SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

configuration guide for users with Enterprise Console

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 at the Sophos Central edition of this configuration guide instead.

2 Configure policies

You configure Sophos for Virtual Environments by using Sophos 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 Sophos 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 Sophos 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 9).

2.1 Anti-virus and HIPS policy

By default, the Security VM does as follows:

- 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 Sophos 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.

The options on each tab are shown below.

Scanning	Supported	Notes
Check files on Read/Rename/Write	No	If one or more of the options are enabled,the Security VM scans in all three scenarios. **If all three options are disabled, 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	Supported	Notes
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	Supported	Notes
Windows Exclusions tab	Yes	To exclude a folder, you must specify the full path, including the drive letter or network share name, for example, "C:\Tools\logs\" or "\\Server\Tools\logs\". For more information, 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	Supported	Notes
Cleanup of viruses/spyware	Yes	The alternative actions to be applied if cleanup fails have no effect. The Security VM always denies access to infected items.
Cleanup of suspicious files	No	

For more information about the settings and which settings to choose, see the Sophos 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.

Go to **Add/Edit > Scheduled scan settings**.

Scheduled scan settings	Supported	Notes
Local hard disks	Yes	
Floppy disk and removable drives	Yes	
CD drives	Yes	
When scan occurs	Yes	The Security VM starts the scan at the scheduled time, but by default scans only two guest VMs at a time, to limit the impact on system performance.

Go to **Add/Edit > Scheduled scan settings > Configure > Scanning and cleanup settings**

Scanning and cleanup	Supported	Notes
Scanning tab		
Scan files for Adware and PUAs/Suspicious files/Rootkits	No	
Scan inside archive files	Yes	
Scan system memory	No	System memory is 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	

Go to **Extensions and Exclusions > Scheduled scan extensions and exclusions**

Extensions and Exclusions	Supported	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		

Extensions and Exclusions	Supported	Notes
Windows Exclusions tab	Yes	To exclude a folder from scanning, you must specify the full path, including the drive letter or network share name, for example, "C:\Tools\logs\" or "\\Server\Tools\logs\". For more information, see the Sophos Enterprise Console Help.
Mac Exclusions tab	No	
Linux/UNIX Exclusions tab	No	

Sophos Live Protection

Live Protection checks suspicious files against the latest malware information in the SophosLabs database.

Option	Supported	Notes
Enable Live Protection	Yes	
Enable Live Protection for on-demand scanning	Yes	
Automatically send file samples to Sophos	No	

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

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

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

2.2 Updating policy

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

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

3 Check that guest VMs are protected

This section tells you how to check that your guest VMs are protected. You can:

- Check the protection settings on a guest VM.
- Test real-time scanning on a guest VM.
- Troubleshoot real-time scanning.

3.1 Check the protection settings

To check that a guest VM is protected:

1. Go to the guest VM and search for **Security and Maintenance** from the start menu. If this option is not found search for **Action Center**.

   Attention
   If neither of these options are found then the guest VM does not provide Windows Security Center. You must check whether the guest VM is protected using the steps described in Test real-time scanning (page 7).

2. Click the drop-down arrow beside **Security**. You should see that Sophos for Virtual Environments is enabled.

   Note
   If it is not enabled, see Troubleshoot on-access scanning (page 8)

3.2 Test real-time scanning

Real-time scanning is your main method of protection against threats. When you open, write, move, or rename a file the Security VM scans the file and grants access to it only if it does not pose a threat. When you run a program the Security VM scans the executable file and any other files it loads.

Important
Ensure that Sophos Endpoint for Windows is **not** installed on any guest VMs that are protected with a Security VM.

To check that a security VM is scanning files on access:

1. Go to eicar.org/86-0-Intended-use.html. Copy the EICAR test string to a new file. Give the file a name with a .com extension and save it to one of the guest VMs.
2. Try to access the file from the guest VM.
3. In Sophos Enterprise Console, in the computer list in the lower right part of the window, click the **Status** tab.
4. In the list of computers, look for the Security VM.

- **If you have automatic cleanup on**, double-click the Security VM to open the **Computer Details** dialog box. In the "History" section, you should see that EICAR has been detected and cleaned up.
- **If you don't have automatic cleanup on**, you should see an alert in the **Alerts and errors** column. Right-click the security VM. In the **Resolve alerts and errors** dialog, you should see that EICAR has been detected but not cleaned up.

If EICAR has not been detected, see Troubleshoot on-access scanning (page 8). If EICAR is not cleaned up, simply delete it.

