

# Sophos Anti-Virus for NetApp Storage Systems **startup guide**

Runs on Windows 2000 and later

Product version: 1

Document date: April 2012

# Contents

1 About this guide.....	3
2 About Sophos Anti-Virus for NetApp Storage Systems .....	4
3 System requirements.....	5
4 Before you install Sophos Anti-Virus .....	6
5 Installing Sophos Anti-Virus .....	12
6 Managing Sophos Anti-Virus from MMC.....	14
7 Technical support.....	18
8 Legal notices.....	19

# 1 About this guide

This guide explains how to:

- Install Sophos Anti-Virus on a Windows computer to provide offboard anti-virus scanning.
- Manage Sophos Anti-Virus from a Microsoft Management Console (MMC) snap-in.

The guide applies to filers that are running in 7-Mode.

To install Sophos Anti-Virus on a NetApp filer to provide *onboard* anti-virus scanning for filers running in Cluster-Mode, see the *Sophos Anti-Virus for NetApp Data ONTAP startup guide* instead of this guide.

Sophos documentation is published at [www.sophos.com/support/docs/](http://www.sophos.com/support/docs/).

## **2 About Sophos Anti-Virus for NetApp Storage Systems**

### **What is Sophos Anti-Virus for NetApp Storage Systems for?**

Sophos Anti-Virus for NetApp Storage Systems provides on-access scanning of files held on a Network Appliance filer.

### **How does it work?**

You install and run Sophos Endpoint Security and Control on a Windows computer that will provide virus scanning. In this guide, this is referred to as the *anti-virus server*.

When a workstation attempts to access a file held on the Network Appliance filer, Endpoint Security and Control intercepts the file and scans it. If the file is found to be clean, access can go ahead. If the file is infected, access is denied.

### **How is it managed?**

You manage Sophos Anti-Virus from an MMC snap-in, which can be on the anti-virus server itself, or on a different computer.

### **3 System requirements**

For system requirements, go to the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

You must have internet access in order to download the installation software from the Sophos website.

## 4 Before you install Sophos Anti-Virus

### 4.1 Installing Endpoint Security and Control

Before you install Sophos Anti-Virus, you must install Sophos Endpoint Security and Control on the computer that you want to use as an anti-virus server, to provide virus scanning.

If Endpoint Security and Control has already been installed on the computer, go straight to [Configuring Endpoint Security and Control for use with a Network Appliance filer](#) (page 8).

Otherwise, do one of the following:

- Use Sophos Enterprise Console to create a managed installation of Endpoint Security and Control (anti-virus component only).
- Create a standalone installation of Endpoint Security and Control (anti-virus component only).

#### 4.1.1 Create a managed installation

- Refer to the *Sophos Endpoint Security and Control quick startup guide* . Put the anti-virus server in a separate Enterprise Console group, so that you can apply a new anti-virus policy to just that computer.

Now go to [Configuring Endpoint Security and Control for use with a Network Appliance filer](#) (page 8).

#### 4.1.2 Create a standalone installation

##### 4.1.2.1 Download the installer

1. At the Windows computer that you want to use as an anti-virus server or another computer that has internet access, go to <http://www.sophos.com/support/updates/windows.html>.
2. Type your MySophos username and password.
3. Download the anti-virus only installer for Windows.
4. Ensure that the installer is in a location that can be accessed from the computer that you want to use as an anti-virus server.

Alternatively, copy it to a CD or DVD.

##### 4.1.2.2 Run the installer

At the Windows computer that you want to use as an anti-virus server, you must log on as an administrator.

If you have third-party security software installed:

- Ensure that its user interface is closed.

- Ensure that third-party firewall and HIPS software is turned off or configured to allow the Sophos installer to run.

1. Locate the installer that you downloaded and double-click it.
2. In the installer window, click **Install**.

A wizard guides you through installation. Accept the default options, except as shown below.

On the **Update source** page, enter the location from which Endpoint Security and Control will download updates. We recommend that you do this now.

