directly on the SMA:

1. Log on to the SMA using Terminal Services.
2. Run the Trend Micro ServerProtect setup program.
3. Follow the ServerProtect installation instructions, taking note of the following steps:
   - Clear the Information Server and the Management Console on the **Select Components** screen, as the installation of these components on the SMA is not supported.
   - On the **Input Logon Information** screen:
     - Enter the domain name managed by the Information Server that the Normal Server will be a member of.
     - Enter the local SMA administrator account and password.
   - Select the appropriate Information Server on your network and double-click its entry.
     - Enter the password for the Information Server in the dialog box.
     - The domain created on the Information Server is displayed. Select that domain, and be sure to copy it to the Information Server field.

4. When the installation is complete, verify that Normal Server is visible from the SeverProtect Management Console. If it is not visible, follow the instructions in the ServerProtect documentation to connect to the Normal Server and verify that it is properly configured.

Note: If an error occurs during the installation, ensure that you have enabled file and printer sharing on the Information Server and try again.

Running Scans

You can now perform or create tasks for On-Demand or Real Time scans and for virus pattern, scan engine, or program updates. You may also set up notifications for virus scan alerts. Be sure the Information Server in your network is configured to regularly download virus pattern updates from Trend Micro's ActiveUpdate server to ensure the highest level of protection in your environment. Refer to the Trend Micro ServerProtect documentation for more details.

Installing ServerProtect Normal Server Remotely

Use the ServerProtect Management Console located in the target domain to remotely install the Normal Server on the SMA.

File and printer sharing for Microsoft networks must be enabled on the SMA to install ServerProtect using the Management Console. See "Enabling File and Printer Sharing" on page 6.

To remotely install ServerProtect Normal Server:

1. Select the domain from the domain browser tree in the ServerProtect Management Console.
2. Choose **Domain > Install New SPNT(s)** to start the installation wizard.
3. Follow the ServerProtect installation instructions, taking note of the following steps:
   - When entering the Server Name, if DNS cannot resolve the SMA server name, use its IP address instead.
   - On the **Logon to target servers** page, enter the proper domain for your Information Server, the local SMA administrator account and password, and the software serial number.

Note: If an error occurs during this phase, ensure that you have enabled file and printer sharing on the SMA.

4. After ServerProtect is installed on the SMA, verify that the SMA appears in the domain browser tree of the Management Console.

   You can now use ServerProtect to create tasks (see "Running Scans" on page 14).

eTrust InoculateIT

The Storage Management Appliance lets you install, operate, and uninstall Computer Associates eTrust InoculateIT v6.0 client software for local system antivirus protection. The client software can be installed on the SMA directly by using Terminal Services or remotely by using the eTrust InoculateIT Admin Server and the Remote Install Utility. Follow the appropriate installation instructions below.

Installing the eTrust InoculateIT Client Directly

To install the client software directly on the SMA:

1. Log on to the SMA using Terminal Services.
2. Run the eTrust InoculateIT setup program and select the following component to install:

   eTrust InoculateIT Clients > for Windows > Setup
3. Reboot the SMA after the installation.
4. Configure the desired eTrust InoculateIT features. Refer to the eTrust InoculateIT documentation for details.

You may perform local scans, customize the realtime monitoring facility, and schedule virus updates to be downloaded. Refer to the eTrust InoculateIT documentation for descriptions of these features.

Installing the eTrust InoculateIT Client Remotely

You can install the eTrust InoculateIT client software using the Remote Install Utility from the eTrust Inoculate Admin Server. File and printer sharing for Microsoft networks must be enabled on the SMA before you install InoculateIT. See “Enabling File and Printer Sharing” on page 6.

To install the client software on the SMA using the Remote Install Utility:

1. Ensure that the Remote Install Utility is installed on the eTrust InoculateIT Admin Server. If it isn’t installed, run the eTrust InoculateIT setup on the eTrust InoculateIT Admin Server and choose the following component to install:

   eTrust InoculateIT Clients > for Windows > Remote Setup

2. Launch the Remote Install utility and perform the following steps:
   a. Create an Installation Configuration File (ICF).

      This file is used to preconfigure the InoculateIT installation and the settings for distribution to the target machine. Choose **File > Create ICF File**. Refer to the eTrust InoculateIT documentation for more details on how to customize the options to work in your environment. Save this file to the default location.

   b. Add the SMA as a target (**Target > New**).
   c. Enter the appropriate information for the SMA and ICF file in the **Installation Target** dialog box.
      — If your SMA name is not resolved by DNS, it might be necessary to enter ***appliance IP address*\administrator** for logon information.
      — Be sure to use the SMA administrator account and password. Test the logon using this username/password pair to ensure connectivity and proper authentication.

Note: If you get an error during the test that the machine is not available, ensure that you have enabled file and printer sharing on the SMA.

---

   d. In the right pane of the **Remote Install** window, select the SMA entry. Choose **Target > Start Install** to install the eTrust InoculateIT client onto the SMA. Allow the Remote Install to set the proper permissions on the eTrust subdirectories.
3. Log on to the SMA using Terminal Services and set the eTrust InoculateIT options as required in your environment. Refer to the eTrust InoculateIT documentation for details.

Once this product has been installed, you may perform local scans, customize the realtime monitoring facility, and schedule virus updates to be downloaded. Refer to the eTrust InoculateIT documentation for descriptions of these features.

Recommendations for using eTrust InoculateIT

- The Computer Associates support website posts updates to its Virus Signature Update files. Check http://esupport.ca.com for these updates.
- When downloading Virus Signature Updates, ensure that your ftp and Internet connectivity are working. Select incremental signature updates (**Perform Fast Download** checkbox), if appropriate, to reduce the overhead. Although eTrust InoculateIT supports the redistribution of these virus updates, HP only supports downloading these updates directly to the SMA.