SOPHOS
Security made simple.

Sophos for Virtual Environments

startup guide -- Enterprise Console edition

Contents

1 About this guide

This guide tells you how to:

- Use Sophos for Virtual Environments to provide central threat protection for virtual machines (VMs) in a VMware ESXi or Microsoft Hyper-V environment.
- Use Sophos Enterprise Console to manage Sophos for Virtual Environments.

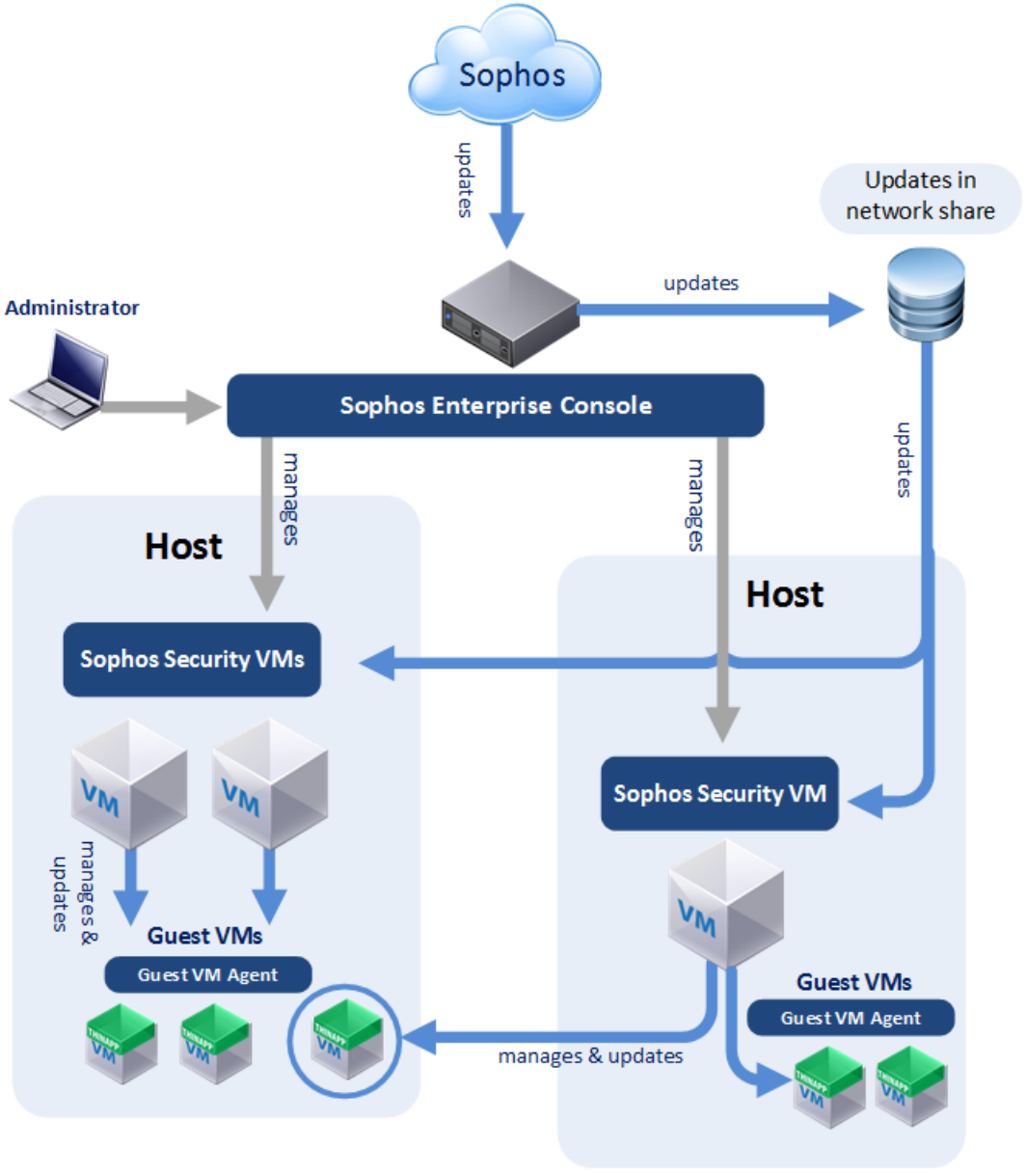
If you are migrating to Sophos for Virtual Environments, see Migrate to Sophos for Virtual Environments (page 25).