- In the **Address** box, select Sophos or, if you download updates to your website or network, type the relevant web or network address.
- In the **Username** box, type the username that is needed to access the update source.
- In the **Password** and **Confirm password** boxes, type and confirm the password that is needed to access the update source.
- If you access the internet via a proxy, select the **Access the update source via a proxy** checkbox.

On the **Remove third-party security software** page, select the **Remove third-party security software** check box if you have third-party anti-virus software installed.

**Note:** Third-party security software removal does not, by default, remove the associated update tools, because other third-party security software might still be using them. However, if they are not being used, you can remove them via Control Panel.

3. On the last page of the wizard, choose whether to restart the computer. Click **Finish**.

You need to restart the computer to complete the removal of third-party security software.

Installation is complete when the Endpoint Security and Control icon is displayed in the notification area.



If you specified an update source from which Endpoint Security and Control will download updates, Endpoint Security and Control will update every 60 minutes, provided that the update source is accessible. Now go to [Configuring Endpoint Security and Control for use with a Network Appliance filer](#) (page 8).

If you did not specify an update source, go to the next section.

#### 4.1.2.3 Configure Endpoint Security and Control to update

You only need to follow the instructions in this section if you did not specify an update source during installation.

Make sure that you are logged on as an administrator.

1. In the notification area, right-click the Endpoint Security and Control icon, and then click **Open Sophos Endpoint Security and Control**.
2. In the **Sophos Endpoint Security and Control** window, on the **Configure** menu, click **Updating**.
3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Primary location** tab.
  - In the **Address** box, select Sophos or, if you download updates to your website or network, type the relevant web or network address.
  - In the **User name** box, type the username that is needed to access the update source.
  - In the **Password** and **Confirm password** boxes, type and confirm the password that is needed to access the update source.
4. If you access the internet via a proxy, click **Apply**, and then click **Proxy Details**.
  - Select the **Access the location via a proxy** check box.
  - In the **Address** and **Port** boxes, type the proxy server address and port number.
  - If necessary, in the **User name** box, type a username to access the proxy server. If the username needs to be qualified to indicate the domain, use the form domain\username. In the **Password** and **Confirm password** boxes, type and confirm the password that is needed.
  - Click **OK**.
5. In the **Properties for Sophos AutoUpdate** dialog box, click **OK**.

Endpoint Security and Control will update every 60 minutes, provided that the update source is accessible.

Now configure Endpoint Security and Control for use with a Network Appliance filer.

## 4.2 Configuring Endpoint Security and Control for use with a Network Appliance filer

You must configure Endpoint Security and Control to:

- Scan files when they are copied, moved or opened.
- Scan files with an unknown filename extension.
- Scan remote files.
- Move all infected files to a quarantine folder.
- Move all suspicious files to a quarantine folder.
- Not display messages on the screen when scanning files.

How you do this depends on whether you have a *managed* installation of Endpoint Security and Control or a *standalone* installation.

## 4.2.1 Configure a managed installation

1. At the computer that is running Enterprise Console, if Enterprise Console is not already open, click **Start > All Programs > Sophos > Enterprise Console** .
2. Create a new anti-virus policy to contain settings for the anti-virus server.
3. Double-click the policy to edit it.
4. In the **Anti-Virus and HIPS Policy** dialog box, click the **Configure** button for on-access scanning.
5. In the **On-access scan settings** dialog box, on the **Scanning** tab, ensure that the **Read** check box is selected. Otherwise, no files are scanned.
6. Click the **Extensions** tab. Click **Add**. In the extensions list box, type **???** and press ENTER.
7. Click the **Windows Exclusions** tab. Ensure that the **Exclude remote files** check box is not selected.
8. Click the **Cleanup** tab.
9. Ensure that the **Automatically clean up items that contain a virus/spyware** check box is cleared. Click **Deny access and move to**. Using the **Browse** button, specify the path of the folder to which infected files should be moved.  
  
The folder must be on the anti-virus server, and should preferably be accessible to anti-virus administrators only.
10. Under **Suspicious files**, click **Deny access and move to**. Using the **Browse** button, specify the path of the folder to which suspicious files should be moved.  
  
