Cybersecurity made simple.

Sophos Central Admin help
# Contents

About this Help.................................................................................................................................................................1
Activate Your License...............................................................................................................................................................2
Overview.................................................................................................................................................................................3
Dashboard..................................................................................................................................................................................3
Alerts.........................................................................................................................................................................................4
Threat Analysis Center...............................................................................................................................................................18
Logs & Reports.............................................................................................................................................................................34
People.......................................................................................................................................................................................55
Devices.....................................................................................................................................................................................66
Global Settings..........................................................................................................................................................................88
Protect Devices........................................................................................................................................................................160
Endpoint Protection.....................................................................................................................................................................175
Dashboard..................................................................................................................................................................................175
Logs & Reports............................................................................................................................................................................176
People.......................................................................................................................................................................................179
Computers.................................................................................................................................................................................190
Computer Groups.................................................................................................................................................................199
Policies.......................................................................................................................................................................................200
Settings.....................................................................................................................................................................................224
Protect Devices...........................................................................................................................................................................259
Encryption..................................................................................................................................................................................269
Dashboard..................................................................................................................................................................................269
Logs & Reports............................................................................................................................................................................269
People.......................................................................................................................................................................................271
Computers.................................................................................................................................................................................282
Unmanaged computers............................................................................................................................................................291
Computer Groups.................................................................................................................................................................291
Policies.......................................................................................................................................................................................292
Settings.....................................................................................................................................................................................298
Protect Devices...........................................................................................................................................................................314
Server Protection.......................................................................................................................................................................316
Dashboard..................................................................................................................................................................................316
Logs & Reports............................................................................................................................................................................316
Servers......................................................................................................................................................................................319
Servers on AWS........................................................................................................................................................................329
Policies.......................................................................................................................................................................................332
Settings.....................................................................................................................................................................................361
Protect Devices...........................................................................................................................................................................395
Wireless.....................................................................................................................................................................................400
Wireless Dashboard.................................................................................................................................................................400
Wireless Alerts............................................................................................................................................................................402
Devices.......................................................................................................................................................................................403
Usage Insight..............................................................................................................................................................................403
Wireless Diagnostics.............................................................................................................................................................404
Access points............................................................................................................................................................................411
SSIDs.........................................................................................................................................................................................416
Sites.........................................................................................................................................................................................428
Settings.....................................................................................................................................................................................430
Email Gateway...........................................................................................................................................................................432
Add mailboxes to Email Gateway........................................................................................................................................432
Domains Settings/Status...........................................................................................................................................................433
Policies and Settings.................................................................................................................................................................434

(2020/06/19)
1 About this Help

This Help tells you how to use all the features in Sophos Central.
If you can't find the help you need here, go to the Support section of our website and search there. This finds knowledge base articles or discussions in the Sophos Community.

**Tip**
Not using Sophos Central yet? Sign in [here](#) and we’ll help you get started.

You can sign in with your Microsoft sign-in details if your administrator has set this up. Click [Sign In with Microsoft](#) and enter your Microsoft sign-in details.
2 Activate Your License

When you buy a new license, you need to activate it.

You do this in Sophos Central (unless a Sophos Partner handles license activation for you).

When you buy an upgrade, it may be activated automatically or you may need to activate it.

Note

If you are starting a trial of Sophos Central, you don’t need to activate a license yet. You do this only when you upgrade to a paid license.

To activate a license, do as follows.

1. Ensure you have the license key shown in the License Schedule that Sophos sent you.
2. Look for your account name in the upper right of the user interface. Click the name and select Licensing.
3. Now use your license key.
   - If you see Apply Activation Code, enter your key and click Apply.
   - If you see an Apply License Key link, click it. Enter your key and click Apply.
4. If your account already has licenses for the features included on the key, you see another dialog. This lets you choose how to use your new licenses.
   - **Renew** starts the new licenses when your current licenses expire.
   - **Change** starts the new licenses now. We’ll adjust the license term so that all your licenses expire on the same date.

Click Apply again.

How the "Change" option works

A customer orders 50 licenses for one year. Six months later, they place another order for 50 licenses for one year.

If the customer selects Change, we do as follows:

- Add the new licenses to the older ones. The customer now has 100 licenses.
- Add the remaining time on the older licenses (50 licenses x 6 months = 300) to the time on the new licenses (50 licenses x 12 months = 600). The total is 900 months.
- Distribute the time over all 100 licenses. Each user’s license now runs for 9 months from the date when the key was applied (and the expiry date is adjusted accordingly).

The customer now has 100 licenses that will all expire 9 months from now.

In most cases the existing license expiry date gets extended but do check the new expiry date shown.
3 Overview

The main menu lists the functions available to you in Sophos Central. These are listed under their product names, for example Endpoint Protection. There is also an Overview that amalgamates the functions for all of your licensed products.

3.1 Dashboard

The Dashboard is the start page of Sophos Central and lets you see the most important information at a glance. It consists of these areas.

Most Recent Alerts

Most Recent Alerts shows the latest few alerts. Informational alerts are for information only and don’t require you to take action.

Click View All Alerts to see all alerts.

Devices and users: summary

Devices and users: summary shows details of usage and protection for users or protected devices. It also shows the number of unprotected users or devices.

Click on the tabs to see information for each device type or for users.

Click See Report to open a detailed report for the tab you have selected.

Email Security

Inbound shows information about the following message categories:

- **Legitimate**: Messages that are classified as clean, and therefore delivered.
- **DLP policy violations**: Messages that violated Data Loss Prevention policies.
- **Spam**: Messages classified as spam.
- **Advanced threat**: Messages classified as containing advanced threats.
- **Virus**: Messages classified as containing viruses.
- **Authentication failure**: Messages that failed authentication checks by DMARC, SPF or DKIM.
- **Realtime blocklist**: Messages detected due to a blacklisted sending IP.
- **Company blocklist**: Messages sent from an address that has already been added to the company blocklist (inbound allow/block).

Outbound shows the total number of outbound email messages scanned by Email Security for your protected mailboxes for the last 30 days. It also shows the number of legitimate messages processed, the number of spam and virus messages detected and the number of messages violating DLP policies.
Click **See Report** to open the **Message Summary** report and review the details of the processed messages, see [Message Summary Report](#).

**Web control**

**Web control** shows statistics for your Web Control protection.

The figures are for threats blocked, policy violations blocked, and policy warnings. There is also a figure for "policy warnings proceeded", which is the number of users who have bypassed a warning to visit a website.

Click on a figure to open a detailed report.

**Web Gateway Blocked Summary**

**Web Gateway Blocked Summary** shows statistics for your Web Gateway protection (you see this only if you have a Web Gateway license).

The figures are for malware blocked and websites blocked.

Click on a figure to open a detailed report.

**Related concepts**

[Message Summary Report](#) (page 52)

The **Message Summary** report details the email messages processed by **Email Gateway** for your protected mailboxes.

### 3.2 Alerts

The **Alerts** page lists all the alerts that require your action.

**Restriction**

Some features might not be available for all customers yet.

Alerts that are resolved automatically are not shown. To view all events, go to **Logs & Reports > Events**.

**Note**

The alert event time is not updated if the same event occurs repeatedly.

On the **Alerts** page, you can do as follows:

- Group alerts.
- Filter alerts.
- Take action against alerts.
- Change the frequency of email alerts.

For information about the different types of alerts, see the other Help pages in this section.
Note
If you have Intercept X Advanced with EDR you can investigate, block and clean up threats from Threat Cases.

Group alerts
You can group together all alerts for a specific threat or event under a single entry in the list. This makes alerts easier to manage.
Enable Group (upper right of the page).
To see the number of alerts for each group entry, look in the Count column.
To display all the alerts in a group, click the fold-out arrow on the right.

Filter alerts
To view alerts with a specific priority, click the figures for High Alerts, Medium Alerts or Low Alerts at the top of the page.
To view alerts for a specific product or threat type, use the drop-down filters above the alerts list.

Take action against alerts
You can take action against alerts.
To take action against an individual alert, click the drop-down arrow next to an alert to open its details. In Actions, click an action link (if available).
If you’re viewing groups of alerts, click an action button (if available) next to the group in the list.

Note
If you want to allow an application that Sophos deep learning reports as malware, you do it from the Events page, not here.

The following actions are available for alerts, depending on the alert type.
• Mark As Acknowledged: Click this to remove an alert from the list. The alert will not be displayed again.
  This does not resolve threats and does not remove threat details from the quarantine manager on the computer or server.
• Mark As Resolved: Click this if the threat has already been resolved on the endpoint computer or server. This action clears the alert from the list in Sophos Central and also clears threat details from the quarantine manager on the computer or server.
  This action does not resolve threats.
  This action is only available for Windows endpoint computers or servers.
• Clean Up: Click this to remove ransomware from a server.
• Reinstall Endpoint Protection: Click this to go to the Protect Devices page, where you can download the Sophos agent software.
- **Contact Support**: Click this to get additional help. This action becomes available when you might need help, for example when malware cleanup fails.

- **Clean Up PUA**: Click this to clean up a Potentially Unwanted Application (PUA) that has been detected.
  
  This action is available only for computers.
  
  This action might not be available if the PUA has been detected in a network share. This is because the Sophos Endpoint Protection agent does not have sufficient rights to clean up files there. For more information on dealing with PUAs.

- **Authorize PUA**: Click this to authorize a Potentially Unwanted Application (PUA) to run on all computers. You might do this if you consider the application useful.
  
  This action is available only for computers.

### Change the frequency of email alerts

You can change the frequency with which an alert type is sent.

Click the drop-down arrow next to an alert to open its details. In **Email Alert**, select the frequency for sending this type of alert.

This setting will be added to the **Exceptions** in your email alert settings. You can also edit the setting there.

### Related concepts

- **How to deal with threats** (page 11)
- **Threat Cases** (page 19)
- **Allowed applications** (page 130)
- **Alerts for Threat Protection** (page 6)
- **Alerts for Installation, Updating and Compliance** (page 10)
- **Events Report** (page 35)
- **Configure email alerts** (page 123)

You can manage how admins receive email alerts.

### 3.2.1 Alerts for Threat Protection

There are the following types of threat protection alerts.

For information about a threat and advice on how to deal with it, click its name in the alert.

Alternatively, go to the **Threat Analysis** page on the Sophos website. Under **Browse threat analyses**, click the link for the type of threat, and then do a search for the threat or look in the list of latest items.

You might also see malware detections shown in the Events list as ML/PE-A.
Real-time protection has been disabled for a computer for more than 2.5 hours. Real-time protection should be turned on at all times. Sophos Support may advise you to turn it off for a short period of time in order to carry out an investigation.

**Malware not cleaned up**

Some detected malware could not be removed after a period of 24 hours, even if automatic cleanup is available. The malware was probably detected via a scan that does not provide automatic cleanup, e.g., an on-demand scan configured locally. You can deal with the malware in one of these ways:

- Clean it up centrally, by scheduling a scan in the policy (which will then have automatic cleanup enabled).
- Clean it up locally, via the Quarantine Manager.

**Manual cleanup required**

Some detected malware could not be removed automatically because automatic cleanup is not available. Click on the “Description” in the alert to go to the Sophos website, where you can read advice on how to remove the threat. If you need help, contact Sophos Support.

**Running malware not cleaned up**

A program that was running on a computer and exhibited malicious or suspicious behavior could not be cleaned up. Click on the “Description” in the alert to learn more about the threat and how to deal with it. If you need help, contact Sophos Support.

**Malicious traffic detected**

Malicious network traffic, possibly headed to a command-and-control server involved in a botnet or other malware attack, has been detected. Click on the “Description” in the alert to learn more about the threat and how to deal with it. If you need help, contact Sophos Support.

**Recurring infection**

A computer has become reinfected after Sophos Central attempted to remove the threat. It may be because the threat has hidden components that haven't been detected. An in-depth analysis of the threat may be required. Please contact Sophos Support for assistance.

**Ransomware detected**

We have detected ransomware and blocked its access to the file-system. If the computer is a workstation, we clean up the ransomware automatically. You need to do as follows:

- If you still need to clean up: Move the computer temporarily to a network where it is not a risk to other computers. Go to the computer and run Sophos Clean (if it isn’t installed, download it from our website).

  You can run Sophos Clean on a server from Sophos Central. See Alerts.

- If automatic sample submission isn't enabled, send us a sample of the ransomware. We'll classify it and update our rules: if it's malicious, Sophos Central will block it in future.

- Go to Sophos Central, go to Alerts, and mark the alert as resolved.

**Ransomware attacking a remote machine detected**

We have detected that this computer is trying to encrypt files on other computers.

We have blocked the computer’s write access to the network shares. If the computer is a workstation, and Protect document files from ransomware (CryptoGuard) is enabled, we clean up the ransomware automatically.

You need to do as follows:

- Make sure that Protect document files from ransomware (CryptoGuard) is enabled in the Sophos Central policy. This provides more information.
If cleanup doesn’t happen automatically: Move the computer to a network where it is not a risk to other computers. Then go to the computer and run Sophos Clean (if it isn't installed, download it from our website).

- Go to Sophos Central, go to Alerts, and mark the alert as resolved.

### Medium

**Potentially Unwanted Application (PUA) detected**

Some software has been detected that might be adware or other potentially unwanted software. By default, potentially unwanted applications are blocked. You can either authorize it, if you consider it useful, or clean it up.

**Authorize PUAs**

You can authorize a PUA in one of two ways, depending on whether you want to authorize it on all computers or only some:

- On the Alerts page, select the alert and click the Authorize PUA button in the upper right of the page. This authorizes the PUA on all computers.
- Add the PUA to the scanning exclusions in the malware protection policy. This authorizes the PUA only on computers to which the policy applies.

**Clean up PUAs**

You can clean a PUA up in one of two ways:

- On the Alerts page, select the alert and click the Cleanup PUA(s) button in the upper right of the page.
- Clean it up in the agent software's Quarantine Manager on the affected computer.

**Note**

Cleanup might not be available if the PUA has been detected in a network share. This is because the Sophos agent does not have sufficient rights to clean up files there.

**Potentially unwanted application not cleaned up**

Potentially unwanted application could not be removed. Manual cleanup may be required. Click on the “Description” in the alert to learn more about the application and how to deal with it. If you need help, contact Sophos Support.

**Computer scan required to complete cleanup**

A threat cleanup requires a full computer scan. To scan a computer, go to the Computers page, click on the name of the computer to open its details page, and then click the Scan now button.

The scan may take some time. When complete, you can see a "Scan 'Scan my computer' completed" event and any successful cleanup events on the Logs & Reports > Events page. You can see alerts about unsuccessful cleanup on the Alerts page.

If the computer is offline, it will be scanned when it is back online. If a computer scan is already running, the new scan request will be ignored and the earlier scan will carry on.

Alternatively, you can run the scan locally using the Sophos agent software on the affected computer. Use the Scan option in Sophos Endpoint on a Windows computer, or the Scan This Mac option in Sophos Anti-Virus on a Mac.

**Reboot required to complete cleanup**
The threat has been partially removed, but the endpoint computer needs to be restarted to complete the cleanup.

**Remotely-run ransomware detected**

We detected ransomware running on a remote computer and trying to encrypt files on network shares.

We have blocked write access to the network shares from the remote computer's IP address. If the computer with that address is a workstation managed by Sophos Central, and Protect document files from ransomware (CryptoGuard) is enabled, we clean up the ransomware automatically.

You need to do as follows:

- Find the computer where the ransomware is running.
- If the computer is managed by Sophos Central, make sure that Protect document files from ransomware (CryptoGuard) is enabled in the policy.
- If cleanup doesn’t happen automatically: Move the computer to a network where it is not a risk to other computers. Then go to the computer and run Sophos Clean (if it isn’t installed, download it from our website).
- Go to Sophos Central, go to Alerts, and mark the alert as resolved.

**Related concepts**

- Alerts (page 4)
  The Alerts page lists all the alerts that require your action.

**Related information**

- Threat Analysis
- ML/PE-A detection explained

### 3.2.2 Alerts for Device Encryption

There are the following types of alerts for Device Encryption:

**Medium**

- **Device is not encrypted**
  A volume is not encrypted even though it is supposed to be encrypted. A possible reason is that the user postponed encryption when the policy was applied.

- **Recovery key is missing**
  A recovery key for an encrypted volume cannot be found in the Sophos Central database.

- **Device Encryption is suspended**
  If you did not suspend Device Encryption, possible reasons are:
  - The recovery key is not yet stored in Sophos Central. Make sure that the endpoint has an internet connection.
  - Pre-provisioned BitLocker is not yet activated. Users need to define a PIN, password, or USB key to activate BitLocker.
  - Windows updates are being installed. BitLocker will automatically be un-suspended after the next restart.
3.2.3 Alerts for Installation, Updating and Compliance

There are the following types of alerts for issues that affect installation of Sophos agents, updating of Sophos agents, or policy compliance:

High

Failed to protect computer or server
A computer has started installation of the agent software but has not become protected for one hour. The installer that has been run on the affected computer may provide more information about the reason of the failure.

Medium

Computer or server out of date
A computer that has not been updated in the last 24 hours has been communicating with Sophos Central in the last 6 hours, and did not update in the following 2 hours. Normally, a computer will attempt to update about 5 minutes after it has been started, and then regularly every 60 minutes. If re-applying the policy fails repeatedly, it may be due to a more serious problem. In those cases, re-installation may solve the problem.

Reboot required
The reboot of a computer is needed to complete an update of the agent software, but the computer has not been restarted for 2 weeks. Sometimes, after installing/updating the agent software, a restart is needed to fully enable the capabilities of the new/updated version of the software. Although an update does not need to be performed immediately, it is advisable to perform it as soon as possible.

Policy non-compliance
A device may not comply with a policy for various reasons, for example because the settings have been changed on the device itself. In that case, after two hours of non-compliance, the system will raise an alert and will try to re-apply the corresponding policy. When the device is back in compliance, the alert will be automatically cleared. If re-applying fails repeatedly, it may be due to a more serious problem. In those cases, re-installation may solve the problem.

Peripheral detected
A removable media or peripheral device has been detected on a device monitored by Sophos Central.

Duplicate device detection
A duplicate device has been detected. If devices have been cloned from an image they have the same ID. Duplicate IDs can cause management issues. Duplicate devices are re-registered with a new ID.

Notes:
- Computers running Windows XP/Vista or Server 2003/2008 are not detected as duplicates. However, if they have the same ID as the one running a supported OS (e.g. Windows 10), they are detected as duplicates but not re-registered.
- Any Windows servers with the server lockdown product installed and locked are not re-registered if they are detected as duplicates.
• We don't support duplicate device detection on VDI style environments such as VMware Horizon or Citrix PVS or Citrix MCS.

Related information
Duplicate device detection

3.2.4 Wireless Alerts

View access point generated wireless alerts.

High

Access Point has bad health: The load on the access point is too high. There are too many devices connected. Check you have enough access points to cover the area.

Medium

Access Point is offline: The access point has no internet connection, no power, or has experienced a software error. You can try restarting. Restarts can resolve software errors.

Access Point is not broadcasting any network: The access point isn't configured. To configure the access point click Wireless > Access Points.

Access Point command done: The restart is complete.

Restarting the access point may resolve the following alerts:

• Access Point configuration failed
• Access Points failed to update to the new firmware

If the problem continues, contact Sophos Support. They will need remote access to investigate the issue. Go to Wireless > Settings > Diagnostics > Remote Login to Access Points for Sophos Support to allow remote access.

Low

Access Point will be updated with new firmware: Wireless will be turned off for approximately 5 minutes.

All Access Points will be updated with new firmware: Wireless will be turned off for approximately 5 minutes.

Access Point has been successfully updated with new firmware

All Access Points have been successfully updated

3.2.5 How to deal with threats

For advice on dealing with threats, see:

• Deal with ransomware.
• Deal with exploits.
• Deal with web browser attacks.
• Deal with malware detected by deep learning.
• Deal with application lockdown events.
• Deal with false positives.

For advice on malware, see the sections on malware alerts listed in Alerts for Threat Protection.

Related concepts
Alerts (page 4)
The Alerts page lists all the alerts that require your action.
Deal with ransomware (page 12)
Deal with exploits (page 13)
Deal with web browser attacks (page 14)
Deal with malware detected by deep learning (page 14)
Deal with application lockdown events (page 15)
Deal with false positives (page 16)
Alerts for Threat Protection (page 6)

Deal with ransomware

This is what happens when we detect ransomware and what to do about it.
If you know a detection is a false positive, see Deal with false positives.

What happens when we detect ransomware

When we detect ransomware:
• We check whether it's a legitimate application like a file/folder encryption product. If it isn't, we stop it running.
• Files are restored to their pre-modification state.
• The end user is notified.
• A threat case is generated. This helps you decide whether to take additional actions.
• A scan starts to identify and clean up any other malware on the device.
• The device's health state returns to Green.

What to do if you see “Ransomware detected”

If you still need to clean up, do as follows:
• If automatic sample submission isn't enabled, send us a sample of the ransomware. We'll classify it and update our rules: if it's malicious, Sophos Central will block it in future.
• Move the computer temporarily to a network where it is not a risk to other computers. Go to the computer and run Sophos Clean (if it isn't installed, download it from our website).
  You can run Sophos Clean on a server from Sophos Central.
• Go to Sophos Central, go to Alerts, and mark the alert as resolved.
What to do if you see "**Remotely-run ransomware detected**"

We detected ransomware running on a remote computer and trying to encrypt files on network shares.

We have blocked write access to the network shares from the remote computer’s IP address. If the computer with that address is a workstation managed by Sophos Central, and **Protect document files from ransomware (CryptoGuard)** is enabled, we clean up the ransomware automatically.

You need to do as follows:

- Find the computer where the ransomware is running.
- If the computer is managed by Sophos Central, make sure that **Protect document files from ransomware (CryptoGuard)** is enabled in the policy.
- If cleanup doesn’t happen automatically: Move the computer to a network where it is not a risk to other computers. Then go to the computer and run Sophos Clean (if it isn’t installed, download it from our website).
- Go to Sophos Central, go to **Alerts**, and mark the alert as resolved.

What to do if you see "**Ransomware attacking a remote machine detected**"

We have detected that this computer is trying to encrypt files on other computers.

We have blocked the computer’s write access to the network shares. If the computer is a workstation, and **Protect document files from ransomware (CryptoGuard)** is enabled, we clean up the ransomware automatically.

You need to do as follows:

- Make sure that **Protect document files from ransomware (CryptoGuard)** is enabled in the Sophos Central policy. This provides more information.
- If cleanup doesn’t happen automatically: Move the computer to a network where it is not a risk to other computers. Then go to the computer and run Sophos Clean (if it isn't installed, download it from our website).
- Go to Sophos Central, go to **Alerts**, and mark the alert as resolved.

**Related concepts**
- [Deal with false positives](#)
- [Alerts](#)

**Related information**
- [How to submit samples of suspicious files to Sophos](#)

**Deal with exploits**

This topic tells you what to do about exploits.

If you know a detection is a false positive, see [Deal with false positives](#).
What happens when an exploit is detected

When an exploit is detected, the following things happen:

- The exploit is stopped.
- The user is notified.
- A scan starts to clean up threats.
- A threat case is generated.

What you should do

Go to **Threat Analysis Center > Threat Cases** and review the case details to find out where the attack started, how it spread, and which processes or files it affected.

Often a user has downloaded or authorized an application that gave an attacker access. To avoid this, give users training in safe browsing.

**Related concepts**

[Deal with false positives](page 16)

Deal with web browser attacks

What happens when we detect a web browser threat

When an attack is detected:

- Intercept X warns the user to close the browser.
- A Sophos Clean scan starts.
- A threat case is generated.

What you should do

You should do as follows:

- Use the threat case to identify the IP and URL connection associated with the attack.
- Decide whether to block that location in the corporate firewall. (If the attack wasn’t detected by your web protection, it isn’t classified as malicious.)
- If the user entered a password, tell them to change it.
- If the user was contacting their bank, tell them to check there’s been no unusual activity on their account.

Deal with malware detected by deep learning

Deep learning uses advanced machine learning to detect malware or PUAs without using signatures. Malware that’s detected by deep learning is shown in alerts with an “ML/” prefix.
PE files (applications, libraries, system files) that have been detected are quarantined. You can restore and allow them if they’re safe.

What happens when we detect malware

When deep learning identifies a file as malicious, these steps are taken:

- We check whether the file has been added to an allowed applications list. (This list lets you exclude a file from checking if it's been incorrectly detected as malware.)
- If the file is not on an allowed list, it’s reported as malware and put into quarantine.
- A threat case is generated.
- The computer’s security health is shown as green because the malware is quarantined.

What you should do

As the malware has been quarantined, you don’t usually need to take any action.

However, deep learning can occasionally report a legitimate file as malware (a false positive). If you’re sure that the file is safe, you can restore it and allow your users to use it again.

To restore and allow a file, follow the steps in Allowed applications.

Related concepts

Allowed applications (page 130)

Deal with application lockdown events

The application lockdown feature stops attacks that abuse legitimate features in commonly-used applications to perform an attack or launch malware.

What happens when we detect an attack

When an application under lockdown does something prohibited, such as installing other software or changing system settings, these steps are taken:

- Intercept X automatically closes the application.
- The user is notified.
- A Sophos Clean scan starts. This can identify other potential malware components.
- A threat case is generated.

What you should do

You should do as follows:

- Use the threat case to identify the file or activity that is the cause of the attack.
- Confirm that no other action is required.
Deal with false positives

Our software can detect threats that are previously unknown. However, it may sometimes identify an application as malware or report an exploit, even though you know the application’s safe. This is a “false positive”.

When a false positive happens, you can prevent the software from detecting the threat again and (if applicable) restore files that have been removed.

Related concepts
Stop detecting an application (page 16)
Stop detecting an exploit (page 16)
Stop detecting ransomware (page 17)

Stop detecting an application

If PE (Portable Executable) files, like applications, libraries and system files, are detected, they are quarantined and can be restored.

To allow an application that Sophos has detected and removed, do as follows.

• This allows the application for all computers and users.
• This allows the application to start, but we’ll still check it for threats, exploits and malicious behavior when it’s running.

1. Go to the Computers or Servers page, depending on where the application was detected.
2. Find the computer where the detection happened and click on it to view its details.
3. On the Events tab, find the detection event and click Details.
4. In the Event details dialog, look under Allow this application.
5. Select the method of allowing the application:
   • Certificate: This is recommended. It also allows other applications with the same certificate.
   • SHA-256: This allows this version of the application. However, if the application is updated, it could be detected again.
   • Path: This allows the application as long as it’s installed in the path (location) shown. You can edit the path (now or later) and you can use variables if the application is installed in different locations on different computers.
6. Click Allow.

Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again.

This will apply to all your users and computers.

Note
These instructions assume you use options available in your events list. Alternatively, you can use policy settings or global settings. See the other sections on this page.

1. Go to the Computers or Servers page, depending on where the application was detected.
2. Find the computer where the detection happened and click on it to view its details.
3. On the Events tab, find the detection event and click Details.
4. In Event details, look for Don’t detect this again and select an option:
• Exclude this Detection ID from checking prevents this detection on this app.

• Exclude this application from checking prevents any checks for exploits on this app.

Try excluding the Detection ID first as that is better targeted. If the same detection happens again, exclude the application next time.

5. Click Exclude.

We’ll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting an exploit (using policy settings)

You can stop detecting an exploit for the application where it was detected.

If you use this method, we’ll continue to check for other exploits that affect this application.

1. In Policies, find the Threat Detection Policy that applies to the computers.

2. Under Scanning Exclusions, click Add Exclusion.

3. In the Exclusion Type drop-down list, select Detected Exploit.

4. Select the exploit and click Add.

You can also use a policy to stop detecting exploits for all applications of a certain type. To do this, go to the threat protection policy and turn off exploit mitigation (which is under "Runtime protection") for that application type.

Note
We don't recommend turning off exploit mitigation.

Stop detecting exploits (using global settings)

You can stop detecting all exploits for an application.

If you use this method, we won’t check the application for exploits, but will still check it for ransomware behavior and for malware.

1. Go to Global settings > Exploit mitigation exclusions.

2. Click Add Exclusion.

3. In the dialog that opens, select an Application.

4. Click Add.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again.

This will apply to all your users and computers.

1. Go to the Computers or Servers page, depending on where the application was detected.

2. Find the computer where the detection happened and click on it to view its details.

3. On the Events tab, find the detection event and click Details.

4. In Event details, look for Don’t detect this again.

   Select Exclude this Detection ID from checking. This prevents this detection on this app.
5. Click **Exclude**.
   We'll add your exclusion to the Global Exclusions list.

### 3.3 Threat Analysis Center

The Dashboard lets you see the most important information at a glance.
It consists of these areas.

#### Most recent threat cases

Threat cases let you investigate malware attacks. Click on a case to find out where an attack started, how it spread, and which processes or files it has affected.

Click **See all threat cases** to see all threat cases.

Threat cases are available only for Windows devices.

If you have an MTR license, the area is split into tabs for threat cases that have been generated as follows:
- Automatically generated by Sophos
- Generated by a Sophos Central admin
- Generated by the Sophos Managed Threat Response (MTR) team (unused at present)

#### Threat search

This option is available if you have Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server.

Search for potential threats on your network.

You can search for SHA-256 file hashes, file names, IP addresses or domains (either complete or partial), or command lines. Typically, you get this search information from other security products or threat notification services.

Threat searches find the following:
- Portable executable files (like applications, libraries, system files) with an uncertain or bad reputation.
- IP addresses or domains that those files have connected to.
- Admin tools that have been run. These tools can be misused.

**Note**
You can also run a threat search from within a threat case. That finds more examples of the potential threats identified in that case.

**Note**
Searches for command lines and admin tools may not be available for all customers yet.
Recent threat searches

This option is available if you have Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server.

This shows threat searches that you have run and saved recently. Click on a search to re-run it, find affected devices and take action.

Click **See all searches** to see all the searches.

Top threat indicators

Threat indicators are suspicious files that Sophos hasn’t blocked but that you may want to investigate.

The top threat indicators list shows you the most prevalent threat indicators, with these details:

- **Suspicion** level. This is the probability that the file is malicious.
- The number of devices affected.

To see the full list and do further analysis, click **See all threat indicators**.

3.3.1 Threat Cases

Threat cases let you investigate and clean up malware attacks.

You can find out where an attack started, how it spread, and which processes or files it has affected. This helps you improve security.

This feature is available only to customers with an Intercept X or Intercept X Advanced with EDR license. If you have an Intercept X Advanced with EDR or Intercept X Advanced for Server with EDR license, you can also do the following:

- Isolate affected devices.
- Search for more examples of the threat on your network.
- Clean up and block the threat.
- Obtain further advanced threat intelligence.

We create a threat case for you whenever we detect malware that you need to investigate further.

**Note**
This is currently only available for Windows devices.

How to investigate and clean up threats

This is an overview of how you might typically investigate a case. For details of all options, see Threat case analysis page.

Some options are only available if you have an Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server license.

1. Click **Threat Cases** in the main menu and then click on a case.
This displays the case details page.

2. Look at **Summary** to see where the attack started and which files might be affected.

3. Look at **Suggested next steps**. You can change the priority for the case and see which processes to investigate.
   
   If this is a high priority case, and you have Intercept X Advanced with EDR, you can click **Isolate this device**. This isolates the affected device from the network. You can still manage the device from Sophos Central.

   **Note**
   
   You don't see this option if the device has isolated itself automatically.

4. On the **Analyze** tab, you can see a diagram showing the progress of the attack. Clicking items shows more details.

5. Click the root cause or another process to show its details.

6. To make sure you have the latest analysis from Sophos, click **Request latest intelligence**.
   
   This sends files to Sophos for analysis. If we have new information about the file's reputation and prevalence, you'll see it here in a few minutes.

   **Restriction**
   
   If you have Intercept X Advanced with EDR or Intercept X Advanced for Server with EDR, you'll see more advanced analysis, see Process details. You can also do further detection and cleanup, as shown in the steps that follow.

7. Click **Search for item** to search for more examples of the file on your network.
   
   If the **Item Search Results** page shows any more examples of the file, you can click **Isolate device** there to isolate affected devices.

8. Return to the threat case details page and look at the latest threat intelligence.

9. If you're confident that the file is malicious, you can click **Clean and block**.
   
   This cleans up the item on devices where it's been found and blocks it on all devices.

10. If you're confident that you've dealt with the threat, you can remove the device from isolation (if necessary). Go to **Suggested next steps** and click **Remove from isolation**.

    If you isolated multiple devices, go to **Settings > Admin Isolated Devices** and remove them from isolation.

11. Go back to the **Detected Threat Cases** list, select the case and click **Close**.

**About the threat cases list**

The **Detected Threat Cases** page lists all threat cases for the past 90 days.

If you have an MTR license, the page is split into tabs for threat cases that have been generated as follows:

- Automatically generated by Sophos
- Generated by a Sophos Central admin
- Generated by the Sophos Managed Threat Response (MTR) team (unused at present)
If you do not have an MTR license, the page is not split into tabs.

You can filter the cases by **Device**, **Status**, or **Priority**.

You can use **Search** to view the cases for a certain user, device, or threat name (for example, "Troj/Agent-AJWL").

For each case, the list shows most of the following information. Which columns are shown depends on whether the page is split into tabs:

- **Status**: The status is **New** by default. You can change it when you view the case.
- **Time created**: Time and date when the case was created.
- **Priority**: A priority is set when the case is created. You can change it when you view the case.
- **Name**: Click the threat name to view the details of the case.
- **Generated by**: The Sophos Central admin who generated the threat case.
- **User**: The user that caused the infection. Click the username to view the user's details.
- **Device**: The device that caused the infection. Click the device name to see its details.
- **Device type**: The type of the device, for example **Computer** or **Server**.

You can click any column to sort the cases.

**Related concepts**

- **Alerts** (page 4)
  The **Alerts** page lists all the alerts that require your action.

- **Threat Case analysis page** (page 21)
  You can investigate a threat case by going to its details page and using the analysis tools there.

- **Threat Protection Policy** (page 203)
  Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

**Threat Case analysis page**

You can investigate a threat case by going to its details page and using the analysis tools there.

Find the threat case on the **Detected Threat Cases** page. Click its name to see a simplified event chain, summary, details of the artifacts (processes, files, keys) affected, and a diagram showing how the threat developed. The following screenshot shows an HPmal/Eicar-A detection triggered by downloading a file `sophos_hips_test.exe` from a website using Internet Explorer 11:
For an overview of what to do, see How to investigate and clean up threats.

For more details of all the options, read the sections on this page.

Note
The options you see may depend on your license and on the severity of the threat.

Summary

The Summary shows you a summary of the threat, including these details:

• **Root cause**: Where the infection entered your system.
• **Possible data involved**: Files that might contain important data. Check them to see if data has been encrypted or stolen.
• **Where**: Name of the device and its user.
• **When**: Detection time and date.

Suggested next steps

The Suggested next steps pane shows you the following:

**Priority**: A priority is set automatically. You can change it.

**Status**: The status is **New** by default. You can change it.

Note
Once you set the status to **In progress** you cannot reset it to **New**.
**Isolate this device**: You see this if the case is high priority and if you have Intercept X Advanced with EDR or Intercept X Advanced for Server with EDR. It enables you to isolate the device while you investigate potential threats.

You can still manage the device from Sophos Central. You can also still submit files from the isolated device to Sophos for analysis.

You can also allow isolated devices to communicate with other devices in limited circumstances. For more information, see Device isolation exclusions (Windows).

You can remove the device from isolation at any time. You'll see a **Remove from isolation** option under **Suggested next steps**.

**Note**

You don't see **Isolate this device** if the device has already isolated itself automatically. See the **Device Isolation** option in Threat Protection Policy.

**Scan the device**: You can use this link to scan the affected device for threats.

**Analyze**

The **Analyze** tab shows the chain of events in the malware infection.

A menu on the right of the tab lets you choose how much detail you see:

- **Show direct path**: This shows the chain of directly-involved items between the root cause and the item where the infection was detected (the “beacon”).

- **Show full graph**: This shows the root cause, beacon, affected artifacts (applications, files, keys), the path of the infection (shown by arrows), and how the infection occurred. This is the default setting.

To display or hide the different types of artifact, use the checkboxes above the diagram.

To see details of an item, click it. This opens a details pane on the right of the diagram.

**Case record**

The **Case record** tab shows the history of the threat case, from its creation by Sophos or the admin. You can post comments to record actions that have been taken and other relevant information.

**Process details**

When you click an affected item, you see the **Process details** pane. If someone has already submitted the file to Sophos, you see the latest threat intelligence.

If the file hasn't been submitted, or you want to see if there's any updated intelligence, click **Request latest intelligence**.

This shows the latest information about the file's global reputation and whether you need to investigate.
Artifacts list

This is a list below the diagram of the malware attack. It shows all the affected items, for example business files, processes, registry keys, or IP addresses.

You can export a comma separated (CSV) file containing a list of the affected artifacts, by clicking on Export to CSV at the top right of the tab.

The list shows:

- **Name**: Click the name to see more information in a details pane.
- **Type**: The type of artifact, such as a business file or a registry key.
- **Reputation**
- **Time logged**: The time and date a process was accessed.
- **Interactions**

Create forensic snapshot

You can create a "forensic snapshot" of data from the device. This gets data from a Sophos log of the device's activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

You'll need a converter (which we provide) to read the data.

**Note**

You can choose how much data you want in snapshots and where to upload them. To do this, go to Global Settings > Forensic Snapshots. These options may not be available for all customers yet.

To create a snapshot:

1. Go to a threat case's Analyze tab.
   Alternatively, on the details page of the device, open the Status tab.
2. Click Create forensic snapshot.
3. Follow the steps in Upload a forensic snapshot to an AWS S3 bucket.

You can find the snapshots you generated in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Forensic Snapshots\.
Snapsots generated from detections are in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Saved Data\.

**Note**

You need to be an administrator with access to the tamper protection password and run a command prompt as an administrator to access the saved snapshots.

**Related concepts**

Threat Cases (page 19)
Threat cases let you investigate and clean up malware attacks.

**Threat Protection Policy** (page 203)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

**Threat Searches** (page 31)
You can search for potential threats on your network.

**Admin Isolated Devices** (page 137)
**Forensic snapshots** (page 138)
Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

**Related tasks**
**Convert a forensic snapshot** (page 139)
Use the SDR Exporter tool to convert forensic snapshots so you can run queries on them.

**Related reference**
**Device isolation exclusions (Windows)** (page 117)
You can allow isolated devices to have limited communications with other devices.

**Related information**
**Upload a forensic snapshot to an AWS S3 bucket** (page 140)
Follow these instructions to upload a forensic snapshot.

**Process details**

When you click an affected file in a threat case, the **Process details** pane shows the latest details of the file.

These include the global reputation of the file, path, name, command line, process ID, executing user, SHA256, start and end time, and duration. The following screenshot shows the details of a process associated with Internet Explorer 11:
Request latest intelligence

If the file has not been submitted to Sophos for additional analysis, you see the text **No current intelligence on this file**. If the file hasn’t been submitted, or you want to see if there’s any updated intelligence, click **Request latest intelligence**. This sends a request to the computer to upload the file to SophosLabs.

When the file has been analyzed, you see the latest information about the file’s global reputation and whether you need to investigate.

The reputation score shows the trustworthiness of the file. Sophos scores the reputation on a scale from red (bad) to green (good). Known clean files are shown in the green range of the scale and known malicious files are shown in the red range.
The reputation score goes up or down for many reasons, including when and how many times the file was seen by Sophos and the static/behavioral properties of the file. When the file is seen for the first time, it may get a score in the orange range (unknown) because it is a new file. After Sophos has analyzed it, the score may move to the known bad or known good range.

If you have Intercept X Advanced with EDR or Intercept X Advanced for Server with EDR, you also see more information and options, as follows.

Report summary

Under Report summary, you can see the file's reputation and prevalence and the results of our machine learning analysis, which indicate how suspicious the file is.

**Prevalence** indicates how often SophosLabs has seen the file.

**First seen** is when SophosLabs first saw the file in the wild.

**Last seen** is when SophosLabs last saw the file in the wild.

**Machine learning analysis** summarizes how suspicious the file is.

Machine learning analysis

Under Machine learning analysis, you can see full results of our analysis.

**Attributes** shows a comparison of the file's attributes with those in millions of known bad and known good files. This enables you to determine how suspicious each attribute is and therefore whether the file is likely to be good or bad. You may see the following attributes:

- **Imports** describes the functionality that the file uses from external DLLs.
- **Strings** describes the most significant strings in the file.
- **Compilers** specifies what was used to compile the source code, for example C++, Delphi, Visual Basic, .NET.
- **Mitigation** describes techniques that the file uses to avoid being exploited.
- **Resources** specifies a resource that seems to be compressed or encrypted.
- **Summary** often relates to build or compilation dates, for example.
- **Packer** often specifies something of note about a specific section of the file, for example a suspicious section name or the fact that a section is both writable and executable.
- **Peid** refers to the output of PEiD, a third-party tool that scans a PE file against various malware signatures.
- **Btcaddress** shows any valid Bitcoin address that is found in the file.
- **Findcrypt** shows any suspicious cryptographic constants.

**Code similarity** shows a comparison of the file with millions of known bad and known good files, and lists the closest matches. Other matches count toward the result and may affect the rating for the file. The more bad files the file matches and the more closely it matches them, the more suspicious the file is.

