SOPHOS

Security made simple.

Sophos for Virtual Environments

Configuration guide -- Enterprise Console edition

Product version: 1.1

Contents

1 About this guide

This guide tells you how to configure Sophos for Virtual Environments.

The guide assumes that you use Sophos Enterprise Console to manage your security software.

Note: If you use Sophos Central, look in the Sophos Central Admin Help instead.

2 Configure policies

You configure Sophos for Virtual Environments by using Enterprise Console policies.

When you put your Sophos Security VM in a Sophos Enterprise Console group, policies are applied that protect and update the guest VMs.

We recommend that you use the default settings, as they provide the best balance between protection and system performance. However, you can change the settings in these policies:

- Anti-Virus and HIPS
- Updating

The other Enterprise Console policies don't apply to the Security VM.

Note: All guest VMs protected by a Security VM use the same policies as the Security VM. To apply a different policy to some guest VMs, move them to a different Security VM in a different Enterprise Console group. Then apply a different policy to that group. For instructions on how to move guest VMs, see the *Sophos for Virtual Environments Startup guide -- Enterprise Console edition*.

To view a list of all guest VMs managed by a Security VM, see View protected guest VMs (page 11).

2.1 Anti-virus and HIPS policy

By default, the Sophos Security VM:

- Scans files when they are accessed on the guest VMs.
- Blocks access to infected files.
- Cleans up detected threats automatically.

The anti-virus and HIPS policy settings don't all apply to the Security VM. This section describes which scanning options apply and can be configured centrally.

For more information about the settings, see the Sophos Enterprise Console Help.

On-access scanning

On-access scan settings are supported as detailed below. Behavior monitoring is not supported.

To open the on-access scanning settings pages in Enterprise Console:

1. In the **Policies** pane, double-click **Anti-virus and HIPS**.
2. Double-click the policy you want to change.
3. In the **Anti-Virus and HIPS Policy** dialog, look for the **On-access scanning** panel. Beside **Enable on-access scanning**, click **Configure**.

   The **On-access scan settings** dialog is displayed.

On-access scan setting	Applies to Security VM?	Notes
Scanning tab		
Check files on Read/Rename/Write	No	If one or more of the three options —Read, Rename, and Write—are enabled then the Security VM will scan in all three scenarios. **Important:** If all three options are disabled, on-access scanning is disabled and your system is not protected.
Scan for Adware and PUAs/Suspicious files	No	
Allow access to drives with infected boot sectors	No	
Scan inside archive files (not recommended)	Yes	
Scan system memory	No	.
Extensions tab		
Scan all files (not recommended)	Yes	
Scan only executable and other vulnerable files	Yes	
Additional file type extensions to be scanned	Yes	
Scan files with no extension	Yes	
Exclude file types from scanning	Yes	
Exclusions tabs		
Windows Exclusions tab	Yes	To exclude a folder from scanning, you must always specify the full path to the folder, including the drive letter or network share name, for example, "C:\Tools\logs\" or "\\Server\Tools\logs\". The Security VM cannot exclude

On-access scan setting	Applies to Security VM?	Notes
		folders based only on their name. For example, "\Tools\logs\" won't work. For more information about Windows exclusions, for example, how to use wildcards, see the Sophos Enterprise Console Help, in the section about configuring the anti-virus and HIPS policy.
Mac Exclusions tab	No	
Linux/UNIX Exclusions tab	No	
Cleanup tab		
Cleanup of viruses/spyware	Yes	The alternative actions to be applied if cleanup fails have no effect. The Security VM will always deny access to infected items.
Cleanup of suspicious files	No	

For more information about the settings and which settings to choose, see the Enterprise Console Help.

Scheduled scanning

To set up or edit a scheduled scan:

- In the **Anti-Virus and HIPS Policy** dialog, look for the **Scheduled scanning** panel.
- Click **Add** or **Edit**.

You can also specify additional file types to be scanned or exclude items from scanning by clicking **Extensions and Exclusions**.

Scheduled scan settings are supported as detailed below.

Scheduled scan setting	Applies to Security VM?	Notes
Add/Edit > Scheduled scan settings		
What to scan		

Scheduled scan setting	Applies to Security VM?	Notes
Local hard disks	Yes	
Floppy disk and removable drives	Yes	
CD drives	Yes	
When scan occurs	Yes	The Security VM will start the scan at the time and day requested. However, by default, it will scan only two guest VMs at a time, so as not to impact your system's performance. Therefore, it may take longer for the scanning of all guest VMs to complete.
Add/Edit > Scheduled scan settings > Configure > Scanning and cleanup settings		
Scanning tab		
Scan files for Adware and PUAs/Suspicious files/Rootkits	No	
Scan inside archive files	Yes	
Scan system memory	No	System memory will be scanned by default. You cannot configure this option.
Run scan at lower priority	No	
Cleanup tab		
Cleanup of viruses/spyware	Yes	The Security VM doesn't automatically clean up floppy disk drives, CD drives or network locations. Actions for infected items if cleanup has not taken place have no effect. The Security VM will always log the event when cleanup has not taken place.
Cleanup of adware and PUA	No	
Cleanup of suspicious files	No	
Extensions and Exclusions > Scheduled scan extensions and exclusions		