The folder must be on the anti-virus server, and should preferably be accessible to anti-virus administrators only.
11. Click **OK** to close the **On-access scan settings** dialog box.
12. In the **Anti-Virus and HIPS Policy** dialog box, click **Messaging**.
13. In the **Messaging** dialog box, click the **Desktop Messaging** tab. Clear the **Enable desktop messaging** check box. Click **OK**.
14. Click **OK** to close the **Anti-Virus and HIPS Policy** dialog box.
15. Click the policy and drag it onto the group that contains the anti-virus server. When prompted, confirm that you want to continue.

The policy settings will be applied to Endpoint Security and Control on the anti-virus server.

You have configured Endpoint Security and Control for use with a filer.

If the anti-virus server is running Windows Server 2008 R2 or Server 2008, you must configure the Windows security options.

Otherwise, go straight to [Installing Sophos Anti-Virus](#) (page 12).

## 4.2.2 Configure a standalone installation

1. At the anti-virus server, if Endpoint Security and Control is not already open, in the notification area, right-click the Endpoint Security and Control icon, and then click **Open Endpoint Security and Control**.
2. In the **Sophos Endpoint Security and Control** window, on the **Configure** menu, point to **Anti-Virus**, and then click **On-access scanning**.
3. In the **On-access scan settings for this computer** dialog box, on the **Scanning** tab, ensure that the **Read** check box is selected. Otherwise, no files are scanned.
4. Click the **Extensions** tab. Click **Add**. In the extensions list box, type **???** and press ENTER.
5. Click the **Cleanup** tab.
6. Ensure that the **Automatically clean up items that contain virus/spyware** check box is cleared. Click **Deny access and move to**. Using the **Browse** button, specify the path of the folder to which infected files should be moved.  
The folder must be on this computer, and should preferably be accessible to anti-virus administrators only.
7. Under **Suspicious files**, click **Deny access and move to**. Using the **Browse** button, specify the path of the folder to which suspicious files should be moved.  
The folder must be on this computer, and should preferably be accessible to anti-virus administrators only.
8. Click **OK** to close the **On-access scan settings for this computer** dialog box.
9. On the **Configure** menu, point to **Anti-virus**, and then click **Messaging**.
10. In the **Messaging** dialog box, click the **Desktop messaging** tab. Clear the **Enable desktop messaging** check box. Click **OK**.

You have configured Endpoint Security and Control for use with a filer.

If the anti-virus server is running Windows Server 2008 R2 or Server 2008, you must configure the Windows security options.

Otherwise, go straight to [Installing Sophos Anti-Virus](#) (page 12).

## 4.3 Configure Windows Server 2008 R2 and Server 2008 security options

If the anti-virus server is running Windows Server 2008 R2 or Server 2008, you must configure the Windows security options.

1. On the taskbar, click **Start**, point to **Administrative Tools**, and then click **Local Security Policy**.
2. In the **Local Security Policy** window, in the left-hand pane, double-click the **Local Policies** folder to expand it. Select **Security Options**.
3. Enable the option **Network access: Let Everyone permissions apply to anonymous users**.

4. Restart the computer.

You have configured Windows Server 2008 security options.

Now install Sophos Anti-Virus.

## 5 Installing Sophos Anti-Virus

Sophos Anti-Virus has two components:

- The Sophos Anti-Virus for NetApp service.
- An MMC snap-in, which is used to manage the Sophos Anti-Virus for NetApp service.

You can install the components on the same computer, or on separate computers.

### 5.1 Download the installer

1. At the Windows computer on which you want to install Sophos Anti-Virus or another computer that has internet access, go to <https://secure.sophos.com/support/updates/storage.html>.
2. Type your MySophos username and password.
3. Download the installer for NetApp.
4. Ensure that the installer is in a location that can be accessed from the computer on which you want to install Sophos Anti-Virus.

Alternatively, copy it to a CD or DVD.