**File/path** shows a comparison of the file's path with that of millions of known bad and known good files. If the file's path more closely matches the path of known bad files, the file is more likely to be suspicious. The path and file name used for comparison are either yours (if you requested the latest intelligence) or those from the last customer who sent us a file. We hide sensitive information in other customers’ paths.
File properties

Under File properties, you can see key information about the file itself, for example product, type, copyright information, version, company name, size, and timestamp.

File breakdown

**PE file sections** shows information about each section of the file, for example code, data, or resources. Section names may indicate specific packers, compilers, or functionality, for example. Malware can make itself obvious by including strings that include expletives, slang, and so on.

There is also information about the size of the sections, on disk and in memory. Sometimes, a section is very small or very big, and sometimes only on disk or in memory. You can see the entropy of the section, and whether it's readable, writable, or executable. All of this helps you to determine whether a section is packed, contains data, contains code, or is unusual.

For more information about file sections, see Section Table (Section Headers).

**PE imports** shows which DLLs the file uses and, if you expand each one, which APIs are imported from them. You can see DLLs used for network activity or APIs that may help with password extraction. The DLL names may be really common. Alternatively, they may be unusual enough that an internet search indicates that they're suspicious or malicious, and therefore that the file importing from them is too. For more information about PE imports, see Import Library Format.

You may also see **PE exports**, which shows what code the file makes available for other files to use. This may appear to be harmless or obviously bad. For more information about PE exports, see The .edata Section (Image Only).

Search

Click **Search** to find more examples of the file on your network.

You can also perform searches from the Threat Searches page or from the Threat search pane in the Dashboard.

Clean and block

If the file is suspicious, you can use **Clean and block**.

This cleans up the file (and associated files and keys) on any device it's already on. It also adds it to a blocked list so that it can't run on other devices. You can see blocked items under **Global Settings > Blocked Items**.

Related information

Section Table (Section Headers)
Import Library Format
The .edata Section (Image Only)
3.3.2 Live Discover

Live Discover enables you to check the devices that Sophos Central is managing, to look for signs of a threat, or to assess compliance.

Introduction

Restriction
This feature is available only if you have joined the early access program.

You can use Live Discover in two ways:

- **Proactively:** You can search devices for signs of threats that haven’t been detected by other Sophos features. Such signs may be unusual changes to the registry, failed authentications, or a process running that is very rarely run. You can also check the compliance of each device. For example, you can check for out-of-date software or whether browsers are using secure settings.

- **Reactively:** You can search devices for signs of a suspected or known threat. For example, Sophos Central has alerted you or a user has reported suspicious behavior on their device.

We provide a range of queries for you to use to check your devices. You can use them as they are or you can edit them to modify their behavior. You can also create your own queries.

Live Discover shows the results for each query that you run. It also shows telemetry data that shows how successful it has been in retrieving the results. You can export the results and telemetry data.

To start, select which devices to query.

Related information
OSQuery reference

Select devices to query

You need to select the computers and servers that Live Discover should query.

1. In Live Discover, to expand Device selector, click the arrow.
   
   **Available devices** shows all the computers and servers that are managed by Sophos Central. **Selected devices** shows the subset of available devices that you have selected to query.

2. Under Available devices, click Show filters to filter the devices that are shown. Click Apply.
   
   Text that you enter in the filter boxes is not case-sensitive and does not have to be an exact match.

3. Select the devices that you want to query and click Update selected devices list.

4. Under Selected devices, if you want to refine the list further, do one or both of the following:
   
   - Click Show filters. Filter the selected devices.
   - Deselect devices and click Update selected devices list.

The devices that are selected under Selected devices are those that Live Discover will query.
Select query

You can select a pre-prepared query that Live Discover will run.

If you want to create a new query, see Edit or create query instead.

1. In Live Discover, click the arrow to expand Query.
   A list of query categories is shown, containing queries that have been written by Sophos.
2. Click the category that you want to use.
   The list of queries in that category is displayed. Performance indicates the average effect the query had on each device’s performance based on the most recent usage. For example, a query that runs quickly and generates little data has little impact and is rated Excellent.
3. If there are a lot of queries in that category, at the top of the list of queries, filter or search the queries if you want to shorten the list.
4. Click the query that you want to run.
   The query is shown, including the supported operating systems, performance data, and the Osquery code for the query.

When you have selected a query, you can run it. If you want to edit it first, see Edit or create query.

Edit or create query

You can edit a query that you’ve selected to modify its behavior, if you want to, or you can create a new one.

The query is written in Osquery, which uses basic Structured Query Language (SQL) commands. You must be familiar with Osquery or SQL to edit the query.

1. In Live Discover, with Query expanded, do one of the following:
   - To edit a query, ensure that you have selected it. Then click Edit.
   - To create a query, ensure that you are looking at the list of query categories. Then click Create new query.
2. Enter a new name for the query.
3. Enter the category in which the query will be listed, the description, and the operating systems on which it can run.
4. In the SQL box, enter the changes that you want to make to the existing query or enter the new query.
   A query must contain at least 15 characters in order to run on the selected devices.
   For information about the tables and data available, see OSQuery reference.
5. You can add a variable to the query and assign a value to it. You can then use the value in a conditional statement, for example. To do this, do as follows:
   a) Ensure that the variable editor is expanded.
   b) Click + Add variable.
   c) Enter a name for the variable. As you type, SQL variable name is automatically filled in.
      You may include spaces in the name but not dollar symbols.
   d) Specify the variable type and the value that you want to use when the query is run.
   e) In the SQL box, enter the SQL variable name, including the dollar symbols, where you want to use the variable.
For example, if you enter `File path` for the variable name, **SQL variable name** becomes `$File path$`. So, enter `$File path$` in the **SQL** box:

```sql
SELECT * FROM processes
WHERE filepath = '$File path$
```

6. Click **Save**.

The query is saved to the category that you specified.

When you finish editing or creating the query, you can run it.

**Run query**

Run the query that you’ve selected or created on the devices that you’ve selected.

In Live Discover, with **Query** expanded, click **Run query**.

The query results are shown below the query panel. These are the items that the query has discovered on each device. You have the option to export the results to a CSV file.

The telemetry is shown below the query results. This is the data about how successful the query was in getting information from each device, for example how long it took to get the information from each device.

When the query stops running, the full query results and telemetry data are available. You can click a device name in either list to view the device’s details page.

You can change the selected devices or edit the query while it is running if you want to.

**Telemetry**

Under **Device Telemetry**, you can see data about how successful the Live Discover query was in getting information from each device.

You can use **Progress** to select which telemetry status types to show. The status indicates whether the query has completed and whether the device sent data back.

The device list includes the following columns:

- **Performance**: This indicates what effect the query had on the device’s performance. For example, a query that runs quickly and generates little data has little impact and is rated **Excellent**.
- **Data XFR**: The amount of data that the query generated.

To export the content of the list to a CSV file, click **Export**.

### 3.3.3 Threat Searches

You can search for potential threats on your network.

This option is available if you have Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server.

You can search for SHA-256 file hashes, file names, IP addresses or domains (either complete or partial), or command lines. Typically, you get this search information from other security products or threat notification services.

Threat searches find the following:

- Portable executable files (like applications, libraries, system files) with an uncertain or bad reputation.
• IP addresses or domains that those files have connected to.
• Admin tools that have been run. These tools can be misused.

Note
You can also run a threat search from within a threat case. That finds more examples of the potential threats identified in that case.

Note
Searches for command lines and admin tools may not be available for all customers yet.

You can save threat searches. Re-running searches let you check whether potential threats have spread to more devices.

New threat search
To find potential threats:
1. In New threat search enter SHA-256 file hashes, file names, IP addresses or domains (either complete or partial), or command lines.
2. Click Search.
3. Review the results on the Threat Search Results page. You can also take action there to isolate devices and clean up threats.
4. Select the search and click Save search if you want to re-run it later.

Saved searches
Re-running saved threat searches lets you do as follows:
• See if potential threats have spread to more devices.
• Check the latest status of the threats on each device.
To re-run a search, click it in the Saved searches list.

Related concepts
Threat Case analysis page (page 21)
You can investigate a threat case by going to its details page and using the analysis tools there.
Threat Search Results (page 32)
When you run a threat search, you'll see a list of devices where the search has detected suspicious files or threats.

Threat Search Results
When you run a threat search, you'll see a list of devices where the search has detected suspicious files or threats.

Threat searches are only available if you have Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server.
Click See details next to a device. This opens a page where you can see the history of each item.
On the details page, you can also take these actions (depending on the item detected):
- Isolate the device.
- Clean up and block applications.
- Generate a new threat case (if required) or view an existing case.

Alternatively, if you have several affected devices, you can isolate them all at once on the main results page.

**Latest status**

The **Latest status** column shows these events for suspicious files:

- **Discovered**: The search discovered the file but didn't detect a threat in it.
- **Detected**: The search detected a threat in the file.
- **Added**: The file was added to the device.
- **Executed**: The file was run.
- **Reputation Updated**: Sophos updated the file's reputation level or a Sophos Central admin allowed or blocked the file (which updates its "local" reputation).
- **Path Updated**: The file was moved.
- **Removed**: The file was removed from the device.

**Note**

Different details are shown for network connections and admin tools.

**Isolate the device**

To isolate the device, select it and click **Isolate**.

You can allow isolated devices to communicate with other devices in limited circumstances. You can do this in the endpoint and server threat protection policies.

**Clean up and block**

To review, clean up and block a threat:

1. Click **See details**.
2. Review the details of the threat.
   
   To deal with a suspicious application:
   a) If the device is not already isolated, click **Isolate**.
   b) To clean up and block the application, click **Actions > Clean and block**.
      
      This cleans up the suspicious application on devices where it's been found and blocks it on all devices.

   **Note**
   
   You can also clean up and block applications by adding them to the **Blocked Items** list.
You can remove devices from isolation after you have investigated and taken action.

**Related concepts**
- Blocked items (page 132)
- Admin Isolated Devices (page 137)

### 3.3.4 Threat Indicators

Threat indicators highlight suspicious files that Sophos hasn't blocked but that you may want to investigate.

You can review threat indicators and take action as follows:

1. Go to **Overview > Threat Analysis Center > Threat Indicators**.
2. On the **Suspicious items** tab, you see a list of files. This shows:
   - **Suspicion** level: The probability that the file is malicious.
   - **Executed**: Whether the file has been executed.
   - **Devices affected**: The number of devices where the file has been seen.
3. For more details of a file, click **View details** (on the right of the table). You can also:
   - Click the file’s **SHA 256** hash to search for more instances of the file on your network.
   - Click **Generate threat case** to do a more in-depth analysis of the file history.
4. In the details pane, to make sure you have the latest analysis from Sophos, click **Request latest intelligence**.
   This sends the file to Sophos for analysis. If we have new information about the file’s reputation and prevalence, you’ll see it here in a few minutes.
5. When you have finished your analysis, you can take action.
   - If a file is believed to be malicious, click **Clean and block**.
   - If you don't believe the file is malicious and don't want to take further action, click **Dismiss**. The file will no longer show in the threat indicators list.

**Clean and block** prevents the suspicious applications from being accessed or run on your devices. The file is added to the **Blocked Items** list (in your Global Settings).

Actions you’ve taken are shown on the **Actions taken** tab.

**Related concepts**
- Threat Searches (page 31)
You can search for potential threats on your network.
- Threat Cases (page 19)
Threat cases let you investigate and clean up malware attacks.

### 3.4 Logs & Reports

The **Logs & Reports** page lists the reports that you can generate about security features in Sophos Central.

The page also lists any **Saved Reports**. These are custom reports that you or other administrators for this account have saved.

To find out more about logs, see **Logs**.
To find out how reports work and how you can customize, save and schedule them, see Reports.

Related concepts
Logs (page 35)
Reports (page 51)

3.4.1 Logs

The logs that you can see depend on your license.

The following logs are available:

Events. All events on your devices, see Events Report.

Malware and PUAs blocked. A simplified version of the Events log. It shows the malware and potentially unwanted applications (PUAs) that we have detected and blocked.

Audit Logs. A record of all activities that are monitored by Sophos Central. Access to this log is dependent on your administrator role, see Audit Logs.

Data Loss Prevention. All events triggered by data loss prevention rules for computers or servers, see Data Loss Prevention Events Log.

Message History. The email messages processed by Email Security for your protected mailboxes, see Message History Report.

Gateway Activity Logs. All the network activity logs associated with your Web Gateway protection, see Gateway Activity.

Related concepts
Events Report (page 35)
Audit Logs (page 47)

You can view and export a record of all activities that are monitored by Sophos Central using the Audit Log report.

Data Loss Prevention Events Log (page 48)
Message History Report (page 49)

The Message History report details the emails processed by Email Gateway for your protected mailboxes.

Gateway Activity (page 50)

Events Report

The Events Report page provides information about all events on your devices.

Events that require you to take action are also shown on the Alerts page, where you can deal with them.

Some events cause alerts as soon as they happen. Others are promoted to alerts later (for example, if a computer is non-compliant with policy for two hours).

For information about the different types of event, see Event types.

For advice on what to do about threats, see How to deal with threats.

Malware and PUAs blocked. A simplified version of the Events log. It shows the malware and potentially unwanted applications (PUAs) that we have detected and blocked.
Configure the events report

You can use the following options to configure the report:

**Search**: If you want to view events for a certain user, device, or threat name (for example, “Troj/Agent-AJW”), enter the name of the user, device, or threat in the search box.

**Note**
In this version of Sophos Central, you cannot search events for a file name, for example, an executable file mentioned in the event.

**Choose period**: Use the box to select the time period for which you want to view events. If you select **Custom**, use the **From** and **To** fields to select the dates between which you want to view events. You can view events that occurred in the past 90 days or less.

**Event type and count**: The table on the left of the page displays the count for each type of event over the specified time range. It also allows you to display only certain categories or types of event. You do this by selecting or clearing the checkboxes next to the event type categories, or by expanding the categories and selecting or clearing the checkboxes next to the event types. By default, all events are displayed.

**Update**: Click this to display any new events reported since the page was last opened or refreshed.

**Graph**: The graph shows you at a glance the number of events that occurred per day.

The events list

The events list provides these event details:

- **Sev**: Severity of the event
- **Date**: Time and date when the event occurred
- **Event**: Type of event
- **User**: Source that caused the event, for example, the name of a user or system
- **User Groups**: Group that the user is a member of
- **Device**: Device that caused the event
- **Device Group**: Group that the device is a member of

**Save as Custom Report** lets you save the report settings in the **Saved Reports** table on the **Logs & Reports** page.

The **Export** menu (on the right of the table) lets you export the current view or the report for the past 90 days as a CSV (comma separated value) or PDF file.

**Related concepts**
**Event types** (page 36)

**Event types**

Depending on the features included in your license, you may see all or some of the following event types:

Events that require you to take action are also shown on the **Alerts** page, where you can deal with them.
After you have taken an action or ignored the alert, it is no longer displayed on the Alerts page, but the event remains in the Events list.

## Runtime Detections

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running malware detected</td>
<td>Medium</td>
<td>No</td>
<td>A program that was running on a computer and exhibited malicious or suspicious behavior has been detected. Sophos Central will attempt to remove the threat. If it succeeds, no alerts will be displayed on the Alerts page, and a Running malware cleaned up event will be added to the events list.</td>
</tr>
<tr>
<td>Running malware not cleaned up</td>
<td>High</td>
<td>Yes</td>
<td>A program that was running on a computer and exhibited malicious or suspicious behavior could not be cleaned up. The following events may be displayed for this event type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Running malware requires manual cleanup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Computer scan required to complete running malware cleanup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Reboot required to complete running malware cleanup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Running malware not cleaned up.</td>
</tr>
<tr>
<td>Running malware cleaned up</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Event type</td>
<td>Severity</td>
<td>Action required?</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malicious activity detected</td>
<td>High</td>
<td>Yes</td>
<td>Malicious network traffic, possibly headed to a command-and-control server involved in a botnet or other malware attack, has been detected.</td>
</tr>
<tr>
<td>Running malware locally cleared</td>
<td>Low</td>
<td>No</td>
<td>A running malware alert has been cleared from the alerts list on an endpoint computer.</td>
</tr>
<tr>
<td>Ransomware detected</td>
<td>High</td>
<td>No</td>
<td>An unauthorized program attempted to encrypt a protected application.</td>
</tr>
<tr>
<td>Ransomware attack resolved</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Remotely-run ransomware detected</td>
<td>Medium</td>
<td>Yes</td>
<td>An unauthorized program attempted to remotely encrypt a protected application.</td>
</tr>
<tr>
<td>Remotely-run ransomware attack resolved</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Ransomware attacking a remote machine</td>
<td>High</td>
<td>Yes</td>
<td>This computer has been detected attempting to remotely encrypt applications on another computer.</td>
</tr>
<tr>
<td>Safe Browsing detected compromised browser</td>
<td>Medium</td>
<td>Yes</td>
<td>An attempt to exploit a vulnerability in an internet browser has been blocked.</td>
</tr>
<tr>
<td>Exploit prevented</td>
<td>Low</td>
<td>No</td>
<td>An attempt to exploit a vulnerability in an application, on an endpoint computer, has been blocked.</td>
</tr>
<tr>
<td>Application hijacking prevented</td>
<td>Low</td>
<td>No</td>
<td>Application hijacking was prevented on an endpoint computer.</td>
</tr>
</tbody>
</table>
### Behavioral

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral</td>
<td>Low</td>
<td>Yes</td>
<td>This application has been detected behaving suspiciously. In some instances a reboot is required to complete the cleanup process. A reboot event is shown if this happens. This type of detection is only available if you are signed up to the Early Access Program.</td>
</tr>
</tbody>
</table>

### Application Control

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application blocked</td>
<td>Medium</td>
<td>No</td>
<td>A controlled application has been detected and then allowed.</td>
</tr>
<tr>
<td>Application allowed</td>
<td>Low</td>
<td>No</td>
<td>A controlled application has been detected and then allowed.</td>
</tr>
</tbody>
</table>

### Malware

If you have deep learning enabled, you may see malware detections shown as ML/PE-A.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware detected</td>
<td>Medium</td>
<td>No</td>
<td>Malware has been detected on a device monitored by Sophos Central. Sophos Central will attempt to remove the threat. If successful, no alerts will be displayed on the Alerts page, and a &quot;Malware cleaned up&quot; event will appear on the events list.</td>
</tr>
<tr>
<td>Event type</td>
<td>Severity</td>
<td>Action required?</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malware not cleaned up</td>
<td>High</td>
<td>Yes</td>
<td>The following events may be displayed for this event type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Manual cleanup required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Computer scan required to complete cleanup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Reboot required to complete cleanup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Malware not cleaned up.</td>
</tr>
<tr>
<td>Malware cleaned up</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Recurring infection</td>
<td>High</td>
<td>Yes</td>
<td>A computer has become reinfected after Sophos Central attempted to remove</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the threat. It may be because the threat has hidden components that</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>haven't been detected.</td>
</tr>
<tr>
<td>Threat removed</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Malware locally cleared</td>
<td>Low</td>
<td>No</td>
<td>A malware alert has been cleared from the alerts list on an endpoint</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>computer.</td>
</tr>
</tbody>
</table>

**Potentially Unwanted Application (PUA)**

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentially Unwanted Application (PUA) blocked</td>
<td>Medium</td>
<td>Yes</td>
<td>A potentially unwanted application has been detected and blocked.</td>
</tr>
</tbody>
</table>
### Event type

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentially Unwanted Application (PUA) not cleaned up</td>
<td>Medium</td>
<td>Yes</td>
<td>The following events may be displayed for this event type:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Manual PUA cleanup required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Computer scan required to complete PUA cleanup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Reboot required to complete PUA cleanup.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• PUA not cleaned up.</td>
</tr>
<tr>
<td>Potentially Unwanted Application (PUA) cleaned up</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Potentially Unwanted Application (PUA) locally cleared</td>
<td>Low</td>
<td>No</td>
<td>A potentially unwanted application alert has been cleared from the alerts list on an endpoint computer.</td>
</tr>
</tbody>
</table>

### Policy Violations

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy non-compliance</td>
<td>Medium</td>
<td>Yes</td>
<td>An alert will be displayed on the Alerts page if a computer remains non-compliant for more than two hours.</td>
</tr>
<tr>
<td>Policy in compliance</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Real-time protection disabled</td>
<td>High</td>
<td>Yes</td>
<td>An alert will be displayed on the Alerts page if real-time protection has been disabled for a computer for more than 2.5 hours.</td>
</tr>
<tr>
<td>Real-time protection re-enabled</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
## Web Control

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web policy events</td>
<td>Low</td>
<td>No</td>
<td>Examine the appropriate reports for detailed information on how users are accessing sites, who is violating policy, and which users have downloaded malware.</td>
</tr>
<tr>
<td>Web threat events</td>
<td>Low</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

## Product Updates

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer or server out of date</td>
<td>Medium</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Update succeeded</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Update failed</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Reboot recommended</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Reboot required</td>
<td>Medium</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

## Protection Issues

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New computer or server registered</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Computer or server re-protected</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New computer or server protected</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Failed to protect computer or server

**Description:** A computer has started installation of the agent software but has not become protected for one hour.

**Severity:** High  
**Action required:** Yes

### Error reported

**Severity:** Low  
**Action required:** No

### Scan completion

**Severity:** Low  
**Action required:** No

### New logins added

**Severity:** Low  
**Action required:** No

### New users added automatically

**Severity:** Low  
**Action required:** No

---

### Peripherals Control

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripheral detected</td>
<td>Medium</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Peripheral allowed</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Peripheral restricted to read-only</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Peripheral blocked</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

---

### Duplicate devices

Sophos Central warns you if it detects duplicate devices. If devices have been cloned from an image they have the same ID. Duplicate IDs can cause management issues.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate device detection</td>
<td>Medium</td>
<td>No</td>
<td>An alert will appear on the Alerts page if a duplicate device is detected. Duplicated devices are re-registered with a new ID.</td>
</tr>
<tr>
<td>Device de-duplicated</td>
<td>Low</td>
<td>Yes</td>
<td>Check that the groups and policies for the de-duplicated devices are correct.</td>
</tr>
</tbody>
</table>
### Active Directory Synchronization

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory synchronization error</td>
<td>High</td>
<td>Yes</td>
<td>An alert will appear on the Alerts page if an Active Directory synchronization error is not resolved automatically for more than one hour.</td>
</tr>
<tr>
<td>Active Directory synchronization succeeded</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Active Directory synchronization warning</td>
<td>Medium</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Download Reputation

Sophos Central warns end users if a download has a low reputation. This reputation is based on a file’s source, how often it is downloaded and other factors.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User deleted low reputation download</td>
<td>Low</td>
<td>No</td>
<td>A user deleted a download after Sophos Central warned that it had a low reputation.</td>
</tr>
<tr>
<td>User trusted low reputation download</td>
<td>Low</td>
<td>No</td>
<td>A user trusted a download after Sophos Central warned that it had a low reputation.</td>
</tr>
<tr>
<td>Low reputation download automatically trusted</td>
<td>Low</td>
<td>No</td>
<td>Sophos Central detected a low reputation download and trusted it automatically. This occurs only if you change your reputation checking settings to &quot;Log only&quot;.</td>
</tr>
</tbody>
</table>
Firewall

If you have a Sophos XG Firewall registered with Sophos Central, your computers can send regular reports on their security status or "health" to Sophos XG Firewall. These reports are known as "security heartbeats".

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing heartbeat reported</td>
<td>High</td>
<td>Yes</td>
<td>A computer is no longer sending security heartbeat signals to a Sophos XG Firewall but is still sending network traffic. The computer may be compromised. A Sophos XG Firewall may have restricted the computer's network access (depending on the policy your company set).</td>
</tr>
<tr>
<td>Restored heartbeat reported</td>
<td>Low</td>
<td>No</td>
<td>A computer has resumed sending security heartbeat signals to a Sophos XG Firewall.</td>
</tr>
</tbody>
</table>

Device Encryption

Note
For most device encryption alerts, you should restart the computer and let it sync with the server.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key creation failed</td>
<td>Medium</td>
<td>See Note</td>
<td>A key could not be created (TPM key, TPM+PIN key, USB key, recovery key).</td>
</tr>
<tr>
<td>Device Encryption failed</td>
<td>Medium</td>
<td>See Note</td>
<td>A volume could not be encrypted.</td>
</tr>
<tr>
<td>Device Encryption information</td>
<td>Low</td>
<td>See Note</td>
<td>Information on various events, for example the user postponed encryption or a PIN/passphrase was reset.</td>
</tr>
<tr>
<td>Event type</td>
<td>Severity</td>
<td>Action required?</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption.</td>
</tr>
<tr>
<td>Device Encryption status changed</td>
<td>Low</td>
<td>See Note</td>
<td>The Device Encryption status changed from one status to another status. See Computers.</td>
</tr>
<tr>
<td>Device Encryption is suspended</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption.</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption.</td>
</tr>
<tr>
<td>Received recovery keys</td>
<td>Low</td>
<td>See Note</td>
<td>Sophos Central received a recovery key from an endpoint computer.</td>
</tr>
<tr>
<td>Revoked keys</td>
<td>Low</td>
<td>See Note</td>
<td>A recovery key has been viewed in Sophos Central, so it has been revoked and will be replaced.</td>
</tr>
</tbody>
</table>

**Data Loss Prevention**

<table>
<thead>
<tr>
<th>Event type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An &quot;allow transfer on acceptance by user&quot; action was taken</td>
<td>A file containing controlled information was transferred after a user acknowledged they were transferring the information.</td>
</tr>
<tr>
<td>An &quot;allow file transfer&quot; action was taken</td>
<td>A file containing controlled information was transferred.</td>
</tr>
<tr>
<td>A &quot;block transfer&quot; action was taken</td>
<td>A transfer of a file containing controlled information was blocked.</td>
</tr>
</tbody>
</table>

**Amazon Web Services (AWS)**

Sophos Central reports any AWS connection errors.

**Related concepts**

Alerts (page 4)
The **Alerts** page lists all the alerts that require your action.

**Alerts for Device Encryption** (page 9)

**Computers** (page 66)

On the **Computers** page, you can manage your protected computers.

**Related information**

- Duplicate device detection
- Download Reputation
- ML/PE-A detection explained

### Audit Logs

You can view and export a record of all activities that are monitored by Sophos Central using the Audit Log report.

To find the Audit Log reports, go to the **Logs & Reports** page and select **Audit Logs**.

All activities for the past 7 days are shown in the Audit Log by default. You can view all activities for up to 90 days. You can export an Audit Log report containing a record of all activities.

The Audit Log lists the following for each activity:

- **Date**: Date and time when the activity or change occurred.
- **Modified by**: The Sophos Central Admin account that made the change or signed in.
- **Item type**: The type of activity or change. For example Users and Groups were changed.
- **Item modified**: What was added, changed or deleted. For example the name of a new user that was added.
- **Description**: More details about the activity or change. For example a successful authentication by a Sophos Central account.
- **IP address**: The IP Address from where activity or change was carried out.

You can filter the Audit Log by date range and by search results. You must click **Update** to apply the filters.

- **From** and **To**: Use these options to set the date range for the activities you want to view. You can select any date within the last 90 days. The date range works with the **Search** field and the Audit Log shows the items related to your selected date range and search term. If you do not enter a search term the Audit Log shows all activities for your selected date range.

- **Search**: There is a limited search available. The Audit Log shows the items related to your search term and the selected date range. If you do not set a date range the Audit Log shows the items related to your search term for the last 7 days, by default. You can search by:
  - **IP address**: Shows all changes and activity from an IP Address over the selected date range.
  - **Modified By**: Shows all changes and actions made by a Sophos Central account over the selected date range.

### Export

You can export an Audit Log report that contains a record of activities for a selected date range or the last 90 days. You can filter the Audit Log before exporting. Search filtering applies to all export options. The date range does not.

To export an audit report:

1. Filter the Audit Log, if required. Click **Update** to apply the filters to the Audit Log.
2. Click **Export** on the right-hand side of the Audit Log page and choose an option from the drop-down list.

   - **CSV of current view** or **PDF of current view**: Exports the current view as a comma separated file or as a PDF file. If you select one of these options all currently selected filters are applied to the exported file.
   - **CSV of past 90 days** or **PDF of past 90 days**: Exports activities from the past 90 days as a comma separated file or as a PDF file. If you select one of these options only search filtering is applied to the exported file.

3. Review the audit report to check that it contains the information you require.

4. Change the audit report name.
   
   Audit reports are exported as audit.csv or audit.pdf.

### Data Loss Prevention Events Log

The **Data Loss Prevention Events Log** displays all events triggered by data loss prevention rules for computers or servers.

**Note**

An endpoint computer can send a maximum of 50 data control events per hour to Sophos Central. All events are logged locally on the endpoint computer.

You can find the following features and information on the **Data Loss Prevention Events Log**:

**Search**: If you want to view events for a certain user, device or rule name, enter the name of the user, device, or rule in the search box.

**Choose period**: Use the box to select the time period for which you want to view events. If you select Custom, use the From and To fields to select the dates between which you want to view events. You can view events that occurred in the past 90 days or less.

**Filter by rule name**: You can filter the events by rule name.

**Filter by file type**: You can filter the events by file type.

**Update**: Click this to display any new events reported since the page was last opened or refreshed.

### Event table

The event table provides these event details:

- **Date and time**: Time and date when the event occurred
- **User**: Source that caused the event, for example, the name of a user or system
- **Device**: Device that caused the event
- **Rule name**: Data loss prevention rule that caused the event
- **Rule action**: Data loss prevention action that caused the event
- **File name**: Name of the file that caused the event
- **Destination type**: Name of the destination that caused the event

**Save as Custom Report** lets you save the report settings in the **Saved Reports** table on the Logs & Reports page.
The Export menu (on the right of the table) lets you export the current view or the report for the past 90 days as a CSV (comma separated value) or PDF file.

**Message History Report**

The Message History report details the emails processed by Email Gateway for your protected mailboxes.

**Restriction**
This option is only available if your license includes Sophos Email.

You can search emails by **Subject**, **Sender** or **Recipient**.

You can select the time period for which you want to view the email processing history. By default the report displays the emails that have been processed during the current day.

You can order messages by **Direction** or **Date**. You can filter emails by **Status**.

Click **Update** to refresh the report if you have changed the date range, entered a search term or filtered the emails. This shows the results of the changes you selected.

**Report Details**

For each message the report shows:

The **Status** of the email message.

- **Delivered Successfully**: The email was processed successfully and is being sent for delivery.
- **Quarantined**: The email was marked as spam due to its content or block list configuration. You can view quarantined emails on the Quarantined Messages page.
- **Deleted**: The email was deleted due to its content or block list configuration. When you select Deleted, you can select a Reason for deletion from the drop-down menu.
- **Processing**: The email is temporarily still being processed. This applies to emails in the Sandbox environment and emails that have been queued for delivery.
- **Accepted**: The email has been received successfully and is being processed by our system.
- **Delivery Failed**: Delivery of the email was attempted several times but it could not be delivered and the request timed out.
- **Queued for Delivery**: The initial delivery attempt failed, so the email will be re-queued for delivery. We will attempt to deliver the email for up to 5 days. Possible reasons for the initial delivery attempt failing are the recipient mail server being offline and issues retrieving the DNS records for the recipient. Emails that have been queued for delivery and are now in the processing phase will show up as Processing.
- **Processing Encryption**: The email is still in the process of being encrypted, or the encrypted email is waiting to be delivered after the recipient sets their password.

**Note**
Whether an email is quarantined or deleted depends on the spam protection settings you have chosen.
Message Details

To view Message Details, click the Subject line. You can click on the following tabs for more information about the message.

Message Details: shows general information about the message.

Select Block IP if you want to add the IP to the Inbound Allow/Block list then click Block to confirm your choice. Any sender using this IP address is blocked. Click Cancel to cancel the action.

Select the show more icon to see message events with timestamps. If an email is queued for delivery, you will see a Delivery Status Notification (DSN) error code underneath the Queued for Delivery status. This is the code returned by the recipient's mail server when you have attempted to deliver an email and the email isn't delivered. The code is helpful for troubleshooting the reason the email isn't delivered.

Raw Header: shows the email header details.

Attachments: shows the name and size of attachments.

Related concepts
Email Security Policy (page 458)
You can apply security settings to your mailboxes using Email Security policies.

Inbound Allow/Block (page 151)
You can create a list of email domains and addresses that you trust or don't trust.

Quarantined Messages (page 454)
The Quarantined Messages page lists the email messages that have been quarantined for all your protected mailboxes.

Related information
Enhanced Mail System Status Codes

Gateway Activity

The Web Gateway Network Activity page lets you see all the network activity logs associated with your Web Gateway protection.

You can filter logs by:

• Action (Allow, Audit, Block)
• Filter type (Category, Malware, Phishing, URL, Data)
• Website Category and/or
• User.

The Search box for users will attempt to auto-complete as you type.

You can limit report data to a specific date range by entering a From and To date. Once you have a date range specified you can:

• Update: Update the data displayed in the report for the specified date range.
• Export: Export the data to XSLX, ODS, CSV, or XML format.
3.4.2 Reports

The reports that you can see depend on your license.
You can customize reports, save them and send them out as scheduled emails.

Note
A report may not support all the customization or viewing options.

Limit report data to a specific time range

In some reports, you can limit report data to a specific date range by entering a From and To date.
In some reports, you can select a time period.

Filter reports

In some reports, you can filter the displayed information by clicking on the category tiles. For example in the Computers report you can show all the active computers by clicking on Active.
You may also be able to filter by groups.
You can also use Search to filter for specific information.

Print or export reports

You can print or export your reports.

- **Print**: Click this to open a printer-friendly view. Then press Ctrl+P to open the printer dialog.
- **Export to CSV**: Click this to export the current view as a comma separated file.
- **Export to PDF**: Click this to export the current view as a PDF file.

Save and email custom reports

You can create and save custom reports. A list of the saved reports is shown at the top of the Logs & Reports page.
You can also choose to send custom reports by email and set up a schedule for them. You can save as many reports as you like, but you can only schedule up to 25.

1. Set up the report by selecting the appropriate filters.
2. Click **Save as Custom Report**.
   This opens the **Save Report** dialog.
3. Enter a **Name** for the report.
4. If you want to send the report by email, select one of these options:
   - **Send a link to the report**.
   - **Attach the report to the email**.
We recommend that you send a link if the report includes personally identifiable information. You need to enter Sophos Central sign-in credentials to view reports from a link.

5. Select the **Frequency**. You can choose from monthly or weekly.

6. Select the format: **PDF** or **CSV**.

7. Click **Save**.

The email is received by the user who signs in and creates the report.

**Note**

Scheduled emails stop after six months. You can reschedule them if you want to.

**Recover tamper protection passwords**

You can recover the tamper protection passwords of devices that you’ve recently deleted. You might need to do this so that you can uninstall Sophos software that is still on those devices.

1. Go to **Logs & Reports**.

2. In **Reports**, under **Endpoint & Server Protection**, click **Recover Tamper Protection passwords**. You see a list of deleted devices.

3. Find the device you want.

4. In the **Password(s)** column, click **View password details**. This shows you the password (and previous passwords).

**Gateway Reports**

The **Web Gateway Reports** page lets you see all the reports for your Web Gateway protection. Please note that reports update about once an hour.

You can limit report data to a specific date range by entering a **From** and **To** date. You can also filter the report using the filters shown.

Once you have set the date range and filters, you can:

- **Update**: Update the data displayed in the report for the specified date range.
- **Print**: Send a copy of the report to the printer.
- **Export**: Export the data to XSLX, ODS, CSV or XML format.

**Message Summary Report**

The **Message Summary** report details the email messages processed by **Email Gateway** for your protected mailboxes.

**Restriction**

This option is only available if your license includes **Sophos Email**.

You can view messages that occurred in the past 365 days or less. Messages for the last 30 days are shown by default.

**Direction**: Select **Inbound** or **Outbound** from the drop-down menu to view messages that have been received or sent.
All scanned messages are shown in the report by default. The messages are classified as follows:

- **Scanned**: All messages processed by Email Gateway.
- **Legitimate**: Messages that have been allowed.
- **Spam**: Messages classified as spam.
- **Virus**: Messages classified as containing viruses.
- **DLP policy violations**: Messages that violated Data Loss Prevention policies.
- **Advanced threat**: Messages classified as containing advanced threats.
- **Realtime blocklist**: Messages detected due to a blacklisted sending IP.
- **Company blocklist**: Messages sent from an address that has already been added to the company blocklist (inbound allow/block).
- **Authentication failures**: Messages that failed authentication by DMARC, SPF or DKIM.

The graph shows you at a glance the number of messages that were processed per day. The message table shows the number of email messages processed for each date listed. It reflects the selected date and all message types.

### Advanced Threat Report

The **Advanced Threat Report** details all emails submitted to Sophos Labs Intelix for advanced threat analysis.

You can view messages that occurred in the past 365 days or less. Messages for the last 30 days are shown by default.

The report shows clean, likely clean, suspicious, and malicious emails in graph form and in a list. They are categorized by the level of threat and you can filter the graph by **Scan result**. You can export the list in CSV or PDF format. Any emails that encounter errors are quarantined.

You can click the subject of any email to see **Message Details**. This shows you more information about the contents of a specific email and the results of the analysis. There are the following sections:

- **Summary**: Details of the email and whether it was delivered.
- **Threat prevalence**: How many times this malware has been received at your organization and other organizations.
- **Static analysis**: Details of machine learning analysis.
- **Dynamic analysis**: Results from tests run in a sandboxed environment.

If analysis is still in progress, you can't click the subject.

Use this information to determine the severity of the threat in an email.

### Time of Click Summary

The **Time of Click Summary** report details the email messages processed by Time of Click URL Protection for your protected mailboxes.

**Restriction**

This option is only available with an **Email Advanced** license.
You can view messages that occurred in the past 365 days or less. Messages for the last 30 days are shown by default.

All scanned messages are shown in the report by default. The messages are classified as follows:

- **Total Clicks**: All links that were clicked.
- **# Clicks Allowed**: All links that were allowed.
- **# Clicks Warned**: All links that generated a warning.
- **# Clicks Blocked**: All links that were blocked.

The graph shows you at a glance the number of messages that were processed per day.

The message table shows the number of email messages processed for each date listed. It reflects the date range selected and all message types.

**At risk users**

This report lists users who are most at risk.

**Restriction**
This option is only available with an Email Advanced license.

This report uses information from the Time of Click URL Protection and Impersonation Protection features. Details for the last 30 days are shown by default.

To educate high-risk users there are direct links to Phish Threat training from the report. The Phish Threat campaign wizard automatically includes the at risk users for the date range you have selected. You can also add and remove users manually.

**Related concepts**

Enhanced Email Malware Scan (page 464)
You can apply enhanced email content scanning.

Impersonation Protection and VIP Management (page 159)
Impersonation Protection detects phishing emails that pretend to come from well-known brands or from important people within your organization.

**Related tasks**
Create a Phish Threat Campaign (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

**Data loss prevention policy violations**

This shows all the emails that have violated email Data Loss Prevention (DLP) policies.

**Restriction**
This option is only available with an Email Advanced license.

Select the time period for which you want to view details of policy violations. Details for the last 30 days are shown by default.

You can see the following information:

- **Direction**: You can choose to view all processed emails, all inbound or all outbound.
• **Category**: You can filter the report by the type of information affected, for example financial information (FI).

• **Action**: You can filter the report by the action taken.

You can also click **Create Phish Threat campaign** to create training for your users.

**Restriction**
This option is only available with a Sophos **Phish Threat** license.

The users who have been logged by the data loss prevention policies for the date range you have selected are automatically included in the campaign. You can also add and remove users manually.

**Related concepts**
- **Data Loss Prevention policy** (page 467)
- **Data Loss Prevention** (DLP) stops data from being leaked by email.
- **Phish Threat** (page 596)

### 3.5 People

On the **People** page, you can manage your users and user groups.

#### 3.5.1 Users

On the **Users** tab of the **People** page, you can add or manage users, and get the users’ computers protected.

You can also enable the users to protect their own devices by emailing them a setup link.

The current users are listed with their details.

**Health Status.** An icon shows whether the user has security alerts on any of their devices.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="green.png" alt="Green" /></td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td><img src="amber.png" alt="Amber" /></td>
<td>Amber warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td><img src="red.png" alt="Red" /></td>
<td>Red warning sign if there are critical alerts.</td>
</tr>
</tbody>
</table>

**Name** Click the user’s name to see details of devices and to see which has an alert.

**Email.**

**Exchange Login.**

**Last Active.** The last time a user reported to Sophos Central.

**Group Name.** This is shown if the user has been added to a user group.

**Role.** This shows what administration role, if any, the user has. This column is only visible if you are an administrator.
Click any column header to sort the users. By default, users are sorted according to the **Last Active** time.

To see full details for a user, click the user’s name.

You can add users manually or automatically by protecting their devices. You can also import users in bulk from a CSV file or from Active Directory. You can also protect existing users.

To modify users, click the user’s name to open and edit their user details.

You can also delete users and export lists of users.