3.3 Troubleshoot on-access scanning

If on-access scanning is not working:

1. Ensure that the Security VM is in a group whose anti-virus policy specifies that on-access scanning should be turned on:
   a) In Enterprise Console, in the **Groups** pane, right-click the group that contains the Security VM and select **View/Edit Group Policy Details**. Check which anti-virus and HIPS policy is used.
   b) In the **Policies** pane, double-click **Anti-virus and HIPS**.
   c) Double-click the policy that is used by the group that contains the Security VM.
   d) In the **On-access scanning** panel, ensure that the **Enable on-access scanning** check box is selected. Click **OK**.
   e) In the computer list, right-click the security VM and select **Comply with**. Then select **Group anti-virus and HIPS policy**.
   f) Check that the Security VM is shown as compliant with the policy.
2. Ensure that the guest VM is protected. Go to the Security VM host and look in the log file.
3. Ensure that Windows Security Center shows the guest VM as protected by Sophos for Virtual Environments.
4. Check that there are no pending restarts requested by Microsoft updates. These can prevent installation of the Sophos Guest VM Agent from being completed.
5. Check that there are no other anti-virus products installed. On server platforms where the security center is not present check that Windows Defender isn't active. Remember that you cannot use Sophos for Virtual Environments to protect guest VMs that run other anti-virus products.
6. If on-access scanning is still not working, contact Sophos Technical Support.

4 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.

5 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 Sophos 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 Sophos 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 Sophos Enterprise Console.
2. Create a scheduled scan, as explained in the Sophos 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 Sophos 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.

6 Find out about a threat

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

1. In Sophos 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.

7 Clean up a threat

The Security VM can clean up threats automatically for you, or you can clean up manually.

For details, see the sections that follow.

7.1 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, Sophos Enterprise Console does as follows:

- 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.

7.2 Manual cleanup

You can clean up a threat manually.

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

7.2.1 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.

7.2.2 Clear an alert from Sophos Enterprise Console

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

1. In Sophos 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 Sophos Enterprise Console.

8 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, you see these alerts in Sophos 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 Sophos 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 Sophos Enterprise Console.

The cleanup is also reported in Sophos 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.

9 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 Sophos Enterprise Console, see the Sophos Enterprise Console Help.

10 Uninstall the Security VM

To uninstall a Security VM, you delete it.

Before you start, ensure that guest VMs will continue to be protected. Go to the Security VM and View protected guest VMs (page 9). Then move guest VMs to another Security VM with similar policy settings.

To move your guest VMs:

1. Uninstall the Guest VM Agent, see Uninstall the Guest VM Agent (page 17).
2. Reinstall the Guest VM Agent with the new Security VM IP address. See the Sophos for Virtual Environments startup guide.

Once you have moved your guest VMs you can delete the Security VM. To do this:

1. Go to your hypervisor.
2. Power down the Security VM.
3. Delete the VM.

11 Uninstall the Guest VM Agent

You can uninstall the Guest VM Agent from Control Panel.

1. On the guest VM, open **Control Panel**.
2. Click **Programs and Features**.
3. Select these features and click **Uninstall**:
    - Sophos for Virtual Environments
    - Sophos Guest VM Scanning Service
    - Sophos Virus Removal Tool.

12 Appendix: Add Security VMs for guest VM migration

At any time you can add more Security VMs that will be available to protect migrating guest VMs.

Important
You need to perform these steps on the Security VM that you want to add and on the existing Security VMs.

1. Using SSH, open the additional_svms.txt configuration file for editing:
   /opt/sophos-svms/etc/additional_svms.txt
2. Edit the file to add or remove IP addresses of Security VMs that are available to protect migrating guest VMs.
   - Put one IP address per line with no additional separating characters. For example:
     1.2.3.4
     5.6.7.8
   - You don't need to include the IP address for the Security VM you're currently logged in to.
3. Save and close the file.
4. Check the SVM log (/var/log/ssvm.log) to see if there were any errors in processing the additional Security VMs list.
   If there are no errors, the updated list is sent to all connected guest VMs so that they can get protection from the new Security VMs.

13 Appendix: Add CPUs to the Security VM

If you have many guest VMs on a host, you should ensure that the Security VM has enough processing power to scan the files they use when they all start up.

To do this, add more CPUs for the Security VM. You can do this any time.

Note
If you add CPUs after you put the Security VM in a computer group in Sophos Enterprise Console, you should wait until the Security VM complies with group policy.

Depending on the type of load, adding CPUs can also improve overall system performance.

Add CPUs in VMware ESXi

Add CPUs as follows:

1. Power off the Security VM.
2. In vSphere Client, select the Security VM.
3. Select **Edit Settings > Hardware > CPUs.** Then specify the number of CPUs.

Add CPUs in Microsoft Hyper-V

Add CPUs as follows:

1. Click **Start**, select **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the results pane, under **Virtual Machines**, select the Security VM.
3. In the **Action** pane, under the VM name, click **Settings**.
4. Click **Processor** and specify the number of processors.

14 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 knowledge base 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.

15 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.