SOPHOS

Cybersecurity made simple.

Sophos Endpoint for Mac

Help

Contents

1 Sophos Endpoint

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.

The tasks that can be done on the Mac are as follows:

- Check the Status (page 2) of the Mac.
- Scan a file (page 8) or Scan the Mac (page 8) for threats.
- See details of Events (page 3) on the Mac, such as threats detected.
- Clean up a threat (page 8).
- Change security settings (page 8). For example, you can turn off features so that you can troubleshoot.
- Update now (page 9).
- Troubleshoot (page 9).

Note
You need to use **Admin Login** and enter the tamper protection password to clean up threats or change settings.

2 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 installed features and their security status.

Note
The **About** link lets you update your virus definitions 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.

 Gray. The status is unknown.

Below this, all installed features are shown with their individual security status.

Scan the Mac

Click **Scan Now** to scan all files on the Mac for threats.

Note
If a threat is detected, **Scan Now** is not available. You can click **View Details** instead for more information about the threat.

When the scan is complete, you see a summary of the scan results. If threats are detected, you can click **View Details** or **Events** for more details.

3 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.

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 shows whether the event is high-priority, medium-priority, or a notification.
- The source. An icon 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 (if any action is needed). You only see this if you have signed in as an administrator.

To view details of an event, click its entry in the list.

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.

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. You can block these.

Controlled Items

This 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.

- Files containing sensitive information (like personal or financial details) that you don't want to leak.

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 Detections

You can scan the Mac for threats, and see the threats that Sophos has detected and protected against.

Scan the computer

Click **Scan Now** to scan all files on the Mac for threats.

When the scan is complete, you'll see a summary of the scan results. If threats are detected, you can go to the **Events** page to see details.

Malware and PUA Event History

Shows the history of detected malware and PUAs. Click the arrow to see details on the **Events** page.

Detection History

Shows how many threats of a specific type have been detected. Click on a type to see details of the detected threats of that type on the **Events** page.

Reset Summary

Click **Reset Summary** to set the history counters shown in the **Detections** page to zero.

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 use **Admin Login** and enter 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

Turn on **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 automatically change back to the centrally-enforced policy settings.

Note
You can change the settings back sooner if you want to. You can't do this for individual features. You must turn off **Override Sophos Central Policy for up to 4 hours to troubleshoot**, which applies to all the features.

Real-time Scanning

Real-time scanning scans items as users attempt to access them, and grants access only if 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**. This lets you control access to peripherals and removable media.
- **Application Control**. This 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**. This 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 on Macs. You can select:

- **Malicious Traffic Detection**. This detects traffic between a Mac and a server that indicates a possible attempt to take control of the Mac.
- **Ransomware Detection (CryptoGuard)**. This protects against malware that restricts access to files and then demands a fee to release them.

6 How to ...

6.1 Scan a file

To scan individual files:

In Finder, right-click the file and select **Scan with Sophos Endpoint**.

A **Finder Item Scan** dialog is shown so that you can see scanning progress and results.

6.2 Scan the Mac

To scan all files on the Mac:

1. Go to the **Status** page or the **Detections** page.
2. Click **Scan Now**.
   When the scan is complete, you'll see a summary of the scan results.
3. If threats are detected, you can go to the **Events** page to see details.

6.3 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).
   The **Settings** link in the menu bar is now active.
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.

6.4 Change security settings

To change security settings:

1. Click **Admin Login** and enter the tamper protection password (available from the Sophos Central administrator).
   The **Settings** link in the menu bar is now active.
2. Go to the **Settings** page.
3. Turn on **Override Sophos Central Policy for up to 4 hours to troubleshoot**.
4. Use the controls on the page to turn security features off or on.

After four hours, the settings automatically change back to the centrally-enforced policy settings.

Note
You can change the settings back sooner if you want to. You can't do this for individual features. You must turn off **Override Sophos Central Policy for up to 4 hours to troubleshoot** which applies to all the features.

6.5 Update now

To update:

1. Click **About**.
2. Click **Update Now**.

6.6 Troubleshoot

To troubleshoot problems:

1. Click **About**.
2. Click **Run Diagnostic Tool** to gather data on the problem.

You can also click **Community Forum** for more information.

6.7 Encrypt the Mac

The device encryption feature encrypts the Mac's hard disk using FileVault 2 technology. When your administrator activates the **Device Encryption** feature, the **Sophos Device Encryption** dialog is shown.

1. In the **Sophos Device Encryption** dialog, enter your login password and click **Encrypt**. This turns on device encryption. Alternatively, click **Postpone** to start the process later.
2. Your recovery key is automatically stored in Sophos Central.

When the system disk is encrypted, the internal data volumes are automatically encrypted. Encrypted disks are automatically unlocked when the Mac starts. Removable data volumes such as USB drives are not encrypted.

6.8 Access your Mac if you forget the password

If you cannot log on to your Mac 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 Sophos Central help.
- Ask your administrator to retrieve the recovery key for you, as described in Use FileVault recovery (page 10). Do this if you cannot use the Self Service Portal.

6.8.1 Use FileVault recovery

To get an administrator to retrieve a recovery key for you, follow these steps.

1. Restart your Mac and wait until the **Recovery key ID** is shown.
   The **Recovery key ID** is shown for a short time. To show it again, you must restart your Mac.
2. Contact your administrator and give them the **Recovery key ID**.
   Your administrator needs to find the recovery key for your Mac in Sophos Central and give you the key.
3. Click the question mark in the **Password** field.
   A message is shown.
4. Click the arrow 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 Mac again.

7 Why is my file transfer blocked?

You might see a message telling you that a file transfer (for example, copying, moving or emailing files) has been blocked.

This happens because your company has set up a policy to ensure that you don't unintentionally send sensitive information to users who should not have it.

There are two types of message.

Transfer is blocked

If you receive a "file transfer blocked" message, you cannot transfer the files. Your administrator may have added some advice to this message.

Transfer can be allowed

If you receive a "file transfer request blocked" message, you can decide whether to transfer the files. Your administrator may have added some advice to this message. Click **Allow** if you're sure it's safe to go ahead.

8 Get additional help

You can find technical support as follows:

- 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.

9 Legal notices