

# SOPHOS

Cybersecurity  
made  
simple.

## Sophos Web Appliance Virtual Appliance Setup Guide

product version: 4.3.7

# Contents

Virtual appliances.....	1
30-day trial.....	1
Installing a virtual appliance.....	2
Supported VMWare platforms.....	2
Configuring Ports.....	2
Resource requirements.....	6
Download installation files.....	7
Install a virtual appliance on VMWare ESX/VMWare ESXi.....	7
Install a virtual appliance on VMWare Workstation.....	8
Configuring a virtual appliance.....	10
Start a virtual appliance.....	10
Configure network settings.....	10
Cloning a virtual appliance.....	12
Clone a virtual appliance.....	12
Copyrights and trademarks.....	14

# 1 Virtual appliances

As an alternative to the hardware-based Sophos Web Appliance, you can deploy appliances as virtual machines using VMWare®. You can group these appliances with other virtual appliances or with hardware appliances.

Once installation is complete, you can configure the appliance using the setup wizard. See the [Sophos Web Appliance configuration guide](#) for more information.

## Note

If you are not deploying a virtual appliance, refer to the setup guide that was shipped with your hardware appliance.

## 1.1 30-day trial

The 30-day trial offers an opportunity to configure and deploy a virtual appliance much the same as you would the full product.

In trial mode, the following restrictions apply:

- The trial includes the virtual web appliance only. The virtual management appliance and hardware-based appliances are not included, but are available in a full-product evaluation.
- Central Management functionality is not included. You cannot control the trial appliance from a management appliance.
- Sophos Technical Support contact and support alerts are not included. However, they are available in a full-product evaluation.
- Endpoint Web Control is not included. However, it is available in a full-product evaluation.
- Re-registering and cloning are not supported.

After the 30-day trial ends, contact Sophos Sales to start a free, full-product evaluation or to purchase a license. You can continue to use the product with the configuration you created during the trial.

## 2 Installing a virtual appliance

You can use the import wizard in VMWare to add a virtual appliance. Use the procedure that corresponds to your version of VMWare.

Before you begin, make sure that you have a supported VMWare platform, that your network allows access to the necessary ports, and that you have sufficient resources. You also need the following:

- Activation code (not required for 30-day trial)
- IP address of default gateway (not required if using DHCP)
- IP addresses of DNS servers (not required if using DHCP)

### 2.1 Supported VMWare platforms

You can install and run virtual appliances on the following VMWare platforms:

- VMWare ESX®/VMWare ESXi™ 3.5 or 4.x
- VMWare ESXi 5.x
- VMWare Workstation™ 6.5 or 7.1

#### Note

VMWare Workstation is supported for testing and is not intended for use in a production environment. If you want to deploy the virtual appliance in a production environment, use VMWare ESX/VMWare ESXi.

### 2.2 Configuring Ports

To ensure the functionality of the Sophos Web Appliance, configure your network to allow access on the ports listed below. Some ports are required only for specific situation, such as when you enable FTP backups or central management.

**Table 1: External Connections**

Port	Function	Service	Protocol	Connection
22	Remote assistance	SSH	TCP	Outbound from appliance to sophos.com
22	Central configuration, status and reporting	SSH	TCP	Outbound from web appliance to management appliance (if not collocated)
25	Remote assistance notification	SMTP	TCP	Outbound from appliance to sophos.com

Port	Function	Service	Protocol	Connection
80	Outbound network web traffic	HTTP	TCP	Outbound from appliance to internet
123	Network time synchronization	NTP	UDP	Outbound from appliance to internet
443	Outbound network web traffic	HTTPS	TCP	Outbound from appliance to internet

**Note**

Opening ports 80 and 443 is a standard best practice. However, certain web sites may also require other ports to be opened.