Scheduled scan setting	Applies to Security VM?	Notes
Extensions tab		
Scan all files (not recommended)	Yes	
Scan only executable and other vulnerable files	Yes	
Additional file type extensions to be scanned	Yes	
Scan files with no extension	Yes	
Exclude file types from scanning	Yes	
Exclusions tabs		
Windows Exclusions tab	Yes	To exclude a folder from scanning, you must always specify the full path to the folder, including the drive letter or network share name, for example, "C:\Tools\logs\" or "\\Server\Tools\logs\". The Security VM cannot exclude folders based only on their name. For example, "\Tools\logs\" won't work. For more information about Windows exclusions, for example, how to use wildcards, see the Enterprise Console Help.
Mac Exclusions tab	No	
Linux/UNIX Exclusions tab	No	

Sophos Live Protection

Sophos Live Protection is supported, except for file submission.

Web protection

Not supported.

Authorization

Authorization, as well as detection, of adware and other potentially unwanted applications (PUAs) is not supported.

Messaging

Only email messaging is supported.

2.1.1 Scanned file extensions

Files with the following extensions are scanned by default.

386	docx	Jpz	pl	vxd
3gr	dot	js	pot	wbk
add	drv	jse	pps	wma
ani	eml	lnk	ppt	wmf
asp	exe	lsp	pptm	wsf
aspx	fas	mnl	pptx	xl?
asx	flt	mod	prc	xlsm
bat	fon	mpd	rtf	xlsx
cab	fot	mpp	scr	xsn
chm	hlp	mpt	sh	zip
class	ht?	mso	shb	zipx
cmd	hta	mui	shs	
com	html	nws	src	
cpl	i13	o	swf	
dbx	ifs	ocx	sys	
dex	inf	ov?	tif	
dll	ini	pdf	tiff	
dmd	jar	pdr	vb?	
doc	jpeg	php	vlx	
docm	jpg	pif	vs?	

The following additional extensions are scanned by default if the **Scan inside archive files** option is enabled in the anti-virus and HIPS policy applied to the security VM.

7z	lha
7zip	lzh
??_	rar
a	rpm
arj	tar
bin	taz
bz2	tbz
gz	tbz2
hqx	tgz

hxs	uue z

You can add additional extensions for scanning or exclude extensions from scanning, as described in the Enterprise Console Help, in the section about configuring the anti-virus and HIPS policy.

2.2 Updating policy

All the settings in the Enterprise Console updating policy apply to the Security VM.

For more information, see the Enterprise Console Help, in **Updating computers** > **Configuring the updating policy**.

3 View protected guest VMs

You can view all guest VMs that are protected by a Security VM.

1. Browse to the Security VM. You must use Windows Explorer and you must use the IP address.
2. Double-click the **Logs** share.
3. When prompted, enter your credentials:
   - Username is "Sophos".
   - Password is the access password you set when you installed the Security VM.
4. Open **ProtectedGVMs.log** to view the protected guest VMs.

   Note: The ProtectedGVMs.log file only appears when the Security VM starts protecting guest VMs.

4 Scan guest VMs

Sophos for Virtual Environments scans files on access, that is, when they are opened and closed (if you have on-access scanning enabled in your policy).

A Security VM can also perform a full scan of all the guest VMs it manages. You can either run a scan immediately or at set times.

The full system scan detects but doesn't clean up threats.

Note: The Security VM cannot run a scan if it is still in the Enterprise Console **Unassigned** group. It must be in a group to which you have applied policies.

Note: The Security VM staggers scans so that the hypervisor is not placed under a high load. By default, two guest VMs are scanned at a time. Scanning a large number of guest VMs can take a considerable time.

Scan guest VMs now

To run a full scan of all the guest VMs immediately:

1. Go to Enterprise Console and find the Security VM in the computer list.
2. Right-click the Security VM and select **Full System Scan**.

   Note: Alternatively, on the **Actions** menu, select **Full System Scan**.

Scan guest VMs at set times

To run a full scan of all the guest VMs at set times:

1. Go to Enterprise Console.
2. Create a scheduled scan, as explained in the Enterprise Console Help, in the section about configuring the anti-virus and HIPS policy.