### 5.2 Run the installer

At the Windows computer on which you want to install Sophos Anti-Virus, you must log on as an administrator.

If you are installing the Sophos Anti-Virus for NetApp service (that is, if this computer will be an anti-virus server), this section assumes you have installed and configured Sophos Endpoint Security and Control (as explained in [Before you install Sophos Anti-Virus](#) (page 6)).

If you are installing the MMC snap-in, this section assumes that this computer is running MMC version 1.2 or later.

1. Locate the installer that you downloaded and double-click it.
2. In the installer window, click **Install**.

A wizard guides you through installation.

3. On the **Welcome** page, click **Next**.
4. On the **End-user licence agreement** page, read the licence agreement. If you accept it, click **I accept the terms of the licence agreement**, and click **Next**.

5. On the **Custom setup** page, select the features to install.

The selection depends on the use you want to make of this computer.

- To use the computer as an anti-virus server and to manage Sophos Anti-Virus from MMC, click **Next** and continue to step 6.
- To use the computer only as an anti-virus server, click the down arrow next to **MMC snap-in**. Select **Entire feature will be unavailable**. Click **Next** and continue to step 6.
- To use the computer only to manage Sophos Anti-Virus from MMC, click the down arrow next to **Anti-virus service**. Select **Entire feature will be unavailable**. Click **Next** and go straight to step 8.

6. On the **Filer name** page, type the name of the filer. You can specify only one filer for this computer to perform scanning for. Click **Next**.
7. On the **Account information** page, enter the details of an account in the domain containing the filer that this computer is serving. The account must have Administrator or Backup Operator level rights. Click **Next**.

**Note:** If the installation wizard then displays a warning that the account details are invalid, ensure that the local security setting **Network access: Sharing and security model for local accounts** is set to **Classic - local users authenticate as themselves**.

8. On the **Ready to install** page, click **Install** to begin the installation.
9. On the last page, click **Finish**.

You have installed Sophos Anti-Virus.

**Note:** If you want to ensure that anti-virus scanning can be carried out if the anti-virus server is unavailable (for example, while Endpoint Security and Control is updating), install Endpoint Security and Control and Sophos Anti-Virus on another computer as well. On the filer, define that computer as a secondary server. (To find out how to do this, refer to the Data ONTAP documentation.) Then, the secondary server can handle scanning requests if the primary server is unavailable.

If you want to install the Sophos Anti-Virus for NetApp service and/or the MMC snap-in on another computer, repeat this section.

You must ensure that the filer has been configured to send files for virus scanning. To find out how to do this, refer to the Data ONTAP documentation.

To manage Sophos Anti-Virus from MMC, continue to the next section.

## 6 Managing Sophos Anti-Virus from MMC

### 6.1 Snap in Sophos Anti-Virus to MMC

This section assumes you installed the Microsoft Management Console (MMC) snap-in for Sophos Anti-Virus during the Sophos Anti-Virus installation procedure.

1. At the computer where you installed the MMC snap-in, at the taskbar, click **Start**, and then click **Run**.

If the computer is running a 32-bit version of Windows, in the **Run** dialog box, type **mmc**.

Otherwise, in the **Run** dialog box, type **mmc /32**.

Click **OK**.

2. In the **Console1** console, on the **File** menu, click **Add/Remove Snap-in**.

For MMC versions earlier than 2.0, this command is on the **Console** menu.

3. If the computer is running Windows 7, Server 2008 R2, or Server 2008, in the **Add or Remove Snap-ins** dialog box, in the **Available snap-ins** list box, select Sophos Anti-Virus for NetApp Storage Systems. Click **Add**.

Otherwise, in the **Add/Remove Snap-in** dialog box, on the **Standalone** tab, click **Add**. In the **Add Standalone Snap-in** dialog box, in the **Available Standalone Snap-ins** list box, select Sophos Anti-Virus for NetApp Storage Systems. Click **Add**, then **Close**.

4. Click **OK** to return to the **Console1** console. On the **File** menu, click **Save**. In the **Save As** dialog box, choose a location and type a filename for the console settings. Click **Save**.

