### Contents

About Sophos Endpoint for Mac.............................................................................................................. 1
Sophos Endpoint...................................................................................................................................... 2
Status........................................................................................................................................................ 3
Events....................................................................................................................................................... 5
Settings..................................................................................................................................................... 6
Scan Info.................................................................................................................................................. 8
How to .................................................................................................................................................. 9
  Scan a File.................................................................................................................................... 9
  Scan the Mac................................................................................................................................ 9
  Change Security Settings.............................................................................................................. 9
  Clean Up a Threat........................................................................................................................ 9
  Update Now.................................................................................................................................. 10
Troubleshoot................................................................................................................................ 10
Uninstall Sophos Endpoint........................................................................................................... 10
Encrypt the computer......................................................................................................................... 10
Access the computer when you forget the password................................................................. 11
Technical support............................................................................................................................... 12

(2019/07/10)
1 About Sophos Endpoint for Mac

This Help file provides information about Sophos Endpoint for Mac and explains procedures step by step.
2 Sophos Endpoint

Sophos Endpoint runs on Macs to protect them.

Note
You may not have all the features described in this Help. This depends on your license.

Sophos Endpoint is configured and managed centrally from the Sophos Central Admin console.

However, you can do some tasks on the Mac:

- Check the Status (page 3) of the Mac.
- Scan a File (page 9) or Scan the Mac (page 9) for threats.
- See details of Events (page 5) on the Mac, such as threats detected.
- Clean Up a Threat (page 9).
- Change Security Settings (page 9). For example, you can turn off features so that you can troubleshoot.
- Update Now (page 10).
- Troubleshoot (page 10).
- Uninstall Sophos Endpoint (page 10).

Note
You need to use Admin login and enter the Tamper Protection password to clean up threats or change settings.
3 Status

Note
You may not have all the features described here. This depends on your license.

The Status page lets you:
• See the security status of the Mac.
• Scan the Mac for threats.
• See the threats that Sophos has detected and protected against.

Note
The About link in the lower right of the page lets you update or troubleshoot the product.

Security Status
An icon in the upper part of the page shows the status.

- Green. There are no alerts, or only low-priority alerts.
- Red. There are high-priority alerts.
- Yellow. There are medium-priority alerts.

Scan the Mac
Click Scan Now to scan all files on the Mac for threats.
When you start a scan, the Scan Info page is displayed so that you can see scanning progress and results. If threats are detected, you can go to the Events page to see details.

See threat details
Each tile on the Status page shows how many threats of a particular type have been detected.
If you click on a tile, you see details of the detected threats of that type on the Events page.
For more information on each type of threat, click on the links below.

Malware and PUAs
Malware is a general term for malicious software. It includes viruses, worms, Trojans and spyware.
Potentially unwanted applications (PUA) are programs that aren't malicious, such as dialers, remote administration tools and hacking tools, but are generally considered unsuitable for most business networks.

Web Threats

Web threats include malicious websites and risky downloads.
Some websites are also generally considered unsuitable for business networks, for example adult websites or social media. These can be blocked.

Controlled Items

The Controlled items category includes:
• Applications that are not a security threat, but that you decide are unsuitable for use in the office.
• Peripherals and removable media.
• Risky downloads or websites that are inappropriate for the office.
• Uncategorized websites.

Malicious Traffic

Malicious traffic is traffic between computers that indicates a possible attempt to take control of the Mac (a “command and control” attack).

Ransomware

Ransomware is malicious software that denies you access to your files until you pay a ransom.
4 Events

Note
You may not have all the features described here. This depends on your license.

The Events page shows events on the Mac, for example threats detected.

The events listed depend on how you reached this page:

• If you clicked on a tile on the Status page, you'll see only events relevant to that threat type.
• If you clicked on Events in the menu, you'll see all events logged on the Mac.

You can filter events, for example to show only events that require you to take action, or search for specific types of events.

The Events list

The Events list shows:

• The severity. An icon on the far left of the list shows whether the event is high-priority, medium priority, or a notification.
• The source. An icon on the left of the list indicates the Sophos feature that reported the event.
• The date and time when the event occurred.
• A description of the event.
• A link that lets you take action. You see this only if the event requires action and if you are logged in as an administrator.

The actions you can take are the same as those available in the Sophos Central Admin console. See the list on the “Alerts” page in Sophos Central Help.
5 Settings

Note
You may not have all the features described here. This depends on your license.

The Settings page is only available if you have entered the Tamper Protection password (available from the Sophos Central administrator).

You can temporarily change the security settings on this Mac.
You might need to do this to troubleshoot. For example, you might want to turn off a feature to see if it is causing problems on the Mac.

How to change settings

Check the box marked **Override Sophos Central Policy for up to 4 hours to troubleshoot**.
You can now make changes on this page. The changes temporarily override the policy that you (or another administrator) have applied from the Sophos Central Admin console.
After four hours, the settings will automatically change back to the centrally-enforced policy settings.

Note
You can change the settings back sooner if you want to. To change an individual setting back, use its slider control. To change all settings back, uncheck the “Override Sophos Central Policy …” box.