To view details of the scan after it has been run:

In Enterprise Console, in the computer list in the lower right part of the window, double-click the Security VM to display the **Computer details** dialog box.

5 Find out about a threat

To find out more about a threat and how to deal with it:

1. In Enterprise Console, in the computer list in the lower right part of the window, double-click the Security VM to display the **Computer details** dialog box.

   In the **History** section, **Items detected** are listed. The name of the threat is shown in the **Name** column and the affected guest VM and file are shown in the **Details** column.

2. Click the name of the threat.

   This connects you to the Sophos website, where you can read a description of the item and advice on what actions to take against it.

6 Clean up a threat

6.1 Automatic cleanup

The Security VM can automatically clean up threats that it detects.

Note: Automatic cleanup is not available on CDs or other read-only file systems and media, or on remote file systems.

What happens when there is an automatic cleanup?

When a threat is detected and cleaned up automatically, Enterprise Console:

- Shows that the threat has been blocked (see the "History" section of the **Computer Details** dialog box).
- Displays an alert that shows what the threat is and whether it is cleanable.
- Removes the alert if cleanup is successful, and marks it as "Not Cleanable" if cleanup fails.

Occasionally a guest VM needs to be restarted to complete the cleanup. In this case, a "Restart required" alert is displayed for the Security VM. To find out which guest VM the alert applies to, double-click the Security VM to open the **Computer details** dialog box and look in the description of the alert in the **Outstanding alerts and errors** section.

6.2 Manual cleanup

You can clean up a threat manually.

You must clear the alert from Enterprise Console once you have removed the threat.

6.2.1 Clean up a guest VM

To clean up manually, you restore the guest VM. Note that you will lose your data when you do this. Use one of these methods:

- Revert the affected guest VM to the previous known clean snapshot.
- Delete the affected guest VM and reclone it from the template image.

Make sure that the template image has the required Sophos tools installed (see *Sophos for Virtual Environments Startup guide --Enterprise Console edition*).

Whichever method you use, run a full scan of the guest VM afterwards to ensure that it is clean.

6.2.2 Clear an alert from Enterprise Console

When you are sure that the affected guest VM is clean, clear the alert from Enterprise Console:

1. In Enterprise Console, in the computer list in the lower right part of the window, right-click the Security VM and select **Resolve Alerts and Errors**.
2. In the **Resolve Alerts and Errors** dialog box, on the **Alerts** tab, select the alert and click **Acknowledge**.

The alert is no longer displayed in Enterprise Console.

7 Alerts

This section describes the alerts the Security VM sends when threats are detected and cleaned up.

Threat alerts

If the Security VM detects a threat on a guest VM, it will send alerts as follows:

In Enterprise Console:

- An alert is displayed on the dashboard.
- A red warning icon is displayed in the computer list, on the **Status** tab, next to the Security VM in the **Alerts and errors** column.

If the threat is cleaned up automatically, the threat alert is cleared from Enterprise Console.

To find out which guest VM the alert applies to, double-click the Security VM in the computer list. In **Computer details**, under **Outstanding alerts and errors**, look for the alert description. The guest VM details are shown, followed by the path of the threat, like this:

```
MachineName(IP address)/C:\threat.exe
```

If the Security VM detects a threat when a user tries to access a file, a message may also be displayed on the guest VM informing the user that the file cannot be accessed. This depends on the application used to access the file.

Alerts after cleanup

If a threat is cleaned up, the alert is cleared from Enterprise Console.

The cleanup is also reported in Enterprise Console. To see the report, double-click the Security VM in the computer list to open the **Computer Details** dialog and look for **History**.

If the threat has been partially removed, but the guest VM needs to be restarted to complete the cleanup, a "Restart required" alert is displayed.

8 Logs

On a guest VM, the logs are written to the Windows Application event log. You can find the log in **Applications and Services Logs** > **Sophos** > **SVE**.

On a Security VM, you can collect the logs and retrieve them from the shared logs directory. To do this:

1. Open a console to the Security VM.
2. Log on:
   - Username is "sophos".
   - Password is the access password you set when you installed the Security VM.
3. Enter the following command:

   ```
   sudo /opt/sophox/logcollector/diagnose
   ```

   Enter your access password when prompted. (This may take a minute to complete).
4. In Windows Explorer, you can now access the collected logs in `\\<SVM-IP-Address>\logs\logs.tgz`. Enter your credentials when prompted:
   - Username is "sophos".
   - Password is the access password you set when you installed the Security VM.

For information about logging in Enterprise Console, see the Enterprise Console Help.

9 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

10 Legal notices

Third-party licenses

For third-party licenses that apply to your use of this product, please refer to the following folder on the Sophos Security VM: `/usr/share/doc`.

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by following the instructions in knowledge base article 124427.

20170803