**Table 2: Internal Connections**

Port	Function	Service	Protocol	Connection
21	Backups using passive FTP	FTP	TCP	Outbound from appliance to FTP server
22	Central configuration, status and reporting	SSH	TCP	Outbound from web appliance to management appliance (if collocated)
53	DNS queries	DNS	UDP	Outbound from appliance to LAN
80	Administrative web interface	HTTP	TCP	Inbound from LAN to appliance
88	Kerberos authentication	KERBEROS	TCP/UDP	Inbound/outbound between appliance and AD server
139	MS NetBIOS session	NETBIOS-SSN	TCP/UDP	Inbound/outbound between appliance and AD server
389	Directory services synchronization	LDAP	TCP/UDP	Inbound/outbound between appliance and AD server
443	Administrative web interface	HTTPS	TCP	Inbound from LAN to appliance
445	MS server message block	SMB	TCP/UDP	Inbound/outbound between appliance and AD server
636	LDAP synchronization	LDAPS	TCP	Inbound/outbound between appliance and eDirectory server
1024–1300, 49152–65535	Dynamic RPC	RPC	TCP	Inbound/outbound between appliance and AD server
3268	MS AD Global Catalog synchronization	MSGC	TCP/UDP	Inbound/outbound between appliance and AD server
8080	Proxy (end user web browsing)	HTTP/HTTPS	TCP	Inbound/outbound between LAN and appliance

**Table 3: Internal Connections**

Port	Function	Service	Protocol	Connection
21	Backups using passive FTP	FTP	TCP	Outbound from appliance to FTP server
22	Central configuration, status and reporting	SSH	TCP	Outbound from web appliance to management appliance (if collocated)
53	DNS queries	DNS	UDP	Outbound from appliance to LAN
80	Administrative web interface	HTTP	TCP	Inbound from LAN to appliance
88	Kerberos authentication	KERBEROS	TCP/UDP	Inbound/outbound between appliance and AD server
139	MS NetBIOS session	NETBIOS-SSN	TCP/UDP	Inbound/outbound between appliance and AD server
389	Directory services synchronization	LDAP	TCP/UDP	Inbound/outbound between appliance and AD server
443	Administrative web interface	HTTPS	TCP	Inbound from LAN to appliance
445	MS server message block	SMB	TCP/UDP	Inbound/outbound between appliance and AD server
636	LDAP synchronization	LDAPS	TCP	Inbound/outbound between appliance and eDirectory server
1024–1300, 49152–65535	Dynamic RPC	RPC	TCP	Inbound/outbound between appliance and AD server
3268	MS AD Global Catalog synchronization	MSGC	TCP/UDP	Inbound/outbound between appliance and AD server
8080	Proxy (end user web browsing)	HTTP/HTTPS	TCP	Inbound/outbound between LAN and appliance

## 2.3 Resource requirements

Use the following recommendations to estimate CPUs, memory, and disk space.

### Note

The following recommendations are guidelines only. The amount of disk space required varies between environments and is highly dependent on policies and the amount of traffic you expect your virtual appliance to process.

A virtual appliance uses 1GB of memory and 1 CPU by default. You can adjust these settings after installation, but you are advised to consider them beforehand.

If you are running VMWare ESX 4.x or VMWare ESXi 4.x/5.x, you can use the virtual appliance's installation wizard to select a profile that corresponds with the table below. Otherwise, you can change the settings in VMWare once you have installed the appliance.

Although the installation wizard allows you to select the CPU and RAM, you must adjust the disk space in VMWare. If necessary, you can increase the amount of disk space following installation. (You cannot decrease the disk space following installation.) See the VMWare documentation for details.

### Note

There is a separate set of recommendations for multiple appliances that are joined to a management appliance.

**Table 4: Recommended resources**

Maximum users	Virtual appliance profile	CPUs	Minimum RAM	Minimum disk space (stand-alone)	Minimum disk space (joined)
Single user/testing	Single user (demo)	1	1 GB	41 GB	41 GB
≤400 users per appliance	Small	2	2 GB	120 GB	41 GB
≤750 users per appliance	Medium	2	4 GB	160 GB	41 GB
≤1200 users per appliance	Large	4	8 GB	250 GB	41 GB

If you need to serve more than 1200 users, use multiple virtual appliances and administer them through a management appliance. For instance, if you have 3500 users, you could configure three "Large" virtual Web Appliances joined to a virtual management appliance.

The virtual management appliance can act as a load balancer to evenly distribute web traffic across the three virtual Web Appliances. For information about calculating disk space for a management appliance, see "Estimating Disk Space" in the [Virtual Management Appliance setup guide](#).

When you view the properties of your virtual appliance in VMWare, the larger of the two disks represents the virtual disk size of the appliance. Hard Disk 2 contains temporary installation files. You can safely delete this disk once configuration is complete.

## 2.4 Download installation files

Obtain the installation files from the Sophos website and save them on your computer.