### Related concepts

**User Summary** (page 56)

**Administration Roles** (page 93)
Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

### Related tasks

**Add a user manually** (page 61)
You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

**Add users automatically** (page 62)
You can add users automatically by protecting their devices.

**Import users from a CSV file** (page 63)
You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

**Import users from Active Directory** (page 63)
You can import users and groups from Active Directory.

**Protect existing users** (page 64)
You can protect users that you have already added to Sophos Central.

**Delete users** (page 64)
You can delete users from Sophos Central if you are a Super Admin.

**Export to CSV** (page 64)
You can export lists of users as CSV files.

### User Summary

The **Summary** tab in a user’s details page shows a summary of the following:

- The user’s security status, administration role, if any, and account details.
- Recent events on the user’s devices.
- Mailboxes associated with the user.
- Devices associated with the user.
- Policies that apply to the user.
- Groups that the user belongs to.
- Logins.

You can find details of each below.

The security status and account details are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.
You can click on the other tabs for more on **Devices**, **Events**, and **Policies**.

### Health Status

In the left-hand pane, an icon shows you whether the user has security alerts on any of their devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green check mark" /></td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td><img src="image" alt="Orange warning sign" /></td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td><img src="image" alt="Red warning sign" /></td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>

You can see which devices have alerts in the **Devices** tab.

A padlock icon shows that the user has been imported from Active Directory.

A badge shows the user's assigned administration role. Click on the role name to view the settings for the role.

**Note**
Role information is only displayed for administration roles.

### Account details

In the left-hand pane, you can modify or delete the user's account.

**Note**
If a user has been imported from Active Directory, you cannot change the account details. However, you can add the user to a new Sophos Central group or add another login.

**Modify the account**

1. Click **Edit** and enter the following settings:

   **First & Last name**: Enter the name of the user. Do not include a domain name.
   
   **Role**: Select a role for the user. Choose from: **Super Admin**, **Admin**, **Help Desk**, **Read-only**, or **User**.
   
   **Restriction**
   You can only see the **Role** option and assign administrator roles if you are a Super Admin.

   **Note**
   You cannot amend your own administration role.
Note
Anyone with a User role only has access to the Self Service Portal.

Email Address: Enter the email address of the user.
Exchange Login (optional): Enter the Exchange account name of the user.

Note
In Sophos Mobile policies, you can use the placeholder %USERNAME% to refer to this setting.

Add to groups: Select one of the available user groups and use the picker arrows to move it to the assigned groups.

Email Setup Link: Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs.

Note
The user needs administrative privileges and internet access in order to protect their computer.

Note
Web Gateway provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

2. Click Save.

Delete the account
To delete the account, click Delete User in the left-hand pane. Logins assigned to this user can afterward be assigned to another user.

Restriction
You cannot delete users who have an assigned administration role.

Multi-factor authentication
If the user is an admin, the left-hand pane shows whether multi-factor authentication (MFA) is enabled for them. If it is enabled, the admin must use another form of authentication, as well as their user name and password, to sign in.

If you’re a Super Admin, you can edit the settings as follows:
Click Reset to let the admin set up their MFA sign-in details again.
Click MFA Settings to go to a page where you can enable or disable multi-factor authentication for the admin.

Recent Events
This lists recent events on the user’s devices.
For a full list, click the Events tab.
**Mailboxes**

This lists all email addresses, including distribution lists and public folders, associated with the user. Primary indicates the user's primary email address. Owner indicates the user controls a distribution list or public folder.

For full details, click an email address.

**Devices**

This shows a summary of the devices associated with the user.

Click the device name to go to the device's details page for more information.

Click **Actions** to carry out any of the same actions that are available on the device's details page (for example, Scan Now and Update Now for a computer).

For full details of the user's devices, click the **Devices** tab.

**Policies**

This shows a summary of the policies applied to the user.

The list shows the policy name, whether the policy is enabled or not, and icons that indicate the features included in the policy.

Click on a policy name to view and edit the user policy.

**Note**

Editing the policy affects all users to which this policy is applied.

For full details of all the policies applied to this user, click the **Policies** tab.

**Groups**

This shows the groups the user belongs to.

Click on a group name to see details of the group.

Click **Edit** (on the right) to change the groups the user belongs to.

**Logins**

This shows the user's logins.

Click **Edit** (on the right) to change the logins assigned to the user.

**Related concepts**

- About Policies (page 200)
- Administration Roles (page 93)
Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

**User Devices**

The **Devices** tab in a user's details page lets you see the devices associated with the user. This tab also shows any servers where the user has logged on with Remote Desktop Services.

For each associated device you can see the device type and the operating system. You also have these options:

- **View Details**: This opens the full device details page.
- **Delete**: This removes the device from the list and stops Sophos Central managing it, but it does not uninstall the Sophos software.
- **Actions**: Actions you can take. These depend on the device type.

**User Events**

The **Events** tab in a user's details page lets you see a list of events detected on the user's devices.

You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

- **Severity**: Hover over an icon to see what it means.
- **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
- **Details**: This link (for certain events) lets you get further details and take action.

**View Events Report** shows events arranged by type and a graph of events day by day.

**Stop detecting an application**

If an application is reported as malware but you know it's safe, you can allow it from the events list.

For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the **Details** link beside the event and then allow the application.

**Note**

This currently applies only to malware events reported by Intercept X.

**Stop detecting an exploit**

If an exploit is detected but you're sure the detection is incorrect, you can stop it happening again.

This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don't detect this again** and select an option:
   - **Exclude this Detection ID from checking**: prevents this detection on this app.
   - **Exclude this application from checking**: prevents any checks for exploits on this app.
Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.

3. Click **Exclude**.

We’ll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again**.
   - Select **Exclude this Detection ID from checking**. This prevents this detection on this app.
3. Click **Exclude**.

We’ll add your exclusion to the Global Exclusions list.

Related information

How to investigate and resolve a potential False Positive or Incorrect Detection

User Policies

The **Policies** tab in a user’s details page lets you see the policies that are enabled and applied to the user.

Click a policy name to view and edit policy details.

Editing the policy affects all users to which this policy is applied.

Add a user manually

You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

To add a user:

1. Go to **Users**.
2. Click **Add** and select **Add User**.
3. In the **Add User** dialog, enter the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First and Last Name</td>
<td>Enter the name of the user. Do not include a domain name.</td>
</tr>
<tr>
<td>Role</td>
<td>Select an administration role for the user. A user who is assigned an administration role will receive an email telling them how to set up their administration account.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>You can only see the Role option and assign administrator roles if you are a Super Admin. Anyone with a User role only has access to the Self Service Portal.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address of the user.</td>
</tr>
<tr>
<td>Add to groups (optional)</td>
<td>Select one of the available user groups and use the picker arrows to move it to the assigned groups. You can start typing a name in the search box to filter the displayed groups.</td>
</tr>
<tr>
<td>Email Setup Link</td>
<td>Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs. The user needs administrative privileges and internet access in order to protect their computer.</td>
</tr>
<tr>
<td>Web Gateway</td>
<td>This provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.</td>
</tr>
</tbody>
</table>

4. Click Save or Save and Add Another. The new user is added to the user list.

When the user downloads and installs the software, their device is automatically associated with the user.

**Add users automatically**

You can add users automatically by protecting their devices.

To add users:
1. Download an installer from Protect Devices.
2. Run the installer on the devices.

This adds the user of each device automatically.

**Related concepts**

Protect Devices (page 160)
You can download Sophos installers and use them to protect your devices.

**Import users from a CSV file**

You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

To import users:
1. Go to **Users**.
2. Click **Add** and click **Import users from CSV**.
3. Click **Browse** and select your CSV file.

**Tip**
You can download template CSV files from the **Import users from CSV** dialog.

The CSV file can include groups a user is assigned to.
4. To create new groups, click **Create new groups**.
5. To send a registration email for the Sophos Central Self Service portal to each imported user, click **Give users access to Sophos Central Self Service**.
6. Click **Add**.

**Note**
The CSV file can include the email address of each user's manager. If there's a manager who isn't already a user in Sophos Central, a user is created. So the number of users imported may exceed the number of rows in the file.

**Note**
If an email address in your CSV file matches an existing user in Sophos Central, the user is updated with the information in your import file.

**Note**
If an email address in your CSV file matches an existing user in Sophos Central that is managed through Active Directory Synchronization, the user is skipped during import and no changes are made to the user account.

**Import users from Active Directory**

You can import users and groups from Active Directory.

To do this:
1. Go to **Users**.
2. Click the **Set up Active Directory Sync** link in the upper right of the page.
3. Follow the set up synchronization process.

**Related tasks**

Set up synchronization with Active Directory (page 89)
Follow these instructions to set up synchronization with Active Directory.

**Protect existing users**

You can protect users that you have already added to Sophos Central.

To protect them you need to email them a setup link. To do this:

1. Go to **Users**.
2. Select the user or users you want to protect.
3. Click **Email Setup Link** in the upper right of the page.
4. In the **Email Setup Link** dialog, select the types of protection the user needs (if your license includes more than one).

   **Web Gateway** provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

   Users need administrative privileges and internet access to use the setup link.

**Delete users**

You can delete users from Sophos Central if you are a Super Admin.

**Restriction**

You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them.

Under some circumstances, the user may be recreated automatically in future:

- If the user logs in to an associated device that is still managed by Sophos Central, they are added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they are added as a user again the next time that Sophos Central synchronizes with Active Directory.

To delete users:

1. Go to **Users**.
2. Click the checkbox next to each user you want to delete.
3. Click **Delete**.

Deleting a user does not delete devices associated with that user or remove the Sophos software from these devices.

Logins assigned to a deleted user can afterwards be assigned to another user. You can edit logins by clicking the **Edit** link on a user's details page.

**Related concepts**

**User Summary** (page 56)

**Export to CSV**

You can export lists of users as CSV files.

You can export lists of different types of user.

For example you can export a list of administrators by applying the **Admins only** filter before you click **Export to CSV**.
To export users:

1. Go to Users.
2. Click Export to CSV. 
   This creates a file called users.csv. Any currently active filters are applied to the list.

### 3.5.2 Groups

On the Groups tab of the People page, you can add or manage groups of users.
You can use groups to assign a policy to multiple users at once.
The sections below tell you about the groups list and how to add, modify or delete groups.

#### About the groups list

The current groups are listed and the number of users in each group is shown.
To see full details for a group, click the group's name.

#### Add a group

1. Click the Add Group button.
2. In the Add Group dialog, enter the following settings:
   - **Group Name**: Enter the name of the new group.
   - **Available Users**: Select users from the list of available users.
     
     **Tip**
     In the Search box you can start typing a name to filter down the displayed entries.

3. Click Save.

#### Modify a group

To modify a group, click the group's name to open and edit the group details. For more information, see User Group Details.

#### Delete a group

To delete a group, select it and click Delete in the upper right of the page.
Deleting a group will not delete its users.

**Related concepts**
User Group Details (page 66)
User Group Details

On a group's details page, you can:

- Add or remove members.
- Delete the group.

Add or remove members

To add or remove members:

1. Click Edit under the group name.
2. In the Edit Group dialog, use the picker arrows to add users to the Assigned Users list or remove them.
3. Click Save.

Delete the group

To delete the group:

1. Click Delete under the group name.
2. In the Confirm Group Deletion pop-up, click Yes.

Deleting a group will not delete its users.

User Group Policies

The Policies tab in a user group's details page lets you see the policies that are enabled and applied to the group.

Click a policy name to view and edit policy details.

Editing the policy affects all groups to which this policy is applied.

3.6 Devices

On the Devices page you can manage your protected devices, for example computers, or servers. The devices are listed by type on different tabs. The tabs displayed depend on the features included in your license.

3.6.1 Computers

On the Computers page, you can manage your protected computers.

They will appear automatically after Sophos agent software has been installed.

You can:

- View details of the computers.
- See the encryption status (if you are using Sophos Device Encryption).
• Delete computers.
• Install or uninstall software.
• Get a recovery key for encrypted computers (if you are using Sophos Device Encryption).
• Export the computers list to CSV.

View computer details

The computers list shows you the current computers with these details:
• Name.
• IP Address. Hover over the icon to see details of all IPv4 and IPv6 addresses.
• Operating System.
• Products installed. For example, Intercept X or Encryption.
• Last user.
• Last active. This is the last time that the computer contacted Sophos.
• Group. The group that the computer belongs to (if it belongs to one).

To search for a computer, enter the name in the search field above the list.
To filter computers according to their type, their health status, or their encryption status, use the filters above the list.
You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

Delete computers

You can delete computers that you no longer need to manage from Sophos Central.
Select the computer or computers you want to delete and click **Delete** (in the upper right of the page).
This deletes the computer and the alerts associated with the computer.

**Warning**
You should uninstall the Sophos software before deleting a computer.

Install or uninstall software

You can select new endpoint software to be installed on computers that are already protected and managed by Sophos Central.
You can also uninstall software.
To do either, do as follows.
1. Click **Manage Endpoint Software** (in the upper right of the page).
2. Select software.
3. Select computers and use the picker arrows to change the software installed, as follows.
   • To install the software, select eligible computers and move them to the assigned list.
- To uninstall the software, select assigned computers and move them to the eligible list. The computers will update to the selected software.

**Export to CSV**

To export a list of computers:

Click **Export to CSV**.

This creates a file called devices.csv. Any currently active filters are applied to the list.

For example you can export a list of Windows computers by applying the *Windows Computers* filter before clicking **Export to CSV**.

**Retrieve recovery key**

This option is available from **More** on the **Computers** page.

If users are unable to log in to their encrypted computer, you can get a recovery key which is used to unlock the computer.

**Related concepts**

*Encryption Recovery Key Search* (page 121)

**Computer Summary**

The **Summary** tab in a computer's details page shows you the following information.

The sections you see depend on your license and the features you've set up.

**Security status**

In the left-hand pane, you can see the security status and take actions.

**Note**

The left-hand pane is always shown, even when you click the other tabs on this page.

An icon shows you whether the computer has any security alerts:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>
Actions you can take

The action buttons are in the left-hand pane.

**Update**: This updates your computer with the latest Sophos software.

**Delete**: This deletes the computer from Sophos Central. It also deletes the alerts associated with the computer.

**Warning**
You should uninstall the Sophos software before deleting a computer.

**Isolate**: This isolates the computer from the network.

**Live Response (Beta)**: This enables you to connect to the computer to investigate and remediate possible security issues.

**Change group**: This lets you add it to a group, move it to a different group, or remove it from its current group.

**Scan Now**: This scans the computer for threats.

The scan may take some time. When complete, you can see a “Scan completed” event and any successful cleanup events on the **Logs & Reports > Events** page. You can see alerts about unsuccessful cleanup on the **Alerts** page.

If the computer is offline, it is scanned when it is back online. If a computer scan is already running, the new scan request will be ignored and the earlier scan will carry on.

**Diagnose**: This diagnoses potential issues with the computer.

**Create forensic snapshot**: This gets data from a Sophos log of the device’s activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

Isolate or remove from isolation

This option is available if you have Intercept X Advanced with EDR.

**Isolate** isolates the computer from the network. You might want to do this if potential threats are found on it. You can still manage the computer from Sophos Central and you can remove it from isolation at any time.

When a computer has been isolated, you see the following under the computer icon and security status.

- The message **Isolated by Admin**.
- A link labeled **Remove from Isolation**. Click it to reconnect the computer to the network.

**Note**
You don’t see the **Isolate** option if the computer has already isolated itself automatically. See **Device Isolation** in Threat Protection Policy.
Live Response (Beta)

This option is available only if you are a Super Admin and you’ve signed in using multi-factor authentication. You must also turn on Allow Live Response connections to computers in Global Settings, see Live Response for devices.

This enables you to connect to the computer to investigate and remediate possible security issues. You might want to do this if an infection or suspicious activity is identified on the computer. You can connect to the computer even if it’s isolated. To connect to the computer, do as follows:

1. Click Live Response (Beta).
2. In Session purpose, summarize the purpose of your session.
3. Click Start.
   A connection to the computer is opened in another browser tab. The tab shows a terminal window.
4. At the command prompt, type commands to perform your investigation or remediation.
   Use DOS, UNIX, or Linux commands depending on the computer to which you’ve connected.
5. When you finish, click End Session.
   The connection is closed, although the tab remains open. You can browse elsewhere in Sophos Central from here.
   The connection is also closed in the following cases:
   • You close the tab.
   • You refresh the tab.
   • You browse elsewhere in Sophos Central from here.
   • There is no activity for 30 minutes.

To see which Live Response sessions have started or ended, view the Sophos Central audit log.

Create forensic snapshot

You can create a “forensic snapshot” of data from the device. This gets data from a Sophos log of the device’s activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

You’ll need a converter (which we provide) to read the data.

Note
You can choose how much data you want in snapshots and where to upload them. To do this, go to Global Settings > Forensic Snapshots. These options may not be available for all customers yet.

To create a snapshot:
1. Go to a threat case’s Analyze tab.
   Alternatively, on the details page of the device, open the Status tab.
2. Click Create forensic snapshot.
3. Follow the steps in Upload a forensic snapshot to an AWS S3 bucket.
You can find the snapshots you generated in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Forensic Snapshots\.

Snapshots generated from detections are in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Saved Data\.

Note
You need to be an administrator with access to the tamper protection password and run a command prompt as an administrator to access the saved snapshots.

Recent Events
This lists recent events on the computer. For a full list, click the Events tab.
The icons indicate which Sophos agent reported each event. Hover over an icon to see what it means.

Agent Summary
The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.
The summary shows the following details. It also includes links to let you update the computer, install products, or change the group the computer's in, as needed.

• **Last Activity**: Shows when the last activity occurred.
• **Last Agent Update**: Shows whether the computer is up to date.
• **Assigned Products**: Shows the Sophos products installed (for example, Intercept X or Device Encryption). Shows the license and the version number for each installed product. The version information is only available for Windows computers.
• **Installed component versions**: Click this to see a full list of the Sophos components and their version numbers. This is only available for Windows computers.
• **Group**: Shows which group the computer is in (if any).

Device Encryption
Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault encryption on Macs.
This summary shows:
• All volumes of the computer.
• The volume ID for each volume.
• The encryption status.
• The authentication type.
• The encryption method.
Volumes can be encrypted with software-based or hardware-based encryption. Device Encryption always uses software-based encryption for new volumes, even if the drive supports hardware-based encryption.
If a drive is already encrypted with hardware-based encryption, it will not be changed.
If a BitLocker group policy setting requires hardware-based encryption, it is used.

**Retrieve Recovery Key**
You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their sign-in credentials.

**Trigger change of password/PIN**
This requires users to immediately change their BitLocker password or PIN. A message is displayed when the request has been sent successfully.

On the endpoint, users are prompted to set a new BitLocker password or PIN. If users close the dialog without entering a new password or PIN, the dialog is shown again after 30 seconds, until they enter a new one. After users have closed the dialog five times without changing the password or PIN an alert is logged.

**Web Gateway summary**
Sophos Web Gateway provides advanced protection against risky or inappropriate web browsing.
The summary shows the last network activity. It also shows the version of the Web Gateway agent (and whether it is up to date).
If you need to update the Web Gateway agent, an **Update** button is displayed.

**Tamper Protection**
This shows whether tamper protection is enabled on the computer or not.
When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:
- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
- Disable tamper protection.
- Uninstall the Sophos agent software.
Click **Disable Tamper Protection** to manage the tamper protection password for the computer. If tamper protection is switched off we recommend you turn it on.

**Update Cache and Message Relay**
Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos. You can also designate servers to communicate with Sophos Central as message relays.
This shows that a cache has been set up for the computer. It shows which server is being used.

**Windows Firewall**
Windows Firewall is active and being managed on the computer. It also shows:
- Whether Windows Group Policy is being used.
• The active network profiles.
• If other registered firewalls are installed and active.

Related concepts

Threat Protection Policy (page 203)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

Encryption Recovery Key Search (page 121)

Forensic snapshots (page 138)
Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

Related tasks

Live Response for devices (page 144)
Turn on Live Response so that you can connect to devices to investigate and remediate possible security issues.

Recover deleted devices (page 87)
You can recover devices that you’ve deleted from Sophos Central if they are synced using Active Directory synchronization.

Convert a forensic snapshot (page 139)
Use the SDR Exporter tool to convert forensic snapshots so you can run queries on them.

Related information

Upload a forensic snapshot to an AWS S3 bucket (page 140)
Follow these instructions to upload a forensic snapshot.

Computer Events

The Events tab in a computer’s details page displays events detected on the computer. You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

• **Sev:** Hover over an icon to see what it means.
• **Type:** An icon shows which Sophos agent reported the event. Hover over it to see what it means.
• **Details:** This link (for certain events) lets you get further details and take action.

**View Events Report:** Shows events arranged by type and a graph of events day by day.

Stop detecting an application

If an application is reported as malware but you know it's safe, you can allow it from the events list.

For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the **Details** link beside the event and then allow the application.

**Note**
This currently applies only to malware events reported by Intercept X.
Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again** and select an option:
   - **Exclude this Detection ID from checking**: prevents this detection on this app.
   - **Exclude this application from checking**: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.

3. Click **Exclude**.

We’ll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again**.

   Select **Exclude this Detection ID from checking**. This prevents this detection on this app.

3. Click **Exclude**.

We’ll add your exclusion to the Global Exclusions list.

**Related concepts**

*Allowed applications* (page 130)

**Related information**

*How to investigate and resolve a potential False Positive or Incorrect Detection*

**Computer Status**

The **Status** tab in a computer’s details page lets you see the computer’s security health and details of any alerts.

It also lets you take action against alerts.

**Security Health**

These status details are only shown if the computer is using the Security Heartbeat feature.

The computer security status is reported by computers running Windows 7 and later.
This shows whether the device has threats detected, has out-of-date software, is not compliant with policy, or is not properly protected. The overall status is the same as that for the highest-priority item listed (red, orange or green).

 Alerts

The page lists any alerts on the device. The details include:

- Alert details: For example, the name of the malware.
- When the alert occurred.
- The actions that you can take. These depend on the type of threat or event and are the same as the actions available in the Dashboard.

 Computer Policies

The Policies tab in a computer’s details page lets you see the policies that are applied to the computer.

You can view and edit policy details by clicking the policy in the list.

 Note
Editing the policy affects all users to which this policy is applied.

3.6.2 Mobile devices

On the Mobile devices page you can manage your mobile devices. They appear after you’ve added them to Sophos Mobile.

 About the devices list

The devices list shows you the current devices with these details:

- Health Status: The health status of the device.
- Name: The name of the device.
- Operating system: The operating system and version.
- User: The Sophos Central user you assigned to the device. Click the name to see details of that user.
- Managed: The management status of the device.
- Container: The management status of the Sophos container.
- Intercept X for Mobile: The management status of Sophos Intercept X for Mobile (Android, iOS) or Sophos Chrome Security (Chrome OS).
- Last active: The last time the device contacted Sophos.

 Search for devices

To search for a device, enter the name or other device properties in the search field above the list.
To filter devices according to their health status, their platform, or their last active time, use the filters above the list.

**Add a device**

To add a device, go to Mobile.

**Delete a device**

You can delete devices you no longer need to manage from Sophos Central.

Select the device or devices you want to delete and click **Delete** (in the upper right of the page).

This deletes the device and the alerts associated with the device.

**CAUTION**

Unenroll the device from Sophos Mobile before deleting it. Otherwise it might become unusable.

**View details of a device**

Click on a device in the list to view its details.

**Export to CSV**

To export a list of devices:

Click **Export to CSV**.

This creates a file called `devices.csv`. Any currently active filters are applied to the list.

For example you can export a list of iPhones and iPads by applying the **iOS devices** filter before clicking **Export to CSV**.

**Related information**

Add devices (Sophos Mobile administrator help)

**Mobile device summary**

The **Summary** tab in a mobile device’s details page lets you see device details and manage the device.

**Health status**

In the left-hand pane, you can see the device’s health status and type. You can also take actions.

**Note**

The left-hand pane is always shown, even when you click the other tabs on this page.
The health status (Green, Yellow, Red) is indicated by the color of the device icon. Depending on the compliance policy you’ve assigned to the device, network access is restricted when the health status is Yellow or Red.

Device type and assigned user

The left-hand pane shows the following device information:

- The device name you set.
- The device model.
- The operating system.
- The user assigned to the device. Click the name to open the user’s details page.

Actions you can take

The actions links and buttons are in the left-hand pane. The actions you see depend on the device type and status.

- **Delete**: Deletes the device and the alerts associated with the device.
  
  **CAUTION**
  
  Unenroll the device from Sophos Mobile before deleting it. Otherwise it might become unusable.

- **Locate**: Gets the device location.
- **Lock**: Activates the screen lock on the device.
- **Unenroll**: Unenrolls the device from Sophos Mobile.
  
  To unenroll a device with Android Enterprise full device management, use the **Wipe** action instead.
  
  To unenroll a device with Android Enterprise work profile management, use the **Wipe Android work profile** action instead.

- **Wipe**: Resets the device to its factory settings.
- **Wipe Android work profile**: Removes the Android Enterprise work profile from the device.
- **More actions**: Opens the device’s details page in Sophos Mobile with more management options.

Recent Events

This lists recent events on the device.

For a full list, click the **Events** tab.

Device summary

This shows essential management information:

- **Management mode**: The type of enrollment with Sophos Mobile, for example if Sophos manages the whole device, the Sophos Intercept X for Mobile app, or the Sophos container.
Device status

This shows the management and security status of the device:

- **Health status**: The health status of the device. If you’ve set up Synchronized Security as described in the Sophos Mobile administrator help, Sophos Central Wireless uses the health status to restrict network access. Note that because Chrome OS doesn’t report the MAC address to Sophos Central, Synchronized Security is not available for Chrome devices.

- **Compliance status**: Shows if the device complies with the compliance policy you’ve assigned to it.
  - Click the status value for details.

- **Tasks**: Shows if there are open tasks for the device.
  - Click the status value to see all completed and pending tasks.

- **Sophos Mobile**: Shows if the device is enrolled with Sophos Mobile.

- **Sophos Intercept X for Mobile**: Shows if the Sophos Intercept X for Mobile app is enrolled with Sophos Mobile.

- **Sophos Chrome Security**: Shows if Sophos Chrome Security is enrolled with Sophos Mobile.

- **Sophos container**: Shows if Sophos Mobile manages a Sophos container on the device.

Device information

This shows hardware-related device information like the device ID.

Click **View on map** to view the last known device location in Google Maps. To get the location, use the **Locate** action.

Related information

- Synchronized Security (Sophos Mobile administrator help)
- Create compliance policy (Sophos Mobile administrator help)
- The Show device page (Sophos Mobile administrator help)

Mobile device events

The **Events** tab in a mobile device’s details page displays events detected on the device.

Click **View Events Report** to see events arranged by type and a graph of events day by day.

3.6.3 Servers

On the **Servers** page you can view and manage your protected servers.

The sections below tell you about the servers list and also how to:

- Add a server.
- View full details of a server and manage it.
• Export the list.

About the servers list

The servers list shows you the current servers with these details:

• **Name.**
• **IP.** Hover over the icon to see details of all IPv4 and IPv6 addresses.
• **OS.** "Sophos Security VM" indicates a host where Sophos protects the guest VMs.
• **Last Active.** This is the last time that the server contacted Sophos.
• **Group.** The group that the server belongs to (if it belongs to one).
• **Lockdown status.** This shows whether Sophos Lockdown has been installed to prevent unauthorized changes on the server:
  — "Locked Down" shows that Sophos Lockdown has been installed.
  — "Not installed" shows that Sophos Lockdown is not installed. Click **Lock Down** to install it and lock the server.

To search for a server, enter the name in the search field above the list.

To display different types of server, or servers with a specific health status, use the filters above the list.

For example, the **Sophos Security VMs** filter displays instances of Sophos Security VM on a hypervisor.

Add a server

To add a server (that is to protect and manage a server, so that it appears in the list), click **Add Server** in the upper right of the page.

This takes you to the **Protect Devices** page, where you can download the installers you need to protect your servers. For help with the server installers, see **Server Protection**.

View full details of a server

For details of a server, click on its entry in the list to open the server details. You can then view full details of the server, and also update, scan, lock, unlock or delete it.

Export to CSV

To export a list of servers:

Click on **Export to CSV**.

This creates a file called servers.csv. Any currently active filters are applied to the list.

For example you can export a list of Windows servers with a bad health status by applying the **Windows servers** and **Servers with a bad status** filters before clicking **Export to CSV**.

**Related concepts**

**Server Summary** (page 80)
The Summary tab in a server's details page lets you see server details.

Server Protection (page 170)
You install a Server Protection agent on servers to protect them against malware, risky file types and websites, and malicious network traffic.

Server Summary
The Summary tab in a server's details page lets you see server details.
You can manage the server from here.
The sections you see depend on your license and the features you've set up.

Security status
In the left-hand pane, you can see the security status and take actions.

Note
The left-hand pane is always shown, even when you click the other tabs on this page.

If you see "Sophos Security VM" under the server name, the server is a host with a Sophos security VM installed. You'll also see additional information in the "Device Status" summary.

Actions you can take
The actions links and buttons are in the left-hand pane.

Restriction
Some actions are only available for Windows servers.

- Isolate: This isolates the server from the network.
- Delete: Deletes the server from Sophos Central.

Warning
You should uninstall the Sophos software before deleting a server.

- Scan Now: Scans the server immediately.
  The scan may take some time. When complete, you can see a "Scan 'Scan my computer' completed" event and any successful cleanup events on the Logs & Reports > Events page. You can see alerts about unsuccessful cleanup on the Alerts page.
  If the server is offline, it will be scanned when it is back online. If a computer scan is already running, the new scan request will be ignored and the earlier scan will carry on.
- Lock Down: Prevents unauthorized software from running on the server.
  This option makes a list of the software already installed on the server, checks that it is safe, and allows only that software to run in future.
  If you need to make changes on the server later, either unlock it or use the Server Lockdown preferences in the server policy.
• **Unlock**: Unlocks the server. This button is available if you have previously locked down the server.

• **Diagnose**: Runs the Sophos Diagnostic Utility.

• **Live Response (Beta)**: Enables you to connect to the server to investigate and remediate possible security issues.

### Live Response (Beta)

This option is available only if you are a Super Admin and you've signed in using multi-factor authentication. **Allow Live Response connections to servers** must also be turned on in **Global Settings**: see Live Response for devices.

This enables you to connect to the server to investigate and remediate possible security issues. You might want to do this if an infection or suspicious activity is identified on the server. You can connect to the server even if it's isolated. To connect to the server, do as follows:

1. Click **Live Response (Beta)**.
2. In **Session purpose**, summarize the purpose of your session.
3. Click **Start**.
   A connection to the server is opened in another browser tab. The tab shows a terminal window.
4. At the command prompt, type commands to perform your investigation or remediation.
   Use DOS, UNIX, or Linux commands depending on the computer to which you've connected.
5. When you finish, click **End Session**.
   The connection is closed, although the tab remains open. You can browse elsewhere in Sophos Central from here.

   The connection is also closed in the following cases:
   - You close the tab.
   - You refresh the tab.
   - You browse elsewhere in Sophos Central from here.
   - There is no activity for 30 minutes.

To see which Live Response sessions have started or ended, view the Sophos Central audit log.

### Recent Events

This lists recent events on the server.

For a full list, click the **Events** tab.

### Agent Summary

The summary shows the following details.

**Restriction**
Some details are only available for Windows servers.

• **Last Sophos Central Activity**: The last time the server communicated with Sophos Central.
Sophos Central Admin

- **Last Agent Update**: The last time the Sophos agent was updated. **Update Now** updates the Sophos agent.

- **Agent Version**: The version number of the Sophos agent.

- **Assigned Products**: Shows the Sophos products installed (for example, Intercept X). Shows the license and the version number for each installed product.

- **Installed component versions**: Click this to see a full list of the Sophos components and their version numbers.

- **IPv4 Address**

- **IPv6 Address**

- **Operating System**: If this is shown as "Sophos Security VM", the server is a host with a Sophos security VM installed.

- **Lockdown Status**: Shows the status of Server Lockdown, which prevents unauthorized software from running on servers.

- **Group**: Shows the group the server belongs to (if any). **Change group** lets you add it to a group, move it to a different group, or remove it from its current group. A server can only be in one group.

- **Connected Guest VMs**: You see this only if the server is a host with a Sophos Security VM. It shows the number of guest VMs connected to the Security VM. Click the number to see a list of the guest VMs.
  - If no guest VMs are powered on, or if you’re still installing agents on them, you may see zero guest VMs.
  - If you have enabled guest VMs to migrate between Security VMs, this can affect the number of guest VMs connected.
  - Usually, a connected guest VM is protected. However, if the agent is newly installed, or there is a problem, scanning for threats may not have started yet.

- **Tamper Protection**: This shows whether Tamper Protection is enabled on the server or not. Click **Disable Tamper Protection** to manage the tamper protection password for the server.

**Update Cache and Message Relay Status**

If you’re using update caches or message relays on your network, you see this status information.

If the server is being used as an update cache or a message relay, you see:

- The status of the cache and when the last update was made. It also shows how many computers are using it as a cache.
- The status of the relay and how many computers are using it.

Alternatively, if the server is getting its updates from a cache (or using a relay) that's been set up elsewhere, you see details of where that cache or relay is.

**Windows Firewall**

Windows Firewall is active and being managed on the computer. It also shows:

- Whether Windows Group Policy is being used.
- The active network profiles.
- If other registered firewalls are installed and active.
Sophos Central Admin

Related concepts
Tamper Protection (page 102)
Manage Update Caches and Message Relays (page 128)
Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos.

Related tasks
Live Response for devices (page 144)
Turn on Live Response so that you can connect to devices to investigate and remediate possible security issues.
Recover deleted devices (page 87)
You can recover devices that you’ve deleted from Sophos Central if they are synced using Active Directory synchronization.

Server Events

The Events tab in a server’s details page lets you see events detected on the server.

You can see details and, in some cases, take action to prevent unwanted detections.

On this tab, you can also see details of events on guest VMs (if you're using Sophos for Virtual Environments).

Stop detecting an application

If an application is reported as malware but you know it's safe, you can allow it from the events list.

For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the Details link beside the event and then allow the application.

Note
This currently applies only to malware events reported by Intercept X.

Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again.

This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again and select an option:
   - Exclude this Detection ID from checking: prevents this detection on this app.
   - Exclude this application from checking: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.

3. Click Exclude.

   We’ll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.
Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again**.
   - Select **Exclude this Detection ID from checking**. This prevents this detection on this app.
3. Click **Exclude**.
   We’ll add your exclusion to the Global Exclusions list.

Events on guest VMs

If the server is a Sophos security VM, click **See all events** (on the right of the page) to change to a view where you can see which guest VM the event occurred on.

If you have enabled guest VMs to migrate between Security VMs, a threat detection might remain in the events list here even if the guest VM has migrated and the threat has been cleaned up elsewhere.

**Related concepts**
- Allowed applications (page 130)

**Related information**
- How to investigate and resolve a potential False Positive or Incorrect Detection

Server Status

The **Status** tab in a server’s details page lets you see the server’s security health and details of any alerts.

It also lets you take action against alerts.

Security Health

**Note**
These status details are only shown if the server is using the Security Heartbeat feature.

This shows whether the device has threats detected, has out-of-date software, is not compliant with policy, or is not properly protected. The overall status is the same as that for the highest-priority item listed (red, orange or green).

This section also shows which Sophos services are running on the server.

Alerts

The page lists any alerts on the device. The details include:
- Alert details: For example, the name of the malware.
• When the alert occurred.
• The actions that you can take. These depend on the type of threat or event and are the same as the actions available in the Dashboard.

Create forensic snapshot

You can create a "forensic snapshot" of data from the device.

This gets data from a Sophos log of the device's activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

You'll need a converter (which we provide) to read the data (see Convert a forensic snapshot).

Note
You can choose how much data you want in snapshots and where to upload them. To do this, go to Global Settings > Forensic Snapshots. These options may not be available for all customers yet.

To create a snapshot:
1. Go to a threat case’s Analyze tab.
   Alternatively, on the details page of the device, open the Status tab.
2. Click Create forensic snapshot.
3. Follow the steps in Upload a forensic snapshot to an AWS S3 bucket.

You can find the snapshots you generated in %PROGRAMDATA%\Sophos\Endpoint Defense\Data\Forensic Snapshots.

Snapshots generated from detections are in %PROGRAMDATA%\Sophos\Endpoint Defense\Data\Saved Data.\n
Note
You need to be an administrator with access to the tamper protection password and run a command prompt as an administrator to access the saved snapshots.

Related concepts
Forensic snapshots (page 138)
Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

Alerts (page 4)
The Alerts page lists all the alerts that require your action.

Related tasks
Convert a forensic snapshot (page 139)
Use the SDR Exporter tool to convert forensic snapshots so you can run queries on them.

Related information
Upload a forensic snapshot to an AWS S3 bucket (page 140)
Follow these instructions to upload a forensic snapshot.

**Server Exclusions**

The **Exclusions** tab in a server's details page lets you see a list of files or applications excluded from scanning for threats.

By default, Sophos Central automatically uses vendor-recommended exclusions for certain widely-used applications. You can also set up your own exclusions in your policy.

**Note**

Some automatic exclusions shown in the list might not work on servers running Windows Server 2003.

**Related concepts**

Server Threat Protection Policy (page 335)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

**Server Applications**

The **Applications** tab on a server's details page lets you see a list of applications installed on the server.

You can search the installed applications.

**Server Lockdown Events**

The **Lockdown Events** tab in a server's details page lets you see "events" in which Server Lockdown blocked unauthorized activity on the server.

Examples of such events are: a user trying to run an unauthorized program on the server, an unknown updater trying to update files, or a user trying to modify files with a program that isn't authorized for the purpose.

The tab is displayed only for servers that you have locked down.

To see the report, click **Update Report**. This creates a report on events in the previous twenty-four hours.

The list shows:

- The event type.
- When each event happened.
- The Parent. This is the program, script or parent process that was active.
- The Target. This is the file or program that was the target of the activity.

**Server Policies**

The **Policies** tab in a server's details page lets you see the policies that are applied to the server.

The **Type** column indicates the security settings (such as threat protection) included in each policy.

You can view and edit policy details by clicking the policy in the table.
Note
Editing the policy affects all servers to which this policy is applied.

3.6.4 Recover deleted devices

You can recover devices that you’ve deleted from Sophos Central if they are synced using Active Directory synchronization.

When the devices reappear in Sophos Central as a result of Active Directory synchronization, they no longer report to, or communicate with, Sophos Central. To reconnect them, do as follows:

1. Go to Logs & Reports > Recover Tamper Protection passwords.

   ![Recover Tamper Protection passwords](image)

   The report shows devices that have been deleted in the last 60 days.

2. For each device, re-install the Sophos Central endpoint software.

3.6.5 How to find out a file's SHA-256 hash

You may need a file's SHA-256 hash to confirm that the file hasn't changed.

This can be useful when you work with Sophos Support to investigate an infection or potential false positive. It is also an easy way to confirm that a file hasn’t been changed or corrupted after sharing it by email, FTP, and so on. Any changes cause the hash to change.

If the file has not been detected by Sophos, you can use the Sophos Endpoint Self Help tool, which is installed on every Sophos Central endpoint.

If the file has been detected by Sophos, use the event details in Sophos Central, as follows:

1. On the Computers page or the Servers page, find the device on which the file has been detected and click the device name.

2. Click Events.

3. Find the detection event (not the cleanup event).

   • If there is a Details link next to the event, click it to show Event details. Here you can see the SHA-256 hash.

   ![Event details](image)

   • Otherwise, check if a threat case has been created for the detection. This shows the SHA-256 hash of any processes involved.

If you cannot find the hash or have any questions, contact Sophos Support.

Related concepts

Threat Cases (page 19)
Threat cases let you investigate and clean up malware attacks.

Related information

Sophos Endpoint Self Help: File Info
3.7 Global Settings

The **Global Settings** pages are used to specify security settings that apply to all your users and devices.

The pages displayed depend on the features included in your license.

*Note*
If you want to apply settings only to certain users, use the **Policies** pages instead.

3.7.1 Active Directory Sync

You can import users and user groups from Active Directory to Sophos Central.

In Settings, on the **Active Directory Sync** page, you can select the Active Directory service you want to use.

- There is a download link for the Sophos Central Active Directory synchronization utility.
- In **Endpoint Protection** and **Email Gateway** you can use Azure Active Directory synchronization instead.

*Note*
If you are using Office 365 you must use Azure Active Directory synchronization.

For instructions on setting up the utility, see the Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

For instructions on configuring Azure Active Directory synchronization, see the Azure Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

*Note*
Azure Active Directory synchronization does not support Azure Active Directories that contain data migrated from on-premise Active Directories.

*Note*
Sophos Azure Active Directory synchronization can be used with Sophos Endpoint Protection and Sophos Email. It has not been tested with other Sophos products.

**Related concepts**

**Active Directory Sync Status** (page 89)
On the **Active Directory Sync** page, you can check the sync status and download the installer.

**Azure AD Sync Status** (page 91)
Monitor your Azure Active Directory (AD) synchronization.

**About Active Directory synchronization** (page 89)
Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

**Related tasks**

Set up synchronization with Active Directory (page 89)
Follow these instructions to set up synchronization with Active Directory.

Set up synchronization with Azure Active Directory (page 92)
Follow these instructions to synchronize with Azure Active Directory.

**Related information**

Join your work device to your organization's network

---

**Active Directory Sync Status**

On the Active Directory Sync page, you can check the sync status and download the installer.