Real-time Scanning

Real-time scanning scans items as users attempt to access them, and denies access unless they are clean. You can select:

- **Files**. This scans local files and (if this is selected in the policy) network shares.
- **Internet**. This scans internet resources. It can scan downloads in progress, block access to malicious websites, and detect low-reputation websites.

Controls on Users

- **Peripheral Control** lets you control access to peripherals and removable media.
- **Application Control** lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office.
- **Web Control** lets you protect against risky downloads, control the sites that users can visit, and prevent data loss.
Runtime Protection

Runtime protection protects against threats by detecting suspicious or malicious behavior or traffic. You can select:

- **Ransomware Detection (CryptoGuard).** This protects against malware that restricts access to files and then demands a fee to release them.

- **Malicious Traffic Detection.** This detects traffic between a Mac and a server that indicates a possible attempt to take control of the Mac.
6 Scan Info

The Scan Info page lets you scan the computer for threats and view scan results.

Note
The Scan Info page is displayed automatically if you start a scan from the Status page.

Start or stop a scan

To start a scan, click Scan Now.
To stop a scan that is already in progress, click Stop Scan.
7 How to ...

7.1 Scan a File

To scan individual files:
In Finder, right-click on the file and select Scan Now.
A Finder Item Scan dialog is displayed so that you can see scanning progress and results.

7.2 Scan the Mac

To scan all files on the Mac:
1. Go to the Status page.
2. Click the Scan Now button.
   The Scan Info page is displayed so that you can see scanning progress and results.
3. If threats are detected, you can click Go to Events to see details.

7.3 Change Security Settings

To change security settings:
1. Click Admin login in the upper right of the interface.
2. Enter the Tamper Protection password (available from the Sophos Central administrator).
   There is now a Settings link in the menu bar.
3. Go to the Settings page.
4. Check the box marked Override Sophos Central Policy for up to 4 hours to troubleshoot.
5. Use the slider controls on the page to turn off security features.
After four hours, the settings will automatically change back to the centrally-enforced policy settings.

Note
You can change the settings back sooner if you want to. You can't use the slider controls to do this for individual features. Instead, uncheck the “Override Sophos Central Policy …” box.

7.4 Clean Up a Threat

To clean up a threat that has been detected:
1. Click Admin login and enter the Tamper Protection password (available from the Sophos Central administrator).
2. Go to the Events page to see details of the threat that has been detected.
3. Look for an action link beside the threat details.
The actions you can take are the same as those available in the Sophos Central Admin console. See the list on the "Alerts" page in Sophos Central Help.

7.5 Update Now

To update:
1. Click About in the lower right of the user interface.
2. Click Update Now.

7.6 Troubleshoot

To troubleshoot problems:
1. Click About in the lower right of the user interface.
2. Click Run Diagnostic Tool to gather data on the problem, or follow the link to the Community Forum.

7.7 Uninstall Sophos Endpoint

To uninstall the Sophos Endpoint software from a Mac, do as follows.
1. Open Launchpad.
2. Find the Remove Sophos Endpoint icon and click it.

7.8 Encrypt the computer

The Device Encryption feature encrypts the hard disk of your computer using FileVault 2 technology. When your administrator activates the Device Encryption feature, the Sophos Device Encryption dialog is displayed.

1. In the Sophos Device Encryption dialog, enter your login password and click Encrypt. This enables Sophos Device Encryption. Alternatively, click Postpone to start the process later.
2. Your recovery key is automatically stored in Sophos Central.
3. Click Restart when prompted to restart your computer.

Important
Do not restart your computer until the restart notification is displayed. If you restart your computer without the recovery key safely stored and you forget your login password, you cannot access your computer. Recovery is not possible in this case.

When the system disk is encrypted, the internal data volumes are automatically encrypted. Encrypted disks are automatically unlocked when the computer starts. Removable data volumes such as USB drives are not encrypted.
7.9 Access the computer when you forget the password

If you cannot log on to your computer because you have forgotten your login password, you need a recovery key.

If you are using Sophos Device Encryption, the recovery key is stored in Sophos Central. To get your recovery key, do one of the following:

• Log on to the Sophos Self Service Portal and follow the instructions in the Help.
• Ask your administrator to retrieve the recovery key for you, as described in Use FileVault recovery (page 11). Do this if you cannot use the Self Service Portal.

7.9.1 Use FileVault recovery

1. Restart your computer and wait until the Recovery key ID is displayed. The Recovery key ID is displayed for a short time. To display it again, you must restart the computer.
2. Contact your administrator and give them the Recovery key ID. Your administrator needs to find the recovery key to your computer in Sophos Central and give you the key.
3. Click the question mark icon in the Password field. A message is displayed.
4. Click the arrow icon next to the message to switch to the recovery key field.
5. Enter the recovery key.
6. Follow the on-screen instructions to create a new password. If your user account was imported from Active Directory, click Cancel in the Reset Password dialog and ask your administrator to reset the password for you.
7. If prompted, click Create New Keychain.

You can access your computer again.
8 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.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.