If you want to use Sophos Central instead of Sophos Enterprise Console, see *Sophos for Virtual Environments Startup guide -- Sophos Central edition*.

2 About Sophos for Virtual Environments

Sophos for Virtual Environments is a security system that protects VMs. It works like this:

- You put one or more installations of Sophos Security VM on each hypervisor host. The Sophos Security VM can then detect and block threats on guest VMs connected to it.
- You must put a Sophos Guest VM Agent on each guest VM.
- You use Sophos Enterprise Console on another computer to manage the Security VMs and keep them up to date.



Which environments can Sophos be used in?

Sophos for Virtual Environments can protect VMs in a VMware ESXi environment or a Microsoft Hyper-V environment.

Which guest VMs can be protected?

The Sophos Security VM can protect guest VMs that run Windows operating systems. For supported versions, see Guest VM requirements (page 7).

The Security VM can protect guest VMs that are on a different host.

How does scanning work?

When a guest VM tries to access a file:

- The Sophos Guest VM Agent running on the VM notifies the Security VM.
- The Security VM scans the file.
- If the Security VM detects a threat, access to the file is blocked, and the Security VM sends an alert to Enterprise Console.

The Security VM can also perform a full scan of all the guest VMs. You can run this scan immediately or schedule it.

The file scanner uses intelligent caching to retain the results of previous scans. This helps improve overall performance when there are many connected guest VMs or when the same file is accessed repeatedly.

Can guest VMs move between Security VMs?

You can enable guest VMs to move between Security VMs for protection.

This keeps guest VMs protected if they can't connect to their current Security VM. It also spreads the workload between Security VMs.

Guest VMs cloned from a single template can also migrate between Security VMs. When you create the template, you can list all the available Security VMs, so that the clones can connect to any of them. See knowledge base article 127955.

You can set up guest VM migration during installation.

How is the Security VM managed?

Sophos Enterprise Console displays the status of the Security VM, including how up to date it is and whether it has detected any threats.

Sophos Enterprise Console also enables you to configure scanning by means of a policy.

How do you deal with threats?

The Security VM provides the ability to clean up threats automatically, see *Sophos for Virtual Environments Configuration guide--Enterprise Console edition*.

How is the Security VM updated?

Sophos Enterprise Console keeps the Security VM updated.

Sophos Enterprise Console downloads the latest threat data, maintenance updates and new versions of the product from Sophos and puts them in a network share. The Security VM fetches and installs updates automatically.

The date on which you get a maintenance update can depend on whether you subscribe to Recommended or Preview releases.

How is the Guest VM Agent updated?

The Guest VM Agent is updated automatically.

The agent doesn't scan files, so it doesn't need updated threat identities. However, it does get updates when we improve the product.

The Security VM fetches these product updates and applies them to the guest VMs.

Updates are staggered to minimize the load on the Security VM and the underlying hypervisor host.

3 Key steps in installation

Installation involves these key steps, which are described in the sections that follow:

- Check the system requirements.
- Uninstall other anti-virus products.
- Set up the Sophos management software (Sophos Enterprise Console).
- Install the Sophos Security VM and apply policies.
- Install the Sophos Guest VM Agent on guest VMs.
- Check that guest VMs are protected.

4 Check the system requirements

This section tells you the system requirements and how to check that you comply with them.

It also tells you about any information (such as computer details) that you should gather now so that you will have it available when you install a Security VM.

It covers requirements for both VMware EXSi or Microsoft Hyper-V environments.

4.1 VMware requirements

This section shows you the software you need in a VMware environment.

4.1.1 VMware ESXi host

You should install the following on each host that will run a Sophos Security VM:

- VMware ESXi host 5.5, 6.0, or 6.5.

> **Note**
> We recommend that you configure the host to get updates from VMware.