You need to set up Active Directory synchronization before you can see these options.

You can download the latest installer for setting up synchronization with Active Directory.

**Sync status**

This shows your synchronization status and the synchronization settings in Active Directory.

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The time of the last synchronization with Active Directory.
- The number of users and groups imported from Active Directory.

You can view Active Directory synchronization alerts on the Overview > Alerts page. You can view synchronization events on the Overview > Logs & Reports > Events page.

**About Active Directory synchronization**

Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

To synchronize with Active Directory, you need to download and install the Sophos Central Active Directory Sync utility. The utility works as follows.

It synchronizes active users and user groups.

It can run automatically on a regular basis, as set up by the Sophos Central administrator.

It doesn't duplicate existing users or groups when they are matched to an existing Sophos Central user or group. For example, an email address from Active Directory may be added to an existing user in Sophos Central.

It supports only the Active Directory service.

It can synchronize multiple Active Directory forests. To do this, you need to install the utility on multiple machines and configure each utility to synchronize a different Active Directory forest. We strongly recommend to synchronize different Active Directory forests at different times of day, so that the synchronizations do not overlap.

It doesn't help you to deploy the Sophos agent software to your users' devices. Use other methods of deployment with Active Directory.

Set up synchronization with Active Directory
Follow these instructions to set up synchronization with Active Directory.

Before you can set up synchronization, you need .NET Framework 4 on the computer where you will run the Sophos Central AD Sync Utility.
Warning
Before you proceed, make sure all your active directory users are set up correctly with an email address. Users without an email address aren't protected and email going to an email address not tied to a user isn't delivered.

You need to use API credentials to synchronize with Active Directory.

To set up synchronization with Active Directory:
1. Set up your API credentials for AD sync. To do this, click Settings > API credentials.
2. Add a new credential. Enter the following information:
   - Credential name
   - Description
3. Copy the Client ID and Client Secret.
4. Click Settings > Active Directory Sync, and click the link to download the Sophos Central AD Synchronization Utility installer. Then run it.
   Alternatively, go to the Start menu and click Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.
   The Sophos Central AD Sync Utility Setup assistant starts.
5. In the setup wizard, enter the information required.
   Follow the instructions in the Sophos Central AD Sync Utility Setup assistant.
6. On the last page of the setup assistant, select Launch Sophos Central AD Sync Utility and click Finish.
7. In the Active Directory Synchronization Setup utility, on the Sophos Credentials page, enter your Client ID and Client Secret instead of your Sophos Central account credentials.
8. On the AD Configuration page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.
   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the Use LDAP over an SSL connection (recommended) checkbox selected. If your LDAP environment doesn’t support SSL, clear the Use LDAP over an SSL connection (recommended) checkbox and change the port number. The port number is usually 636 for SSL connections and 389 for insecure connections.
9. If you don’t want to synchronize the entire forest, on the AD Filters page, you can specify which domains to include in the synchronization. You can also specify additional search options (search bases and LDAP query filters) for each domain. Distinct options can be specified for users and user groups.

Note
AD Sync will only create groups that have members which include discovered users or devices, regardless of group filter settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search bases</td>
<td>You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format:</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| OU=Finance,DC=myCompany,DC=com | To filter users, for example, by group membership, you can define a user query filter in this format:  
memberOf=CN=testGroup, DC=myCompany, DC=com  
The above query limits user discovery to users belonging to "testGroup". Note that if you don't specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to "testGroup", you could define the following group query filter:  
CN=testGroup |

**Note**  
If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

10. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.

**Note**  
A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select **Never. Only sync when manually initiated.**
11. Click **Finished**.
12. To synchronize immediately, in the AD Sync Utility, click **Preview and Sync**. Review the changes that will be made during the synchronization. If you are happy with the changes, click **Approve Changes and Continue**.

The Active Directory users and groups are imported from the Active Directory to Sophos Central.
To stop the synchronization in progress, click **Stop**.

**Azure AD Sync Status**

Monitor your Azure Active Directory (AD) synchronization.

In Settings, on the **Azure Sync Settings/Status** page, once you configure Azure Active Directory synchronization, you can view:

- The status of Azure Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Azure Active Directory.
• The time of the last synchronization with Azure Active Directory.

Note
Auto synchronization happens every 6 hours. You cannot change this interval.

• The configuration settings for Azure Active Directory synchronization.

You can amend these by selecting Edit. See Set up synchronization with Azure Active Directory.

Select Sync to run the synchronization process.

You can validate the Azure Active Directory synchronization connection by selecting Test Connection.

You can view Azure Active Directory synchronization alerts on the Alerts page. You can view synchronization events on the Logs & Reports > Events page.

Related tasks
Set up synchronization with Azure Active Directory (page 92)

Follow these instructions to synchronize with Azure Active Directory.

You need:
• A Microsoft Azure subscription.
• Azure Active Directory.

CAUTION
You can use either Azure Active Directory synchronization or Active Directory Sync. You can’t set up Azure Active Directory synchronization if you are already using Active Directory Sync.

To configure Azure Active Directory synchronization:

1. Set up your Azure applications. To do this follow the instructions in Prerequisites to access the Azure Active Directory reporting API and the instructions in the next two steps.

2. In To register an Azure AD application, do as follows:
   a) Enter a Name.
   b) Enter https://central.sophos.com in Redirect URI.

3. In Get your application’s client secret, do as follows:
   a) Enter a description and expiry date.
   b) Make a note of your Client secret and Secret expiration date.
   c) Make a note of your Application (client) ID and Primary Domain.

4. In Sophos Central, in the left-hand pane, select Settings.

5. On the Settings page, under Administration, select Azure AD Sync Settings/Status.


7. In the Edit Azure AD Sync dialog box, enter the following information, which you obtained when you set up your Azure applications:
   • Client ID
   • Tenant Domain
- **Application Key** (client secret)
- **Application Key Expiration**
  
  You do not have to set the expiration date. We recommend that you do enter it so that Sophos Central can send you notifications of when your key is about to expire.

8. Select **Test Connection** to validate the Azure Sync connection.
9. Select **Save**.
10. On the next menu, select **Sync** to import users.
    
    Synchronization starts. This process may take some time.

**Related information**

Prerequisites to access the Azure Active Directory reporting API

### 3.7.2 Role Management

You can use pre-defined administration roles to divide up security tasks according to the administrators’ responsibility level.

In **Settings**, the **Role Management** page shows a list of administration roles and the number of users assigned to each role.

You can only see this option if you are a Super Admin administrator.

Click on a role name to see a detailed description of the role and the names of the people that have that role assigned to them. You can manage the people assigned to a specific role in that role’s page.

**Restriction**

An administrator role affects what a user can do.

**Administration Roles**

Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

Predefined roles cannot be edited or deleted.

Your assigned administrator role affects what you can do.

A Super Admin can add custom roles. These roles are based on the predefined roles but you can restrict the access for a custom role to a specific product.

**Restriction**

You can add custom roles only if you are signed up to the Sophos Early Access Program.

**Super Admin**

Administrators with this role have access to everything in Sophos Central.

They can manage roles and role assignments. In addition, they can create, edit, assign, and delete custom roles.

There must be at least one administrator with the Super Admin role.
Admin

Administrators with this role have access to everything in Sophos Central. They can't manage roles and role assignments.

Help Desk

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

- Look at sensitive logs or reports.
- Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.
- Update the Sophos agent software on a computer.
- Scan computers.
- Modify co-branding.

They can't see role management options. Also they can't see some options, such as Edit buttons.

Read-only

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

- Look at sensitive logs or reports.
- Receive alerts.

They can't see role management options. Also they can't see some options, such as Edit buttons.

User

Administrators with this role have no administration capabilities. They have access only to the Self Service Portal.

Related concepts

Administration Roles for Intercept X with EDR (page 95)
Administrators can do more if they have Intercept X with EDR.

User Summary (page 56)

Related tasks

Create an Enterprise Admin (page 629)
Remove administrators (page 99)
You can remove administrators. Removing an administration role from a user does not delete the user.

Add a custom role (page 97)
You can add custom roles if you are a Super Admin.

Delete custom role (page 99)
You can delete custom roles if you are a Super Admin.

Administration role details
If you click a role on the Role Management page, its details are shown on a separate page.

The sections on that page include the following.

Permissions
This is the access level for a role. The options are Full, Help Desk, or Read-only.

Global Settings
These are the specialized capabilities for a role. The settings are:

- **Access sensitive logs & reports**: This option means that an administrator can view sensitive logs and reports; for example the Audit Logs.
- **Access policy management**: This option means that an administrator can change policy settings.
- **Access policy assignment**: This option means that an administrator can assign policies to users and devices.

Role Members
This is a list of the administrators that are assigned to the role. Click on a name to see their full details.

Administration Roles for Intercept X with EDR
Administrators can do more if they have Intercept X with EDR.

Super Admin and Admin
Administrators with these roles can also:

- View the intelligence report.
- Request the intelligence report
- Add items to the “Clean and Block” list.
- Remove items from the “Clean and Block” list.
- View blocked items.
- Request an on-demand threat case.
- View on-demand threat cases.
- Isolate and un-isolate devices.
- Request a forensic snapshot.
- Request a threat search.
- View a saved threat search.
**Help Desk**

Administrators with this role can also:
- View the intelligence report.
- Request the intelligence report.
- View blocked items.
- Request an on-demand threat case.
- View on-demand threat cases.
- Request a forensic snapshot.
- Request a threat search.
- View a saved threat search.

**Read-only**

Administrators with this role can also:
- View the intelligence report.
- View blocked items.
- View on-demand threat cases.
- View a saved threat search.

**Related concepts**

Administration Roles (page 93)
Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

**Add administrators**

You assign administration roles to users using the **Available Users** list.

Existing administration roles, if any, are indicated next to the user's name.

A user can only have one assigned role.

For example if you add a Read-only administrator to the list of Help Desk administrators their assigned role will change to Help Desk administrator. They will no longer be a Read-only administrator.

To add an administrator:

1. In **Settings**, on the **Role Management** page, select the administrator role that you want to assign.
2. On the role details page, next to **Role Members**, click **Edit**.

   **Note**
   You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, select a user in the **Available Users** list and use the picker arrows to add them to the **Assigned Users** list for the role. Select **Save**.
Tip
Enter a name or part of a name in the search box to filter the list of available users.

Add a custom role
You can add custom roles if you are a Super Admin.

Custom roles are based on the predefined roles. You can restrict the access for a custom role to a specific product. You can also create a role that allows an administrator to have full access to one product and read-only access to a second product.

Restriction
If a role doesn’t have access to both Endpoint Protection and Server Protection (in some cases Encryption as well), the shared settings are read-only.

The shared settings are:
- Tamper protection
- Allowed applications
- Website management
- Proxy configuration
- Blocked item
- Bandwidth usage (Encryption access required)
- HTTPS updating
- DLP rules
- Manage content control list
- Reject network connections
- EDR threat analysis center

To create a custom role:
1. In Settings, on the Role Management page, select Add role.
2. Give the custom role a name and a description.
3. Select the Base role you want to use as the basis for the custom role.
   For example, if you choose Help Desk as the Base role, administrators with the custom role have Help Desk permissions.
4. Choose the product and access type you want the role to have.
   For example, you create a custom role called Endpoint Help Desk. This custom role uses Read-only as its Base role and Endpoint Protection as its selected product with an access type of Help Desk.
   This custom role allows any administrators assigned to this role to access Endpoint Protection with Help Desk permissions.
   a) Choose more than one product, if required.
      You can choose different access types for different products.
      For example you can create a custom role that has Help Desk access permissions for Endpoint Protection and Read-only access for Mobile. You can set the permissions for
all other products to **None**. This means that the custom role only has access to **Endpoint Protection** with **Help Desk** permissions and **Mobile** with **Read-only** permissions.

5. Choose the additional access and management options for the custom role.

- **Enable access to logs & reports.**
- **Enable policy management (add, edit, and delete).**
- **Enable policy assignment to users, device, etc..** (turn policies on and off; and add users, user groups, devices and device groups to existing policies).

For example, this allows a Super Admin to add these permissions to a Read-only or Help Desk role. You can also use these options to reduce the permissions for an Admin role. For example, you could prevent the custom role from managing policies.

**Note**

These additional options only apply to the selected products for the custom role.

The additional options are the same for all products and access types for the custom role.

6. Select **Save**.

You can now assign this role to administrators.

**Related concepts**

- **Administration Roles** (page 93)
  Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

- **Related tasks**
  - **Change roles** (page 98)
    You can change the assigned roles for administrators if you are a Super Admin.
  - **Delete custom role** (page 99)
    You can delete custom roles if you are a Super Admin.

**Change roles**

You can change the assigned roles for administrators if you are a Super Admin.

You can change roles for multiple administrators at the same time.

**Restriction**

You can't change roles for administrators who are currently signed in.

To change roles:

1. In **Settings**, on the **Role Management** page, select the administrator role that you want to assign to other administrators. For example, select a read-only administrator role if you want to assign that role to other administrators.

2. On the role details page, next to **Role Members**, click **Edit**.

**Note**

You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, add users from the **Available Users** list or remove users from the **Assigned Users** list. Select **Save**.
Tip
Enter a name or part of a name in the search box to filter the list of available users.

Delete custom role
You can delete custom roles if you are a Super Admin.
You can only delete custom roles. You can't delete roles that have administrators assigned to them.
You must change their role first.
1. In Settings, on the Role Management page, select the role you want to remove and select Delete.
   To select a role, click anywhere in the row apart from the name.
2. Select Delete to confirm role deletion.

Related concepts
Administration Roles (page 93)
Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

Related tasks
Add a custom role (page 97)
You can add custom roles if you are a Super Admin.
Remove administrators (page 99)
You can remove administrators. Removing an administration role from a user does not delete the user.
Change roles (page 98)
You can change the assigned roles for administrators if you are a Super Admin.

Remove administrators
You can remove administrators. Removing an administration role from a user does not delete the user.

Note
You cannot delete a user who has an assigned administration role. You must remove the role from the user before deleting the user.

To delete administrators:
1. In Settings, on the Role Management page, select the administrator role from which you want to remove users.
2. On the role details page, next to Role Members, click Edit.

   Note
   You can only see this option if you are a Super Admin.

3. In Edit Role Members, select a user in the Assigned Users list and use the picker arrows to remove them.
**Tip**
Enter a name or part of a name in the search box to filter the list of assigned users.

**Related concepts**
*Administration Roles* (page 93)
Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

### 3.7.3 Federated sign-in

You can allow your administrators and users to sign in to Sophos Central and the Self-Service Portal (SSP) using their Sophos Central Admin sign-in credentials, their Microsoft sign-in credentials, or both. Turning on federated sign-in in Sophos Central Admin also turns it on in the SSP.

**Note**
Sophos Central is not supported on mobile devices.

You can also add custom sign-in rules for specific administrators.

**Using Microsoft credentials to sign in**

Before an administrator or user can sign in using their Microsoft credentials, the following must happen:

- **An Azure AD administrator must grant consent (permission) to use the credentials stored in your organization's Azure AD tenant to sign in to Sophos Central.**
  
  This consent applies to Sophos Central Admin, Sophos Central Enterprise, and the SSP.
  
  Once an Azure AD administrator gives consent, it means your Azure AD tenant trusts Sophos Central and your administrators and users can sign in with their Microsoft credentials.

- You need to turn on federated sign-in. You need to choose which credentials your administrators and users use to sign in.

If you want to allow your administrators and users to use their Microsoft credentials only to sign in, you also need to know the following:

- **What happens if you change to using Sophos Central Admin sign-in credentials only?**
  
  Administrators and users won't have a password set up to validate against. They need to use “Reset Password” to set a new password and then sign in.

- **Can administrators and users reset their passwords if you turn on Sign in with Microsoft credentials only?**
  
  No, they won't receive reset password emails.

**Note**
Your administrators and users can sign in using their Microsoft credentials if the email address associated with their Sophos Central Admin credentials matches their Microsoft sign-in credentials.
Sophos Central Enterprise administrators and federated sign-in

Note
If an administrator is also an Enterprise admin they can’t use the same Microsoft sign-in credentials to sign in to both consoles.

If you create an Enterprise admin from an existing Sophos Central Admin account the federated sign-in credentials and settings for that account are used for the Sophos Central Enterprise account.

Related tasks
Turn on federated sign-in (page 101)
Follow these instructions to turn on federated sign-in and choose how your administrators and users can sign in.

Related information
Understanding Azure AD application consent experiences
Sophos Central Azure AD Federation
FAQ on Sophos Central Azure AD Federation

Turn on federated sign-in

Follow these instructions to turn on federated sign-in and choose how your administrators and users can sign in.

If you want your administrators and users to sign in using their Microsoft credentials, you must:

• Make sure you have an Azure Active Directory (AD) account with Microsoft. Azure AD is Microsoft’s cloud-based identity and access management service.

• Get consent and authorization from your Azure AD admin to use your company’s Azure AD with Sophos Central.

• Make sure you have a Sophos Central account that matches your Azure AD account (the emails must match).

• You must be a Super Admin to turn on federated sign-in.

To choose how your administrators and users sign in:

1. Click Federated Sign-in in Settings.
2. Make sure that an Azure AD admin has given consent for federated sign-in, if you want to allow users to sign in using their Microsoft credentials.

   Note
   If an Azure AD admin doesn’t give permission for Sophos Central to use federated sign-in before you turn on Sign in with Microsoft credentials only, federated sign-in will fail.

3. Choose how you want your administrators and users to sign in.
   If you choose Sign in with Microsoft credentials only you can send an email to newly-added users to tell them how to sign in.
4. Add custom sign-in rules for specific administrators, if required.
a) If you want your administrators to sign-in using their Microsoft credentials only, we recommend that you create a by-pass custom rule for one of the administrators. Click **Add Admins** to do this.

b) Allow them to sign in using either their Sophos Central Admin or Microsoft credentials.

5. Click **Save**.

### Related concepts

**Federated sign-in** (page 100)
You can allow your administrators and users to sign in to Sophos Central and the Self-Service Portal (SSP) using their Sophos Central Admin sign-in credentials, their Microsoft sign-in credentials, or both.

### 3.7.4 Synchronized Security

Synchronized Security monitors outbound mail, and takes action if 5 or more emails that are classified as spam, or contain viruses are sent from a mailbox within a 10 minute period.

**Note**
Synchronized Security is only available if you have a Sophos Endpoint license and a Sophos Email license.

You can turn the Synchronized Security feature on and off from **Settings > General > Synchronized Security**.

The blocking process works like this:

1. The originating mailbox is identified.
2. The owner of the mailbox is identified, along with any devices assigned to the owner of the mailbox.
3. The mailbox is blocked from sending emails for 1 hour. After 1 hour, the mailbox is unblocked automatically. You can't unblock it any sooner.

   Lockout periods increase every time the blocking process is triggered. The amount of time the mailbox is blocked for is doubled every time the spam threshold is reached. The previous block period needs to end before another can start. These timed blocks can't be removed and you have to let them expire.

   After 6 times, the mailbox will be blocked permanently, and the owner will not be able to send any email from that mailbox. If you believe a permanently blocked mailbox should be unblocked, please contact Sophos support.

4. Sophos Anti-Virus runs an on-demand scan on the devices linked to the mailbox.
5. An alert is sent to the administrator saying that the sender has been blocked.
6. The events report is updated to show that the mailbox has been blocked.

**Note**
If Synchronized Security is turned off, this will only disable the endpoint scan. The senders of outgoing spam and virus emails will still be blocked.

### 3.7.5 Tamper Protection

You can enable or disable tamper protection for all your servers and users' computers.
To do this, in **Settings**, open the **Tamper Protection** page.  

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:

- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
- Disable tamper protection.
- Uninstall the Sophos agent software.

### Manage tamper protection for a specific device

You can change the tamper protection settings for a specific device or server.  

Open the device's details page and look under **Tamper Protection**. There you can do as follows:

- View the password.
- Generate a new password.
- Temporarily disable tamper protection for that device.

### Recover tamper protection passwords

You can recover the tamper protection passwords of devices that you’ve recently deleted.  

You might need to do this so that you can uninstall Sophos software that is still on those devices.

### 3.7.6 API Token Management

You can generate and manage the API token used for secure access to the Security Information and Event Management (SIEM) Integration API. This enables you to pull new event and alert data from Sophos Central. For further information, click the knowledge base article link provided on the page.

To add a token:

1. In **Settings**, open the **API Token Management** page.
2. Click **Add Token**.
3. Give the token a name and click **Save**.  
   This generates the API token. The token is valid for a year.

Click **Renew** to extend the validity of the token.

Click **Delete** to remove the token.

### 3.7.7 API credentials

You can manage and add credentials for Sophos Central Admin.

**Note**

The first time you click **API credentials** you must read and accept the terms and conditions of use.

To add credentials, do the following:
1. Click **Add Credential** and give the credential details.
   This generates the credential, together with a **Client ID** and a **Client Secret**.
2. Copy the **Client ID** and **Client Secret**.

   **Note**
   You can only see the **Client Secret** once.

To delete an API credential, select it in **API credentials** and click **Delete**.

### 3.7.8 Website Management

**This page is not available if you do not have a Web Control or Web Gateway license.**

**Note**
If an option is locked, global settings have been applied by your partner or Enterprise administrator.

You can extend the website filtering provided by Sophos Central. For more information on how Sophos filters websites see [Sophos Web Security and Control Test Site](#).

In **Settings**, on the **Website Management** page, you can use a website list to:

- Control websites not in one of the Sophos categories.
- Tag websites to put them in groups, which are like custom categories. You can then use policies to control these websites for certain users.
- Override the Sophos category for a site. This changes that site’s category for all your users.

**Note**
If you think Sophos has put a website in the wrong category, you can ask us to change it. To do this, see Open a Support Case. We suggest you try this instead of overriding the category.

To add a site to the website list:

1. Click **Add** in the upper right of the page.
   The **Add Website Customization** dialog is displayed.
2. Enter sites.
   Entries in the website list can be single URLs, full domains, TLDs, IP addresses, CIDR ranges, or even top level domains.

   **Note**
   Managing websites using IP addresses only controls browser-based access. It does not block other applications or interact with rules for a local firewall.

3. Select **Enable Category Override** if you want to associate a specific category with the sites you have entered. Then select a **Category**.
4. Select **Enable Tags** to associate a tag with the sites you have entered. Then type a tag name.
   Tags can be used when creating web control policies for endpoint computers or servers. See the Log web control events section in Web Control Policy.
5. Enter text in the **Comments** text box.
   
   It can be helpful to include information about tags you have created and categories you have overridden for troubleshooting policy issues in the future.

6. Click **Save**.
   
   Your entry will be added to the website list.

   You can also edit entries in the list or delete them.

   To edit an entry, click the edit icon 🟢. The icon is on the right of the entry.

   To delete an entry, select the checkbox to the left of the entry and click **Delete**.

**Related information**

- [Open a Support Case](#)
- [Sophos Web Security and Control Test Site](#)

### 3.7.9 Registered Firewall Appliances

In **Settings**, on the **Registered Firewall Appliances** page, you can view Sophos XG Firewalls that have been registered with Sophos Central. You can also deregister (or "disconnect") them.

**Note**

You can only register a Sophos XG Firewall from a Sophos XG Firewall console (Go to **Central synchronization**).

**About registered Firewalls**

When a Sophos XG Firewall is registered with Sophos Central, your computers can send regular reports on their security status or "health" to Sophos XG Firewall. These reports are known as "Security Heartbeats".

If more than one Sophos XG Firewall is registered, computers send Security Heartbeats to the nearest one available.

If the Security Heartbeat reports show that a computer might have been compromised, the Sophos XG Firewall can restrict its network access. A Sophos XG Firewall admin and a Sophos Central administrator also receive alerts that tell them what to do to restore the computer's health.

**View Firewalls**

The page displays details of Sophos XG Firewalls that are registered with Sophos Central:

- **Name**
- **IP Address**
- **Active**. This indicates whether a Sophos XG Firewall has received Security Heartbeats within the previous hour.

To find a Sophos XG Firewall, start to enter the name in the **Search for a Firewall** field. As you type, the list is filtered to show only Sophos XG Firewalls that match.
Deregister Firewalls

You can deregister Sophos XG Firewalls from Sophos Central. For example, if you no longer use a Sophos XG Firewall, you could deregister it so that it is no longer shown here.

When you deregister a Sophos XG Firewall, you continue to protect and manage the computers that are associated with it, but the Security Heartbeats feature will no longer work.

1. Select a Sophos XG Firewall you want to deregister.
2. Click the **Delete** button in the upper-right of the page.
3. When prompted, click **OK** to confirm that you want to deregister a Sophos XG Firewall.

The selected Sophos XG Firewall is removed from the list. You can deregister more than one Sophos XG Firewall at a time.

If you deregister all the Sophos XG Firewalls, this page will still be displayed and you will still be able to see old events and alerts related to the Security Heartbeat feature.

### 3.7.10 User access

You can automatically give your users access to the Sophos Central Self Service Portal (SSP).

To do this go to **Settings > User Access**.

Turn on **Sophos Central Self Service Portal access**.

New users will now have access to the SSP when you add them to Sophos Central. They will receive an email with sign-in instructions.

Any existing users without access will also be given access and sent an email.

If you turn off automatic access, any users that have access at that point can still sign in to the SSP. Only users added after you turn it off won't have access.

### 3.7.11 Global Exclusions

You can exclude files, websites and applications from scanning for threats.

**Introduction**

You use exclusions to tune the detection behavior of Sophos Central.

**Related tasks**

- **Exploit Mitigation Exclusions** (page 117)
  You can exclude applications from protection against security exploits.

**Related reference**

- **Website exclusions** (page 116)
  You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

- **Process exclusions (Windows)** (page 116)
You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

**Malicious Network Traffic Prevention (IPS) (Windows) exclusions** (page 120)
You can exclude specific network traffic from inspection.

**Device isolation exclusions (Windows)** (page 117)
You can allow isolated devices to have limited communications with other devices.

**Windows Scanning Exclusions: Wildcards and Variables** (page 110)
When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

**macOS Scanning Exclusions** (page 112)
You can add scanning exclusions for macOS workstations.

**Virtual Server Scanning Exclusions: Wildcards** (page 114)
**Virtual Server** exclusions let you exclude items from scanning on Windows guest VMs that are protected by a Sophos security VM.

**Related information**
Sophos Threat Center

## Exclusions

Global exclusions apply to all your users (and their devices) and servers.

If you want exclusions to apply only to certain users or servers, use policy exclusions instead.

You can set up the following types of exclusion:

- Exclude files or folders from scanning.
  
  If you exclude files from scanning, we'll still check the excluded items for exploits.

- Exclude from checking any process that runs from an application.

- Exclude websites from checking.

- Exclude applications from protection against security exploits.

- Exclude applications that are normally detected as spyware and previously detected exploits from scanning and detection.

- Exclude previously detected malicious behavior exploits. This is only available if you are signed up to the Early Access Program.

You can also use exclusions to allow isolated devices to communicate with other devices under restrictions. This feature is available if you have Intercept X Advanced with EDR.

**Warning**
Think carefully before you add global exclusions because doing so may reduce your protection.

### Can’t edit the exclusions?

If an option is locked global settings have been applied by your partner or Enterprise administrator.
You can still stop detecting applications, exploits and ransomware from events.
Exploit exclusions

If you exclude files from scanning, we'll still check the excluded items for exploits. If you want exclusions from exploit checking, do as follows:

• To stop checking for an exploit that has been detected, use a Detected Exploits exclusion.
• To exclude certain applications from checking, use Exploit Mitigation Exclusions.
• To stop checking for a malicious behavior exploit that has been detected, use a Behavioral Protection exclusion.

Set up exclusions

You can exclude files, websites and applications from scanning for threats.

To set exclusions:
1. Go to Global Exclusions.
2. Click Add Exclusion.
   The Add Exclusion dialog is displayed.
3. In the Exclusion Type drop-down list select what you want to exclude.
4. Specify the item or items you want to exclude.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File or folder (Windows)</td>
<td>You can exclude a drive, folder or file by full path. You can use the wildcard * for file name or extension but <em>:</em> is not valid.</td>
</tr>
<tr>
<td>File or folder (Mac/Linux)</td>
<td>You can exclude a folder or file. You can use the wildcards ? and *.</td>
</tr>
<tr>
<td>File or folder (Sophos Security VM)</td>
<td>On Windows guest VMs protected by a Sophos security VM, you can exclude a drive, folder or file by full path. You can use the wildcards * and ? but only for file names.</td>
</tr>
<tr>
<td>Process (Windows)</td>
<td>You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process). If possible, enter the full path from the application.</td>
</tr>
<tr>
<td>Website (Windows/Mac)</td>
<td>You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.</td>
</tr>
<tr>
<td>Potentially Unwanted Application (Windows/Mac)</td>
<td>You can exclude applications that are normally detected as spyware. Specify the exclusion using the same name under which it was detected by the system.</td>
</tr>
<tr>
<td></td>
<td>Find more information about PUAs in the Sophos Threat Center.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Detected Exploits (Windows/Mac)</td>
<td>You can exclude any exploit that has already been detected. We'll no longer detect it for the affected application and no longer block the application.</td>
</tr>
<tr>
<td>Device isolation (Windows)</td>
<td>You can allow isolated devices to have limited communications with other devices. Choose whether isolated devices will use outbound or inbound communications, or both. You can then restrict communications.</td>
</tr>
<tr>
<td>Malicious Network Traffic Prevention (IPS) (Windows)</td>
<td>You can exclude specific network traffic from inspection. Choose whether to exclude outbound or inbound traffic. Then specify the address or ports the traffic uses.</td>
</tr>
<tr>
<td>Exploit Mitigation (Windows)</td>
<td>You can exclude applications from protection against security exploits. For example, you might want to exclude an application that is incorrectly detected as a threat until the problem has been resolved.</td>
</tr>
<tr>
<td>AMSI Protection (Windows)</td>
<td>You can exclude a drive, folder or file by full path. Code in this location is not scanned. You can use the wildcard * for file name or extension.</td>
</tr>
<tr>
<td>Behavioral Protection (Windows)</td>
<td>You can exclude applications from protection against behavioral exploits. For example, you might want to exclude an application that has been incorrectly detected as behaving maliciously. You can't edit these exclusions after you create them. This option is only available if you are signed up to the Early Access Program.</td>
</tr>
</tbody>
</table>

5. For File or folder exclusions, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.

6. Click **Add** or **Add Another**. The exclusion is added to the scanning exclusions list.

To edit an exclusion later, click its name in the exclusions list, enter new settings and click **Update**.
Windows Scanning Exclusions: Wildcards and Variables

When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

Note
Some wildcards or variables cannot be used for exclusions from real-time scanning on Windows XP or Windows Server 2003.

**Warning**
Scanning exclusions may significantly reduce your protection. Only use them if you understand the risks.

Wildcards

You can use the wildcards shown in this table.

Note
Only * and ? can be used on Windows XP and Windows Server 2003.

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>* (Star)</td>
<td>Zero or more of any character except \ or /</td>
<td></td>
</tr>
<tr>
<td>** (Star Star)</td>
<td>Zero or more characters including \ and /, when bracketed by \ or / characters or used at the start or end of an exclusion.</td>
<td>Any other use of a ** is treated as a single * and matches zero or more characters excluding \ and /. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• c:\foo**\bar matches: c:\foo\bar, c:\foo\more \bar, c:\foo\even\more \bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• **\bar matches c:\foo\bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• c:\foo** matches c:\foo more\bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• c:\foo**bar matches c:\foomorebar but NOT c:\foo\more\bar</td>
</tr>
<tr>
<td>\ (Backslash)</td>
<td>Either \ or /</td>
<td></td>
</tr>
<tr>
<td>/ (Forward slash)</td>
<td>Either / or \</td>
<td></td>
</tr>
<tr>
<td>? (Question mark)</td>
<td>One single character. If it is at the end of a string it can match zero characters.</td>
<td></td>
</tr>
</tbody>
</table>
### Token

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>. (Period)</td>
<td>A period OR the empty string at the end of a filename, if the pattern ends in a period and the filename does not have an extension.</td>
<td>Note that: • <em>.</em> matches all files • * matches all files without an extension • &quot;foo.&quot; matches &quot;foo&quot; and &quot;foo.&quot;</td>
</tr>
</tbody>
</table>

### Example wildcards

Here are some examples of the use of wildcards.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Interpreted as</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo</td>
<td>**\foo</td>
<td>Exclude any file named foo (in any location).</td>
</tr>
<tr>
<td>foo\bar</td>
<td>**\foo\bar</td>
<td>Exclude any file named bar in a folder named foo (in any location).</td>
</tr>
<tr>
<td>*.txt</td>
<td>***.txt</td>
<td>Exclude all files named *.txt (in any location).</td>
</tr>
<tr>
<td>D:\</td>
<td>D:\</td>
<td>Exclude the entire drive D: from scanning. Use with care. PE files (such as applications), including malware, will be able to run on this drive without detection.</td>
</tr>
<tr>
<td>C:\foo\</td>
<td>C:\foo\</td>
<td>All files and folders underneath C:foo, including C:\foo itself.</td>
</tr>
<tr>
<td>C:\foo*.txt</td>
<td>C:\foo*.txt</td>
<td>All files or folders contained in C:foo named *.txt.</td>
</tr>
</tbody>
</table>

### Variables for exclusions

You can use variables when you set up scanning exclusions. The table below shows the variables and examples of the locations they correspond to on each operating system.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Windows 7 and later</th>
<th>Windows XP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2008 and later</td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>$allusersprofile%</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users</td>
</tr>
<tr>
<td>$appdata%</td>
<td>C:\Users*\AppData \Roaming</td>
<td>C:\Documents and Settings*\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>$commonprogramfiles%</td>
<td>C:\Program Files\Common Files</td>
<td></td>
</tr>
<tr>
<td>$commonprogramfiles(x86)%</td>
<td>C:\Program Files (x86)\Common Files</td>
<td></td>
</tr>
<tr>
<td>$localappdata%</td>
<td>C:\Users*\AppData \Local</td>
<td>C:\Documents and Settings*\Local Settings\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>$programdata%</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users \Application Data</td>
</tr>
<tr>
<td>$programfiles%</td>
<td>C:\Program Files</td>
<td></td>
</tr>
<tr>
<td>$programfiles(x86)%</td>
<td>C:\Program Files (x86)</td>
<td></td>
</tr>
<tr>
<td>$systemdrive%</td>
<td>C:</td>
<td></td>
</tr>
<tr>
<td>$systemroot%</td>
<td>C:\Windows</td>
<td></td>
</tr>
<tr>
<td>$temp% or $tmp%</td>
<td>C:\Users*\AppData \Local\Temp</td>
<td>C:\Documents and Settings*\Local Settings\Temp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>$userprofile%</td>
<td>C:\Users*</td>
<td>C:\Documents and Settings*</td>
</tr>
<tr>
<td>$windir%</td>
<td>C:\Windows</td>
<td></td>
</tr>
</tbody>
</table>

**macOS Scanning Exclusions**

You can add scanning exclusions for macOS workstations.

When you add or edit an exclusion, you can type any POSIX path, whether it is a volume, folder, or file.
Example: /Volumes/excluded (Mac)

**CAUTION**
Think carefully before you add scanning exclusions because doing so may reduce your protection.

To specify which items are excluded, use the rules in the table below.

### Exclusion rules

<table>
<thead>
<tr>
<th>Token</th>
<th>Syntax to use</th>
<th>Item(s) to exclude</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td><strong>Suffix</strong> the exclusion with a slash</td>
<td>A folder and sub-folders recursively</td>
</tr>
<tr>
<td>//</td>
<td><strong>Suffix</strong> the exclusion with a double slash</td>
<td>A folder but not sub-folders</td>
</tr>
<tr>
<td>&lt;filename&gt;</td>
<td>Do not <strong>suffix</strong> the exclusion with a slash or double slash</td>
<td>A file</td>
</tr>
<tr>
<td>/</td>
<td><strong>Prefix</strong> the exclusion with a slash</td>
<td>A folder or file in a specific location</td>
</tr>
<tr>
<td>&lt;folder&gt;</td>
<td>Do not <strong>prefix</strong> the exclusion with a slash</td>
<td>A folder or file anywhere locally or on the network</td>
</tr>
<tr>
<td>&lt;file&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>Substitute an asterisk for the filename stem</td>
<td>A file whose name has a specific filename extension</td>
</tr>
</tbody>
</table>

### Examples

<table>
<thead>
<tr>
<th>Exclusion path</th>
<th>Item(s) that are excluded</th>
</tr>
</thead>
<tbody>
<tr>
<td>/myfolder/myapplication</td>
<td>The file myapplication in a specific folder</td>
</tr>
<tr>
<td>/myfolder/</td>
<td>All files in the folder myfolder in a specific location and sub-folders recursively</td>
</tr>
<tr>
<td>/myfolder//</td>
<td>All files in the folder myfolder in a specific location but not sub-folders</td>
</tr>
<tr>
<td>myfolder/myapplication</td>
<td>The file myapplication in any folder that is called myfolder locally or on the network</td>
</tr>
<tr>
<td>myfolder/</td>
<td>All files in any folder that is called myfolder, locally or on the network, and sub-folders recursively</td>
</tr>
<tr>
<td>myfolder//</td>
<td>All files in any folder that is called myfolder, locally or on the network, but not sub-folders</td>
</tr>
</tbody>
</table>
### Virtual Server Scanning Exclusions: Wildcards

**Virtual Server** exclusions let you exclude items from scanning on Windows guest VMs that are protected by a Sophos security VM.

**CAUTION**
Think carefully before you add scanning exclusions because doing so may reduce your protection.

You can exclude a drive, folder or file by full path, just as you can for other Windows computers. However, there are restrictions on specifying items without a full path and also on the use of wildcards. See the details below and the examples.

#### Items without a full path

You can specify a file without a full path, for example `<file>.com`. You must include the extension. The security VM will exclude any file with this name.

You cannot specify folders without a full path.

#### Wildcards

You can use the wildcards shown in this table.

**Note**
Only `*` and `?` can be used on Windows XP and Windows Server 2003.

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>*</code></td>
<td>Zero or more of any character except <code>\</code> or <code>/</code></td>
<td></td>
</tr>
</tbody>
</table>
** (Star Star)

Zero or more characters including \ and /, when bracketed by \ or / characters or used at the start or end of an exclusion.

Any other use of a ** is treated as a single * and matches zero or more characters excluding \ and /.

For example:

- `c:\foo\**\bar` matches: `c:\foo\bar, c:\foo\more \bar, c:\foo\even\more \bar`
- `**\bar` matches `c:\foo\bar`
- `c:\foo\**` matches `c:\foo\more\bar`
- `c:\foo\**\bar` matches `c:\foomorebar` but NOT `c:\foo\more\bar`

\ (Backslash)

Either \ or /

/ (Forward slash)

Either / or \

? (Question mark)

One single character. If it is at the end of a string it can match zero characters.

. (Period)

A period OR the empty string at the end of a filename, if the pattern ends in a period and the filename does not have an extension.

Note that:

- `.*` matches all files
- `*.` matches all files without an extension
- `"foo.\"` matches "foo" and "foo."

Exclusions that work

The expressions shown in this table are valid for Virtual Server exclusions.

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>D:</td>
<td>Excludes the entire drive.</td>
</tr>
<tr>
<td>C:\programdata\adobe\photoshop\</td>
<td>Excludes the folder (you must include the final slash).</td>
</tr>
<tr>
<td>C:\program files\program*.com</td>
<td>Excludes files with a .com extension in the specified folder.</td>
</tr>
<tr>
<td>file.com</td>
<td>Excludes files with this name in any location (full path not needed).</td>
</tr>
<tr>
<td>file.*</td>
<td>Excludes all files called &quot;file&quot;, with any extension, in all locations.</td>
</tr>
<tr>
<td>*.com</td>
<td>Excludes all files with a .com extension in all locations.</td>
</tr>
</tbody>
</table>
### Process exclusions (Windows)

You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

If possible, enter the full path from the application, not just the process name shown in Task Manager.

**Example:**

```plaintext
%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe
```

**Note**

To see all processes or other items that you need to exclude for an application, see the application vendor’s documentation.

**Note**

You can use wildcards and variables.

### Related reference

**Windows Scanning Exclusions: Wildcards and Variables** (page 110)

When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

### Website exclusions

You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

**Examples:**

- IP address: 192.168.0.1
- IP address range: 192.168.0.0/24
- The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range.

Thus /24 equals the netmask:

```
11111111.11111111.11111111.00000000
```

In our example, the range includes all IP addresses starting with 192.168.0.

- Domain: google.com

---

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.</td>
<td>Excludes all files in all locations.</td>
</tr>
<tr>
<td>C:\file???.docx</td>
<td>Excludes C:\file12.exe but not C:\file123.exe.</td>
</tr>
</tbody>
</table>
**Device isolation exclusions (Windows)**

You can allow isolated devices to have limited communications with other devices. You can choose whether isolated devices will use outbound or inbound communications, or both. Use the following settings to restrict communications:

- **Local Port**: Any device can use this port on isolated devices.
- **Remote Port**: Isolated devices can use this port on any device.
- **Remote Address**: Isolated devices can only communicate with the device with this IP.

**Example 1**

You want remote desktop access to an isolated device so that you can troubleshoot.

- In **Direction**, select **Inbound Connection**.
- In **Local Port**, enter the port number.