1. Locate the email message that contains your product activation code and click the link to the downloads page on the Sophos website.

### Note

If you have opted for the 30-day trial, no activation code is required, and you can proceed directly to the downloads page.

### Note

If you are an existing customer with a MySophos account, you can log in and retrieve the files from the Downloads and Updates section.

2. On the downloads page, locate the section that matches your VMWare platform and click the links to retrieve an .ovf file, two .vmdk files, and an .mf file.

### Note

You must download all files to the same directory and preserve the file extensions.

If you are using VMWare ESX/VMWare ESXi 3.5 or VMWare Workstation 6.5 or 7.1, download a version 0.9 .ovf file.

If you are using VMWare ESX/VMWare ESXi 4.x or VMWare ESXi 5.x, download a version 1.0 .ovf file.

The .mf file contains SHA1 checksums used to verify the download contents.

## 2.5 Install a virtual appliance on VMWare ESX/VMWare ESXi

1. Log on to VMWare vSphere® or VMWare vCenter Server® and launch the import wizard.
2. Browse to the directory where you saved the installation files and click **Next**.  
Details of the virtual appliance you are about to import are displayed.
3. On the details page, click **Next**.
4. Type a name for the virtual appliance and click **Next**.
5. If prompted, select a resource pool in which to run the virtual machine and click **Next**.
6. [Version 4.x and higher] On the Deployment Configuration page, select a user profile for the virtual appliance.  
For more information, see [Resource requirements](#).
7. To accept the settings, click **Finish**.  
A message box is displayed, indicating the progress of the import.
8. When the import is complete, click **Close**.  
The virtual appliance appears in the inventory tree.

**Important**

Do not power on the virtual appliance yet.

9. Edit the VMWare power controls so that your virtual machine's "power off" option is configured to Shut Down Guest, and the "reset" option is configured to Restart Guest.
10. View the properties for your virtual appliance to confirm that the disk space, memory, and CPU settings are as desired. Or, if you are using a supported VMWare version lower than 4.x, manually adjust these settings as necessary. If prompted, ensure that sufficient space is allocated for hard disk growth.

For more information, see [Resource requirements](#).

## 2.6 Install a virtual appliance on VMWare Workstation

**Note**

VMWare Workstation is supported for testing and is not intended for use in a production environment. If you want to deploy the virtual appliance in a production environment, use VMWare ESX/VMWare ESXi.

1. In VMWare Workstation, select **File > Import or Export** to launch the conversion wizard.
2. In the conversion wizard, click **Next**.  
A list of conversion sources that includes virtual appliance (industry-standard OVF) is displayed.
3. Click **Next**.  
The Source Type page appears.
4. On the Source Type page, select Virtual Appliance and click **Next**.  
The Location page appears.
5. On the Location page, browse to the directory where you saved the installation files and click **Next**.  
Details of the virtual appliance you are about to import are displayed.
6. On the details page, click **Next**.
7. Now you are ready to choose a destination for the virtual machine. Click **Next**.
8. On the Destination Type page, select **Other Virtual Machine** and click **Next**.  
The Name and Location page appears.
9. On the Name and Location page, type a name for the virtual appliance, browse to the desired location for the installation, and click **Next**.
10. If prompted, set VM options and click **Next**.  
The Networks page appears.
11. On the Networks page, click **Next**.  
The Customization page appears, but the options are unavailable.
12. On the Customization page, click **Next**.  
The installation begins. When complete, the virtual appliance appears in the inventory tree.

**Important**

Do not power on the virtual appliance yet.

13. Edit the VMWare power controls so that your virtual machine's "power off" option is configured to Shut Down Guest, and the "reset" option is configured to Restart Guest.
14. View the properties for your virtual appliance to confirm that the disk space, memory, and CPU settings are as desired. Or, if you are using a supported VMWare version lower than 4.x, manually adjust these settings as necessary. If prompted, ensure that sufficient space is allocated for hard disk growth.

For more information, see [Resource requirements](#).

## 3 Configuring a virtual appliance

When you power on the appliance for the first time, it will initialize and then reboot to apply the settings that you configured using VMWare. After rebooting, configure network settings using the wizard provided in the console.

### 3.1 Start a virtual appliance

Power on the appliance for the first time.