Hardware requirements

The VMware ESXi host must be able to allocate the following resources for each Sophos Security VM:

- 2 CPUs.
- 20 Gb disk space.
- 4 Gb RAM.

Notes

You should not place a CPU resource limit on the Sophos Security VM.

By default, 2 CPUs are allocated. If you have many guest VMs to protect, you can configure more CPUs after you install the security VM. This guide tells you how.

The Security VM reserves memory. High-availability and load-balancing systems make automatic choices based on resource reservations for the VMs in your VMware environment. You should not remove the Security VM memory reservation.

4.1.2 VMware vCenter and vSphere

You require the following vCenter and vSphere software.

Software	Version	Notes
vCenter	Version 5.5, 6.0, 6.5	You will also need: The network address. An administrator account.
vSphere Client	Version 5.5, 6.0, 6.5	

4.1.3 VMware Tools

We recommend that you use VMware tools on Guest Virtual Machines because they can improve performance.

4.2 Microsoft Hyper-V requirements

This section shows you the software you need in a Microsoft Hyper-V environment.

The Microsoft Hyper-V system should be one of the following:

- Hyper-V in Windows Server 2012 (Core, full)
- Hyper-V in Windows Server 2012 R2 (Core, full)
- Hyper-V in Windows Server 2016 (Core, Server with Desktop Experience)

Microsoft Hyper-V integration components

The Microsoft Hyper-V integration components will install automatically if Windows updating is enabled and works successfully. Without these tools your VM performance maybe degraded.

Guidelines for anti-virus for Microsoft Hyper-V

Microsoft publish guidelines for how to secure your Hyper-V server most effectively. See Microsoft KBA 3105657.

4.3 Guest VM requirements

Guest VMs should run one of the operating systems listed here.

Operating system	Service packs	Comments
Windows 10 (32 and 64-bit). Knowledge base article 125679 lists all supported versions.		Windows and Hyper-V containers not supported.
Windows 8.1 (32 and 64-bit)	---	
Windows 7 (32 and 64-bit).	SP1+	
Windows Server 2016 (64-bit). Knowledge base article 125679 lists all supported versions.		Windows and Hyper-V containers not supported.

Operating system	Service packs	Comments
Windows Server 2012 R2 (64-bit)	---	
Windows Server 2012 (64-bit)	---	
Windows Server 2008 R2 (64-bit)	---	

4.4 Network requirements

The infrastructure requirements are as follows:

- The Security VM and guest VMs need to share a network connection. Ideally this should be a high-speed LAN with no network traffic throttling.
- The network traffic between Security VM and guest VMs should not be blocked by firewalls or network access controllers.

4.4.1 NAT networks requirements

If you have guest VMs inside a NAT (Network Address Translation) network, you can protect them with a Security VM inside or outside of that network.

During installation you must configure the Security VM with the following:

- A primary IP address outside of the NAT (this address must be able to communicate with the management console)
- A secondary IP address that is within the NAT.

4.4.2 Subnets

You can configure the Security VM with up to five IP addresses. Each IP address must be on a different subnet.

4.5 Sophos management requirements

You need the following Sophos software before you can install and use the Sophos Security VM. If you don't have this software, follow the instructions in Set up Sophos management software (page 10).

Software	Version	Notes
Sophos Enterprise Console	Version 5.4 or later.	We recommend version 5.5.
Sophos for Virtual Environments network share	No minimum version.	You must set up a network share where Sophos Enterprise Console makes the latest updates available for your Security VM. This guide tells you how.

5 Uninstall other anti-virus products

You should uninstall any anti-virus products, including Sophos products, that are already installed on your guest VMs.

You need to disable Windows Defender on server platforms where the security center is not present. We recommend that you do this using a group policy.

You cannot use Sophos for Virtual Environments to protect guest VMs that run other anti-virus products. If you try to do this, there may be reduced performance or a system deadlock in which the guest VM stops responding.

This limitation also applies to VMs with Sophos gateway or server products that include or require anti-virus components.

For more information, see knowledgebase article 125679.