**Example 2**

You want to be able to go to an isolated device and download cleanup tools from a server.

- In **Direction**, select **Outbound Connection**.
- In **Remote Address**, enter the address of the server.

**Exploit Mitigation Exclusions**

You can exclude applications from protection against security exploits. For example, you might want to exclude an application that is incorrectly detected as a threat until the problem has been resolved.

**Note**

These applications are excluded from exploit protection for all your users and their devices.

**CAUTION**

Think carefully before you add exclusions because it reduces your protection.

To exclude an application:

1. Go to **Settings > Global Exclusions**.
2. Click **Add Exclusion** (upper right of the exclusions list).
3. In **Exclusion Type**, select **Exploit Mitigation (Windows)**. You see a list of **Protected Applications** found on your network.
4. Select an application you want to exclude.
5. If you don’t see the application you want, click **Application not listed?** You can then exclude an application by its file path. Optionally, use any of the variables.
6. Under Mitigations, you can:
- Turn off **Protect Application**. The application won’t be checked for any exploits.
- Keep **Protect Application** turned on and select the exploit types that you do or don’t want to check for.

6. Click **Add** or **Add Another**. The exclusion is added to the list on the **Global Exclusions** page.

To edit an exclusion later, click its name in the exclusions list, enter new settings, and click **Update**.

**Related reference**

**Exploit mitigation exclusions: variables** (page 118)

You can use variables when you exclude applications from checking for exploits.

**Exploit mitigation exclusions: variables**

You can use variables when you exclude applications from checking for exploits.

### Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td><strong>All available drives.</strong> For example, $\text{app.exe}$ excludes $\text{app.exe}$ on drive C:, drive D:, etc.</td>
</tr>
</tbody>
</table>
| $\text{admintools}$ | C:\Users\<user>\Administrative Tools  
C:\ProgramData\Microsoft\Windows \Start Menu\Programs\Administrative Tools  
CSIDL_COMMON_ADMINTOOLS |
| $\text{appdata}$ | C:\Users\<user>\AppData\Local  
C:\Users\<user>\AppData\Roaming  
CSIDL_COMMON_APPDATA  
FOLDERID_LocalAppDataLow |
| $\text{cache}$ | C:\Users\<user>\Cache  
C:\Users\<user>\AppData\Local \Microsoft\Windows\INetCache  
CSIDL_INTERNET_CACHE |
| $\text{clickonce}$ | C:\Users\<user>\AppData\Local\Apps \2.0\17NXGR82.QZW\OM7PJ9G.3YE \cust...app_234e |
| $\text{commonprogramfiles}$ | C:\Program Files (x86)\Common Files  
C:\Program Files\Common Files |
<table>
<thead>
<tr>
<th>Variable</th>
<th>Example</th>
</tr>
</thead>
</table>
| `$contacts` | C:\users\<user>\Contacts  
FOLDERID_Contacts |
| `$desktop`  | C:\Users\<user>\Desktop  
CSIDL_COMMON_DESKTOPDIRECTORY |
| `$downloads` | C:\Users\<user>\Downloads  
FOLDERID_Downloads |
| `$favorites` | C:\Users\<user>\Favorites |
| `$fonts`     | C:\Windows\Fonts  
C:\Users\<user>\Fonts  
CSIDL_FONTS |
| `$links`     | C:\Users\<user>\Links  
FOLDERID_Links |
| `$music`     | C:\Users\<user>\My Music |
| `$nethood`   | %USERPROFILE%\Appdata\Roaming  
\Microsoft\Windows\Network Shortcuts  
C:\Users\<user>\NetHood |
| `$personal`  | C:\Users\<user>\My Documents |
| `$pictures`  | C:\Users\<user>\My Pictures |
| `$printhood` | %USERPROFILE%\Appdata\Roaming  
\Microsoft\Windows\Printer Shortcuts  
C:\Users\<user>\PrintHood |
| `$profile`   | C:\Users\<user> |
| `$programfiles` | C:\Program Files (x86)  
C:\Program Files |
| `$programs`  | %USERPROFILE%\AppData\Roaming  
\Microsoft\Windows\Start Menu  
\Programs  
C:\Users\<user>\Programs  
CSIDL_COMMON_PROGRAMS |
<table>
<thead>
<tr>
<th>Variable</th>
<th>Example</th>
</tr>
</thead>
</table>
| $sendto   | %USERPROFILE%\AppData\Roaming \Microsoft\Windows\SendTo  
C:Users\<user>\SendTo |
| $startmenu| %USERPROFILE%\AppData\Roaming \Microsoft\Windows\Start Menu  
C:Users\<user>\StartMenu |
| $startup  | %USERPROFILE%\AppData\Roaming \Microsoft\Windows\Start Menu \Programs\Startup  
C:Users\<user>\Startup  
CSIDL_COMMON_STARTUP |
| $system32 | C:\Windows\system32  
C:\Windows\SysWOW64 |
| $temp     | C:\Windows\Temp  
%TEMP% |
| $templates| %USERPROFILE%\AppData\Roaming \Microsoft\Windows\Templates  
C:Users\<user>\Templates |
| $video    | C:Users\<user>\My Video |
| $windows  | C:\Windows  
CSIDL_WINDOWS |
| $winsxs   | C:Windows\winsxs\*\ |

**Malicious Network Traffic Prevention (IPS) (Windows) exclusions**

You can exclude specific network traffic from inspection.

You can choose whether the exclusion applies to outbound or inbound traffic, or to both.

Use the following settings to specify which traffic to exclude:

- **Remote address**: The address of another computer that traffic goes to or from.
- **Remote port**: The port that traffic goes to or from on other computers.
- **Local port**: The port that traffic goes to or from on the local computer.

You must set at least one of the address or port options.

**Example**

If you want to exclude traffic that comes from port 123 on any other computer:
• In **Direction**, select **Inbound Connection**.
• In **Using this remote port**, enter the port number 123.

### 3.7.12 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

**Set the bandwidth used**

In **Settings**, on the **Bandwidth Usage** page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.

This helps to ensure that updating does not cause computers to run slowly.

You can specify a custom bandwidth or unlimited bandwidth.

**Note**

This setting is for Windows computers only.

**Note**

This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos. To save bandwidth in this case, see [Manage Update Caches and Message Relays](page 128)

**Related concepts**

[Manage Update Caches and Message Relays](page 128)

Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos.

### 3.7.13 Encryption Recovery Key Search

You can get a device encryption recovery key by entering a volume or recovery identifier.

**Retrieve recovery key (Windows computers)**

If users are unable to log in to their encrypted computer, you can get a recovery key which is used to unlock the computer. There is a recovery key for each volume of a BitLocker protected computer. It is created and backed up in Sophos Central before the computer is encrypted.

**Note**

When Sophos Device Encryption is installed, existing BitLocker recovery keys are replaced automatically and can no longer be used.
Note
Even if a policy has been disabled and the computer's Device Encryption status is shown as "Unmanaged", you can get a recovery key if one is available.

To get the recovery key, go to **Computers**, select the computer you want to recover, and click **More > Retrieve Recovery Key**. If you cannot find the computer in the list, you need the recovery key identifier or the volume identifier and use it in the recovery wizard, as follows:

1. Tell the user to restart the computer and press the Esc key in the **BitLocker** logon screen.
2. Ask the user to provide you with the information displayed in the **BitLocker recovery** screen.
3. In Sophos Central, go to **Computers** and click **More > Retrieve Recovery Key**.
4. Enter at least five characters of the recovery key identifier or the volume identifier provided by the user.
5. Click **Show Key** to display the recovery key.

**Note**
If you enter a volume identifier, Sophos Central displays all available recovery keys for this volume. The latest recovery key is the top one.

6. Make sure that the user is authorized to access the encrypted device before you provide the recovery key.

**Note**
As soon as a recovery key is displayed to you as administrator, it is marked as used and will be replaced at the next synchronization.

7. Give the recovery key to the user.

The user can now unlock the computer. Users of computers running Windows 8 or later are prompted to create a new PIN or password. Instructions for creating the PIN or password are displayed automatically.

After the computer has been recovered, a new recovery key will be created and backed up in Sophos Central. The old one will be deleted from the computer.

**Retrieve recovery key (Macs)**

If users forget their login password, you can get a recovery key which is used to unlock the computer.

To get the recovery key, go to **Computers**, select the computer you want to recover, and click **More > Retrieve Recovery Key**. If you cannot find the computer in the list, you need the recovery key identifier or the volume identifier and use it in the recovery wizard, as follows:

1. Tell the user to switch on their computer and wait until the Recovery Key ID is displayed.

**Note**
The recovery key ID is displayed for a short time. To display it again, users must restart their computer.
2. Ask the user to tell you the Recovery Key ID.
3. In Sophos Central, go to Computers and click More > Retrieve Recovery Key.
4. Enter at least five characters of the recovery key identifier.
5. Click Show Key to display the recovery key.
6. Make sure that the user is authorized to access the encrypted device before you provide the recovery key.
7. Give the recovery key to the user.
   • For users imported from Active Directory, continue to step 8.
   • For all other users, go straight to step 10.
8. Reset the existing password in Active Directory. Then generate a preliminary password and give it to the user.
9. Tell the user to click Cancel in the Reset Password dialog and enter the preliminary password instead.
10. Tell the user to do as follows:
    • Create a new password.
    • Click Create New Keychain if prompted.

The user can access the computer again.

On endpoints running macOS 10.12 or earlier, a new recovery key is created and stored in Sophos Central. A recovery key can only be used once. If you need to recover a computer again later, you need to retrieve a new recovery key.

On endpoints running macOS 10.13 and Apple File System (APFS), no new recovery key is created. The existing recovery key remains valid.

### 3.7.14 HTTPS updating

Your computers and servers can get their Sophos updates via HTTPS. We recommend that you use HTTPS for greater security.

To use HTTPS updating:
1. Go to Settings > HTTPS Updating.
2. Turn on HTTPS Updating.

### 3.7.15 Configure email alerts

You can manage how admins receive email alerts.

**Restriction**
You must be a Super Admin to manage email alerts.

You can:
- Manage which administrators get email alerts.
- Add distribution lists or email addresses that you want to receive email alerts.
- Manage the frequency of email alerts.
Sophos Central Admin

- Set custom rules to specify which alerts an administrator gets.
- Edit the exceptions that have been set up for individual alert types.

You can change these settings on the **Global Settings > Configure email alerts** page.

**Note**
If these options are locked your Sophos partner or enterprise admin is managing email alerts.

### Administrators

The **Administrators** list shows who receives email alerts by default. The list shows the name, email address and admin role for each administrator.

You can choose which administrators you want to receive alerts. Click **Yes** or **No** in the administrator’s details to do this.

### Distribution lists

You can manage the distribution lists or email addresses that you want to receive email alerts. Use this option to add the email addresses of your distribution lists, ticketing system or people you want to notify about alerts, but do not have access to Sophos Central Admin.

If you want to provide access to Sophos Central Admin, add the person as an administrator.

- Click **Add email address**. Enter the email address and give a description and click **Save**.
- To remove an email address, select the address and click **Delete**.

**Restriction**
If you have a Sophos Central trial account, you cannot use distribution lists.

### Frequency

You can manage the frequency with which admins receive email alerts. You can set the frequency depending on one of the following:

- The severity of the alert.
- The product.
- The category the alert is in.

**Note**
You can only use one of these attributes to set frequency.

You can choose between **Immediately, Hourly, Daily, or Never**.

For the **Hourly** and **Daily** options, emails are sent immediately but with a maximum of one email for each alert per device per hour or per day. For example, if you set the frequency to **Hourly** and five devices have an alert at 11 am, five emails are sent at 11 am. If the same alert occurs again at 11.24 am, no further emails are sent. If the same alert occurs again at 12.01 pm on all five devices, five more emails are sent at 12.01 pm.
Custom rules

By default, admins see all alerts.

Custom rules make it easy to specify that some admins will only get alerts for certain products or events, or alerts of a certain severity.

**CAUTION**

Using a custom rule stops any email alerts going to existing recipients. When you turn on your first custom rule, all existing recipient settings are turned off in Administrators & Distribution lists. If you want to continue using your administrator and distribution lists, set up a separate custom rule to do this.

Set up a custom rule as follows:

1. Click **+ Create rule**.
2. In **Role**, choose an administrator role that this rule will apply to. Click **Next**.
3. In **Administrators & Distribution lists**, choose administrators that this rule will apply to.
   
   You can also add distribution lists. Use this option to add the email address of your distribution lists, ticketing system, or people you want to notify about alerts, but do not have access to Sophos Central Admin.
   
   Click **Next**.
4. In **Alert Types**, choose the types of alert to send. You can select the type by severity, product or alert category. Click **Next**.

   **Note**

   You must choose at least one option for each attribute.

5. Give your rule a **Name** and **Description**. Click **Save**.

The rule is now shown in the **Custom rules** list.

To see details of a rule, click the fold-out arrow next to it in the list.

To pause a rule, edit it or delete it, click the appropriate icon beside it in the list. Hover over icons to see what they do.

Exceptions

The **Exceptions** list shows the exceptions you have set up. These change the frequency of email alerts for certain alert types.

You set them in individual alert details on the **Alerts** page. You can also edit them here.
3.7.16 Multi-factor authentication

If you're a Super Admin, you can make some or all of the Sophos Central admins sign in with multi-factor authentication.

Introduction

Using multi-factor authentication means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos or Google Authenticator, SMS or email authentication to sign in.

Multi-factor authentication is turned on by default for newly created Sophos Central accounts.

This page tells you how to do the following:

• Set up multi-factor authentication.
• Sign in with multi-factor authentication for the first time.
• Add another method for multi-factor authentication.
• Sign in with email authentication if you don't have Sophos or Google Authenticator.
• Reset an admin's sign-in details, for example if they lose their phone.
• Turn off multi-factor authentication for an admin.

Set up multi-factor authentication

If you're a Super Admin, you can choose how your administrators sign in.

To set up multi-factor authentication, do as follows:

1. Go to Settings > Multi-factor Authentication (MFA).
2. Choose how you want admins to sign in:
   • No MFA needed.
   • All admins need MFA. This is the default for new accounts.
   • Select admins who will need MFA. This lets you select individual admins.
3. If you choose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). Move admins to the Assigned Users list and click Add.
4. Click Save.

When admins next sign in, they are prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

The first time you sign in with MFA, do as follows:

1. At the sign-in screen, enter your user ID (email address) and password.
   A Set Up Your Login Information dialog explains that signing in needs additional authentication.
2. In the next dialog:
   a) Enter the security code that has been sent to you in an email.
b) Create a 4-digit PIN. This enables you to use email as an authentication method.

3. In the next dialog, choose authentication type.
4. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.

   You also need to enter a security code to verify a device if you have chosen SMS as your authentication type.

   Sophos Central Admin opens.

The next time you sign in, you only need to enter a code from Sophos or Google Authenticator when prompted.

Add another authentication option for multi-factor authentication

You can set up multiple authentication options for a Sophos Central Admin account.

You can authenticate with SMS and Sophos or Google Authenticator.

You must have an authentication option already set up.

To set up another authentication option, do as follows:

1. Sign in to Sophos Central Admin.
2. Click your account name and click Manage Login Settings.
3. Click Create New Method.
4. Choose another authentication method.
5. Click Next.
6. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
7. To confirm that the new method has been added, click your account name and click Manage Login Settings.
   An additional authentication method has been added.

Sign in with email authentication

If you don't have access to Sophos or Google Authenticator, you can sign in with email authentication instead.

1. At the sign-in screen, enter the user ID (email address) and password.
2. In Verify Your Login, click Choose Another Method.
3. In Pick Your Challenge, click the email option.
   An email is sent to you.
4. Open the email and find the security code.
5. In Verify Your Login, enter the security code and your 4-digit PIN.

You'll be asked for the security code and PIN each time you sign in from now on, until you switch back to using Sophos or Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can allow them to set up their sign-in again.

1. On the People page, under Users, find the user and click their name to open their details.
2. In the user details, on the left of the screen, you'll see their MFA status and settings. Click Reset and confirm that you want to do a reset.
The next time the admin tries to sign in, they’ll need to go through the setup steps again.

**Turn off multi-factor authentication**

If you're a Super Admin, you can turn off multi-factor authentication for an administrator.

To turn off multi-factor authentication, do as follows:

1. Go to **Settings > Multi-factor Authentication (MFA)**.
2. Click **Select admins who will need MFA**.
3. Click **Add admins**.
4. Move the administrator from the **Assigned Users** list and to the **Available Users** list.
5. Click **Add**.
6. Click **Save**.

### 3.7.17 Manage Update Caches and Message Relays

Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos.

This saves you bandwidth, as updates are downloaded only once, by the server.

You can also enable computers to communicate with Sophos Central through a message relay on a server on your network.

A message relay server must also have an update cache set up on it.

This help page tells you how caches and relays work and how you set them up.

**Tip**

Computers can get the latest Sophos agent from a cache the first time you run the Sophos installer on them. You need to set up your caches before installation. If you have endpoints that can't connect to Sophos directly, you also need to set up your update caches as message relays.

**Note**

If you use the **Reject network connections** feature (for customers with Sophos XG Firewall), it could prevent a cache server from delivering updates. To avoid this, see **Reject network connections**.

### How caches and relays work

When you set up a cache (and optionally relay) on a server, Sophos Central does as follows:

- Installs Sophos caching software (and relay software).
- Fetches updates from Sophos and puts them in a cache.
- Automatically configures computers in your network to update from a cache (and use a relay).

You can also assign computers to use a specific cache or relay.

Using caches doesn't affect how often or when computers are updated.
Computers that can use caches and relays

You can install caches and relays on Windows Server 2008 or later (2008 R2 for relays). The following computers can use caches or relays:

- Windows 7 and later (including servers), Macs and Linux computers can use a cache.
- Windows 7 and later (including servers) and Linux computers can use a relay.

Set up a cache/relay

You can set up a cache and a relay at the same time, or a cache only. You can also set up a relay on a server that already has a cache.

Before you set up a cache or a relay, ensure that:

- The server is running Windows Server 2008 or later.
- The server has at least 5GB free disk space.
- Port 8190 and 8191 are available and accessible to computers that will update from the cache and use the relays.

   The installers will open ports 8190 and 8191 in Windows Firewall. When Update Cache or Message Relay are uninstalled, the ports are closed again.

If you use the Reject network connections feature (for customers with Sophos XG Firewall), you might need to add the server to the exclusions. See Reject network connections.

To set up a cache or a relay:

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. In the filter above the table, click the drop-down arrow and select Cache Capable Servers to see which servers are suitable for a cache and a relay. If you have already set up a cache on some servers, to hide them from view, select Servers without Update Cache. If you want to set up a relay on a server with a cache, select Servers with Update Cache.
3. Select the server or servers where you want to set up a cache or relay.

Sophos Central automatically configures computers in your network to use a cache or relay. You can also manually assign computers to use a specific cache or relay.

Assign computers to a cache/relay

You can manually assign computers to use a specific cache or relay.

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. For the server on which the cache or relay is installed, click the link displaying the number of computers using the Update Cache or Message Relay, in the Updated from cache column or the Using Relay column, respectively.
3. Click Manual assignment.
4. Select the computers.
5. Click Save.
See which computers use caches and relays

On the Manage Update Caches and Message Relays page you can view which servers have update caches and message relays. You can see how many computers are using them as caches or relays and the activity of the update caches.

Click a server to see the details of the computers using its update cache or message relay.

Remove a cache/relay

Note
If you want to remove a cache that has computers manually assigned to it you must reassign them first.

When you remove a cache, Sophos Central does as follows:

• Uninstalls caching software, removes the cache of downloaded updates, and closes port 8191 in Windows Firewall.
• Also uninstalls the message relay software (if installed) and closes port 8190 in Windows Firewall.
• Reconfigures computers that update from this server to update from another update cache, if you have one.
• Reconfigures computers that use the relay to use another message relay, if you have one.

If you remove all your caches, computers will update directly from Sophos.

If you remove all of your message relays, computers will communicate directly with Sophos Central.

To remove a cache/relay:
1. In Settings, go to the Manage Update Caches and Message Relays page.
2. In the filter above the table, click the drop-down arrow and select Servers with Update Cache to see which servers have a cache set up. You can also select Servers with Message Relay to see which servers have a message relay set up.
3. Select the server or servers you want to remove a cache/relay from.
4. Click Remove Cache/Relay.

Related concepts
Reject network connections (page 136)
You can configure devices to reject connections from other devices on the network that may be unsafe.

3.7.18 Allowed applications

On the Settings > Allowed Applications page you can see applications that you have allowed to run on your endpoint computers.

The page shows where the application was originally detected (if applicable) and how it was allowed.
About allowed applications

Our software detects threats that are previously unknown. However, it may sometimes identify an application as a threat, even though you know that it’s safe. When this happens, you can “allow” the application. This does as follows:

• Prevents this detection from happening again.
• Restores all copies that have been cleaned up (removed from computers).

Alternatively, you can allow an application in advance, so that it won’t be detected when you install it for users.

**CAUTION**
Think carefully before you allow applications because it reduces your protection.

Note
If an option is locked global settings have been applied by your partner or Enterprise administrator. You can still stop detecting applications, exploits and ransomware by going to the events list.

Allow an application that's been detected

Only allow an application if you know it's safe. For help deciding, see How to investigate and resolve a potential False Positive or Incorrect Detection.

To allow an application that Sophos has detected and removed, do as follows.

Note that:
• This allows the application for all computers and users.
• This allows the application to start, but we’ll still check it for threats, exploits and malicious behavior when it’s running.

1. Go to the Computers or Servers page, depending on where the application was detected.
2. Find the computer where the detection happened and click on it to view its details.
3. On the Events tab, find the detection event and click Details.
4. In the Event details dialog, look under Allow this application.
5. Select the method of allowing the application:
   • **Certificate**: This is recommended. It also allows other applications with the same certificate.
   • **SHA-256**: This allows this version of the application. However, if the application is updated, it could be detected again.
   • **Path**: This allows the application as long as it's installed in the path (location) shown. You can edit the path (now or later) and you can use variables if the application is installed in different locations on different computers.
6. Click Allow.
Edit the path for an allowed application

You can change the path that you specified when you allowed an application.

1. On the **Allowed Applications** page, find the application. The current path is shown in the details.
2. Click the edit icon (the pen) on the far right of the page.

3. In the **Edit path** dialog, enter the new path.

When you edit a path, details of the original detection (user, computer and path) are removed from the list.

Start detecting an application again

If you want Sophos to start detecting and removing an application again, you remove it from the **Allowed Applications** list.

Select the application and click **Remove** (in the upper right of the page).

**Related information**

How to investigate and resolve a potential False Positive or Incorrect Detection

3.7.19 Blocked items

This option is available if you have Intercept X Advanced with EDR.

On the **Settings > Blocked Items** page, you can block and clean up suspicious applications.

You can also see applications that you have blocked from running on your computers. You can see who blocked the application and why.

About blocked applications

You can block applications using their SHA-256 hash. This prevents suspicious applications from running on your computers.

You can only block applications. SHA-256 hashes for other items, or for files Sophos believes to be safe, are ignored.

When you block an application it's cleaned up on any devices it's already on.

You can also clean up and block applications when you investigate a threat case or review the results of a threat search.

Block an application

To block and clean up an application:

1. Click **Add**.
2. Enter the application's SHA-256 hash.
3. Enter a reason for blocking the application.
4. Click Add.
   • Click Add Another if you want to block more than one application.
5. When you have finished, click Save on the Blocked Items page.
This blocks the application on all computers and cleans it up on computers it's already on.

Remove an application from the block list

You can remove applications from the block list if you've decided that they aren't suspicious. To do this:
1. Select the application in the list and click Remove.

Related concepts
Threat Cases (page 19)
Threat cases let you investigate and clean up malware attacks.
Threat Searches (page 31)
You can search for potential threats on your network.
Admin Isolated Devices (page 137)

3.7.20 Controlled updates

By default, computers get the latest Sophos product updates automatically. If you prefer, you can control how your computers update.

For example, you can stop updates on all computers during a busy period, or test updates on selected computers before they are rolled out to the rest of the network.

Restriction
You can control updates on Windows and Linux devices, but not Macs.

To control updates, go to Settings > Controlled Updates.
You have these options.
• Pause Updates Now
• Pause Updates on a Set Date
• Control Updates Manually

If updates are already controlled, you see a list of computers whose updates are controlled instead of these options.

Note
Computers still get automatic security updates to protect them against the latest threats.

You can go back to automatic updating at any time.

Related concepts
Pause updates now (page 134)
You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

Control updates manually (page 134)
You can control product updates manually.

Related tasks
Pause updates on a set date (page 134)
You can choose dates when you want to stop and restart product updates on all computers.

Pause updates now
You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

Restriction
You can control updates on Windows and Linux devices, but not Macs.

On the Settings > Controlled Updates page, click Pause Updates Now.
This stops automatic updates on all your computers immediately.
Updates start again automatically after 90 days.

Tip
If you want to start updates again earlier, click Resume Automatic Updating.

Pause updates on a set date
You can choose dates when you want to stop and restart product updates on all computers.
Automatic updates will stop for 90 days. Your computers will still get security updates.

Restriction
You can control updates on Windows and Linux devices, but not Macs.

1. On the Settings > Controlled Updates page, click Pause Updates on a Set Date.
2. Select a Pause date and a Restart date. Click Apply.
On the restart date, the computers will start updating automatically and get any updates that are available.

Tip
If you want to restart updating earlier, click Resume Automatic Updating.

Control updates manually
You can control product updates manually.

Restriction
You can control updates on Windows and Linux devices, but not Macs.
This stops automatic updating so that you can decide when to test new product versions and roll them out to your computers.

Note
Your computers will still get automatic security updates.

This Help topic tells you how to set up manual updating, and how to test and roll out updates.

How to set up manual updating

On the Settings > Controlled Updates page, click Control Updates Manually.

Note
This stops all automatic updates. You are not asked for confirmation.

Initially, your situation is this:

- All your computers are on the Newest (recommended) version. They’ll be shown as being on this version until Sophos issues a newer version.
- No computers will get any further updates until you update them.

Now you should set up test computers (if you want to).

Set up test computers

You can use test computers to try out new versions.

1. In the Test computers table, click Add.
2. Select computers from the Available Computers list.

You’re now ready to test updates and roll them out manually.

Test and roll out updates

When Sophos releases a new product version:

- You receive an email alert.
- Computers that were on the Newest (recommended) version are now shown as being on the Oldest.

In the table of versions, you can use the buttons in the Action column to update computers when you want to.

Typically, you would want to test the new version on selected computers and then roll it out to all the other computers.

In the Action column, next to Test Computers, click Update test computers to newest version.

When you’re ready to update all your other computers, in the Action column, next to Non-test computers, click Update to match test computers.

This forces the non-test computers to update at the time of the next automatic update, which by default is every 60 minutes. Note that this update will not follow any schedule that you’ve set in the Update Management policy for servers.
Why can I see a 'Previous' version now?

If Sophos releases another product update when you already have test computers on **Newest (recommended)** and the rest on **Oldest**:

- Test computers are now shown as being on the **Previous** version (the version that has just been replaced by a newer one).
- Non-test computers are on **Oldest**.

You can use an action button next to the test computers to **Update test computers to newest version**.

You can use an action button next to non-test computers to **Update to match test computers**.

What happens when a version expires?

Sophos product updates expire after 90 days. When the **Oldest** version expires, computers are forced to update as follows:

- If all computers are on **Oldest**, they resume automatic updating.

  **Note**
  
  If this happens, all computers get the newest version. You no longer control updates manually.

- If non-test computers are on **Oldest**, but test computers are on a newer version, the non-test computers are updated to the same version as the test computers.

### 3.7.21 Reject network connections

You can configure devices to reject connections from other devices on the network that may be unsafe.

This setting only applies to devices connected to an XG firewall.

When you turn on the setting, it rejects connections to or from devices with red health or with a missing Security Heartbeat.

1. Go to **Global Settings > Reject Network Connections**.
2. Turn on **Allow devices to reject connections from other devices with red health**.
3. Set up **Exclusions** if you need to.
4. Click **Save**.

When a device triggers a red health or missing Security Heartbeat alert, all other devices on the same subnet are informed that the device is unsafe.

If the unsafe device tries to access another device, you will see an event logged in Sophos Endpoint on the destination device:

```
Access request from computer computer name denied because it may be unsafe
```

If a device tries to access an unsafe device, you will see an event logged in Sophos Endpoint on the source device:

```
Access to computer computer name denied because it may be unsafe
```
You cannot override the rejected state on a rejected device locally. To allow access to or from the device, it must revert to a healthy state.

**Exclusions for servers**

You might have servers that are critical for your organization. In this case, set up exclusions to ensure that devices always accept connections from these servers even if their health is red. Servers that are used as an update cache or message relay are excluded by default. This allows them to offer updates or a communication route for your devices.

1. On the **Reject Network Connections** page, go to **Exclusions**.
2. Select the server or servers and move them to the **Excluded** list.
3. Click **Save**.

### 3.7.22 Admin Isolated Devices

On the **Settings > Admin Isolated Devices** page you can see which devices you've isolated and remove them from isolation.

**Note**

This list doesn't include devices that have isolated themselves automatically because their health is red, see **Device Isolation** in **Threat Protection Policy**.

You can isolate affected devices while you investigate a threat case, see **Threat Cases**. You can also search for other affected devices and isolate those from your threat search results, see **Threat Searches**.

You can allow isolated devices to communicate with other devices in limited circumstances, see **Global Exclusions**.

After you have cleaned up and blocked any suspicious applications you can remove the affected devices from isolation.

To do this:

1. Select the device and click **Remove from Isolation**.

**Related concepts**

- **Threat Protection Policy** (page 203)
  Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.
- **Threat Cases** (page 19)
  Threat cases let you investigate and clean up malware attacks.
- **Threat Searches** (page 31)
  You can search for potential threats on your network.

**Related information**

- **Global Exclusions** (page 106)
You can exclude files, websites and applications from scanning for threats.

### 3.7.23 Sample Submission

To help Sophos identify new threats and update your protection, sample files are automatically submitted to us.

“Sample files” are copies of your files (which may include emails and URLs).

If a file is deemed potentially malicious but cannot be positively identified as malicious based on its characteristics alone, Sample Submission allows Sophos servers to request a copy (sample) of the file. If Sophos does not already hold a sample of the file, the file is submitted to Sophos automatically.

Submission of such sample files helps Sophos to enhance detection of malware continuously and reduce the risk of false positives.

**Note**

The maximum sample size is 10 MB. The timeout period for sample upload is 30 seconds.

Because Sample Submission increases the protection that our software provides, we strongly recommend that this feature be left turned on to provide a more secure experience. However, to turn it off:

1. Go to **Global Settings > Malware Sample Submission**.
2. Turn off **Submit sample files to Sophos automatically**.
3. Click **Save**.

### 3.7.24 Forensic snapshots

Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

You can create a forensic snapshot from a threat case or from the **Status** tab in a device’s details page.

On the **Global Settings > Forensic Snapshots** page, you can configure how much data you want in your snapshots and where you want to put them.

**Note**

The configuration options may not be available for all customers yet.

**Set the time period for the forensic snapshot**

By default, a snapshot includes data for the previous two weeks.

Here you can set a different time period or choose to include all the available data.

**Upload forensic snapshot to an AWS S3 bucket**

By default, snapshots are saved on the local computer.
You can upload snapshots to an AWS S3 bucket instead. This lets you access your snapshots easily in a central location, rather than going to each computer.

1. Enter the S3 bucket name and directory where you want to upload snapshots.

2. Go to your AWS console and create a new IAM role. You need to include the details of the Sophos proxy account that will put the snapshot data in your S3 bucket. Use the **AWS Account ID** and **AWS External ID** we provide.

   For full details of how to set up an AWS S3 bucket so that you can upload snapshots, see [Upload a forensic snapshot to an AWS S3 bucket](#).

3. Go back to the **Forensic Snapshots** page and enter your ARN (Amazon Resource Name).

4. Click **Save**.

**Note**
If you use Sophos XG Firewall, it might block traffic to the S3 bucket. If this happens, update the firewall's policy to allow this traffic.

**Restriction**
A limitation that is set by AWS means that uploads time out if they take longer than one hour. This is more likely if the data in the snapshot covers a long time period.

**Related concepts**
- [Threat Case analysis page](#) (page 21)
  You can investigate a threat case by going to its details page and using the analysis tools there.
- [Computer Summary](#) (page 68)
  The **Summary** tab in a computer's details page shows you the following information.
- [Server Status](#) (page 84)
  The **Status** tab in a server's details page lets you see the server's security health and details of any alerts.

**Related information**
- [Object Key and Metadata](#)

**Convert a forensic snapshot**

Use the SDR Exporter tool to convert forensic snapshots so you can run queries on them.

The SDR Exporter tool is used to convert forensic snapshots on a device into a format where advanced queries can be run. The snapshots can then be converted to an SQLite database or a JSON formatted file.

There are several versions of the tool available. Download the appropriate version.

To convert a snapshot:

- Specify the path and filename of the snapshot to be converted and the path and filename of the output file and the format. You must use at least these options. The command you use depends on the version of the tool you are using.
  - 64 bit: `SDRExporterx64.exe -i <path to snapshot tgz> -o <path to output file> -f <format to output sqlite or json>`
Sophos Central Admin

- **32 bit:** SDRExporterx86.exe -i <path to snapshot tgz> -o <path to output file> -f <format to output sqlite or json>

| Options: |
|———|
| -h [ --help ] Print help message |
| -i [ --input-path ] arg Path to input snapshot container file |
| -o [ --output-path ] arg Path to output file |
| -f [ --output-format ] arg (=sqlite) Output format (choices: sqlite or json) |
| -v [ --output-version ] rg Output version - default is latest |

**Related concepts**

**Forensic snapshots** *(page 138)*
Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

**Related information**

**Upload a forensic snapshot to an AWS S3 bucket** *(page 140)*
Follow these instructions to upload a forensic snapshot.

**Sophos Endpoint Core Agent 2.5.0 and Sophos Server Core Agent 2.5.0 and later** - 64 bit version
**Sophos Endpoint Core Agent 2.5.0 and Sophos Server Core Agent 2.5.0 and later** - 32 bit version
**Sophos Endpoint Core Agent 2.4.1 and Sophos Server Core Agent 2.2.7 and earlier** - 64 bit version
**Sophos Endpoint Core Agent 2.4.1 and Sophos Server Core Agent 2.2.7 and earlier** - 32 bit version

**Upload a forensic snapshot to an AWS S3 bucket**

Follow these instructions to upload a forensic snapshot.

**Introduction**

**Note**
This option is currently available for Windows computers only and requires Core Agent 2.5.0 and later.

By default, snapshots are saved on the local computer. You can upload snapshots to an Amazon Web Services (AWS) S3 bucket instead. This lets you access your snapshots easily in a central location, rather than going to each computer.

To upload snapshots you must have an available AWS S3 bucket. You also need to do the following:

- Create a managed policy in AWS.
- Add your AWS account to Sophos Central.
- Create an AWS bucket policy to restrict access to the S3 bucket.

**Related concepts**

**Threat Case analysis page** *(page 21)*
You can investigate a threat case by going to its details page and using the analysis tools there.

**Related information**

**Object Key and Metadata**

**Create a managed policy**

Follow these instructions to create a managed policy in AWS.