1. In the VMWare inventory tree, select the virtual appliance.
2. Power on the appliance and view the VMWare console.  
The console displays a message advising you that the appliance is initializing. When initialization is successful, the console advises you that the appliance is rebooting. There will be a slight delay while the system completes these tasks.

#### Note

If you have difficulty viewing the text in the Sophos splash screen, launch a separate virtual machine console.

You can now configure network settings using the wizard in the console.

### 3.2 Configure network settings

Configure network settings using the wizard in the console.

Your virtual appliance must be powered on to configure network settings.

1. In the inventory tree, select the virtual appliance, and click the **Console** tab.

#### Tip

If you plan to create additional virtual appliances in the future, take a moment now to clone this virtual appliance before configuring.

2. Type a fully qualified domain name, and press Enter.
3. Specify DHCP settings.
  - Type `no` and press Enter. Then, specify an IP address, netmask, IP address of the default gateway, and DNS servers.

#### Note

Specifying a tertiary DNS server is optional.

- Type `yes` and press Enter. When prompted to use DHCP for subsequent settings, press Enter.
4. When prompted to apply the settings, press Enter.

In a web browser, enter the URL for the virtual appliance that is displayed in the console (https://<IPaddress>) to launch the appliance setup wizard.

Refer to the “Initial Configuration” section of the [Sophos Web Appliance configuration guide](#) and [Sophos Management Appliance configuration guide](#) for further instructions. Ignore the initial steps (they apply to hardware-based appliances only), and begin at step 4.

## 4 Cloning a virtual appliance

Cloning can be an efficient way to create additional capacity or add redundancy. For more information about cloning, see the VMWare website.

### Note

Cloning is recommended for experienced VMWare administrators only.

Sophos supports cloning virtual appliances for the following reasons:

- Cloning an appliance prior to joining a group, so that you have an unused appliance already configured should you need to add capacity on short notice.
- Removing an appliance from a group, cloning it, and re-adding it to the group.

### Re-registering a cloned appliance

Re-registering a cloned virtual appliance is necessary to take advantage of reporting and clustering features. If you do not re-register, the cloned appliance cannot be distinguished from the parent appliance (the virtual machine it was cloned from) if both are used on the same network. For example, the hostname and static IP address will be identical to that of the parent virtual appliance.

### Note

You must re-register each cloned instance before you can use it in production mode. If you are creating a clone as backup only, you do not need to re-register until you are ready to use it in production mode.

You can re-register a virtual appliance in the following ways:

- Using the command-line interface of the virtual appliance.
- Using the Re-register button on the Network Interface page of the appliance's administrative interface.

## 4.1 Clone a virtual appliance

### Important

If the appliance you plan to clone belongs to a cluster, you must remove it from the cluster before cloning. Then, after you re-register the cloned virtual appliance, you can join one or both of the appliances to the cluster.

1. Power off the virtual appliance that you want to clone.
2. Clone the virtual appliance. (See the VMWare documentation for instructions.)
3. Power on the newly cloned appliance.
4. In the VMWare inventory tree, select the cloned virtual appliance, and click the **Console** tab.
5. In the console, select **Configure Network Settings** from the **Network Configuration** menu and follow the steps in [Configure network settings](#) (page 10) to assign unique network identifiers to the cloned appliance.

**Note**

You must re-register each cloned instance before you can use it in production mode. If you are creating a clone as backup only, you do not need to re-register until you are ready to use it in production mode.

6. In the console, select Re-register from the **Configuration Options** menu.

a) Optional: Type `yes` to erase duplicate data.

Erasing duplicate data removes logs, reports, and message store data.

b) Type `yes` to re-register the virtual appliance.

The cloned appliance is re-registered and given a unique identity within your network. The new network settings are displayed in the console, and on the **Configuration > Network > Network Interface** page of the administrative interface.

7. Open a browser to the displayed IP address to complete configuration of the cloned virtual appliance.

8. Power on the virtual appliance that was used to create the clone.

9. Optional: Create a cluster using these virtual appliances, or add both to an existing cluster. For more information, see "Grouping Web Appliances" in the [Sophos Web Appliance user guide](#).

## 5 Copyrights and trademarks

Copyright 2000–2018 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

## 6.1 Glossary resource-only keys

## 7.1 Typed external resources

## 8.1 Untyped external resources

## 9.1 Conkeyref sources

## 11.1 Local key definitions

## 12.1 Untyped resources

## 13.1 DITA topics