6 Set up Sophos management software

Before you install Security VMs, you should:

- Install Sophos Enterprise Console (if you do not already have it). You use this to download protection software updates and to manage the VMs you protect.
- Create a Sophos for Virtual Environments network share. The share is used to keep Security VMs up to date.

The following sections describe how to do this.

Already using Sophos Enterprise Console?

Warning
If you already use Sophos Enterprise Console to manage other Sophos products and now want to add Sophos for Virtual Environments, your customer credentials might not let you set up the Sophos network share. If this happens, check that your license includes this product. You can send license queries to customercare@sophos.com

6.1 Install Sophos Enterprise Console

If you already have Sophos Enterprise Console installed, go to Create a Sophos update share (page 11).

You should install Sophos Enterprise Console on a Windows computer that will be on the same network as the Security VMs.

Follow the instructions in the Sophos Enterprise Console quick startup guide. When you are prompted to select the platforms you want to protect, include **Sophos for Virtual Environments**. This creates the Sophos for Virtual Environments network share.

CAUTION
This gives you the Recommended version. If you want the Preview version, which gives you early access to new features, Create a Sophos update share (page 11).

Note
Whether you have Recommended or Preview, you must use the same version when you install the Security VMs later.

After installation, see Check access to the Sophos update share (page 11).

6.2 Create a Sophos update share

If you have just made a new installation of Sophos Enterprise Console and subscribed to Sophos for Virtual Environments, you can skip this section.

1. In Sophos Enterprise Console, on the **View** menu, click **Update Managers**.
2. Set up a "subscription" to Sophos for Virtual Environments:
   a) In the **Software Subscriptions** pane, click **Add** at the top of the pane.
   b) In the **Software Subscription** dialog box, type a name in the **Subscription name** text box.
   c) In the platform list, select **Sophos for Virtual Environments**.

   > **Note**
   > If you cannot see this in the list, your customer credentials need updating. Contact Sophos Technical Support.

   d) In the version box, select **Recommended** or **Preview**.

   > **Note**
   > Preview gives you early access to new features. Read more about Recommended and Preview.

   > **Note**
   > You must use the same version when you install the Security VMs later.

3. Configure the update manager to use this subscription:
   a) In the **Update Managers** pane, select the update manager that is installed on this server. Right-click it and click **View/Edit configuration**.
   b) In the **Configure update manager** dialog box, on the **Subscriptions** tab, ensure that the new subscription is in the **Subscribed to** list.
   c) Click **OK**.

Now continue to the next section.

6.3 Check access to the Sophos update share

You need to locate the Sophos update share and ensure that it can be accessed using either valid credentials or a guest account.

> **Note**
> Unless you specified otherwise, the Sophos update share is accessed by the user account set up during installation of Sophos Enterprise Console. It is described there as the "Update Manager" account and most customers give it the username SophosUpdateMgr.

1. In Sophos Enterprise Console, on the **View** menu, click **Bootstrap Locations**.
   A list of locations is displayed.
2. Find the location for Sophos for Virtual Environments and make a note of it. You will need this when you install the Security VMs.

   You will need the Fully Qualified Domain Name for this location.
3. If the share is on Windows Server 2008 or 2012, you might need to change Windows Firewall settings on the server temporarily to enable the Sophos security VM installer to access it.

   The following Inbound rules must be set to **On** (which is the default):

   - File and Printer Sharing (NB-Datagram-In)
   - File and Printer Sharing (NB-Name-In)
   - File and Printer Sharing (NB-Session-In)

   You can set these rules to **Off** again after you have installed your security VMs.

Notes:

If you have a customised installation of Enterprise Console or you created an additional network share for updating Security VMs, note that:

- If credentials are required, they will need to be stored on Security VMs after they are installed, so we recommend that you use read-only credentials.
- If the network share is on a different computer to Sophos Enterprise Console (or the Update Manager component of Sophos Enterprise Console), ensure that it can also be accessed using an account that has write access.

7 Install the Sophos Security VM

You can install one or more Security VMs on each host where you want to protect guest VMs.