To create a managed policy:

1. In the Amazon Web Services (AWS) dashboard go to **IAM** listed under **Security, Identity and Compliance**.
2. Click **Policies** on the left side navigation bar.
3. Click **Create Policy**.
4. Click **JSON**.
5. Add the following policy:

   ```json
   {
   "Version": "2012-10-17",
   "Statement": [
   {
   "Sid": "AllowPutObject",
   "Effect": "Allow",
   "Action": [
   "s3:PutObject",
   "s3:GetBucketLocation"
   ],
   "Resource": [
   "arn:aws:s3:::<bucket-name>",
   "arn:aws:s3:::<bucket-name>/*"
   ]
   }
   
   ]
   }
   
   Note
   You need to replace `<bucket-name>` with the name of the bucket where your snapshots will be uploaded.

6. Click **Review Policy** to check the copied policy is valid.
7. Name the policy.
   
   Example: Sophos-Central-Forensic-Snapshot-Upload.
8. Give a description.
   
   Example: This policy allows Sophos Central to upload forensic snapshots to a given S3 bucket.
9. Click **Create Policy**.

**Add an AWS account to Sophos Central**

Follow these instructions to add your Amazon Web Services (AWS) account to Sophos Central.

To add your account:

1. In Sophos Central, go to **Global Settings** and click **Forensic Snapshots**.
2. Turn on **Upload forensic snapshot to an AWS S3 bucket**.
3. Make a note of **AWS Account ID** and **AWS External ID**.
4. In Amazon Web Services create the IAM Role by doing the following:
   a) In the Amazon Web Services dashboard go to Identity & Access Management listed under Security & Identity.
   b) Click Roles on the left side navigation bar.
   c) Click Create role.
   d) Click Another AWS account.
   e) Enter the Account ID and External ID provided by Sophos Central.
   f) Turn on Require external ID.
      This is recommended best practice when a third party assumes this role.
   g) Turn off Require MFA.
   h) Click Next: Permissions.
   i) Attach the policy you created earlier, and click Next: Tags.
   j) Leave the optional tags blank and click Next: Review.
   k) Enter a Role name, and optionally a Role description.
   l) Click Create Role and copy the Role ARN (Amazon Resource Name).

5. You need to wait for this role to propagate to all regions in AWS before you can add the account to Sophos Central. This can take up to five minutes.

6. In Sophos Central, on the Forensic Snapshots page, do the following:
   a) Enter the S3 bucket name. This must match the bucket name in the managed policy.
   b) Optionally, enter a bucket directory name where you want the snapshots to be uploaded to in the S3 bucket.
   c) Enter the Role ARN created in AWS.
   d) Click Save.

Create a bucket policy
We recommend you create a bucket policy to restrict access to the S3 bucket that you want to upload forensic snapshots to.

To restrict access:
Add the following bucket policy:

```json
{
    "Version": "2012-10-17",
    "Id": "S3PolicyIPRestrict",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3::<bucket-name>",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.168.143.0/24"
                }
            }
        },
        {
            "Sid": "AllowRead",
            "Action": ["s3:GetObject"],
            "Effect": "Allow",
            "Resource": "arn:aws:s3::<bucket-name>",
            "Principal": {
                "AWS": ["arn:aws:iam::123456789012:root"
            ]
        }
    ]
}
```

This policy:

- Allows only the specified IP addresses to upload snapshots to the bucket. These should be the outward IP addresses of endpoints or firewalls.
- Allows only authorized people to access the snapshots in the bucket.

Are there any issues that I should be aware of?

- Uploading to buckets with KMS encryption is not supported but AES-256 encryption is supported. You don't have to enable AES-256 encryption on an S3 bucket, although we recommend it. Sophos uploads snapshots with an AES-256 encryption header.
- Special characters for bucket names are not supported. For an allowed characters list see Object Key and Metadata.
- Due to a limitation in AWS, snapshots that take longer than 1 hour to upload will time out, preventing the upload from taking place. This is more likely if you chose a longer period of time for the snapshot to contain.
- If you have a firewall in your environment, check that your rules allow the upload of snapshots to the AWS S3 bucket.
3.7.25 Live Response for devices

Turn on Live Response so that you can connect to devices to investigate and remediate possible security issues.

**Restriction**
You must be a Super Admin to configure Live Response.

You need to turn on Live Response for computers and servers separately.

- To be able to connect to servers, do as follows:
  a) Go to Global Settings > Server Protection > Live Response.
  b) Turn on Allow Live Response connections to servers.
  c) Click Save.

- To be able to connect to computers, do as follows:
  a) Go to Global Settings > Endpoint Protection > Live Response.
  b) Turn on Allow Live Response connections to computers.
  c) Click Save.

3.7.26 Amazon Web Services Accounts

On the Settings > Connect AWS Accounts page, you can associate your AWS accounts with your Sophos Central account. This gives you improved management of Sophos Server Protection on AWS EC2 instances and S3 storage buckets.

When you add an AWS account on this page, Sophos Central will do as follows:

- Display AWS instance details.
- Remove terminated AWS instances from the list automatically.
- Let you apply server policies to Auto Scaling Groups.
- Assess the security of your S3 storage buckets.

To associate an AWS Account with Sophos Central:

1. Click Add (on the right of the page).
2. In the Connect to AWS dialog:
   a) Enter a Friendly Connection Name. This will be used to refer to the account in Sophos Central.
   b) Add a new IAM Role in your AWS console.
   c) Enter the Amazon Resource Name (ARN) for the AWS account that you want to connect to.
   d) Select Connect.

   Sophos Central attempts to verify the credentials. While this happens, the account connection health shows a refresh icon.

3. When the page is refreshed, the account has either connected successfully, is still attempting connection or has failed.
If the connection fails see Troubleshooting Sophos Central connections to AWS and Creating an IAM Role for Sophos Central.

When you have added the AWS account:

- AWS instances are listed on the Servers on AWS page, on the AWS Instances tab. Instances without a Sophos Agent installed are only shown here.
- AWS instances with a Sophos agent installed are listed on the Servers page.
- AWS Auto Scaling Groups are listed on the Server Groups page. The number of instances with an installed Sophos agent is indicated for the group.
- Policies assigned to AWS Auto Scaling Groups are automatically assigned to instances that are in that group and have a Sophos agent installed.
- Your S3 storage buckets are assessed and assigned a health status.

Related information
Troubleshooting Sophos Central connections to AWS
Creating an IAM Role for Sophos Central

3.7.27 Connect to Microsoft Azure

In Settings, on the Azure Active Directories page, you can associate your Azure Active Directories with your Sophos Central account. This gives you improved management of Sophos Server Protection on Azure Virtual Machines (VMs).

When you add Azure Active Directories on this page, Sophos Central will do as follows:

- Display Azure Active Directories’ details.
- Remove deleted VMs automatically.

To add an Azure Active Directory:
1. Click Add (on the right of the page).
2. In the Connect a directory dialog:
   a) Enter the Active Directory ID. You can find this in the Active Directory properties in the Azure Portal.
   b) Enter the Application ID from the Azure Portal along with the Application Secret Key that was set up with the App secret key.
   c) Click Add.

Sophos Central tries to verify the credentials. While this happens, the account Connection Status shows a refresh icon.
3. When the page is refreshed, you can see that the account has connected, is still trying to connect, or has failed.
   If the connection fails, see Troubleshooting Sophos Central connections to Azure.

When you have added the Azure Active Directory, the page shows:

- The Azure Active Directory along with any associated Subscriptions.
- Total VMs. Click on the total to see a list of VMs on the Azure VMs page.
- Sophos Agent Installed. The number of VMs protected with a Sophos Server Protection agent.

To modify or delete the connection to an Azure Active Directory, select the directory and use the buttons in the upper right of the page.
Related information
Troubleshooting Sophos Central connections to Azure

3.7.28 Data Loss Prevention Rules

You use data loss prevention (DLP) rules to specify conditions to detect, actions to take, and any files to exclude from scanning.

You can use these rules across multiple policies.

There are two types of rules:

- **Content**: A content rule details the action to be taken if a user attempts to transfer data that matches the Content Control Lists (CCLs) in the rule to the specified destination.
  
  You use CCLs to match file content.

- **File**: A file rule details the action to be taken if a user tries to transfer a file with the specified file name or file type to the designated destination. For example, you can block the transfer of databases to removable storage devices.

When all the conditions listed in a rule are detected, the rule is matched, the action specified in the rule is followed, and the event is logged.

If a file matches rules that specify different actions, the rule that specifies the most restrictive action is applied. For example:

- Rules that block file transfer take priority over the rules that allow file transfer on user acceptance.
- Rules that allow file transfer on user acceptance take priority over the rules that allow file transfer.

Manage Data Loss Prevention Rules

This page lists the existing DLP rules and allows you to manage their use across multiple policies.

The name, source, and type is shown for each rule.

You can create new custom rules, and search existing rules.

You can also filter rules by **Rule Type**.

Click on the name of a rule to edit it.

To view details of a rule, click **Information**.

To clone a rule, click **Clone**.

1. Give a name for the cloned rule.
2. Click **Clone item**. This adds the cloned rule to the list of rules.
3. You can then amend it by clicking its name in the list.

To export custom rules, click **Export**. This creates an xml file containing the rule definition.

To delete a rule, click **Delete**. Click **Delete item** to confirm deletion.

To import rules:

1. Click **Import**.
2. Select the XML file containing the rules.
3. Click **Open**.
   The rules are added to the list.

**Related concepts**

**Content Control Lists** (page 148)
A Content Control List (CCL) describes a single type of data (for example, a postal address or social security number) or a combination of data types (for example, a project name near the term "confidential").

**Related tasks**

**Create a Data Loss Prevention Rule** (page 147)
Follow these instructions to create a DLP rule.

**Create a Data Loss Prevention Rule**

Follow these instructions to create a DLP rule.

There are two stages to creating a DLP rule; creation and configuration.

This stage sets up the rule type, the actions taken if the rule is triggered and whether you want to be alerted to the breaches of the rule.

To create a DLP rule:

1. Click **Create New Rule**.
2. Choose from **New Content Rule** or **New File Rule**.
3. Give the rule a **Name** and a **Description**.
4. Click **Send me email alerts** if you want notifying when the rule is breached.

   **Note**
   You will not get an alert in Sophos Central.

5. For a **File** rule, choose whether you want to match against a file name or a file type as the conditions for the rule. You will give the details when you configure the rule.

   **Note**
   Conditions are required for a **Content** rule and you cannot set the condition type.

6. Specify if you want to exclude by a file name or by file type. You will give the details when you configure the rule.
7. Specify the actions for the rule. Choose from:
   - **Allow file transfer**.
   - **Allow transfer if user confirms**.
   - **Block transfer**.
8. Click **Next: Rule Configuration**.

**Related tasks**

**Configure a Data Loss Prevention Rule** (page 148)
Configure a Data Loss Prevention Rule

You can set up the conditions for monitored files, file types or destinations and the exclusions for a DLP rule.

The conditions you set depend on whether you are creating a File or Content rule.

1. Set up the rule conditions.
   a) To set up conditions for a content rule, click **File Contains** and select the CCLs you want to use.
      You can search the list of CCLs. You can filter the CCLs by **Type**, **Source** (choose from **Sophos Labs** or **Custom**), and **Region**. You can also create a new CCL.
   b) To set up conditions for a file rule, specify the file names or file types for the rule.
2. Click **Destination is** and set the destinations that the rule monitors.
   Destinations include devices (for example, removable storage devices, such as USB flash drives) and applications (for example, internet browsers and email clients).
3. Set the exclusion details for the rule.
4. Click **Finish** to create the rule.

Related tasks

**Create a Data Loss Prevention Rule** (page 147)
Follow these instructions to create a DLP rule.

3.7.29 Content Control Lists

A Content Control List (CCL) describes a single type of data (for example, a postal address or social security number) or a combination of data types (for example, a project name near the term "confidential").

This creates a definition for data that you want to protect. You can then use CCLs in data loss prevention rules to control what happens to this data.

To enable you to quickly define and roll out a data loss prevention policy, SophosLabs maintain a library of sensitive data definitions. SophosLabs CCLs provide expert definitions for common financial and personally identifiable data types, for example, credit card numbers, social security numbers, postal addresses, or email addresses. You cannot edit SophosLabs CCLs, but you can submit a request to Sophos to create a new one.

You can use SophosLabs CCLs in your rules, or create your own CCLs.

You can filter the CCLs.

You also can search the list of CCLs.

To view details of a CCL, click **Information**.

For each custom CCL you can also:

- Click on the name of a CCL to edit it.
- To export a CCL, click **Export**. This creates an XML file containing the definition for the CCL.
To clone a CCL, click **Clone**. Give a name for the cloned CCL and click **Clone item**. This adds the cloned CCL to the list of CCLs. You can then edit it by clicking its name.

To delete a CCL, click **Delete X**. Click **Delete item** to confirm deletion.

You can also import CCLs:

1. Click **Import**.
2. Select the XML file containing the CCLs.
3. Click **Open**.
   
   The CCLs are added to the list.

### Related concepts

**Data Loss Prevention Rules** (page 146)

You use data loss prevention (DLP) rules to specify conditions to detect, actions to take, and any files to exclude from scanning.

### Related tasks

**Create Custom Content Control List** (page 149)

Follow these instructions to create a custom CCL.

#### Create Custom Content Control List

Follow these instructions to create a custom CCL.

To create a custom CCL:

1. Click **Add Custom Content Control List**.
2. Give the CCL a **Name** and a **Description**.
3. Click **Select tags** and add the tags you want to use.
4. Specify the matching criteria for the CCL. Choose from:
   - **Any of these terms**: Enter a term that you want to match in **Terms** and click **Add** to add another term.
   - **All of these terms**: Enter a term that you want to match in **Terms** and click **Add** to add another term.
   - **Exactly this phrase**: Enter the phrase that you want to match in **Phrase**. This option is not case sensitive.
   - **Advanced Setup**: Use this option to set up an advanced expression.
     
     Set the **Trigger score**.
     
     This is the number of times the regular expression must be matched before the CCL is matched.
5. Click **Save** to create the CCL.
Follow these instructions to set up an advanced expression for a custom CCL.

**Set up an advanced expression**

Follow these instructions to set up an advanced expression for a custom CCL.

You can only do this as part of creating a custom CCL.

Select **Advanced Setup** as the matching criteria to enter the details for an advanced expression:

1. **Set the Trigger score.**
   
   This is the number of times the regular expression must be matched before the CCL is matched.

2. **Enter a Perl 5 regular expression in Expression.**
   
   For a description of Perl 5 regular expressions, refer to Perl documentation or go to Perl syntax.

3. **Set the Score for the CCL.** This is the number that is added to the total score for a CCL when the regular expression is matched.

   **Note**
   
   The Score must match the Trigger score.

4. **Set the Max count.** This is the maximum number of matches for the regular expression that can be counted towards the total score.

   For example, an expression with a Score of 5 and a Max count of 2 can add the maximum of 10 to the total score of a CCL. If the expression is found 3 times, it still adds 10 to the total score.

5. **Click Add.**

   To delete an expression, click **Delete**

   To edit an expression, click **Edit**

   Once you have finished your edits, click **Save** to save them.

6. **Add more expressions, if required.**

   Adding more expressions expands the scope of the CCL.

   For example, the following CCL is matched if Data Loss Prevention finds 2 matches of expression A or 1 match of expression A and 1 match of expression B, or 1 match of expression B and 5 matches of expression C.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Score</th>
<th>Max count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expression A</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Expression B</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Expression C</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

**Related tasks**

*Create Custom Content Control List* (page 149)
Follow these instructions to create a custom CCL.

**Related information**
- Perl syntax

### 3.7.30 Inbound Allow/Block

You can create a list of email domains and addresses that you trust or don't trust.

**Restriction**
This option is only available if your license includes *Sophos Email*.

A list of domains and addresses that are allowed to connect with your email system, or are blocked from it, helps you to control spam. This setting only applies to inbound messages.

You can block or allow entire domain names, IP addresses, or specific email addresses. The domain or email address is added to the list and shown as either allowed or blocked. This list is global and applies to all protected mailboxes.

Wildcards are supported for email addresses and domains. For example, *@domain.com* would include any addresses that are part of *domain.com*. Subnet masks are supported from /16 to /32 (inclusive).

You can also use wildcards to block whole top level domains (TLDs). For example, * TOP would block every email from the .top TLD. This is useful for blocking email from generic or geographic TLDs that you do not communicate with, and are common sources of spam.

If you add the same address or domain to both the allow and block lists, select **Override duplicates** to ensure your most recent choice is used.

You can view email domains and addresses that you have already blocked, including IPs that you have blocked, through the **Message History** and **Quarantined Messages** settings.

Go to **Settings > Inbound Allow/Block** to do as follows:

- Add an allowed domain or address.
- Add a blocked domain or address.
- Import a list of domains to block or allow.
- Delete a domain or address.

**Related concepts**
- **Message History Report** (page 49)
  - The **Message History** report details the emails processed by **Email Gateway** for your protected mailboxes.

- **Quarantined Messages** (page 454)
  - The **Quarantined Messages** page lists the email messages that have been quarantined for all your protected mailboxes.

- **Email Security Policy** (page 458)
  - You can apply security settings to your mailboxes using **Email Security** policies.

**Related tasks**
- **Import allow/block list** (page 152)
You can import lists of email domains and addresses to block or allow.

**Import allow/block list**

You can import lists of email domains and addresses to block or allow.

You can import a list of domains and addresses into the Inbound Allow/Block list. When you import, you can download template files that show you the import list format.

1. Select **Add**.
2. Select **Import allow/block list** from the drop-down list.
3. Download the template files.
4. Create your import list in the same format as the template.
5. When you've finished creating your file, return to **Import allow/block list** to import it.

### 3.7.31 Manage settings for Sophos Central Self Service

You can manage self service settings for your users.

**Restriction**

This option is only available if your license includes **Sophos Email**.

You can:

- Turn **Emergency Inbox** on or off. This controls whether your users can access their email from Sophos Central Self Service.
- Turn **Allow/Block list** on or off. This controls whether your users can create their own allow and block rules for email addresses and domains.

### 3.7.32 Domains Settings/Status

Configure and manage email domains protected by **Email Gateway**.

Go to **Settings > Domain Settings/Status**.

**Add a domain**

**Tip**

Instructions on how to set up your domain for common providers are available online. Example: Office 365.

To view the instructions:

1. Expand **Configure External Dependencies**.
2. Under **Inbound Settings**, click the link for your chosen provider.
3. Use the information to help you configure your email domain.
   - Click **Outbound Settings** to view your outbound relay host.

To add a domain:
1. Click **Add Domain**.

2. In the **Email Domain** text field enter your email domain. Example: `example.com`.
   Domain ownership must be verified before mail will be delivered through Sophos Central. To verify domain ownership, you need to add a TXT record to your domain. Adding this record will not affect your email or other services.

3. Click **Verify Domain Ownership**.

4. Use the details given in **Verify Domain Ownership** to add the TXT record to your Domain Name Server (DNS).
   
   **Note**
   This can take up to ten minutes to take effect.

5. Click **Verify**.

   **CAUTION**
   You cannot save an unverified domain. You must correct any issues with the domain ownership verification.

6. Select the direction you want to configure the domain for. If you select **Inbound and Outbound**, you will need to select an outbound gateway from the drop-down list. If you select **Custom Gateway**, at least one IP/CIDR (subnet range) is required. Enter the IP and CIDR and click **Add**. You can add multiple IP addresses/ranges.

7. Select whether you wish to use a mail host or a mail exchange (MX) record in the **Inbound destination** drop-down list.
   
   **Note**
   You must use a mail exchange record if you want to use multiple destinations.
   
   a) If you selected **Mail Host** enter an IP address or an FQDN (fully-qualified domain name) in the **IP/FQDN** text field. Example: `111.111.11.111` or `mymail@example.com`.
   
   b) If you selected **MX** enter an FQDN in the **MX** text field. Example: `mymail@example.com`.

8. In the **Port** text field enter the port information for your email domain.

9. Expand **Information to configure External Dependencies**.
   
   The **Mail Routing Settings** tab shows the Sophos delivery IP addresses and MX record values used for configuring mail flow for your region.
   
   a) Make a note of the appropriate settings so that you know where to allow SMTP traffic from.
   
   b) Ensure that you configure your mail flow for **Email Security**.

10. Click **Save** to validate your settings.

11. Click the **Base Policy** link to configure spam protection.

   **Note**
   Spam protection applies to all protected mailboxes by default. You must review the settings to check that they are appropriate.

   You can add extra domains at any time.
Delete a domain

To delete a domain, click on the gray cross to the right of the domain you wish to remove.

Edit a domain

To edit a domain, click on the domain name in the list, change the settings and click Save.

DKIM keys

Manage your DKIM keys to sign and authenticate outbound emails.

Introduction

DomainKeys Identified Mail (DKIM) is used to authorize an email by verifying its digital signature, which associates a domain name with the email.

Related information

DKIM

Outbound DKIM signing

To set up outbound DKIM signing, you need to generate a DKIM key in Sophos Email.

A public key is generated which you use to create and publish a DKIM TXT record, and a private key in generated in the background.

When you send an email, Sophos Email applies policy settings to the email and then creates a hash of the mail content and adds a new header.

Note

The hash is encrypted by your private key.

When the receiving mail server sees that an email has a DKIM signature, it does a DNS lookup to find the DKIM TXT record associated with the sending domain. It uses the public key to decrypt the digital signature back to the hash value. It then takes the elements of the message that were signed and creates it's own hash that it compares it to the decrypted hash. If these do not match, the DKIM check will fail.

Add a DKIM key

Add a DKIM record to your domain so that outgoing mail will be signed and authenticated against your domain.

Generate a DKIM key in Sophos Email and create a DNS TXT record for your domain.

CAUTION

If you have smart banners turned on, we strongly recommend that you sign emails with a DKIM key. We remove the banners on outbound replies, which modifies the emails.

1. Go to Global Settings > Domains settings/status and click on the domain you want to add a DKIM key to.
2. Click Add key.
3. Copy the DKIM information that is generated automatically and use it to create a DNS TXT record for your domain.
   
   You need to speak to your third party DNS provider about setting this up.
   
   **Note**
   
   A key pair is generated by Sophos Email. The private key is generated in the background and is stored in Sophos Email. The public key is visible in the DKIM information and is used to create your DNS TXT record.
   
4. Wait for the DNS TXT record to propagate. This may take up to an hour.
5. Once your DNS TXT record has been published, click on Test record to check that your DNS TXT record matches the information in Sophos Email.
   
   **Note**
   
   If the test fails, check your DNS TXT record, correct any mistakes, and click Test record.

6. Activate the DKIM key then click Save.
   
   The DKIM key is activated. Note that this deactivates any other active DKIM key for that domain.
   
   You can now add DKIM keys for your other domains.

### 3.7.33 Email Encryption

You can encrypt emails.

**Restriction**

This option is only available with an Email Advanced license.

The encryption type Sophos Email uses is push based email encryption using AES 256.

To turn encryption on or off, go to Settings > Encryption settings.

**Note**

Make sure TLS (Transport Layer Security) v1.2 is enabled on your email gateway before enabling encryption here, otherwise the connection with Sophos will break, and you will not be able to send or receive email. The ciphers required are 'TLSv1.2+FiPS:kRSA+FiPS:leNULL:laNULL'. For more information, see FIPS mode and TLS.
General settings

Warning
- Microsoft Office documents, ZIP files and PDF files are encrypted natively.
- Multiple attachments may be generated from files that have been encrypted natively.
- All other files, for example plain text and HTML will be encrypted as PDFs. Email content will be encrypted as a PDF.
- You need to install Adobe Reader to view encrypted emails and attachments that have been encrypted as PDFs.
- You can view and reply to messages on mobile devices.

- You can select the following encryption options:
  - **Send via TLS if available**
    TLS prevents eavesdropping and tampering with the message in transit.

  **Note**
  If TLS is not available, the entire message will be encrypted as a PDF.

  - **Encrypt entire message**
    The email and attachments are encrypted with a password.
    The first time an encrypted email is sent to you, an email is sent from Sophos asking you to click on a link to set a Sophos Secure Message password. You need to do this within 30 days, otherwise the email expires. When you click on the link, you are directed to Sophos Secure Message where you can set your password.

  **Note**
  The password can only be used for emails within the region that the original email came from. If you receive an email from another region, you need to set another password.

  After setting the password, you receive an email from Sophos including the encrypted email and any encrypted attachments. To access them, open them and type in the password you created.

  You can reply to encrypted emails securely by clicking **Reply** on the encrypted PDF.

  - **Encrypt attachments only**
    The steps are the same as above, however only attachments are encrypted.
    You can also change the language used for notification and registration messages. Select a language from the list.

- **End-user options**
  - **Allow your users to send encrypted messages with a subject line tag.**
    Enter your preferred subject line tag. The tag is not case sensitive.
  - **Outlook Add-in (for Office 365 users only)**
You can allow users to encrypt emails using the Outlook Add-in by downloading and installing the Outlook Add-in relevant for the user’s Outlook client. An Outlook Add-in is available for the Windows client and another Outlook Add-in is available for both Web and Mac clients.

**Note**
The Outlook Add-in used for Mac clients will only work if you have turned on the *Allow your users to send encrypted messages with a subject line tag* option. When the subject line tag is changed, the Outlook Add-in must be downloaded and re-installed on Mac clients.

To download an Outlook Add-in, click **Download Windows Outlook Add-in** or **Download Web/Mac Outlook Add-in**.

For installation instructions, see Installing the Sophos Outlook Add-in for Encryption.

When you compose an email, to encrypt it with the Outlook Client, click **Encrypt**. You can deselect **Encrypt** if you change your mind and do not want to encrypt the email.

In the Web Client and the Windows Client, clicking **Encrypt** will flag the email for encryption (add a header to the email).

In the Mac client, clicking **Encrypt** will tag the message subject for encryption.

### Addresses and domains

Add recipient addresses and domains for which you want to encrypt messages. Text is not case sensitive and wildcards are not supported.

**Related concepts**
Installating the Sophos Outlook Add-in for Encryption (page 489)

**Related information**
FIPS mode and TLS

### 3.7.34 Time of Click Block/Warn Pages

You can add suspicious sites to the **Time of Click Block/Warn Pages**.

**Restriction**
This option is only available with an **Email Advanced** license.

To manage Time of Click URL Protection settings for suspicious sites, go to **Settings > Time of Click Block/Warn Pages**.

Turn on **Custom Block & Warn Pages** to enable customization.

You can enter your own message to be displayed when a URL is either blocked or warned. Click **Preview** to view the page.

You can also upload a custom logo by entering the path where the logo is stored.

Click **Save** when you are satisfied with your changes.
3.7.35 URL allow list

You can add domains to the allow list so that URLs from those domains are neither rewritten nor scanned by Time of Click protection.

**Restriction**
This option is only available with an Email Advanced license.

Click Add and enter the URL you want to allow, for example domain.com, then click Save.

**Note**
Wildcards are supported, for example *.domain.com.

To delete a URL from the allow list, select it and click Delete. You can select single, multiple or all URLs.

3.7.36 Enforced TLS connections

You can force specific external domains to use Transport Layer Security (TLS) connections for email.

**Restriction**
This option is only available with an Email Advanced license.

To manage domain names with TLS connections, go to Settings > Enforced TLS Connections.

You can:

- Add domain names (wildcards are supported).
- Search the list of domains that already have TLS connection enforced.
- Change the settings for a domain.
- Delete domain names from the list.

If you have issues with TLS connections, check that TLS is enabled, with the correct version and correct ciphers (see below). If you still have problems, contact Sophos Email Support.

**Adding a new domain name**

When you add a new domain name to the list, servers connect to and from that domain with TLS. The email gateway connects with servers using TLS 1.2 or later, and with ciphers consistent with our email encryption product. The connection is valid if a STARTTLS ping returns successfully.

**Note**
Make sure TLS 1.2 is enabled on your email gateway before enforcing it on any domains. Otherwise the connection with Sophos breaks and you cannot send or receive email. The ciphers required are ‘TLSv1.2+FIPS:kRSA+FIPS:!eNULL:!aNULL’.
TLS failures

If Sophos Email can't make a TLS connection, email isn't sent. Email is queued for redelivery for 7 days. After this it is deleted.

Logging of TLS connection errors

Each time Sophos Email can't send email due to TLS failures it makes an entry in the history log. After the final failure, an entry saying that the email was deleted because of TLS policy is added to the log. The entries have this format: "Processing: Check TLS".

Related concepts
Email Encryption (page 155)
You can encrypt emails.

Related information
FIPS mode and TLS

3.7.37 Impersonation Protection and VIP Management

Impersonation Protection detects phishing emails that pretend to come from well-known brands or from important people within your organization.

Restriction
This option is only available with an Email Advanced license.

Impersonation Protection looks for two types of impersonation:
1. Imitation of a well-known brand, often a financial organization or online shopping site.
2. Use of the names of important people in phishing emails.

Impersonation Protection is turned on by default and controlled by Email Security policy settings.

VIP management

On the VIP management page you can enter up to 200 email addresses of very important people (VIPs) in your organization. Emails are monitored for signs of impersonation of these addresses.

You can manually add email addresses with the Add VIP function.

The Help me find VIPs function searches a connected Active Directory (AD) service for high-risk users. The more information you've added to your AD entries (for example job titles) the better the results are. You then select users from the search results.

Related concepts
Enhanced Email Malware Scan (page 464)
You can apply enhanced email content scanning.

Email Security Policy (page 458)
You can apply security settings to your mailboxes using **Email Security** policies.

### 3.8 Protect Devices

You can download Sophos installers and use them to protect your devices.

The installers you can see may depend on the license or licenses you have.

Before you start, check which operating systems you can protect with Sophos Central: see the Sophos Central page.

For more details, including what each product does, how you use the installers, and how Sophos Central registers devices and applies policies, read the other topics in this section.

**How to use installers**

After downloading installers for workstations or servers, you can:

- Run the installer to protect the local computer.
- Transfer the installer to other computers and run it on them.
- Use automated software deployment tools such as System Center Configuration Manager (SCCM) to run the installer on large numbers of computers.

**How to find out which data center stores your account**

To find out which data center stores your Sophos Central account data, do as follows:

1. Go to **Protect Devices**.
2. Under **Endpoint Protection** or **Server Protection**, hover the mouse pointer over any of the installer download links.
   
   The data center address is shown in the lower-left corner of the browser:


3. The address shows the geographical location of the data center:

<table>
<thead>
<tr>
<th>Address</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://api-cloudstation-us-east-2.prod.hydra.sophos.com">https://api-cloudstation-us-east-2.prod.hydra.sophos.com</a></td>
<td>US east</td>
</tr>
<tr>
<td><a href="https://api-cloudstation-eu-central-1-prod.hydra.sophos.com">https://api-cloudstation-eu-central-1-prod.hydra.sophos.com</a></td>
<td>EU central</td>
</tr>
</tbody>
</table>

**Related information**

Sophos Central page
### 3.8.1 Endpoint Protection

You install an Endpoint Protection agent on workstations to protect them against malware, risky file types and websites, and malicious network traffic.

It also offers peripheral control, web control and more.

Sophos Device Encryption is also installed automatically on Windows workstations (if you have the required license).

#### Download and run installers

Go to [Protect Devices](#).

Download the installer for your operating system and run it on workstations you want to protect.

- **Download Complete Windows Installer**: Click this for an installer with all endpoint products your license covers.
  
  Alternatively, click [Choose Components…](#) to choose which products will be included in the installer. The choices are:
  
  — **Sophos Intercept X Advanced** (protection from ransomware and exploits).
  
  — **Device Encryption**.

- **Download Complete macOS Installer**: Click this for an installer with all endpoint products your license covers.
  
  Alternatively, click [Choose Components…](#) to choose which products will be included in the installer. The choices are as for Windows above.

- **Send Installers to Users**: Click this to go to a page where you can add users and send them installers that they can use.

**Note**

For Linux, look for “Server Protection”. Sophos Central treats all Linux computers as servers.

#### What happens when you protect a computer

When you protect a computer:

- Each user who logs in is added to the users list in Sophos Central automatically.
- Default policies are applied to each user.
- Each computer is added to the **Computers** list in Sophos Central.

#### How we handle Windows usernames and login names

Users are listed with full login name, including the domain if available (for example, `DOMAINNAME\jdoe`).

If there is no domain, and a user logs in to multiple computers, multiple user entries are displayed for this user, for example `MACHINE1\user1` and `MACHINE2\user1`. To merge these entries, delete...
one and assign the login to the other (and rename the user, if required). See Endpoint protection deployment methods.

**Related reference**

**Installer command-line options for Windows** (page 262)
You can use the following command-line options with the Sophos Central Endpoint installer for Windows.

**Installer command-line options for Mac** (page 266)
The Sophos Central Endpoint installer for Mac supports the following command-line options.

**Related information**
Endpoint protection deployment methods

**Installer command-line options for Windows**

You can use the following command-line options with the Sophos Central Endpoint installer for Windows.

### Command-line options

These options apply to:

- Sophos Endpoint Advanced 11.5.11 and later.
- Sophos Endpoint Standard 11.5.11 and later.

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet</td>
<td>--quiet</td>
<td>Runs the installer without displaying the user interface.</td>
<td></td>
</tr>
<tr>
<td>No proxy detection</td>
<td>--noproxydetection</td>
<td>Doesn’t attempt to perform automatic proxy detection.</td>
<td></td>
</tr>
<tr>
<td>No competitor removal</td>
<td>--nocompetitorremoval</td>
<td>Doesn’t attempt to automatically remove competitors. (Only on installation of Sophos Anti-Virus.)</td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>--language=&lt;language ID&gt;</td>
<td>Allows you to manually set the installer language. By default the installer uses the system language.</td>
<td>Language ID</td>
</tr>
<tr>
<td>Group</td>
<td>--devicegroup=&lt;Central group&gt;</td>
<td>Specifies the Sophos Central device group to join the endpoint to. A group to join. If it doesn’t exist, it is created.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CRT catalog path</td>
<td><code>--crtcatalogpath=&lt;path to CRT catalog&gt;</code></td>
<td>Allows you to specify your own catalog of competitors to remove.</td>
<td>Full path and filename to catalog folder. Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>--crtcatalogpath=C:\catalog\productcatalog.xml</code></td>
</tr>
<tr>
<td>Message relays</td>
<td><code>--messagerelays=&lt;comma-separated message relay list of IPs including the port&gt;</code></td>
<td>Specifies a list of message relays to use.</td>
<td>The IP address of the message relay must be specified along with the port 8190. Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><code>--messagerelays=IPADDRESS:8190</code></td>
</tr>
<tr>
<td>Proxy address</td>
<td><code>--proxyaddress=&lt;custom proxy address&gt;</code></td>
<td>Specifies a custom proxy to use.</td>
<td>URL without protocol (will use HTTPS)</td>
</tr>
<tr>
<td>Proxy username</td>
<td><code>--proxyusername=&lt;custom proxy user name&gt;</code></td>
<td>If a custom proxy has been specified, set the username with this option.</td>
<td>The username of the proxy.</td>
</tr>
<tr>
<td>Proxy password</td>
<td><code>--proxypassword=&lt;custom proxy password&gt;</code></td>
<td>If a custom proxy and username have been specified, set the password with this option.</td>
<td>The password for the proxy.</td>
</tr>
<tr>
<td>Computer name override</td>
<td><code>--computernameoverride=&lt;override for computer name&gt;</code></td>
<td>Overrides the name of the computer to be used in Sophos Central.</td>
<td>Custom computer name.</td>
</tr>
<tr>
<td>Computer description override</td>
<td><code>--computerdescriptionoverride=&lt;override for description&gt;</code></td>
<td>Overrides the description of the computer to be used in Sophos Central.</td>
<td>Custom computer description.</td>
</tr>
<tr>
<td>Domain name override</td>
<td><code>--domainnameoverride=&lt;override for domain&gt;</code></td>
<td>Overrides the domain name of the computer to be used in Sophos Central.</td>
<td>Custom domain name.</td>
</tr>
<tr>
<td>Customer token</td>
<td><code>--customertoken=&lt;the customer token&gt;</code></td>
<td>Specifies the token of the Sophos Central customer to associate the endpoint with.</td>
<td>A UUID which maps to a customer.</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Products to install</td>
<td><code>--products=&lt;comma-separated list of products&gt;</code></td>
<td>Specifies a list of products to install. If you specify a product that you don't have a license for, then it isn't installed.</td>
<td>A list of products to install, comma-separated. Available options are: antivirus, intercept, mdr, deviceEncryption or all.</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local install source</td>
<td><code>--localinstallsource=&lt;path-to-install-source&gt;</code></td>
<td>Specifies a local install source to use during installation. This allows an installation to occur without having to download the installer files.</td>
<td>It isn't necessary to populate the local install source, but it is necessary to create a SophosLocalInstallSource folder. If an empty folder is provided it is populated during the first installation. If you wish to pre-populate the cache you can take a copy of the files from an already installed endpoint or from your update cache:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>%ProgramData %\Sophos \AutoUpdate\data \Warehouse %ProgramData %\Sophos \UpdateCache\www \warehouse Even if a populated local install source is provided, internet access is still required and some files are downloaded. The amount of data downloaded depends on various factors including, for example: Whether the platform of the installation endpoint differs from the files already populated. Whether the warehouse has changes since the local install source was populated. For the purpose of this example SomeContent represents the files and folders within the Warehouse folder. Go to %ProgramData %\ Sophos \AutoUpdate \data \ Warehouse</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Message trail logging</td>
<td>--traillogging</td>
<td>Turns on the logging of message content between the endpoint and Sophos Central during installation. You must switch this option off after installing, see Enabling a diagnostic message trail of Sophos MCS.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
There is no command-line option for installation from an update cache. The installer automatically assesses connectivity to any update caches set up in the Sophos Central account and installs from them.

**Windows examples**

Install Sophos Anti-Virus and Intercept X without user interaction:

```
SophosSetup.exe --products=antivirus,intercept --quiet
```

Install using a proxy:

```
SophosSetup.exe --proxyaddress=<ProxyIP/FQDN>:<Port>
```

Install using a message relay:

```
SophosSetup.exe --messagerelay=192.168.10.100:8190
```

**Language IDs**

<table>
<thead>
<tr>
<th>Language</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>1033</td>
</tr>
<tr>
<td>French</td>
<td>1036</td>
</tr>
<tr>
<td>German</td>
<td>1031</td>
</tr>
<tr>
<td>Japanese</td>
<td>1041</td>
</tr>
<tr>
<td>Spanish</td>
<td>1034</td>
</tr>
<tr>
<td>Italian</td>
<td>1040</td>
</tr>
<tr>
<td>Polish</td>
<td>1045</td>
</tr>
<tr>
<td>Brazilian Portuguese</td>
<td>1046</td>
</tr>
<tr>
<td>Language</td>
<td>ID</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Korean</td>
<td>1042</td>
</tr>
<tr>
<td>Chinese Simplified (Mandarin)</td>
<td>2052</td>
</tr>
<tr>
<td>Chinese Traditional (Cantonese)</td>
<td>3076</td>
</tr>
<tr>
<td>Chinese Hong Kong</td>
<td>3076</td>
</tr>
<tr>
<td>Chinese Macau</td>
<td>3076</td>
</tr>
<tr>
<td>Chinese Singapore</td>
<td>2052</td>
</tr>
</tbody>
</table>

**Related information**

- Enabling a diagnostic message trail of Sophos MCS
- Domains and ports required for communication to and from Sophos Central Admin and the Sophos Central managed endpoint
- Frequently Asked Questions (FAQs)
- New endpoint installer frequently asked questions
- An Internet connection could not be established
- Installer precheck messages

**Installer command-line options for Mac**

The Sophos Central Endpoint installer for Mac supports the following command-line options.

**Mac command line options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet</td>
<td>--quiet --install</td>
<td>Runs the installer without displaying the user interface.</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>--devicegroup &lt;Central group&gt;</td>
<td>Specifies the Sophos Central device group to join the endpoint to.</td>
<td>A group to join. If it doesn't exist, it is created.</td>
</tr>
<tr>
<td>Message relays</td>
<td>--messagerelays &lt;space-separated message relay list of IPs including the port&gt;</td>
<td>Specifies a list of message relays to use.</td>
<td>The IP address of the message relay must be specified along with the port, 8190.</td>
</tr>
</tbody>
</table>

Example: --messagerelays IPADDRESS:8190

IPADDRESS:8190
<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy address</td>
<td>--proxyaddress &lt;custom proxy address&gt;</td>
<td>Specifies a custom proxy to use.</td>
<td>URL without protocol (uses HTTPS).</td>
</tr>
<tr>
<td>Proxy port</td>
<td>--proxyport &lt;proxy port&gt;</td>
<td>Specifies a port that the proxy uses.</td>
<td>Port for the proxy.</td>
</tr>
<tr>
<td>Proxy username</td>
<td>--proxyusername &lt;custom proxy user name&gt;</td>
<td>If a custom proxy has been specified, set the username with this option.</td>
<td>The username for the proxy.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>--proxypassword &lt;custom proxy password&gt;</td>
<td>If a custom proxy and username have been specified, set the password with this option.</td>
<td>The password for the proxy.</td>
</tr>
<tr>
<td>Computer name override</td>
<td>--computernameoverride &lt;override for computer name&gt;</td>
<td>Overrides the name of the computer to be used in Sophos Central.</td>
<td>Custom computer name.</td>
</tr>
<tr>
<td>Computer description override</td>
<td>--computerdescriptionoverride &lt;override for description&gt;</td>
<td>Overrides the description of the computer to be used in Sophos Central.</td>
<td>Custom computer description.</td>
</tr>
<tr>
<td>Domain name override</td>
<td>--domainnameoverride &lt;override for domain&gt;</td>
<td>Overrides the domain name of the computer to be used in Sophos Central.</td>
<td>Custom domain name.</td>
</tr>
<tr>
<td>Preferred domain name for usernames in Sophos Central</td>
<td>--mcsPreferredDomainName</td>
<td>Sets the client to send usernames as domain\username instead of machine \username.</td>
<td></td>
</tr>
<tr>
<td>Registration server</td>
<td>--mgmtserver &lt;registration server URL&gt;</td>
<td>Specifies the MCS server to connect to.</td>
<td>MCS server URL.</td>
</tr>
<tr>
<td>Customer token</td>
<td>--customertoken &lt;the customer token&gt;</td>
<td>Specifies the token of the Sophos Central customer to associate the endpoint with.</td>
<td>A UUID which maps to a customer.</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Products to install</td>
<td>--products &lt;space separated list of products to install&gt;</td>
<td>Specifies a list of products to install. If you specify a product that you don't have a license for, then it isn't installed.</td>
<td>A list of products to install, space-separated. Available options are: antivirus, intercept, deviceEncryption or all.</td>
</tr>
</tbody>
</table>

### Note

The Mac installer is aware of all the message relays and update caches when the installation is downloaded. Changes to caches and relays mean that you need to download a new installation. You can specify relays using the command line as well.

### Mac examples

**Install Sophos Anti-Virus and Intercept X without user interaction:**

```bash
sudo ./Sophos/Installer.app/Contents/MacOs/Sophos/Installer --products antivirus intercept --quiet
```

**Install using a proxy:**

```bash
sudo ./Sophos/Installer.app/Contents/MacOs/Sophos/Installer --proxyaddress <ProxyIP/FQDN> --proxyport <Port>
```

**Install using a message relay:**