For MMC versions earlier than 2.0, the **Save** command is on the **Console** menu.

You have snapped in Sophos Anti-Virus to MMC.

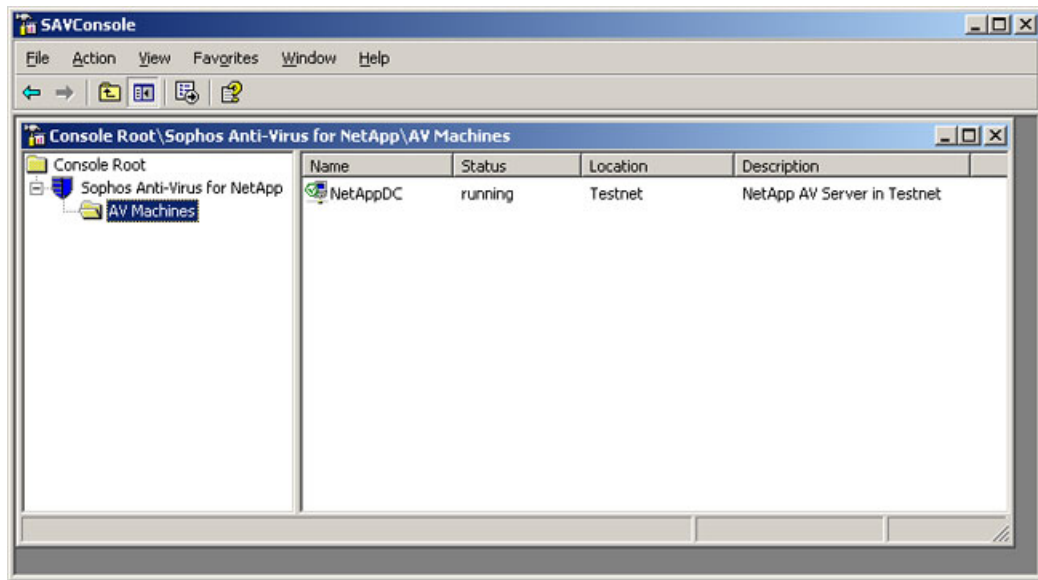
Now add an anti-virus server to MMC.

### 6.2 Add an anti-virus server to MMC

If you have installed the Sophos Anti-Virus for NetApp service on this computer or other computers, you must add these to MMC to enable it to manage Sophos Anti-Virus on these computers.

1. In the console tree, double-click **Sophos Anti-Virus for NetApp**. Click the **AV Machines** folder. On the **Action** menu, click **Administer AV Machine**. In the **Add Sophos Anti-Virus server** dialog box, click **Browse**.
2. In the **Browse for Computer** dialog box, locate the anti-virus server and click **OK**.

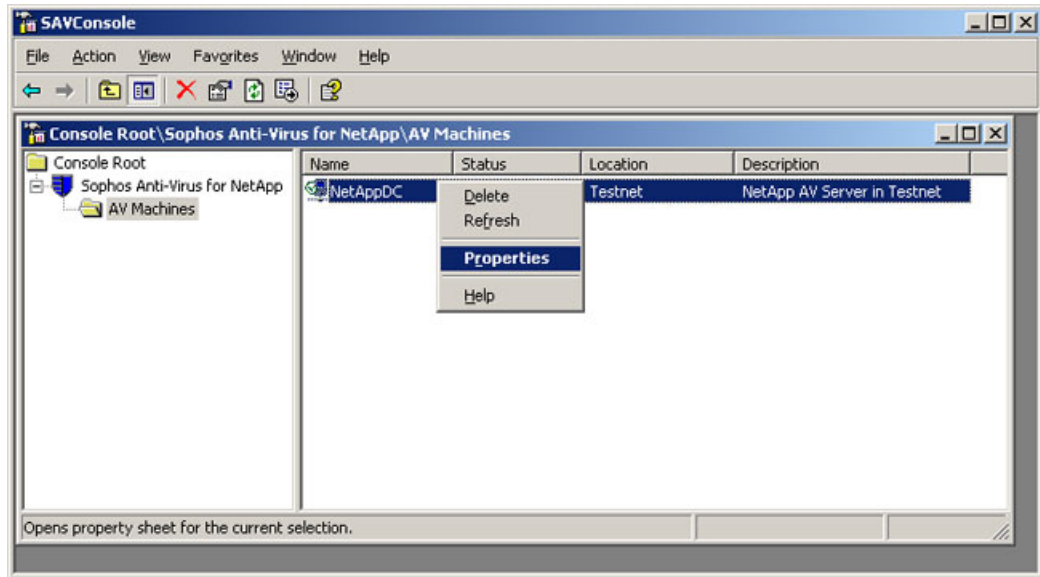
3. In the **Add Sophos Anti-Virus server** dialog box, type a location and description for the anti-virus server if you wish, and click **OK**. The anti-virus server is shown in the right-hand pane of the **AV Machines** console, with the Sophos Anti-Virus for NetApp service running.