Installation involves these steps, which are described in the sections that follow:

- Check that you have the passwords you need.
- Check that systems are synchronized.
- Check the installer requirements.
- Download the installer.
- Install the Security VM.
- Check the Security VM is installed.
- Use Enterprise Console to apply policies to the Security VM.

7.1 Check that you have the passwords you need

When you run the Sophos Security VM installer, you need to enter certain passwords. You should make sure that you have the passwords for the following accounts:

- The account used to access the Sophos for Virtual Environments network share (or "Sophos Update folder").
- If you're in a VMware environment, the vCenter Administrator account.

7.2 Check that systems are synchronized

You must ensure that the time is synchronized on the Sophos Enterprise Console server, on the host where you install the Security VM, and on the guest VMs.

You can use NTP (Network Time Protocol) synchronization for each host.

Warning

If the time is not synchronized, you can install a Security VM but you cannot manage it from Enterprise Console.

7.3 Check the installer requirements

Check that the computer and user account you're going to use meet the requirements.

- The installer must be on a Windows computer that has access to your VMware vCenter or Microsoft Hyper-V server over the network.
- Installation of the Security VM must be done on the local network. The installer does not currently support the use of a proxy.
- The installer cannot be used on a Windows XP or Windows Server 2003 computer.
- If you use Microsoft Hyper-V, you must run the installer as a user with rights to create and control VMs on the Hyper-V server. This can be a local user account on the Hyper-V server or a domain user.

The computer where you put the installer is used only for installation. It is not used for management or protection of your Security VM or guest VMs after installation.

7.4 Download the Security VM installer

You download the Security VM installer from the Sophos website (if you have not already done this).

The following steps assume that you have a MySophos account and that you have associated your license credentials with it. If you need help, go to www.sophos.com/en-us/support/knowledgebase/111195.aspx.

Notes:

- You can download the Security VM installer at any computer and then copy it to the computers where you will use it.
- The installation instructions in later sections tell you which computer or computers you should use the installer on.

To download the installer:

1. Go to www.sophos.com/en-us/support/downloads/.
2. Type your MySophos username and password.
3. If you see a web page that shows your licenses, select a license.
4. Under **Standalone installers**, click **Sophos for Virtual Environments**.
5. On the **Sophos for Virtual Environments** web page, find the installer for the hypervisor you are using (Hyper-V or ESXi).
6. Decide whether you want the **Recommended** or **Preview** version.
7. Download the installer.

After you install the Security VM, you will be able to get the Guest VM Agent from a public share on the Security VM.

7.5 Install the Security VM

Before you start, make sure that you have done the following:

- Download the Security VM installer (page 14)
- Check the installer requirements (page 13)

Some installation steps apply only to VMware ESXi or only to Microsoft Hyper-V. These are indicated at the start of the step.

1. Double-click the installer to run it.
2. Accept the license agreement.
3. At the welcome page, click **Next** to extract the installation files to a folder on your computer.
4. Check the **Prerequisites for installation**.
5. This step is only for VMware ESXi:

   In **VMware vCenter credentials**, enter your details and a name for the Security VM.

> **Note**
> Enter the administrator username in the form you use to log in to vCenter using vSphere Client (with or without the domain prefix, as required, and with the same capitalization).

6. In **ESXi host** or **Hyper-V host name**, specify the host on which you want to install the Security VM.
7. In **Management console**, select **Use Sophos Enterprise Console**.
8. In **Sophos update folder details**, enter details of the Sophos for Virtual Environments network share you created earlier.
   a) Enter the location. Use a UNC path including the fully qualified domain name, or a web address (if the share is on a web server).

      For example:

      \\<Your server name.domain name>\sophosupdate\CIDs\Sxxx\SVE

      Tip: To check the location, go to Sophos Enterprise Console. On the **View** menu, click **Bootstrap Locations** and look for the Sophos for Virtual Environments share.
   b) Enter the username and password. You (or another administrator) set up this user account during Sophos Enterprise Console installation. It is described there as the "Update Manager" account and most customers give it the username SophosUpdateMgr.

      Note that:

      - If you specify a domain user, you must include the domain name.
      - The credentials are securely stored on the Security VM.
9. Create a Password for access to your Security VM.

