SOPHOS

Cybersecurity
made
simple.

Sophos for Virtual Environments

configuration guide for users with Sophos Central

Contents

(2018/10/11)

1 About this guide

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

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

If you use Sophos Enterprise Console, see the configuration guide for Enterprise Console users.

2 Configure policies

You configure Sophos for Virtual Environments by using Sophos Central policies.

You can only use the Threat Protection policy type, but you can create multiple policies if you want to.

By default, Sophos Central applies a base Threat Protection policy to all your Security VMs. The settings in the policy are then used for the guest VMs.

These settings offer:

- Detection of known malware.
- In-the-cloud checks to enable detection of the latest malware known to Sophos.
- Proactive detection of malware that has not been seen before.
- Automatic cleanup of malware.

For full details, see the Sophos Central Help.

You can edit the base policy or create additional policies, which you can use to apply different settings to different Security VMs.

Create or edit a policy

To create or edit a Threat Protection policy:

1. Open Sophos Central and go to **Server Protection > Policies**.
2. Click on a **Threat Protection** policy or click **Add Policy** to create a new one.
3. On the **Servers** tab, select the Security VMs you want to apply the policy to.
4. On the **Settings** tab, enter the settings you want.

   For details of the options that you can use for Security VMs, see the sections below.

Live Protection

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

Option	Supported?
Use Live Protection	Yes
Automatically submit malware samples to SophosLabs	No

Real-time scanning

The options for **Real-time scanning** are as follows.

Option	Supported?
Enable or disable	Yes

Option	Supported?
Scan local, or scan local and remote	Yes
On read	No
On write	No

Real-time scanning - Internet

The options for **Real-time scanning - Internet** are as follows:

Option	Supported?
Scan downloads in progress	No
Block access to malicious websites	No
Detect low-reputation files	No

Remediation

The options for **Remediation** are as follows:

Option	Supported?
Automatic cleanup of malware	Yes

Real-time scanning - Options

The options for **Real-time scanning - Options** are as follows:

Option	Supported?
Automatically exclude activity by known applications	No
Detect malicious behavior (HIPS)	No

Scheduled scanning

The options for **Scheduled scanning** are as follows:

Option	Supported?
Enable scheduled scan	Yes

Runtime protection

The options for **Runtime protection** are as follows.

Option	Supported?
Detect network traffic to command and control servers	No
Protect document files from ransomware (CryptoGuard)	No

Option	Supported?
Enable Sophos Security Heartbeat	No

Scanning exclusions

The options for **Scanning exclusions** are as follows.

Option	Supported?
Global scanning exclusions To edit these, go to **Settings > Global scanning exclusions**.	Yes
Policy scanning exclusions (Windows and Linux)	Yes
Policy Heartbeat exclusions (Windows only)	No
Exclude DNS server (Windows only)	No

Desktop messaging

The options for **Desktop messaging** are as follows.

Option	Supported?
Enable desktop messaging for Threat Protection	No

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 5).

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 real-time scanning (page 6)

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. Log in to Sophos Central.

- **If you have automatic cleanup on**, go to the **Servers** page and click the Security VM to open its details page. On its **Events** tab, you should see that EICAR has been detected and cleaned up.
- **If you don't have automatic cleanup on**, look at the **Alerts** page. You should see an alert on the Security VM. EICAR has been detected but not cleaned up.

If EICAR has not been detected, see Troubleshoot real-time scanning (page 6). If EICAR is not cleaned up, simply delete it.

3.3 Troubleshoot real-time scanning

If real-time scanning is not working:

1. Ensure that real-time scanning is enabled in the server policy applied to the Security VM:
    a) In Sophos Central, go the **Servers** page, find the Security VM and click on it to display its details.
    b) In the **Summary** tab, under **Summary**, you can see the Threat Protection Policy applied to the server. Click the policy name.
    c) In the policy, find the **Real-time scanning** section. Ensure that **Scan** is enabled.
    d) Check that the Security VM is compliant with the policy.
2. Ensure that the guest VM is protected. Go to the Security VM host and look in the log file. For details, see "View protected guest VMs" in the Sophos for Virtual Environments configuration guide.
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 aren't any 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 guest VMs

You can view details of all the guest VMs as follows:

- View connected guest VMs (page 7). You can do this in Sophos Central.
- View protected guest VMs (page 7).

"Connected" guest VMs have the Sophos agent installed and can connect to the Security VM.

Usually, a connected guest VM is also protected. However, if the agent is newly installed, or there is a problem, scanning for threats may not have started yet.

4.1 View connected guest VMs

You can view all the guest VMs that are connected to a Security VM as follows.

1. Log in to Sophos Central.
2. Go to **Server Protection > Servers**.
3. Find the Security VM in the list and click on it to view its details.
4. On the **Summary** tab, under **Virtual Environments Status**, find **Connected Guest VMs**. Click on the number shown.

   Note
   If no guest VMs are powered on, or if you’re still installing agents on them, you may see zero guest VMs.

5. You see a list of VM names and IP addresses.

   You can search the list for a particular guest VM, or use the filter to display desktop or server guest VMs.

4.2 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

The Security VM always scans files on access, that is, when they are opened and closed.

The Security VM can also perform a full scan of all guest VMs. 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 staggers scans so that the host is not placed under a high load. By default, two guest VMs are scanned at a time. Therefore, it may take longer for the scanning of all guest VMs managed by the Security VM to complete.

Scan guest VMs now

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

1. Log in to Sophos Central.
2. Go to the **Servers** page.
3. Find the Sophos Security VM and click on it to open its details page.
4. In the left pane, click **Scan Now**.

Scan guest VMs at set times

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

1. Log in to Sophos Central.
2. Go to the **Servers** page.
3. Find the Sophos Security VM and click on it to view its details page.
4. On the **Summary** tab, look under **Summary** for the Threat Protection policy that applies. Click on it to edit it.
5. In the policy, go to the **Scheduled scanning** section. Enable scanning and specify the times when the scan will be run.

6 What happens when a threat is detected

If the Security VM detects a threat on one of the guest VMs, it does as follows:

- Blocks the threat.
- Attempts to clean up the threat automatically.
- Sends an alert to Sophos Central if you need to take any action.

Note
The Security VM does not automatically clean up threats detected during a full scan of all guest VMs.

What you see in Sophos Central

Sophos Central:

- Shows that the threat has been blocked. See the **Events** tab of the details page for the Security VM.
- Displays an alert in the **Alerts** page. This shows what the threat is, which VM it is on, and whether it is cleanable.
- Removes the alert if automatic cleanup is successful.

If automatic cleanup is not available or is not successful, an alert in the **Alerts** page prompts you to clean up manually.

For more information on cleanup, see Clean up a threat (page 10).

What the user sees on the guest VM

If the Security VM detects a threat when a user tries to access a file, a message may 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.

7 Clean up a threat

This section describes both automatic and manual cleanup of threats.

For information about a threat and advice on cleanup, log in to Sophos Central, go to the **Alerts** page, look for the threat alert, and click on the threat name.

Automatic cleanup

The Security VM automatically cleans up threats it detects.

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

Manual cleanup

You can clean up a guest VM manually.

To clean up manually, you restore the guest VM. Note that you may lose data (see details below).

Use one of these methods:

- Delete the guest VM and reclone it from the template image. You will lose your data.
- Revert the guest VM to the previous known clean snapshot. You will lose data added since the taking the snapshot.

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

8 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 7). 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 12).
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.

9 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.

10 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.

11 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.

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.

12 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.

13 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.