You have added an anti-virus server to MMC.

## 6.3 How to stop the Sophos Anti-Virus for NetApp service on an anti-virus server

1. In the right-hand pane of the **AV Machines** console, right-click the name of the anti-virus server, and then click **Properties**.

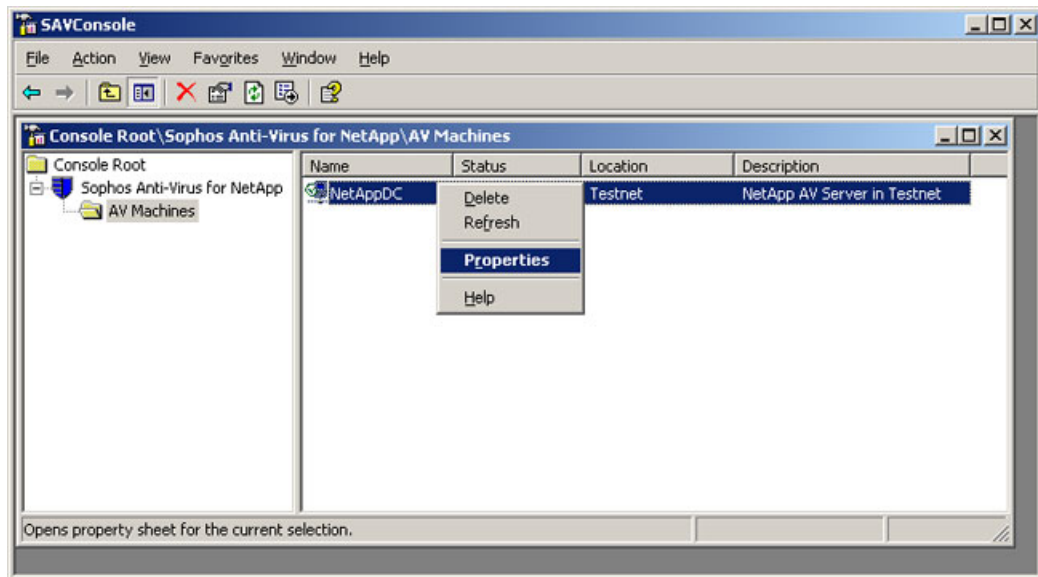


2. In the **Properties** dialog box, on the **General** tab, click **Stop**. Click **OK**.

In the right-hand pane of the console, you should see that the service is not running on the selected anti-virus server.

## 6.4 How to start the Sophos Anti-Virus for NetApp service on an anti-virus server

1. In the right-hand pane of the **AV Machines** console, right-click the name of the anti-virus server, and then click **Properties**.



2. In the **Properties** dialog box, on the **General** tab, click **Start**. Click **OK**.

In the right-hand pane of the console, you should see that the service is running on the selected anti-virus server.

## 7 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to [support@sophos.com](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## **8 Legal notices**

Copyright © 2006–2012 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.