   You need this password to view your protected guest VMs. You also need it to collect logs for troubleshooting.
10. Create a **Password for access to Guest VM Agent installer**.

    You'll need this password later to install agent software on the guest VMs.
11. Select the **Timezone** that the Security VM will use to schedule scans.
12. This step is only for VMware ESXi:

    In **Datastore for the Security VM**, select the type of datastore on which you want to install the Security VM.

> **Note**
> The Security VM protects guest VMs even if their templates are stored in different datastores.

13. In **IP settings for the Security VM**, enter the IP settings for all the networks where you want to protect guest VMs. One Security VM can protect VMs on multiple networks.
    a) In **Select virtual LAN** (ESXi) or **Select vSwitch** (Hyper-V), select from those available.
    b) Enter the **Static IPv4 address**. You can only use static addresses.
    c) Enter the **Subnet mask**.
    d) Enter the **Domain suffix**.
    e) Select **Make Primary** if this is the network that should have access to the Sophos management console. You can only have one primary network.

       You can use the "+" button above the fields to add another network. The "-" button removes a network. The "<" and ">" buttons let you move between your settings for different networks.
14. In **Gateway and DNS server details for the primary network card**, enter details that will enable the Security VM to communicate with the management console and download updates.

> **Note**
> You can enter one DNS Server or, optionally, two.

15. In **Guest VM migration**, you can enable guest VMs to move between Security VMs.
    If you don't enable migration, skip to step 18.
16. In **Guest VM migration: Security VM certificate**, enter details of a certificate bundle.
    For help with creating certificates, see knowledge base article 127562.
17. In **Guest VM migration: Available Security VMs**, enter the IPv4 addresses of Security VMs that will be available to protect guest VMs.
    We recommend that you use Security VMs with the same security policies to ensure consistent cleanup and reporting.
    For migration of guest VMs cloned from a template, seeknowledge base article 127955.
18. This step is only for Hyper-V:
    In **Disk image location**, specify a location for the Security VM disk image. This can be a network share or a local folder on the host.
19. At the **Summary of installation** page, click **Install**.
20. At the **Finished** page, you can see whether installation of the Security VM was successful. If there was a failure, check the log for details.
    Tip: You can click **Start Over** to run another installation or to try again. On Hyper-V, you only see this option if installation has failed.

Follow the instructions in the next two sections to:

- Check that you can see the Security VM in Enterprise Console.
- Use Enterprise Console to apply policies to the Security VM.

Then you need to Install the Sophos Guest VM Agent (page 18).

> **Warning**
> Don't "suspend" the Security VM. If you do, communications with the management software will not be able to resume later.

7.6 Check that the Security VM is installed

This section tells you how to check that Sophos Security VM is installed and has the resources it needs.

Check that you can see the Security VM

When the Security VM has been installed, go to Sophos Enterprise Console.

You should see that the Security VM is registered and placed in the **Unassigned** group of computers.

If you change the name of a Security VM after installation, it is still shown in Sophos Enterprise Console with the name assigned during installation.

Check whether you need to configure resources

Usually you do not need to configure resources for the Security VM. Note that:

- If the Security VM protects a large number of guest VMs, you should ensure that it has enough processing power for scanning. See Appendix: Add CPUs to the Security VM (page 27).
- The installer reserves memory for the Security VM. In a VMware environment, high-availability and load-balancing systems make automatic choices based on resource reservations for the VMs, so these choices could be different after you install the Security VM. You should not remove the Security VM memory reservation.

You are ready to use Sophos Enterprise Console to apply policies to the Security VM.

7.7 Use Sophos Enterprise Console to apply policies

1. In Sophos Enterprise Console, create an updating policy and an anti-virus and HIPS policy. Right-click each policy and select **Reset Policy to Factory Defaults**.
2. Double-click the new updating policy to open it.
3. In the **Updating policy** dialog box:
   a) Click the **Subscription** tab and select the subscription for Sophos for Virtual Environments.
   b) Click the **Primary Server** tab and ensure that the location of the update folder includes the fully qualified domain name. Save the policy.
4. Create a new computer group to contain the Security VM.
5. Apply the new policies to the new group.
6. Drag the Security VM from the **Unassigned** group to the new group.

