1 About Sophos Endpoint for Windows

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

Sophos Endpoint runs on computers and servers 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 computer or server:

- Check the Status (page 3) of the computer.
- Scan a File (page 9) or Scan the Computer or Server (page 9) for threats.
- See details of Events (page 6) on the computer or server, 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).

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 computer or server.
- Scan the computer or server 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.
- Gray. The status is unknown.

Encryption status

If you only have the encryption product, you see this icon and the encryption status (enabled or disabled).

If you have encryption and other features, you can see the encryption status in the lower left of the page.

Important
Device Encryption is only available on endpoint computers.

Scan the computer

Click Scan to scan all files on the computer or server 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.

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, uncategorized 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.

Malicious Behavior

**Malicious behavior** is suspicious behavior detected in software that is already running on the computer or server.

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

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.
- 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 computer or server (a “command and control” attack).
Exploits

Exploits that Sophos can prevent include application hijacking and exploits that take advantage of vulnerabilities in browsers, browser plug-ins, Java applications, media applications and Microsoft Office applications.
4 Events

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

The Events page shows events on the computer or server, 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 computer or server.

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 (if any action is needed). This is shown only if you have 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 computer or server. 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 computer.

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. You can’t use the slider controls to do this for individual features. Instead, uncheck Override Sophos Central Policy for up to 4 hours to troubleshoot.

Deep learning

Deep learning uses advanced machine learning to detect threats. It can identify malware and potentially unwanted applications without using signatures.

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.
Sophos Endpoint for Windows

- **Web Control** lets you protect against risky downloads, control the sites that users can visit, and prevent data loss.
- **Data Loss Prevention** lets you monitor and restrict the transfer of files containing sensitive data.
- **Tamper Protection**. When this is enabled, a local administrator cannot change security settings or uninstall Sophos Endpoint unless they have the necessary password.

**Runtime Protection**

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

- **Ransomware Detection**: This protects against malware that restricts access to files, and then demands a fee to release them.
- **Safe Browsing**: This protects your web browsers against exploitation by malware.
- **Exploit Mitigation**: This protects the applications most prone to exploitation by malware, such as Java applications.
- **Network Threat Protection**: This detects traffic between an endpoint computer and a server that indicates a possible attempt to take control of the endpoint computer. It includes packet inspection, which scans network communications, identifying and blocking threats before they can harm the operating system or applications.

**Note**

If you turn off **Network Threat Protection**, the EDR features, Isolation and Stonewalling, will also be turned off.

- **Malicious Behavior Detection (HIPS)**: This protects against threats that are not yet known. It does this by detecting and blocking behavior that is known to be malicious or is suspicious.

**Computer controls**

You can monitor Windows Firewall (and other registered firewalls) on your computers and servers.
6 How to ...

6.1 Scan a File

To scan individual files:
In Explorer, right-click on the file and select Scan.

6.2 Scan the Computer or Server

To scan all files on the computer or server:
1. Go to the Status page.
2. Click the Scan button.
   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).
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 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.
6.5 Update Now

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

6.6 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.

6.7 Encrypt the computer

**Important**
Device Encryption is only available on endpoint computers.

The Device Encryption feature encrypts the hard disk of your computer using Windows BitLocker technology. Your administrator defines whether you need to authenticate each time you access your computer.

If no authentication is required, the encryption of your hard disk starts automatically as soon as you restart your computer after you received the Sophos Central policy. There is nothing you need to do in this case.

If authentication is required, encrypt the computer as follows:

1. When the **Sophos Device Encryption** dialog is displayed, follow the instructions in the dialog. The specific instructions depend on your system and the policy settings defined by your administrator.
   - If the Device Encryption policy requires a PIN or password for authentication, follow the on-screen instructions to define a PIN or password.

**Note**
Be careful when setting a PIN or password. The pre-boot environment only supports the US-English keyboard layout. If you set a PIN or password now with special characters, you might have to use different keys when you enter it to log on later.
• If the Device Encryption policy requires a USB key for authentication, you need to connect a USB flash drive to your computer. The USB flash drive must be formatted with NTFS, FAT, or FAT32.

2. When you click **Restart and Encrypt**, the computer restarts and encrypts your hard disks. You can work as usual.

   **Note**
   You can select **Do this later** to close the dialog. However, it will appear again next time you log on.

After Sophos Central has encrypted the system volume, the encryption of the data volumes is started. Removable data volumes such as USB drives are not encrypted. When you log on to your computer, you may need a PIN, password, or USB key to unlock your system volume. Data volumes are unlocked automatically.

### 6.8 Access the computer when you forget the password

If you cannot log on to your computer because you have forgotten your PIN, password, or USB key, 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 BitLocker recovery** (page 11). Do this if you cannot use the Self Service Portal.

### 6.8.1 Use BitLocker recovery

1. Restart your computer and press the **Esc** key in the **BitLocker** logon screen.

2. In the **BitLocker recovery** screen, find the **Recovery key ID**. The **Recovery key ID** is displayed for a short time. To display it again, you must restart the computer.

3. 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.

4. In the **BitLocker recovery** screen, enter the recovery key.
   You can now start your computer.

5. Follow the on-screen instructions to create a new BitLocker PIN or password when prompted.
   On computers running Windows 7, you don't see any instructions. You need to reset your PIN/password manually.

   You can access your computer again.
Note
A recovery key can only be used once. If you need to recover your computer again later, you need to get a new recovery key.
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 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.
9 Legal notices

Copyright © 2020 Sophos Limited. All rights reserved. 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.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.