Now you are ready to Install the Sophos Guest VM Agent (page 18) on guest VMs.

For general advice on post-installation and maintenance tasks, see Maintain the Security VM (page 22).

8 Install the Sophos Guest VM Agent

The Sophos Guest VM Agent must be run on each guest VM that you want to protect.

Check which operating systems you can install the Guest VM Agent on. See Guest VM requirements (page 7).

1. On the guest VM, browse to the host where the Security VM is installed. You must use the IP address.
2. In the **Public** share, find the installer **SVE-Guest-Installer.exe**
3. Double-click the installer to run it, or transfer the installer to the guest VM and run it. Follow the on-screen instructions. Alternatively you can:
   - Use the command line. You can choose to install with (limited UI) or without (no UI) a progress bar being displayed to indicate the progression of the installation. The commands are case sensitive. Enter either:

     Limited UI: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /passive`

     No UI: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /quiet`
   - Use Group Policy deployment. For details, see this Microsoft article: http://support.microsoft.com/kb/816102

We recommend that you snapshot the guest VM after installing the agent. This will allow you to revert the guest VM safely later if you need to.

9 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.

9.1 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 19).

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 20)

9.2 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 on-access scanning (page 20). If EICAR is not cleaned up, simply delete it.

9.3 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.

10 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.

11 Maintain the Security VM

This section gives advice on post-installation and maintenance tasks.

- You must power on the Security VM manually whenever the host is taken out of maintenance or standby mode. Do this before you power on the guest VMs, so that the guest VMs are protected immediately.
- Don't "suspend" the Security VM. If you do, communications with the management software will not be able to resume later.
- Verify that the Security VM is receiving security updates from Sophos. You can do this by checking its update status in Enterprise Console.
- Backups. We recommend that the Security VM is excluded from regular backup tasks, as this can degrade its performance. If the Security VM needs to be recovered due to infrastructure failures, we recommend you redeploy the Security VM.

12 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 21). 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 24).
2. Reinstall the Guest VM Agent with the new Security VM IP address, see Install the Sophos Guest VM Agent (page 18).

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.

13 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.

14 Migrate to Sophos for Virtual Environments

Which products can I migrate from?

You can migrate to Sophos for Virtual Environments from these products.

- Sophos Anti-Virus for vShield in a VMWare ESXi environment
- Sophos Anti-Virus running locally on each guest VM in either a VMware ESXi environment or a Microsoft Hyper-V environment
- Sophos for Virtual Environments running in VMware ESXi or Microsoft Hyper-V environments that are managed by Sophos Enterprise Console
- Other vendors' anti-virus products in either a VMware ESXi environment or a Microsoft Hyper-V environment

Note
Sophos for Virtual Environments protects guest VMs on a VMware ESXi host, including when running in a NSX environment. However, Sophos for Virtual Environments does not integrate with the NSX manager. You should not install any anti-virus software to run on NSX as this will impact performance and could cause deadlocks.

Note
Sophos for Virtual Environments uses a Security VM to provide central threat scanning. Once you install this, guest VMs no longer need threat data updates.

How do I migrate?

Follow the steps below. You can find more details on each step in this guide.

Note
If you’re migrating from third-party anti-virus software, be aware that:

- Sophos for Virtual Environments requires network connectivity between the Security VM and guest VMs.
- Sophos for Virtual Environments supports dynamic VM load balancing technologies like vMotion and Live migration, but performance is best if high speed network connectivity between the Security VM and guest VMs is maintained.

To migrate:

1. Install a Security VM.

> **Note**
> This new Security VM can be on the same host as an existing SAV vShield Security VM.

2. Go to your management console and verify that the Security VM is successfully updating.
3. Shut down the old Security VM or uninstall your old anti-virus software.

> **CAUTION**
> Your guest VMs will become unprotected so please ensure their security.

4. Install the new lightweight Sophos Guest VM Agent.
5. Verify, as described in this guide, that all guest VMs are now protected.

15 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.

16 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.

17 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.