```bash
sudo ./Sophos/Installer.app/Contents/MacOs/Sophos/Installer --messagerelays 192.168.10.100:8190
```

### 3.8.2 Encryption

Sophos Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers. Encrypting hard disks keeps data safe, even when a device is lost or stolen.

For full details of how computers are encrypted, see [Sophos Central Device Encryption administrator guide](#).

### Download and run installer

**Go to Protect Devices.**

Download an **Endpoint Protection** installer and run it on the computers you want to protect. You can choose from:

- **Download Complete Windows Installer**: Click this for an installer with all endpoint products your license covers.

  Alternatively, click **Choose Components...** to choose which products will be included in the installer. The choices are:
Sophos Central Admin

— Sophos Intercept X Advanced with EDR (protection from ransomware and exploits).
— Device Encryption.

• Download Complete macOS Installer: Click this for an installer with all endpoint products your
  license covers.
  Alternatively, click Choose Components… to choose which products will be included in the
  installer. The choices are as for Windows above.

• Send Installers to Users: Click this to go to a page where you can add users and send them
  installers that they can use.

Related information
Sophos Central Device Encryption administrator guide

3.8.3 Server Protection

You install a Server Protection agent on servers to protect them against malware, risky file types and
websites, and malicious network traffic.
To protect a server, download the installer for your operating system and run it on the server.

Download and run the Windows installer

1. Go to Protect Devices.
2. Click Download Windows Server Installer.
3. Go to the Downloads folder and run the installer.

Download and run the Linux EDR or Linux MTR installer

If you have a license for Linux EDR (Endpoint Detection and Response) or Linux MTR (Managed
Threat Response), you see a link to the appropriate installer.
1. Go to Protect Devices.
2. To download the installer from your browser, click Download Linux MTR Installer or Download
   Linux EDR Installer.
   Alternatively, to download the installer from a command line or script, do as follows:
   a) Right-click the installer link and copy the link address.
   b) On the Linux server, at a command prompt or in a script, use wget with the link address:
      

   c) Move the installer to the Downloads directory.
3. Run the installer as follows:
   a) Change to the Downloads directory.
   b) Change the file permissions to include “execute”:
      
   c) Run the installer:
If you are not signed in as root, run the installer with the `sudo` command:
```
sudo ./SophosSetup.sh
```

### Download and run the Linux Server installer

The Linux Server installer provides anti-virus protection. It doesn't provide the more advanced features of Linux EDR or Linux MTR.

1. Go to **Protect Devices**.
2. To download the installer from your browser, click **Download Linux Server Installer**.
   Alternatively, to download the installer from a command line or script, do as follows:
   a) Right-click **Download Linux Server Installer** and copy the link address.
   b) On the Linux server, at a command prompt or in a script, use `wget` with the link address:
      ```
      wget Linux installer link
      ```
   c) Move the installer to the **Downloads** directory.
3. Run the installer as follows:
   a) Change to the **Downloads** directory.
   b) Change the file permissions to include “execute”:
      ```
      chmod +x SophosInstall.sh
      ```
   c) Run the installer:
      ```
      ./SophosInstall.sh
      ```
      If you are not signed in as root, run the installer with the `sudo` command:
      ```
      sudo ./SophosInstall.sh
      ```

### What happens when you protect a server

When you protect a server:
- The server is added to the **Servers** list in Sophos Central.
- Default policies are applied to the server.

**Related concepts**

- **Protect Devices** (page 395)

You can download Sophos installers and use them to protect your devices.

### 3.8.4 Server Protection on Microsoft Azure

You can protect Azure VMs with Intercept X Advanced for Server as you create them.
This involves downloading a custom extension script and using it.

1. Go to **Protect Devices**.
2. Find **Server Protection on Microsoft Azure**.
3. Click **Get your VM extension script**. Then click **Download Script**.
   You’ll need an API token so that the script can find and access the installer. If you don’t have a token, we’ll create one for you.

4. Click **Deploy Server Protection to a new Azure VM**. This displays a link to an article on how to use a custom extension script.

5. Follow the steps in the article to deploy the new VM.

**Related concepts**

Protect Devices (page 395)

You can download Sophos installers and use them to protect your devices.

### 3.8.5 Virtual Environment Protection

Sophos for Virtual Environments lets you protect your virtual machines (VMs) and manage them from Sophos Central.

To set up protection for VMs, you do as follows:

- Install Sophos Security VM on your host. This provides central anti-virus scanning for guest VMs.
- Install Sophos Guest VM Agent on your guest VMs. This is required for each guest VM that you want to protect. The agent enables communication between the guest VM and Sophos Security VM as well as automatic cleanup of threats.

**Download the installer**

Go to **Protect Devices**.

To get started, you only need to download the Sophos Security VM installer. You’ll be prompted to get the installer for the agent later.

Select the installer for the environment you want to protect: **Hyper-V** and/or **ESXi**.

We recommend you read the startup guide.

**Note**

If you’ve been managing Sophos for Virtual Environments from Sophos Enterprise Console until now, or if you’re migrating from Sophos Anti-Virus for vShield, see “Migrate to Sophos for Virtual Environments” in the startup guide.

**What happens after installation**

After you install Sophos Security VM on your host:

- This instance of Sophos Security VM is added to the **Servers** list in Sophos Central.
- Server policies are applied to the security VM (by default, these are the Base policies).
- Remember you must have installed Sophos Guest VM Agent on each guest VM and checked it is connected.

**Related concepts**

Protect Devices (page 395)
You can download Sophos installers and use them to protect your devices.

**Related information**
Sophos for Virtual Environments startup guides

### 3.8.6 Web Gateway

You install Sophos Web Gateway on workstations or mobile devices to provide advanced web security. It can block malicious, risky, or inappropriate websites, and provide scanning for secure sites (SSL), keyword filtering, trusted networks, and comprehensive reporting.

**Install Web Gateway on workstations**

Go to **Protect Devices**.
Download the installer for your operating system and run it on workstations you want to protect.

**Note**
You can install Web Gateway alongside the Endpoint Protection agent or on its own.

When you protect a workstation:
- The installer checks if there is already an Endpoint Protection agent on the computer. If not, it asks you for a username.
- If the user is new, they are added to the Users list.
- If the computer is not already in the **Computers** list, it is added.
- If you have a Web Gateway policy enabled for the user or computer, it starts protecting the computer.

**Install Web Gateway on mobile devices**

Go to **Protect Devices**.
Click the operating system you want. You'll see instructions for sending a configuration profile to a mobile device and applying a policy.

### 3.8.7 Firewall Protection

You can install the Sophos XG Firewall to protect your network.

If you haven't managed firewalls from Sophos Central yet, you can start a virtual firewall trial from the **Firewall Management** dashboard.

If you want to install further firewalls, do as follows:

1. Go to **Overview > Protect Devices**.
2. Look for the **Firewall Protection** section.
3. Get your download.
4. Get deployment instructions from Virtual and software appliance install guide.
Related information
Virtual and software appliance install guide
4 Endpoint Protection

Endpoint Protection lets you protect your users and devices against malware, risky file types and websites, and malicious network traffic. It also offers peripheral control, web control and more.

Related information
Sophos Endpoint for Windows help
Sophos Endpoint for Mac help

4.1 Dashboard

The Dashboard is the start page of Endpoint Protection and lets you see the most important information at a glance.

It consists of these areas.

Most recent threat cases

Threat cases let you investigate malware attacks. Click a case to find out where an attack started, how it spread, and which processes or files it has affected.

Click See all threat cases to see all threat cases.

Threat cases are available only for Windows devices.

Devices and users: summary

**Devices and users: summary** shows details of usage and protection for users or protected devices. It also shows the number of unprotected users or devices.

Click on the tabs to see information for each device type or for users.

Click See Report to open a detailed report for the tab you have selected.

Web control

**Web control** shows statistics for your Web Control protection.

The figures are for threats blocked, policy violations blocked, and policy warnings. There is also a figure for "policy warnings proceeded", which is the number of users who have bypassed a warning to visit a website.

Click on a figure to open a detailed report.
4.2 Logs & Reports

The Logs & Reports page lists the reports that you can generate about security features in Sophos Central.

The page also lists any Saved Reports. These are custom reports that you or other administrators for this account have saved.

To find out more about logs, see Logs.

To find out how reports work and how you can customize, save and schedule them, see Reports.

Related concepts
Logs (page 176)
Reports (page 177)

4.2.1 Logs

The following log is available for Endpoint Protection:

• Data Loss Prevention. All events triggered by data loss prevention rules for computers or servers, see Data Loss Prevention Events Log.

Related concepts
Data Loss Prevention Events Log (page 176)

Data Loss Prevention Events Log

The Data Loss Prevention Events Log displays all events triggered by data loss prevention rules for computers or servers.

Note
An endpoint computer can send a maximum of 50 data control events per hour to Sophos Central. All events are logged locally on the endpoint computer.

You can find the following features and information on the Data Loss Prevention Events Log:

Search: If you want to view events for a certain user, device or rule name, enter the name of the user, device, or rule in the search box.

Choose period: Use the box to select the time period for which you want to view events. If you select Custom, use the From and To fields to select the dates between which you want to view events. You can view events that occurred in the past 90 days or less.

Filter by rule name: You can filter the events by rule name.

Filter by file type: You can filter the events by file type.

Update: Click this to display any new events reported since the page was last opened or refreshed.

Event table

The event table provides these event details:
1. **Date and time**: Time and date when the event occurred
2. **User**: Source that caused the event, for example, the name of a user or system
3. **Device**: Device that caused the event
4. **Rule name**: Data loss prevention rule that caused the event
5. **Rule action**: Data loss prevention action that caused the event
6. **File name**: Name of the file that caused the event
7. **Destination type**: Name of the destination that caused the event

**Save as Custom Report** lets you save the report settings in the **Saved Reports** table on the **Logs & Reports** page.

The **Export** menu (on the right of the table) lets you export the current view or the report for the past 90 days as a CSV (comma separated value) or PDF file.

### 4.2.2 Reports

The reports that you can see depend on your license.

You can customize reports, save them and send them out as scheduled emails.

**Note**

A report may not support all the customization or viewing options.

**Limit report data to a specific time range**

In some reports, you can limit report data to a specific date range by entering a **From** and **To** date.

In some reports, you can select a time period.

**Filter reports**

In some reports, you can filter the displayed information by clicking on the category tiles. For example, in the Computers report you can show all the active computers by clicking on **Active**.

You may also be able to filter by groups.

You can also use **Search** to filter for specific information.

**Print or export reports**

You can print or export your reports.

- **Print**: Click this to open a printer-friendly view. Then press Ctrl+P to open the printer dialog.
- **Export to CSV**: Click this to export the current view as a comma separated file.
- **Export to PDF**: Click this to export the current view as a PDF file.
Save and email custom reports

You can create and save custom reports. A list of the saved reports is shown at the top of the Logs & Reports page.

You can also choose to send custom reports by email and set up a schedule for them. You can save as many reports as you like, but you can only schedule up to 25.

1. Set up the report by selecting the appropriate filters.
2. Click Save as Custom Report.
   This opens the Save Report dialog.
3. Enter a Name for the report.
4. If you want to send the report by email, select one of these options:
   • Send a link to the report.
   • Attach the report to the email.
     We recommend that you send a link if the report includes personally identifiable information.
     You need to enter Sophos Central sign-in credentials to view reports from a link.
5. Select the Frequency. You can choose from monthly or weekly.
6. Select the format: PDF or CSV.
7. Click Save.
   The email is received by the user who signs in and creates the report.

Note
Scheduled emails stop after six months. You can reschedule them if you want to.

Recover tamper protection passwords

You can recover the tamper protection passwords of devices that you've recently deleted.

You might need to do this so that you can uninstall Sophos software that is still on those devices.

1. Go to Logs & Reports.
2. In Reports, under Endpoint & Server Protection, click Recover Tamper Protection passwords.
   You see a list of deleted devices.
3. Find the device you want.
4. In the Password(s) column, click View password details.
   This shows you the password (and previous passwords).
4.3 People

On the **People** page, you can manage your users and user groups.

### 4.3.1 Users

On the **Users** tab of the **People** page, you can add or manage users, and get the users’ computers protected.

You can also enable the users to protect their own devices by emailing them a setup link.

The current users are listed with their details.

**Health Status.** An icon shows whether the user has security alerts on any of their devices.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Check Mark]</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>![Amber Warning Sign]</td>
<td>Amber warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>![Red Warning Sign]</td>
<td>Red warning sign if there are critical alerts.</td>
</tr>
</tbody>
</table>

**Name** Click the user's name to see details of devices and to see which has an alert.

**Email.**

**Exchange Login.**

**Last Active.** The last time a user reported to Sophos Central.

**Group Name.** This is shown if the user has been added to a user group.

**Role.** This shows what administration role, if any, the user has. This column is only visible if you are an administrator.

Click any column header to sort the users. By default, users are sorted according to the **Last Active** time.

To see full details for a user, click the user's name.

You can add users manually or automatically by protecting their devices. You can also import users in bulk from a CSV file or from Active Directory. You can also protect existing users.

To modify users, click the user's name to open and edit their user details.

You can also delete users and export lists of users.

**Related concepts**

- [User Summary](#)
- [Administration Roles](#)

**Related tasks**

- [Add a user manually](#)
You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

**Add users automatically** (page 186)
You can add users automatically by protecting their devices.

**Import users from a CSV file** (page 186)
You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

**Import users from Active Directory** (page 187)
You can import users and groups from Active Directory.

**Protect existing users** (page 187)
You can protect users that you have already added to Sophos Central.

**Delete users** (page 188)
You can delete users from Sophos Central if you are a Super Admin.

**Export to CSV** (page 188)
You can export lists of users as CSV files.

### User Summary

The **Summary** tab in a user's details page shows a summary of the following:

- The user's security status, administration role, if any, and account details.
- Recent events on the user's devices.
- Mailboxes associated with the user.
- Devices associated with the user.
- Policies that apply to the user.
- Groups that the user belongs to.
- Logins.

You can find details of each below.

The security status and account details are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.

You can click on the other tabs for more on **Devices**, **Events**, and **Policies**.

### Health Status

In the left-hand pane, an icon shows you whether the user has security alerts on any of their devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>
You can see which devices have alerts in the **Devices** tab.

A padlock icon shows that the user has been imported from Active Directory.

A badge shows the user’s assigned administration role. Click on the role name to view the settings for the role.

**Note**
Role information is only displayed for administration roles.

### Account details

In the left-hand pane, you can modify or delete the user's account.

**Note**
If a user has been imported from Active Directory, you cannot change the account details. However, you can add the user to a new Sophos Central group or add another login.

**Modify the account**

1. Click **Edit** and enter the following settings:
   - **First & Last name**: Enter the name of the user. Do not include a domain name.
   - **Role**: Select a role for the user. Choose from: **Super Admin**, **Admin**, **Help Desk**, **Read-only**, or **User**.

   **Restriction**
   You can only see the **Role** option and assign administrator roles if you are a Super Admin.

   **Note**
   You cannot amend your own administration role.

   **Note**
   Anyone with a **User** role only has access to the Self Service Portal.

   **Email Address**: Enter the email address of the user.

   **Exchange Login** (optional): Enter the Exchange account name of the user.

   **Note**
   In Sophos Mobile policies, you can use the placeholder `%USERNAME%` to refer to this setting.

   **Add to groups**: Select one of the available user groups and use the picker arrows to move it to the assigned groups.

   **Email Setup Link**: Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs.
The user needs administrative privileges and internet access in order to protect their computer.

Web Gateway provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

2. Click Save.

Delete the account
To delete the account, click Delete User in the left-hand pane. Logins assigned to this user can afterward be assigned to another user.

Restriction
You cannot delete users who have an assigned administration role.

Multi-factor authentication
If the user is an admin, the left-hand pane shows whether multi-factor authentication (MFA) is enabled for them. If it is enabled, the admin must use another form of authentication, as well as their user name and password, to sign in.

If you're a Super Admin, you can edit the settings as follows:
Click Reset to let the admin set up their MFA sign-in details again.
Click MFA Settings to go to a page where you can enable or disable multi-factor authentication for the admin.

Recent Events
This lists recent events on the user's devices.
For a full list, click the Events tab.

Mailboxes
This lists all email addresses, including distribution lists and public folders, associated with the user. Primary indicates the user's primary email address. Owner indicates the user controls a distribution list or public folder.
For full details, click an email address.

Devices
This shows a summary of the devices associated with the user.
Click the device name to go to the device's details page for more information.
Click **Actions** to carry out any of the same actions that are available on the device's details page (for example, Scan Now and Update Now for a computer).

For full details of the user's devices, click the **Devices** tab.

### Policies

This shows a summary of the policies applied to the user.

The list shows the policy name, whether the policy is enabled or not, and icons that indicate the features included in the policy.

Click on a policy name to view and edit the user policy.

**Note**

Editing the policy affects all users to which this policy is applied.

For full details of all the policies applied to this user, click the **Policies** tab.

### Groups

This shows the groups the user belongs to.

Click on a group name to see details of the group.

Click **Edit** (on the right) to change the groups the user belongs to.

### Logins

This shows the user's logins.

Click **Edit** (on the right) to change the logins assigned to the user.

### Related concepts

**About Policies**

**Administration Roles** (page 93)

Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

### User Devices

The **Devices** tab in a user's details page lets you see the devices associated with the user.

This tab also shows any servers where the user has logged on with Remote Desktop Services.

For each associated device you can see the device type and the operating system. You also have these options:

- **View Details**: This opens the full device details page.
- **Delete**: This removes the device from the list and stops Sophos Central managing it, but it does not uninstall the Sophos software.
- **Actions**: Actions you can take. These depend on the device type.
User Events

The Events tab in a user's details page lets you see a list of events detected on the user's devices. You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

- **Severity**: Hover over an icon to see what it means.
- **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
- **Details**: This link (for certain events) lets you get further details and take action.

View Events Report shows events arranged by type and a graph of events day by day.

Stop detecting an application

If an application is reported as malware but you know it's safe, you can allow it from the events list. For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the Details link beside the event and then allow the application.

**Note**

This currently applies only to malware events reported by Intercept X.

Stop detecting an exploit

If an exploit is detected but you're sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don't detect this again and select an option:
   - Exclude this Detection ID from checking: prevents this detection on this app.
   - Exclude this application from checking: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.

3. Click Exclude.

We'll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you're sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In **Event details**, look for **Don't detect this again**. Select **Exclude this Detection ID from checking**. This prevents this detection on this app.

3. Click **Exclude**. We'll add your exclusion to the Global Exclusions list.

**Related information**

*How to investigate and resolve a potential False Positive or Incorrect Detection*

**User Policies**

The **Policies** tab in a user's details page lets you see the policies that are enabled and applied to the user. Click a policy name to view and edit policy details. Editing the policy affects all users to which this policy is applied.

**Add a user manually**

You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

To add a user:

1. Go to **Users**.
2. Click Add and select **Add User**.
3. In the **Add User** dialog, enter the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First and Last Name</strong></td>
<td>Enter the name of the user. Do not include a domain name.</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>Select an administration role for the user. A user who is assigned an administration role will receive an email telling them how to set up their administration account. You can only see the <strong>Role</strong> option and assign administrator roles if you are a <strong>Super Admin</strong>. Anyone with a <strong>User</strong> role only has access to the Self Service Portal.</td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
<td>Enter the email address of the user.</td>
</tr>
<tr>
<td><strong>Add to groups</strong> (optional).</td>
<td>Select one of the available user groups and use the picker arrows to move it to the assigned groups. You can start typing a name in the search box to filter the displayed groups.</td>
</tr>
<tr>
<td><strong>Email Setup Link</strong></td>
<td>Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>more than one type of protection, select those the user needs. The user needs administrative privileges and internet access in order to protect their computer.</td>
</tr>
<tr>
<td>Web Gateway</td>
<td>This provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.</td>
</tr>
</tbody>
</table>

4. Click **Save** or **Save and Add Another**. The new user is added to the user list.

When the user downloads and installs the software, their device is automatically associated with the user.

**Add users automatically**

You can add users automatically by protecting their devices.

To add users:

1. Download an installer from **Protect Devices**.
2. Run the installer on the devices.

This adds the user of each device automatically.

**Related tasks**

- **Protect existing users** (page 187)
  You can protect users that you have already added to Sophos Central.

**Import users from a CSV file**

You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

To import users:

1. Go to **Users**.
2. Click **Add** and click **Import users from CSV**.
3. Click **Browse** and select your CSV file.

**Tip**

You can download template CSV files from the **Import users from CSV** dialog.

The CSV file can include groups a user is assigned to.

4. To create new groups, click **Create new groups**.
5. To send a registration email for the Sophos Central Self Service portal to each imported user, click **Give users access to Sophos Central Self Service**.
6. Click **Add**.
Note
The CSV file can include the email address of each user's manager. If there's a manager who isn't already a user in Sophos Central, a user is created. So the number of users imported may exceed the number of rows in the file.

Note
If an email address in your CSV file matches an existing user in Sophos Central, the user is updated with the information in your import file.

Note
If an email address in your CSV file matches an existing user in Sophos Central that is managed through Active Directory Synchronization, the user is skipped during import and no changes are made to the user account.

Import users from Active Directory
You can import users and groups from Active Directory.
To do this:
1. Go to Users.
2. Click the Set up Active Directory Sync link in the upper right of the page.
3. Follow the set up synchronization process.

Related tasks
Set up synchronization with Active Directory (page 226)
Follow these instructions to set up synchronization with Active Directory.

Protect existing users
You can protect users that you have already added to Sophos Central.
To protect them you need to email them a setup link. To do this:
1. Go to Users.
2. Select the user or users you want to protect.
3. Click Email Setup Link in the upper right of the page.
4. In the Email Setup Link dialog, select the types of protection the user needs (if your license includes more than one).

Web Gateway provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.
Users need administrative privileges and internet access to use the setup link.
Delete users
You can delete users from Sophos Central if you are a Super Admin.

Restriction
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them.

Under some circumstances, the user may be recreated automatically in future:
- If the user logs in to an associated device that is still managed by Sophos Central, they are added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they are added as a user again the next time that Sophos Central synchronizes with Active Directory.

To delete users:
1. Go to Users.
2. Click the checkbox next to each user you want to delete.
3. Click Delete.

Deleting a user does not delete devices associated with that user or remove the Sophos software from these devices.

Logins assigned to a deleted user can afterwards be assigned to another user. You can edit logins by clicking the Edit link on a user's details page.

Related concepts
User Summary (page 180)

Export to CSV
You can export lists of users as CSV files.
You can export lists of different types of user.
For example you can export a list of administrators by applying the Admins only filter before you click Export to CSV.

To export users:
1. Go to Users.
2. Click Export to CSV.
   This creates a file called users.csv. Any currently active filters are applied to the list.

4.3.2 Groups
On the Groups tab of the People page, you can add or manage groups of users.
You can use groups to assign a policy to multiple users at once.
The sections below tell you about the groups list and how to add, modify or delete groups.
About the groups list

The current groups are listed and the number of users in each group is shown. To see full details for a group, click the group's name.

Add a group

1. Click the Add Group button.
2. In the Add Group dialog, enter the following settings:
   - **Group Name**: Enter the name of the new group.
   - **Available Users**: Select users from the list of available users.

   **Tip**
   In the Search box you can start typing a name to filter down the displayed entries.

3. Click Save.

Modify a group

To modify a group, click the group's name to open and edit the group details. For more information, see User Group Details.

Delete a group

To delete a group, select it and click Delete in the upper right of the page. Deleting a group will not delete its users.

**Related concepts**
- User Group Details (page 189)
- Active Directory Sync (page 224)
  You can import users and user groups from Active Directory to Sophos Central.
- Azure AD Sync Status (page 228)

**Related tasks**
- Set up synchronization with Azure Active Directory (page 229)

**User Group Details**

On a group's details page, you can:
- Add or remove members.
- Delete the group.
Add or remove members

To add or remove members:
1. Click Edit under the group name.
2. In the Edit Group dialog, use the picker arrows to add users to the Assigned Users list or remove them.
3. Click Save.

Delete the group

To delete the group:
1. Click Delete under the group name.
2. In the Confirm Group Deletion pop-up, click Yes.

Deleting a group will not delete its users.

User Group Policies

The Policies tab in a user group's details page lets you see the policies that are enabled and applied to the group.

Click a policy name to view and edit policy details.

Editing the policy affects all groups to which this policy is applied.

4.4 Computers

On the Computers page, you can manage your protected computers.

They will appear automatically after Sophos agent software has been installed.

You can:
- View details of the computers.
- See the encryption status (if you are using Sophos Device Encryption).
- Delete computers.
- Install or uninstall software.
- Get a recovery key for encrypted computers (if you are using Sophos Device Encryption).
- Export the computers list to CSV.

Sophos Azure Active Directory synchronization can be used with Endpoint Protection and Email Gateway. See Active Directory Sync.

View computer details

The computers list shows you the current computers with these details:
- Name.
• IP Address. Hover over the icon to see details of all IPv4 and IPv6 addresses.
• Operating System.
• Products installed. For example, Intercept X or Encryption.
• Last user.
• Last active. This is the last time that the computer contacted Sophos.
• Group. The group that the computer belongs to (if it belongs to one).

To search for a computer, enter the name in the search field above the list.
To filter computers according to their type, their health status, or their encryption status, use the filters above the list.

You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

Delete computers

You can delete computers that you no longer need to manage from Sophos Central.
Select the computer or computers you want to delete and click Delete (in the upper right of the page).
This deletes the computer and the alerts associated with the computer.

Warning
You should uninstall the Sophos software before deleting a computer.

Install or uninstall software

You can select new endpoint software to be installed on computers that are already protected and managed by Sophos Central.
You can also uninstall software.
To do either, do as follows.
1. Click Manage Endpoint Software (in the upper right of the page).
2. Select software.
3. Select computers and use the picker arrows to change the software installed, as follows.
   • To install the software, select eligible computers and move them to the assigned list.
   • To uninstall the software, select assigned computers and move them to the eligible list.
The computers will update to the selected software.

Export to CSV

To export a list of computers:
Click Export to CSV.
This creates a file called devices.csv. Any currently active filters are applied to the list.
For example you can export a list of Windows computers by applying the **Windows Computers** filter before clicking **Export to CSV**.

**Retrieve recovery key**

This option is available from **More** on the **Computers** page.

If users are unable to log in to their encrypted computer, you can get a recovery key which is used to unlock the computer.

**Related concepts**

- **Encryption Recovery Key Search** (page 247)
- **Active Directory Sync** (page 224)

You can import users and user groups from Active Directory to Sophos Central.

**Azure AD Sync Status** (page 228)

**Related information**

- **Join your work device to your organization's network**

### 4.4.1 Computer Summary

The **Summary** tab in a computer's details page shows you the following information.

The sections you see depend on your license and the features you've set up.

**Security status**

In the left-hand pane, you can see the security status and take actions.

**Note**

The left-hand pane is always shown, even when you click the other tabs on this page.

An icon shows you whether the computer has any security alerts:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="green-check-mark.png" alt="Green check mark" /></td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td><img src="orange-warning-sign.png" alt="Orange warning sign" /></td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td><img src="red-warning-sign.png" alt="Red warning sign" /></td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>

**Actions you can take**

The action buttons are in the left-hand pane.

**Update**: This updates your computer with the latest Sophos software.
Delete: This deletes the computer from Sophos Central. It also deletes the alerts associated with the computer.

Warning
You should uninstall the Sophos software before deleting a computer.

Isolate: This isolates the computer from the network.

Live Response (Beta): This enables you to connect to the computer to investigate and remediate possible security issues.

Change group: This lets you add it to a group, move it to a different group, or remove it from its current group.

Scan Now: This scans the computer for threats.

The scan may take some time. When complete, you can see a "Scan completed" event and any successful cleanup events on the Logs & Reports > Events page. You can see alerts about unsuccessful cleanup on the Alerts page.

If the computer is offline, it is scanned when it is back online. If a computer scan is already running, the new scan request will be ignored and the earlier scan will carry on.

Diagnose: This diagnoses potential issues with the computer.

Create forensic snapshot: This gets data from a Sophos log of the device’s activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

Isolate or remove from isolation

This option is available if you have Intercept X Advanced with EDR.

Isolate isolates the computer from the network. You might want to do this if potential threats are found on it. You can still manage the computer from Sophos Central and you can remove it from isolation at any time.

When a computer has been isolated, you see the following under the computer icon and security status.

• The message Isolated by Admin.
• A link labeled Remove from Isolation. Click it to reconnect the computer to the network.

Note
You don't see the Isolate option if the computer has already isolated itself automatically. See Device Isolation in Threat Protection Policy.

Live Response (Beta)

This option is available only if you are a Super Admin and you’ve signed in using multi-factor authentication. You must also turn on Allow Live Response connections to computers in Global Settings, see Live Response for devices.

This enables you to connect to the computer to investigate and remediate possible security issues. You might want to do this if an infection or suspicious activity is identified on the computer. You can connect to the computer even if it’s isolated. To connect to the computer, do as follows:
1. Click **Live Response (Beta)**.
2. In **Session purpose**, summarize the purpose of your session.
3. Click **Start**.
   
   A connection to the computer is opened in another browser tab. The tab shows a terminal window.
4. At the command prompt, type commands to perform your investigation or remediation.
   
   Use DOS, UNIX, or Linux commands depending on the computer to which you’ve connected.
5. When you finish, click **End Session**.
   
   The connection is closed, although the tab remains open. You can browse elsewhere in Sophos Central from here.
   
   The connection is also closed in the following cases:
   
   - You close the tab.
   - You refresh the tab.
   - You browse elsewhere in Sophos Central from here.
   - There is no activity for 30 minutes.

To see which Live Response sessions have started or ended, view the Sophos Central audit log.

### Create forensic snapshot

You can create a "forensic snapshot" of data from the device. This gets data from a Sophos log of the device's activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

You’ll need a converter (which we provide) to read the data.

**Note**

You can choose how much data you want in snapshots and where to upload them. To do this, go to **Global Settings > Forensic Snapshots**. These options may not be available for all customers yet.

To create a snapshot:

1. Go to a threat case's **Analyze** tab.
   
   Alternatively, on the details page of the device, open the **Status** tab.
2. Click **Create forensic snapshot**.
3. Follow the steps in Upload a forensic snapshot to an AWS S3 bucket.

You can find the snapshots you generated in `%PROGRAMDATA%\Sophos\Endpoint Defense \Data\Forensic Snapshots\`.

Snapshots generated from detections are in `%PROGRAMDATA%\Sophos\Endpoint Defense \Data\Saved Data\`.

**Note**

You need to be an administrator with access to the tamper protection password and run a command prompt as an administrator to access the saved snapshots.
Recent Events

This lists recent events on the computer. For a full list, click the **Events** tab.

The icons indicate which Sophos agent reported each event. Hover over an icon to see what it means.

Agent Summary

The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.

The summary shows the following details. It also includes links to let you update the computer, install products, or change the group the computer's in, as needed.

- **Last Activity**: Shows when the last activity occurred.
- **Last Agent Update**: Shows whether the computer is up to date.
- **Assigned Products**: Shows the Sophos products installed (for example, Intercept X or Device Encryption). Shows the license and the version number for each installed product. The version information is only available for Windows computers.
- **Installed component versions**: Click this to see a full list of the Sophos components and their version numbers. This is only available for Windows computers.
- **Group**: Shows which group the computer is in (if any).

Device Encryption

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault encryption on Macs.

This summary shows:

- All volumes of the computer.
- The volume ID for each volume.
- The encryption status.
- The authentication type.
- The encryption method.

Volumes can be encrypted with software-based or hardware-based encryption. Device Encryption always uses software-based encryption for new volumes, even if the drive supports hardware-based encryption.

If a drive is already encrypted with hardware-based encryption, it will not be changed.

If a BitLocker group policy setting requires hardware-based encryption, it is used.

**Retrieve Recovery Key**

You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their signin credentials.

**Trigger change of password/PIN**
This requires users to immediately change their BitLocker password or PIN. A message is displayed when the request has been sent successfully.

On the endpoint, users are prompted to set a new BitLocker password or PIN. If users close the dialog without entering a new password or PIN, the dialog is shown again after 30 seconds, until they enter a new one. After users have closed the dialog five times without changing the password or PIN an alert is logged.

Web Gateway summary

Sophos Web Gateway provides advanced protection against risky or inappropriate web browsing. The summary shows the last network activity. It also shows the version of the Web Gateway agent (and whether it is up to date).

If you need to update the Web Gateway agent, an Update button is displayed.

Tamper Protection

This shows whether tamper protection is enabled on the computer or not.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:

- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
- Disable tamper protection.
- Uninstall the Sophos agent software.

Click Disable Tamper Protection to manage the tamper protection password for the computer. If tamper protection is switched off we recommend you turn it on.

Update Cache and Message Relay

Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos. You can also designate servers to communicate with Sophos Central as message relays.

This shows that a cache has been set up for the computer. It shows which server is being used.

Windows Firewall

Windows Firewall is active and being managed on the computer. It also shows:

- Whether Windows Group Policy is being used.
- The active network profiles.
- If other registered firewalls are installed and active.

Related concepts
Forensic snapshots (page 138)
Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

**Encryption Recovery Key Search** (page 247)

**Alerts** (page 4)

The **Alerts** page lists all the alerts that require your action.

**Related tasks**

**Live Response for devices** (page 144)

Turn on Live Response so that you can connect to devices to investigate and remediate possible security issues.

**Recover deleted devices** (page 87)

You can recover devices that you’ve deleted from Sophos Central if they are synced using Active Directory synchronization.

### 4.4.2 Computer Events

The **Events** tab in a computer’s details page displays events detected on the computer. You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

- **Sev**: Hover over an icon to see what it means.
- **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
- **Details**: This link (for certain events) lets you get further details and take action.

**View Events Report**: Shows events arranged by type and a graph of events day by day.

**Stop detecting an application**

If an application is reported as malware but you know it’s safe, you can allow it from the events list. For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the **Details** link beside the event and then allow the application.

**Note**

This currently applies only to malware events reported by Intercept X.

**Stop detecting an exploit**

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again** and select an option:
   - **Exclude this Detection ID from checking**: prevents this detection on this app.
   - **Exclude this application from checking**: prevents any checks for exploits on this app.

Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.
3. Click **Exclude**.
   We’ll add your exclusion to a list.
   Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

**Stop detecting ransomware**

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again**.
   Select **Exclude this Detection ID from checking**. This prevents this detection on this app.
3. Click **Exclude**.
   We’ll add your exclusion to the Global Exclusions list.

**Related concepts**
- [Allowed applications](#) (page 248)

**Related information**
- How to investigate and resolve a potential False Positive or Incorrect Detection

### 4.4.3 Computer Status

The **Status** tab in a computer's details page lets you see the computer's security health and details of any alerts.

It also lets you take action against alerts.

**Security Health**

These status details are only shown if the computer is using the Security Heartbeat feature.

The computer security status is reported by computers running Windows 7 and later.

This shows whether the device has threats detected, has out-of-date software, is not compliant with policy, or is not properly protected. The overall status is the same as that for the highest-priority item listed (red, orange or green).

**Alerts**

The page lists any alerts on the device. The details include:

- **Alert details**: For example, the name of the malware.
- **When the alert occurred**.
- **The actions that you can take**. These depend on the type of threat or event and are the same as the actions available in the Dashboard.
**Related information**

Upload a forensic snapshot to an AWS S3 bucket (page 140)

Follow these instructions to upload a forensic snapshot.

### 4.4.4 Computer Policies

The **Policies** tab in a computer's details page lets you see the policies that are applied to the computer.

You can view and edit policy details by clicking the policy in the list.

**Note**

Editing the policy affects all users to which this policy is applied.

### 4.5 Computer Groups

On the **Computer Groups** tab you can add or manage groups of computers.

You can use groups to assign a policy to multiple computers at once.

The sections below tell you about the groups list and how to add, modify or delete groups.

**About the groups list**

The current groups are listed and the number of computers in each group is shown.

To see full details for a group, click on the group's name.

**Add a group**

To add a group click **Add Computer Group** in the upper right of the page. Give a name and description and then assign computers to the group.

**Note**

A computer can only be in one group. If you select a computer that's already in a group, it will be removed from its current group.

**Tip**

In the **Search** box you can start typing a name to filter down the displayed entries.

**Edit a group**

To edit a group, click the group's name to open and edit the group details.

**Delete a group**

To delete a group, select it and click **Delete** in the upper right of the page.
Deleting a group will not delete its computers.
You can also delete a group at the group's details page. Click the group's name to open the details.

4.5.1 Computer Group Summary

The Summary tab in a computer group’s details lets you add or remove computers from groups. You can also delete groups.
To add or remove computers from a group click Edit in the left-hand pane. Amend the Assigned Computers for the group and click Save.
To delete the group, click Delete in the left-hand pane.
Deleting a group will not delete its computers.

4.5.2 Computer Group Policies

The Policies tab in a computer group's details page lets you see the policies that are enabled and applied to the group.
Click a policy name to view and edit policy details.

Note
Editing the policy affects all groups to which this policy is applied.

4.6 Policies

A policy is a set of options (for example, settings for malware protection) that Sophos Central applies to protected users, devices, servers, or networks.
There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).
To find out how policies work and how you can use them to customize security settings, see About Policies.
To find out how to create and edit policies, see Create or Edit a Policy.

Note
Your assigned administrator role affects what you can do.

4.6.1 About Policies

If you’re new to policies, read this page to find out how policies work.

What is a policy?

A policy is a set of options that Sophos Central applies to protected users, devices or servers.
There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).

Users, devices and servers have separate policies.

What is a Base policy?

Each feature has a Base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.

For some features, like threat protection, Sophos configures the Base policy with the best practice settings. You can leave it unchanged if you want to.

For other features, like application control or peripheral control, which are more specific to your network, you must edit the policy to set up the feature.

The Base policy is always available and is used if you don't have other policies activated.

**Note**

You cannot disable or delete the Base policy.

Do I need to add new policies?

You can choose whether to set up your own policies or not.

If you want to apply the same policy to all users or devices or servers, you can simply use the Base policy or adapt it for your needs.

If you want to use different settings for different groups, you can create additional policies.

What can I do with additional policies?

You can set up additional policies to override some or all of the settings in the Base policy.

You can use additional policies to apply different settings to different users, devices or servers. You can also use them to make it easier to switch the settings that are applied quickly.

The order in which you put the policies in the list matters. The policies at the top of the list override the policies at the bottom. See “How do you prioritize policies?” below.

What’s the difference between user policies and computer policies?

A user policy applies to all the devices that a user has.

A “device” or computer policy applies to specific computers or groups of computers, regardless of which user logs on.

Some features let you create either kind of policy. Other features only let you create one kind. For example you can set an updating policy for computers, but not for users.

If you set up a user policy and a computer policy for the same feature, and both could apply to the same computer, the policy that’s higher in your policy list takes priority. See "How are policies prioritized?" below.

You can check which policy is applied to a computer by looking at the **Policies** tab on that computer’s details page.
What is in each policy?

A policy lets you:
- Configure one of the features that you have licensed.
- Specify which users, devices or servers the policy applies to.
- Specify whether the policy is enforced and whether it expires.

A policy contains all the settings for a product or feature. For example, you cannot split up the threat protection settings across several different policies in such a way that a user gets one setting from one policy and another setting from a different policy.

How are policies prioritized?

The order in which you arrange the policies determines which is applied to specific users, devices or servers.

Sophos Central looks through the policies from the top down and applies the first policy it finds that applies to those users or devices.

The Base Policy is always at the bottom, and is applied to any users, devices or servers that aren’t covered by policies higher in the list.

**Tip**
Place the most specific policies at the top and general policies further down. Otherwise, a general policy might apply to a device for which you wanted an individual policy.

To sort policies, grab a policy and drag it to the position where you want to insert it.

### 4.6.2 Create or Edit a Policy

You can create or edit a policy as follows.

#### Create a policy

1. If you have more than one Sophos product, select the one where you want to create a policy.

   **Note**
   You can’t create policies from the **Overview** pages.

2. Go to the **Policies** page.

3. Click **Add Policy** (in the upper right).

4. If you see an **Add Policy** dialog, select:
   - The feature you want.
   - The policy type (applies only to Endpoint Protection).

5. On the policy details page, use the tabs to:
• Assign the policy. For example, assign it to specific users or devices.
• Enter settings for the policy. See the Help topic for that policy type.
• Enable or disable the policy.

Edit a policy

1. If you have more than one Sophos product, select the one where you want to edit a policy.

   Note
   You can't edit policies from the Overview pages.

2. Go to the Policies page.
   You see a list of policy types.
3. Click on the policy type to open a list of policies.
4. Find the policy you want to edit and click it.
5. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users or devices.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.

4.6.3 Threat Protection Policy

Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

CAUTION
This help page describes policy settings for workstation users. Different policy settings apply for servers.

To set it up:
• Create a Threat Protection policy.
• Open the policy's Settings tab and configure it as described below. Make sure the policy is enabled.

You can either use the recommended settings or change them.

Note
SophosLabs can independently control which files are scanned. They may add or remove scanning of certain file types in order to provide the best protection.

Note
If an option is locked global settings have been applied by your partner. You can still stop detecting applications, exploits and ransomware by going to the events list.
Use recommended settings

Click **Use recommended settings** if you want to use the settings Sophos recommends. These provide the best protection you can have without complex configuration.

If we change our recommendations in future, we'll automatically update your policy with new settings.

The recommended settings offer:
- Detection of known malware.
- In-the-cloud checks to enable detection of the latest malware known to Sophos.
- Proactive detection of malware that has not been seen before.
- Automatic cleanup of malware.

**CAUTION**

Think carefully before you change the recommended settings because doing so may reduce your protection.

Live Protection

Live Protection checks suspicious files against the latest malware in the SophosLabs database.

You can select these options:
- **Use Live Protection to check the latest threat information from SophosLabs online.** This checks files during real-time scanning.
- **Use Live Protection during scheduled scans**

Deep Learning

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

Deep learning is only available with Sophos Intercept X.

Real-time Scanning - Local Files and Network Shares

Real-time scanning scans files as users attempt to access them. It allows access if the file is clean.

Local files are scanned by default. You can also select this option:
- **Remote files:** This scans files on network shares.

Real-time Scanning - Internet

Real-time scanning scans internet resources as users attempt to access them. You can select these options:
- **Scan downloads in progress**
• **Block access to malicious websites**: This denies access to websites that are known to host malware.

• **Detect low-reputation files**: This warns if a download has a low reputation. The reputation is based on a file's source, how often it is downloaded and other factors. You can specify:
  — The **Action to take on low-reputation downloads**: If you select **Prompt user**, users will see a warning when they download a low-reputation file. They can then trust or delete the file. This is the default setting.
  — The **Reputation level**: If you select **Strict**, medium-reputation as well as low-reputation files will be detected. The default setting is **Recommended**.

**Remediation**

Remediation options are:

• **Automatically clean up malware**: Sophos Central will try to clean up detected malware automatically.
  If the cleanup succeeds, the malware detected alert is deleted from the alerts list. The detection and cleanup are shown in the events list.

  **Note**
  We always clean up PE (Portable Executable) files like applications, libraries, and system files, even if you turn off automatic cleanup. PE files are quarantined and can be restored.

• **Enable Threat Case creation**: Threat cases let you investigate the chain of events in a malware attack and identify areas where you can improve your security.

• **Allow computers to send data on suspicious files, network events, and admin tool activity to Sophos Central**: This sends details of potential threats to Sophos. Ensure it's turned on in any policy for computers where you want to do threat searches.

  **Note**
  This option is available if you have Intercept X Advanced with EDR.

**Runtime Protection**

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

• **Protect document files from ransomware (CryptoGuard)**: This protects document files against malware that restricts access to files, and then demands a fee to release them. You can also choose to protect 64-bit computers against ransomware run from a remote location.

• **Protect from master boot record ransomware**: This protects the computer from ransomware that encrypts the master boot record (and so prevents startup) and from attacks that wipe the hard disk.

• **Protect critical functions in web browsers (Safe Browsing)**: This protects your web browsers against exploitation by malware.

• **Mitigate exploits in vulnerable applications**: This protects the applications most prone to exploitation by malware. You can select which application types to protect.

• **Advanced: Customize exploit mitigation settings**: This displays more options.
• **Protect processes**: This helps prevent the hijacking of legitimate applications by malware. You can choose to:
  — protect against process replacement attacks (process hollowing attacks).
  — protect against loading .DLL files from untrusted folders.

• **Protect network traffic**: You can choose these options:
  — **Detect malicious connections to command and control servers**. This detects traffic between an endpoint computer and a server that indicates a possible attempt to take control of the endpoint computer.
  — **Prevent malicious network traffic with packet inspection**. This scans traffic at the lowest level and blocks threats before they can harm the operating system or applications.

• **Detect malicious behavior (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.

• **AMSI Protection (with enhanced scan for script-based threats)**: This protects against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI). Code forwarded via AMSI is scanned before it runs and the applications used to run the code are notified of threats by Sophos. If a threat is detected, an event is logged.

**Advanced Settings**

These settings are for testing or troubleshooting only. We recommend that you leave them set to the defaults.

**Device Isolation**

If you select this option, devices will isolate themselves from your network if their health is red. A device's health is red if it has threats detected, has out-of-date software, isn't compliant with policy, or isn't properly protected.

You can still manage isolated devices from Sophos Central. You can also use scanning exclusions or global exclusions to give limited access to them for troubleshooting.

You can't remove these devices from isolation. They will communicate with the network again once their health is green.

**Scheduled Scanning**

Scheduled scanning performs a scan at a time or times that you specify.

You can select these options:

• **Enable scheduled scan**: This lets you define a time and one or more days when scanning should be performed.

  **Note**
  The scheduled scan time is the time on the endpoint computers (not a UTC time).

• **Enable deep scanning**: If you select this option, archives are scanned during scheduled scans. This may increase the system load and make scanning significantly slower.
Scanning exclusions

You can exclude files, folders, websites or applications from scanning for threats, as described below.

We'll still check excluded items for exploits. However, you can stop checking for an exploit that has already been detected (use a Detected Exploits exclusion).

Exclusions set in a policy are only used for the users the policy applies to.

Note
If you want to apply exclusions to all your users and servers, set up global exclusions on the Global Settings > Global Exclusions page.

To create a policy scanning exclusion:
1. Click Add Exclusion (on the right of the page).
   The Add Exclusion dialog is displayed.
2. In the Exclusion Type drop-down list, select a type of item to exclude (file or folder, website, potentially unwanted application or device isolation).
3. Specify the item or items you want to exclude.
4. For File or folder exclusions only, in the Active for drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.
5. Click Add or Add Another. The exclusion is added to the scanning exclusions list.
To edit an exclusion later, click its name in the exclusions list, enter new settings and click Update.

Desktop Messaging

Note
You must switch off Use recommended settings to set up Desktop Messaging.

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

Desktop Messaging is on by default.

Note
If you switch off Desktop Messaging you will not see any notification messages related to Threat Protection.

Click in the message box and enter the text you want to add.

Related concepts
Create or Edit a Policy (page 202)
You can create or edit a policy as follows.

**Threat Cases** (page 19)
Threat cases let you investigate and clean up malware attacks.

**Threat Searches** (page 31)
You can search for potential threats on your network.

**Related reference**

**Windows Scanning Exclusions: Wildcards and Variables** (page 208)
When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

**macOS Scanning Exclusions** (page 211)
You can add scanning exclusions for macOS workstations.

**Device isolation exclusions (Windows)** (page 213)
You can allow isolated devices to have limited communications with other devices.

**Website exclusions** (page 213)
You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

**Malicious Network Traffic Prevention (IPS) (Windows) exclusions** (page 214)
You can exclude specific network traffic from inspection.

**Process exclusions (Windows)** (page 213)
You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

**Related information**

**Global Exclusions** (page 240)
You can exclude files, websites and applications from scanning for threats.

**Sophos Threat Center**
**Antimalware Scan Interface (AMSI)**
**Download Reputation**

---

**Windows Scanning Exclusions: Wildcards and Variables**

When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

**Note**
Some wildcards or variables cannot be used for exclusions from real-time scanning on Windows XP or Windows Server 2003.

**Warning**
Scanning exclusions may significantly reduce your protection. Only use them if you understand the risks.

---

**Wildcards**

You can use the wildcards shown in this table.
**Note**

Only * and ? can be used on Windows XP and Windows Server 2003.

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
<th>For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>* (Star)</td>
<td>Zero or more of any character except \ or /</td>
<td></td>
<td></td>
</tr>
<tr>
<td>** (Star Star)</td>
<td>Zero or more characters including \ and / including \ or / characters or used at the start or end of an exclusion.</td>
<td>Any other use of a ** is treated as a single * and matches zero or more characters excluding \ and /</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- c:\foo**\bar matches: c:\foo\bar, c:\foo\more \bar, c:\foo\even\more \bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- **\bar matches c:\foo\bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- c:\foo** matches c:\foo \more\bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- c:\foo**bar matches c:\foo\foomorebar but NOT c:\foo\more\bar</td>
</tr>
<tr>
<td>\ (Backslash)</td>
<td>Either \ or /</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/ (Forward slash)</td>
<td>Either / or \</td>
<td></td>
<td></td>
</tr>
<tr>
<td>? (Question mark)</td>
<td>One single character. If it is at the end of a string it can match zero characters.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>. (Period)</td>
<td>A period OR the empty string at the end of a filename, if the pattern ends in a period and the filename does not have an extension.</td>
<td>Note that:</td>
<td>- ** matches all files</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- *. matches all files without an extension</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- *foo. matches “foo” and *foo.”</td>
</tr>
</tbody>
</table>

### Example wildcards

Here are some examples of the use of wildcards.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Interpreted as</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo</td>
<td>**\foo</td>
<td>Exclude any file named foo (in any location).</td>
</tr>
<tr>
<td>foo\bar</td>
<td>**\foo\bar</td>
<td>Exclude any file named bar in a folder named foo (in any location).</td>
</tr>
<tr>
<td>Expression</td>
<td>Interpreted as</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>*.txt</td>
<td>***.txt</td>
<td>Exclude all files named *.txt (in any location).</td>
</tr>
<tr>
<td>D:\</td>
<td>D:\</td>
<td>Exclude the entire drive D: from scanning.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use with care. PE files (such as applications), including malware, will be able to run on this drive without detection.</td>
</tr>
<tr>
<td>C:\foo\</td>
<td>C:\foo\</td>
<td>All files and folders underneath C:\foo, including C:\foo itself.</td>
</tr>
<tr>
<td>C:\foo*.txt</td>
<td>C:\foo*.txt</td>
<td>All files or folders contained in C:\foo named *.txt.</td>
</tr>
</tbody>
</table>

### Variables for exclusions

You can use variables when you set up scanning exclusions.

The table below shows the variables and examples of the locations they correspond to on each operating system.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Windows 7 and later</th>
<th>Windows XP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2008 and later</td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>$allusersprofile$</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users</td>
</tr>
<tr>
<td>$appdata$</td>
<td>C:\Users*.\AppData \Roaming</td>
<td>C:\Documents and Settings*.\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>$commonprogramfiles$</td>
<td>C:\Program Files\Common Files</td>
<td></td>
</tr>
<tr>
<td>$commonprogramfiles(x86)$</td>
<td>C:\Program Files (x86)\Common Files</td>
<td></td>
</tr>
<tr>
<td>$localappdata$</td>
<td>C:\Users*.\AppData \Local</td>
<td>C:\Documents and Settings*.\Local Settings\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
</tbody>
</table>
Variable | Windows 7 and later | Windows XP | Windows Server 2008 and later | Windows Server 2003
---|---|---|---|---
$programdata% | C:\ProgramData | C:\Documents and Settings\All Users \Application Data | 
$programfiles% | C:\Program Files | 
$programfiles(x86)% | C:\Program Files (x86) | 
$systemdrive% | C:\ | 
$systemroot% | C:\Windows | 
$temp% or $tmp% | C:\Users\*\AppData \Local\Temp | C:\Documents and Settings\*\Local Settings\Temp | Does not work for real-time scanning.
$userprofile% | C:\Users\* | C:\Documents and Settings\* | 
$windir% | C:\Windows | 

**macOS Scanning Exclusions**

You can add scanning exclusions for macOS workstations.

When you add or edit an exclusion, you can type any POSIX path, whether it is a volume, folder, or file.

**Example:** /Volumes/excluded (Mac)

**CAUTION**

Think carefully before you add scanning exclusions because doing so may reduce your protection.

To specify which items are excluded, use the rules in the table below.

**Exclusion rules**

<table>
<thead>
<tr>
<th>Token</th>
<th>Syntax to use</th>
<th>Item(s) to exclude</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td><strong>Suffix</strong> the exclusion with a slash</td>
<td>A folder and sub-folders recursively</td>
</tr>
<tr>
<td>//</td>
<td><strong>Suffix</strong> the exclusion with a double slash</td>
<td>A folder but not sub-folders</td>
</tr>
</tbody>
</table>
### Token Syntax to use Item(s) to exclude

<table>
<thead>
<tr>
<th>Token</th>
<th>Syntax to use</th>
<th>Item(s) to exclude</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>Do not <strong>suffix</strong> the exclusion with a slash or double slash</td>
<td>A file</td>
</tr>
<tr>
<td><code>/</code></td>
<td><strong>Prefix</strong> the exclusion with a slash</td>
<td>A folder or file in a specific location</td>
</tr>
<tr>
<td><code>&lt;folder&gt;</code></td>
<td>Do <strong>not</strong> prefix the exclusion with a slash</td>
<td>A folder or file anywhere locally or on the network</td>
</tr>
<tr>
<td><code>&lt;file&gt;</code></td>
<td></td>
<td>A file whose name has a specific filename extension</td>
</tr>
<tr>
<td><code>*</code></td>
<td>Substitute an asterisk for the filename stem</td>
<td>A file</td>
</tr>
</tbody>
</table>

### Examples

<table>
<thead>
<tr>
<th>Exclusion path</th>
<th>Item(s) that are excluded</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/myfolder/myapplication</code></td>
<td>The file <em>myapplication</em> in a specific folder</td>
</tr>
<tr>
<td><code>/myfolder/</code></td>
<td>All files in the folder <em>myfolder</em> in a specific location and sub-folders recursively</td>
</tr>
<tr>
<td><code>/myfolder//</code></td>
<td>All files in the folder <em>myfolder</em> in a specific location but not sub-folders</td>
</tr>
<tr>
<td><code>myfolder/myapplication</code></td>
<td>The file <em>myapplication</em> in any folder that is called <em>myfolder</em> locally or on the network</td>
</tr>
<tr>
<td><code>myfolder/</code></td>
<td>All files in any folder that is called <em>myfolder</em>, locally or on the network, and sub-folders recursively</td>
</tr>
<tr>
<td><code>myfolder//</code></td>
<td>All files in any folder that is called <em>myfolder</em>, locally or on the network, but not sub-folders</td>
</tr>
<tr>
<td><code>myapplication</code></td>
<td>The file <em>myapplication</em> anywhere locally or on the network</td>
</tr>
<tr>
<td><code>*.mov</code></td>
<td>All files whose filename extension is <em>.mov</em> anywhere locally or on the network</td>
</tr>
<tr>
<td><code>/myfolder/*.mov</code></td>
<td>All files whose filename extension is <em>.mov</em> in a specific location</td>
</tr>
</tbody>
</table>

### Related concepts

* Threat Protection Policy (page 203)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

**Process exclusions (Windows)**

You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

If possible, enter the full path from the application, not just the process name shown in Task Manager.

Example:

`%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe`

**Note**

To see all processes or other items that you need to exclude for an application, see the application vendor’s documentation.

**Note**

You can use wildcards and variables.

**Related reference**

*Windows Scanning Exclusions: Wildcards and Variables* (page 208)

When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

**Website exclusions**

You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

Examples:

- IP address: 192.168.0.1
- IP address range: 192.168.0.0/24
- The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range.

Thus /24 equals the netmask:

```
11111111.11111111.11111111.00000000
```

In our example, the range includes all IP addresses starting with 192.168.0.

- Domain: google.com

**Device isolation exclusions (Windows)**

You can allow isolated devices to have limited communications with other devices.

You can choose whether isolated devices will use outbound or inbound communications, or both.

Use the following settings to restrict communications:

- **Local Port**: Any device can use this port on isolated devices.
Remote Port: Isolated devices can use this port on any device.
Remote Address: Isolated devices can only communicate with the device with this IP.

Example 1

You want remote desktop access to an isolated device so that you can troubleshoot.
- In Direction, select Inbound Connection.
- In Local Port, enter the port number.

Example 2

You want to be able to go to an isolated device and download cleanup tools from a server.
- In Direction, select Outbound Connection.
- In Remote Address, enter the address of the server.

Malicious Network Traffic Prevention (IPS) (Windows) exclusions

You can exclude specific network traffic from inspection.
You can choose whether the exclusion applies to outbound or inbound traffic, or to both.
Use the following settings to specify which traffic to exclude:
- Remote address: The address of another computer that traffic goes to or from.
- Remote port: The port that traffic goes to or from on other computers.
- Local port: The port that traffic goes to or from on the local computer.
You must set at least one of the address or port options.

Example

If you want to exclude traffic that comes from port 123 on any other computer:
- In Direction, select Inbound Connection.
- In Using this remote port, enter the port number 123.

Advanced exploit mitigation

You can protect computers against a range of exploits or "active adversary" threats.
1. Open a Threat Protection policy.
2. Under Mitigate exploits in vulnerable applications, you see options for protecting various application types.
3. Click Advanced: customize exploit mitigation to see more advanced options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent credential theft</td>
<td>We prevent the theft of passwords and hash information from memory, registry, or hard disk.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Prevent APC violation</td>
<td>We prevent attacks from using Application Procedure Calls (APC) to run their code.</td>
</tr>
<tr>
<td>Prevent privilege escalation</td>
<td>We prevent attacks from escalating a low-privilege process to higher privileges to access your systems.</td>
</tr>
<tr>
<td>Prevent code cave utilisation</td>
<td>We detect malicious code that's been inserted into another, legitimate application.</td>
</tr>
<tr>
<td>Prevent application verifier exploits</td>
<td>We prevent attacks that exploit the application verifier in order to run unauthorized software at startup.</td>
</tr>
</tbody>
</table>

**Related concepts**

[Threat Protection Policy](#) (page 203)

Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

### 4.6.4 Peripheral Control Policy

Peripheral control lets you control access to peripherals and removable media. You can also exempt individual peripherals from that control.

**Note**

If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set it up:

- Create a **Peripheral Control** policy. See [Create or Edit a Policy](#).
- Open the policy’s **Settings** tab and configure it as described below. Make sure the policy is enabled.

**Manage Peripherals**

In **Manage Peripherals**, select how you want to control peripherals:

- **Monitor but do not block**. If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you cannot set access rules for them.
- **Control access by peripheral type and add exemptions**. If you select this, you can go on to set access policies for peripheral types and for individual detected peripherals.

**Set Access Policies**

Set access policies in the table.

The table displays detected peripheral types, the number of each type detected, and the current access policy.
Note
The totals include all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent policies for all devices.

Note
The MTP/PTP category includes devices such as phones, tablets, cameras, and media players that connect using the MTP or PTP protocols.

For each peripheral type, you can change the access policy:
- **Allow**: Peripherals are not restricted in any way.
- **Block**: Peripherals are not allowed at all.
- **Read Only**: Peripherals can be accessed only for reading.

Note
The Bluetooth, Infrared, and Modem categories do not have the Read Only option.

Note
The Wireless Network Adaptor category has a Block Bridged option. This prevents bridging of two networks.

Peripheral Exemptions

Click the Peripheral Exemptions fold-out if you want to exempt individual peripherals from the control settings, or apply less restrictive controls.

1. Click **Add Exemptions**.
2. In the Add Peripheral Exemptions dialog, you see a list of detected peripherals.

   Note
   Peripherals are detected when you are in monitoring mode or if there is an access restriction for that type of peripheral.

   Note
   This list shows all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent exemptions for all devices.

3. Select a peripheral.
4. In the Policy column, you can optionally use the drop-down list to assign a specific access policy to an exempt peripheral.

   Restriction
   Do not set a stricter access policy for an individual peripheral than for its peripheral type. If you do, the setting for the individual policy is ignored and a warning icon is displayed beside it.
5. In the **Enforce By** column, you can optionally use the drop-down menu to apply the policy to all peripherals of that model or to ones with the same ID (the list shows you the model and ID).

6. Click **Add Exemption(s)**.

### Desktop Messaging

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

**Desktop Messaging** is on by default.

**Note**
If you switch off **Desktop Messaging** you will not see any notification messages related to Peripheral Control.

Click in the message box and enter the text you want to add.

**Related concepts**
Create or Edit a Policy (page 202)
You can create or edit a policy as follows.

### 4.6.5 Application Control Policy

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.

**Note**
If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set it up:

- Create an **Application Control** policy. See Create or Edit a Policy.
- Open the policy's **Settings** tab and configure the policy as described below. Make sure the policy is enabled.

We recommend that you detect the applications being used on your network and then decide which to block, as follows.

1. In the **Controlled Applications** list, click **Add/Edit List**.
   This opens a dialog where you can see the categories of applications that you can control. Sophos supplies and updates the list.
2. Click an application category, for example **Browser plug-in**.
   A full list of the applications in that category is displayed in the right-hand table.
3. We recommend that you select the option **Select all applications**. You'll refine your selection later.
4. Click **Save to List** and repeat for each category you want to control.

**Note**
If you want to control an application that isn't in the list supplied by Sophos, you can ask to have it added. Click the **Application Control Request** link at the bottom of the **Settings** tab.
5. In **Detection Options**:
   a) Select *Detect controlled applications during scheduled and on-demand scans*.
   b) Do not select any other options for now.

   **Note**
   Application control uses the scheduled scans and the scanning options (which file types are scanned) that you set in Threat Protection settings.

6. Allow time for all your computers to run a scheduled scan.
7. Go to the **Overview > Logs & Reports > Events** page.
8. In the list of event types, clear all the checkboxes except **Application Control**. Detected applications are now shown in the list of events. Make a note of any you want to continue using.
9. Return to your policy page.
10. In the **Controlled Applications** list, click **Add/Edit List** again. Then:
   a) Find the applications you want to use and clear the checkbox next to them.
   b) Select *New applications added to this category by Sophos* (optional). Any new applications that Sophos adds to this category later will automatically be added to your controlled list. Newer versions of applications already in your list will also be added.

   **CAUTION**
   Only select this if you’re sure you want to control applications in this category from now on.

c) Click **Save to List**.
11. In **Detection Options**:
   a) Select *Detect controlled applications when users access them*.
   b) Select *Block the detected application*.

   **Note**
   If you chose to control any new applications added by Sophos, those new applications will now be blocked.

12. In **Desktop Messaging** you can add a message to the standard notification. If you leave the message box empty only the standard message is shown.

   Desktop messaging is on by default.

   **Note**
   If you switch off desktop messaging you will not see any notification messages related to Application Control.

   a) Click in the message box and enter the text you want to add.

**Related concepts**
*Create or Edit a Policy* (page 202)
You can create or edit a policy as follows.

### 4.6.6 Data Loss Prevention Policy

Data Loss Prevention (DLP) controls accidental data loss. DLP enables you to monitor and restrict the transfer of files containing sensitive data. For example, you can prevent a user sending a file containing sensitive data home using web-based email.

You do this by creating rules, see Data Loss Prevention Rules. You then add the rules to policies, as described below. You can then apply these policies to users, computers and Windows servers, see About Policies.

Data Loss Prevention (DLP) policies include one or more rules that specify conditions and actions to be taken when the rule is matched. When a DLP policy contains several rules, a file that matches any of the rules in the DLP policy violates the policy. A rule can be included in multiple policies. You can add text to the messages shown on protected endpoints or Windows servers when the rules are triggered. There are two types of message:

- A confirmation notification that asks the user to confirm the file transfer.
- A block notification that informs the user that they cannot transfer the file.

You can create custom policies or policies from templates. The templates cover standard data protection for different regions. You can apply these policies to users, computers or Windows servers.

To set up a policy:

1. Choose whether you want to create a policy from a template or a custom policy.
   - To use a template, select a region and a template and click Create from Template. This adds a pre-defined rule to the policy.
   - To create a custom policy, click Create Custom Policy and click Add. Choose whether you want to use an existing rule or create a new rule: see Create a Data Loss Prevention Rule. Select the rules you want to add and click Add.

2. Turn on the options in the Messages For End Users area and click the option names to add your own message to the standard confirmation and block notifications. Each message can have a maximum of 100 characters.

   **Note**
   You can turn off either or both of these messages. The standard notification is shown on the endpoint or server. If you leave the message box blank the standard notification is shown.

   a) Enter the message text.
   b) Click Finish.
You use data loss prevention (DLP) rules to specify conditions to detect, actions to take, and any files to exclude from scanning.

You can create or edit a policy as follows.

Create a Data Loss Prevention Rule (page 256)
Follow these instructions to create a DLP rule.

4.6.7 Web Control Policy

You need to configure the web control options to protect users and computers. There are no default options.

Note
If an option is locked global settings have been applied by your partner.

Note
Web control does not support Desktop Messaging.

To set up a policy:

• Create a Web Control policy. See Create or Edit a Policy.
• Open the policy's Settings tab and configure it as described below. Make sure the policy is enabled.

Additional security options
Select Additional security options to configure access to advertisements, uncategorized sites and risky downloads.

• Block risky downloads: This option blocks risky file types, but allows advertisements and uncategorized files.
• None: This option allows risky file types, advertisements and uncategorized files.
• Let me specify: This allows you to set advertisements and uncategorized file types to Allow or Block.

It also allows you to set Risky File Types to:

— Recommended: This gives you the settings shown in the table of file types below.
— Allow: Allows all risky file types.
— Warn: Warns the user that a file may be risky before they can download it.
— Block: Blocks all risky file types.
— Let me specify: This allows you to set a number of individual file types to Allow, Warn, or Block.
Acceptable web usage

Configure **Acceptable web usage** settings. These control the sites that users are allowed to visit.

Choose from the following options:

- **Keep it clean**: Prevents users from accessing adult and other potentially inappropriate websites.
- **Gentle guidance**: Blocks inappropriate browsing and warns users before visiting website categories that may impact their productivity.
- **Conserve bandwidth**: Blocks inappropriate browsing and warns users before visiting productivity-impacting websites. Blocks site categories likely to consume high bandwidth.
- **Business only**: Only allows site categories that are generally business-related.
- **Let me specify**: Allows you to configure individual site categories. For each group of categories (such as **Productivity-related categories**) you can set the behavior to **Block**, **Warn**, **Allow**, or **Let me specify**. Choosing **Let me specify** allows you to configure individual categories within these groups.

**Note**

For more control over how policy affects websites you can use the **Settings > Website Management** page.

For more information on how Sophos filters websites see [Sophos Web Security and Control Test Site](#).

Protect against data loss

Select **Protect against data loss** to configure data loss settings.

Selecting this option allows you to choose **Block data sharing**, **Allow data sharing**, or **Let me specify**. Setting these options controls access to web-based email and file downloads.

Log web control events

Select **Log web control events** to log attempts to visit blocked websites or websites for which we display a warning.

**Note**

If you do not enable logging, only attempts to visit infected sites will be logged.

Log web control events

You can put websites into your own custom categories ("tag" them) and then use a web control policy to control sites in each category.

To set this up, do as follows.

1. In Endpoint or Server Protection, go to **Settings > Website Management**.
2. Click **Add**.
3. In **Add Website Customization**, enter a website and add a tag. You can either type in a new tag name, or select a tag you’ve used before (you’ll see suggested tags when you start typing). Click **Save**.

4. In Endpoint or Server Protection, go to **Policies > Web Control** and select a policy.

5. Click the **Settings** tab.

6. Turn on **Control sites tagged in Website Management**.

7. Click **Add New** on the right of the page.

8. In **Add Website Tag**, do as follows.

   - Select the website tag you created.
   - Choose the **Action** you want to take against websites.
   - Click **Save**.

9. At the top of the policy, click **Save**.

**Apply this web control policy at set times only**

**Note**
This option is not available in the Base policy.

You can set times when you want to apply the policy.

1. Turn on **Apply this web control policy at set times only**.

2. Click **Add**.

3. Select the days and times when the policy will apply.

**Note**
This option uses the local time on the computers that the policy applies to. This may not be the same as the Sophos Central administrator's local time.

**Related concepts**
Create or Edit a Policy (page 202)
You can create or edit a policy as follows.

**Related tasks**
Website Management (page 237)

**Related information**
Sophos Web Security and Control Test Site

**4.6.8 Updating Policy**

The Updating policy lets you specify when product updates become available on your network. This ensures that your computers don’t start updating until a time that suits you.

**Note**
You can only set this policy as a “Device” policy. You can’t set it for users.
Note
If an option is locked global settings have been applied by your partner.

To set it up:
• Create an Update Management policy. See Create or Edit a Policy.
• Open the policy’s Settings tab and configure the policy as described below. Make sure the policy is enabled.

Scheduled Updates
Enable Scheduled Updates and select the day and time when you want product updates to become available. The time is local to each computer. For example, if you select 9 pm, each computer will get the update at 9 pm local time for the computer. This means that computers in different time zones will not get the update concurrently.

Remember that if computers aren’t on, they won’t get the update until they are next on at the scheduled update time.

Related concepts
Create or Edit a Policy (page 202)
You can create or edit a policy as follows.

4.6.9 Windows Firewall Policy
You can monitor and configure Windows Firewall (and monitor other registered firewalls) on your computers and servers using a Windows Firewall policy.

You can apply a Windows Firewall policy to individual devices (computers or servers) or to groups of devices.

CAUTION
Other firewalls or your Windows Group Policy settings may affect how the policy is applied on individual computers and servers.

We advise that you test any firewall rules you create (locally or via Group Policy) to make sure that communication with Sophos is allowed.

Note
If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set it up:
• Create a Windows Firewall policy. See Create or Edit a Policy.
• Open the policy’s Settings tab and configure it as described below. Make sure the policy is enabled.
Monitor Type

In **Monitor Type**, select the level of monitoring you want:

- **Monitor Only**. Devices will report their firewall status to Sophos Central. This is the default option.

- **Monitor & Configure Network Profiles**. Devices will report their firewall status to Sophos Central. You can also choose whether to block or allow inbound connections on **Domain Networks**, **Private Networks**, and **Public Networks**.

  Choose from:
  - **Block All**
  - **Block (with exceptions)**. You must set up the exceptions locally on the computer or server. If you don’t set up exceptions all inbound connections are blocked.
  - **Allow All**

Related concepts

Create or Edit a Policy (page 202)
You can create or edit a policy as follows.

4.7 Settings

The Settings pages are used to specify security settings that apply to all your users and devices.

The pages displayed depend on the features included in your license. Some of these pages may also be displayed under **Global Settings** in **Overview**.

**Note**
If you want to apply settings only to certain users, servers, or devices, use the **Policies** pages instead.

4.7.1 Active Directory Sync

You can import users and user groups from Active Directory to Sophos Central.

In Settings, on the **Active Directory Sync** page, you can select the Active Directory service you want to use.

- There is a download link for the Sophos Central Active Directory synchronization utility.
- In **Endpoint Protection** and **Email Gateway** you can use Azure Active Directory synchronization instead.

**Note**
If you are using Office 365 you must use Azure Active Directory synchronization.

For instructions on setting up the utility, see the Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.
For instructions on configuring Azure Active Directory synchronization, see the Azure Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

Azure Active Directory Sync and Endpoint Protection

Azure Active Directory Sync now supports Endpoint Protection on Windows computers. After performing an Azure Active Directory Sync, you can install Sophos Endpoint on a Windows computer. The Windows account used on the computer must be joined to your Azure Active Directory domain.

Azure Active Directory Sync does not import any device data and does not support Mac computers.

Note
Each Sophos Central user account can only synchronize with one type of Active Directory platform, either on-premise or Azure.

Related concepts
Active Directory Sync Status (page 225)
On the Active Directory Sync page, you can check the sync status and download the installer.
Azure AD Sync Status (page 228)
About Active Directory synchronization (page 226)
Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

Related tasks
Set up synchronization with Active Directory (page 226)
Follow these instructions to set up synchronization with Active Directory.
Set up synchronization with Azure Active Directory (page 229)

Active Directory Sync Status

On the Active Directory Sync page, you can check the sync status and download the installer.
You need to set up Active Directory synchronization before you can see these options.
You can download the latest installer for setting up synchronization with Active Directory.

Sync status

This shows your synchronization status and the synchronization settings in Active Directory.

• The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
• The time of the last synchronization with Active Directory.
• The number of users and groups imported from Active Directory.
You can view Active Directory synchronization alerts on the Overview > Alerts page. You can view synchronization events on the Overview > Logs & Reports > Events page.
About Active Directory synchronization
Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

To synchronize with Active Directory, you need to download and install the Sophos Central Active Directory Sync utility. The utility works as follows.

It synchronizes active users and user groups.

It can run automatically on a regular basis, as set up by the Sophos Central administrator.

It doesn't duplicate existing users or groups when they are matched to an existing Sophos Central user or group. For example, an email address from Active Directory may be added to an existing user in Sophos Central.

It supports only the Active Directory service.

It can synchronize multiple Active Directory forests. To do this, you need to install the utility on multiple machines and configure each utility to synchronize a different Active Directory forest. We strongly recommend to synchronize different Active Directory forests at different times of day, so that the synchronizations do not overlap.

It doesn't help you to deploy the Sophos agent software to your users' devices. Use other methods of deployment with Active Directory.

Set up synchronization with Active Directory
Follow these instructions to set up synchronization with Active Directory.

Before you can set up synchronization, you need .NET Framework 4 on the computer where you will run the Sophos Central AD Sync Utility.

Warning
Before you proceed, make sure all your active directory users are set up correctly with an email address. Users without an email address aren't protected and email going to an email address not tied to a user isn't delivered.

You need to use API credentials to synchronize with Active Directory.

To set up synchronization with Active Directory:

1. Set up your API credentials for AD sync. To do this, click Settings > API credentials.
2. Add a new credential. Enter the following information:
   - Credential name
   - Description
3. Copy the Client ID and Client Secret.
4. Click Settings > Active Directory Sync, and click the link to download the Sophos Central AD Synchronization Utility installer. Then run it.
   Alternatively, go to the Start menu and click Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.
   The Sophos Central AD Sync Utility Setup assistant starts.
5. In the setup wizard, enter the information required.
   Follow the instructions in the Sophos Central AD Sync Utility Setup assistant.
6. On the last page of the setup assistant, select Launch Sophos Central AD Sync Utility and click Finish.
7. In the Active Directory Synchronization Setup utility, on the Sophos Credentials page, enter your Client ID and Client Secret instead of your Sophos Central account credentials.
8. On the **AD Configuration** page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the **Use LDAP over an SSL connection (recommended)** checkbox selected. If your LDAP environment doesn’t support SSL, clear the **Use LDAP over an SSL connection (recommended)** checkbox and change the port number. The port number is usually 636 for SSL connections and 389 for insecure connections.

9. If you don’t want to synchronize the entire forest, on the **AD Filters** page, you can specify which domains to include in the synchronization. You can also specify additional search options (search bases and LDAP query filters) for each domain. Distinct options can be specified for users and user groups.

**Note**

AD Sync will only create groups that have members which include discovered users or devices, regardless of group filter settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search bases</td>
<td>You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format: OU=Finance,DC=myCompany,DC=com</td>
</tr>
<tr>
<td>LDAP query filters</td>
<td>To filter users, for example, by group membership, you can define a user query filter in this format: memberOf=CN=testGroup, DC=myCompany, DC=com The above query limits user discovery to users belonging to “testGroup”. Note that if you don’t specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter: CN=testGroup</td>
</tr>
</tbody>
</table>

**Note**

If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

10. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.
A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select Never. Only sync when manually initiated.

11. Click Finished.
12. To synchronize immediately, in the AD Sync Utility, click Preview and Sync. Review the changes that will be made during the synchronization. If you are happy with the changes, click Approve Changes and Continue.

The Active Directory users and groups are imported from the Active Directory to Sophos Central.

To stop the synchronization in progress, click Stop.

Related concepts
Active Directory Sync (page 224)
You can import users and user groups from Active Directory to Sophos Central.

Related tasks
Import users from Active Directory (page 187)
You can import users and groups from Active Directory.

Azure AD Sync Status

In Settings, on the Azure Sync Settings/Status page, once you configure Azure Active Directory synchronization, you can view:

• The status of Azure Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
• The number of users and groups imported from Azure Active Directory.
• The time of the last synchronization with Azure Active Directory.

Note
Auto synchronization happens every 6 hours. You cannot change this interval.

• The configuration settings for Azure Active Directory synchronization.
  You can amend these by selecting Edit. See Set up synchronization with Azure Active Directory.
Select Sync to run the synchronization process.

You can validate the Azure Active Directory synchronization connection by selecting Test Connection.

You can view Azure Active Directory synchronization alerts on the Alerts page. You can view synchronization events on the Logs & Reports > Events page.

Related tasks
Set up synchronization with Azure Active Directory (page 229)
Set up synchronization with Azure Active Directory

You need:

- A Microsoft Azure subscription.
- Azure Active Directory.

**CAUTION**

You can use either Azure Active Directory synchronization or **Active Directory Sync**. You can't set up Azure Active Directory synchronization if you are already using **Active Directory Sync**.

To configure Azure Active Directory synchronization:

1. Set up your Azure applications. To do this follow the instructions in Prerequisites to access the Azure Active Directory reporting API and the instructions in the next two steps.

2. In **To register an Azure AD application**, do as follows:
   a) Enter a **Name**.
   b) Enter `https://central.sophos.com` in **Redirect URI**.

3. In **Get your application’s client secret**, do as follows:
   a) Enter a description and expiry date.
   b) Make a note of your **Client secret** and **Secret expiration date**.
   c) Make a note of your **Application (client) ID** and **Primary Domain**.

4. In Sophos Central, in the left-hand pane, select **Settings**.

5. On the **Settings** page, under **Administration**, select **Azure AD Sync Settings/Status**.

6. On the **Azure Sync Settings/Status** page, select **Edit**.

7. In the **Edit Azure AD Sync** dialog box, enter the following information, which you obtained when you set up your Azure applications:
   - **Client ID**
   - **Tenant Domain**
   - **Application Key** (client secret)
   - **Application Key Expiration**

   You do not have to set the expiration date. We recommend that you do enter it so that Sophos Central can send you notifications of when your key is about to expire.

8. Select **Test Connection** to validate the Azure Sync connection.

9. Select **Save**.

10. On the next menu, select **Sync** to import users.

    Synchronization starts. This process may take some time.

**Related concepts**

- **Active Directory Sync** (page 224)
  You can import users and user groups from Active Directory to Sophos Central.

- **Azure AD Sync Status** (page 228)

**Related information**

- Prerequisites to access the Azure Active Directory reporting API
4.7.2 Role Management

You can use pre-defined administration roles to divide up security tasks according to the administrators' responsibility level.

In **Settings**, the **Role Management** page shows a list of administration roles and the number of users assigned to each role.

You can only see this option if you are a Super Admin administrator.

Click on a role name to see a detailed description of the role and the names of the people that have that role assigned to them. You can manage the people assigned to a specific role in that role's page.

**Restriction**

An administrator role affects what a user can do.

Administration Roles

Predefined roles cannot be edited or deleted.

Your assigned administrator role affects what you can do.

A Super Admin can add custom roles. These roles are based on the predefined roles but you can restrict the access for a custom role to a specific product.

**Restriction**

You can add custom roles only if you are signed up to the Sophos Early Access Program.

Super Admin

Administrators with this role have access to everything in Sophos Central.

They can manage roles and role assignments. In addition, they can create, edit, assign, and delete custom roles.

There must be at least one administrator with the Super Admin role.

Admin

Administrators with this role have access to everything in Sophos Central.

They can't manage roles and role assignments.

Help Desk

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

- Look at sensitive logs or reports.
- Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.
• Update the Sophos agent software on a computer.
• Scan computers.
• Modify co-branding.

They can't see role management options. Also they can't see some options, such as Edit buttons.

Read-only

Administrators with this role have read-only access for all settings in Sophos Central. They can also:
• Look at sensitive logs or reports.
• Receive alerts.

They can't see role management options. Also they can't see some options, such as Edit buttons.

User

Administrators with this role have no administration capabilities. They have access only to the Self Service Portal.

Related concepts
Administration Roles for Intercept X with EDR (page 232)
Administrators can do more if they have Intercept X with EDR.

User Summary (page 180)

Related tasks
Remove administrators (page 236)
You can remove administrators. Removing an administration role from a user does not delete the user.

Add administrators (page 233)
You assign administration roles to users using the Available Users list.

Administration role details
If you click a role on the Role Management page, its details are shown on a separate page.

The sections on that page include the following.

Permissions

This is the access level for a role. The options are Full, Help Desk, or Read-only.

Global Settings

These are the specialized capabilities for a role. The settings are:
• Access sensitive logs & reports: This option means that an administrator can view sensitive logs and reports; for example the Audit Logs.
• Access policy management: This option means that an administrator can change policy settings.
• Access policy assignment: This option means that an administrator can assign policies to users and devices.
Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details.

Administration Roles for Intercept X with EDR

Administrators can do more if they have Intercept X with EDR.

Super Admin and Admin

Administrators with these roles can also:
- View the intelligence report.
- Request the intelligence report
- Add items to the “Clean and Block” list.
- Remove items from the “Clean and Block” list.
- View blocked items.
- Request an on-demand threat case.
- View on-demand threat cases.
- Isolate and un-isolate devices.
- Request a forensic snapshot.
- Request a threat search.
- View a saved threat search.

Help Desk

Administrators with this role can also:
- View the intelligence report.
- Request the intelligence report.
- View blocked items.
- Request an on-demand threat case.
- View on-demand threat cases.
- Request a forensic snapshot.
- Request a threat search.
- View a saved threat search.

Read-only

Administrators with this role can also:
- View the intelligence report.
• View blocked items.
• View on-demand threat cases.
• View a saved threat search.

Related concepts
Administration Roles (page 230)

Add administrators

You assign administration roles to users using the Available Users list.

Existing administration roles, if any, are indicated next to the user's name.

A user can only have one assigned role.

For example if you add a Read-only administrator to the list of Help Desk administrators their assigned role will change to Help Desk administrator. They will no longer be a Read-only administrator.

To add an administrator:

1. In Settings, on the Role Management page, select the administrator role that you want to assign.
2. On the role details page, next to Role Members, click Edit.

Note
You can only see this option if you are a Super Admin.

3. In Edit Role Members, select a user in the Available Users list and use the picker arrows to add them to the Assigned Users list for the role. Select Save.

Tip
Enter a name or part of a name in the search box to filter the list of available users.

Add a custom role

You can add custom roles if you are a Super Admin.

Custom roles are based on the predefined roles. You can restrict the access for a custom role to a specific product. You can also create a role that allows an administrator to have full access to one product and read-only access to a second product.

Restriction
If a role doesn't have access to both Endpoint Protection and Server Protection (in some cases Encryption as well), the shared settings are read-only.

The shared settings are:
• Tamper protection
• Allowed applications
• Website management
• Proxy configuration
To create a custom role:

1. In Settings, on the Role Management page, select Add role.
2. Give the custom role a name and a description.
3. Select the Base role you want to use as the basis for the custom role.
   For example, if you choose Help Desk as the Base role, administrators with the custom role have Help Desk permissions.
4. Choose the product and access type you want the role to have.
   For example, you create a custom role called Endpoint Help Desk. This custom role uses Read-only as its Base role and Endpoint Protection as its selected product with an access type of Help Desk.

   This custom role allows any administrators assigned to this role to access Endpoint Protection with Help Desk permissions.

   a) Choose more than one product, if required.

      You can choose different access types for different products.

      For example, you create a custom role that has Help Desk access permissions for Endpoint Protection and Read-only access for Mobile. You can set the permissions for all other products to None. This means that the custom role only has access to Endpoint Protection with Help Desk permissions and Mobile with Read-only permissions.

5. Choose the additional access and management options for the custom role.

   • Enable access to logs & reports.
   • Enable policy management (add, edit, and delete).
   • Enable policy assignment to users, device, etc.. (turn policies on and off; and add users, user groups, devices and device groups to existing policies).

   For example, this allows a Super Admin to add these permissions to a Read-only or Help Desk role. You can also use these options to reduce the permissions for an Admin role. For example, you could prevent the custom role from managing policies.

   Note
   These additional options only apply to the selected products for the custom role.

   The additional options are the same for all products and access types for the custom role.

6. Select Save.

   You can now assign this role to administrators.

Related concepts
Administration Roles (page 230)

Related tasks
Delete custom role (page 235)
You can delete custom roles if you are a Super Admin.

**Remove administrators** (page 236)
You can remove administrators. Removing an administration role from a user does not delete the user.

**Change roles**
You can change the assigned roles for administrators if you are a Super Admin.
You can change roles for multiple administrators at the same time.

**Restriction**
You can't change roles for administrators who are currently signed in.

To change roles:
1. In **Settings**, on the **Role Management** page, select the administrator role that you want to assign to other administrators. For example, select a read-only administrator role if you want to assign that role to other administrators.
2. On the role details page, next to **Role Members**, click **Edit**.

   **Note**
   You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, add users from the **Available Users** list or remove users from the **Assigned Users** list. Select **Save**.

   **Tip**
   Enter a name or part of a name in the search box to filter the list of available users.

**Delete custom role**
You can delete custom roles if you are a Super Admin.
You can only delete custom roles. You can't delete roles that have administrators assigned to them. You must change their role first.

1. In **Settings**, on the **Role Management** page, select the role you want to remove and select **Delete**.

   To select a role, click anywhere in the row apart from the name.

2. Select **Delete** to confirm role deletion.

*Related concepts*
Administration Roles (page 230)

*Related tasks*
Add a custom role (page 233)
You can add custom roles if you are a Super Admin.

Remove administrators (page 236)
You can remove administrators. Removing an administration role from a user does not delete the user.

Change roles (page 235)
You can change the assigned roles for administrators if you are a Super Admin.

**Remove administrators**

You can remove administrators. Removing an administration role from a user does not delete the user.

**Note**

You cannot delete a user who has an assigned administration role. You must remove the role from the user before deleting the user.

To delete administrators:
1. In **Settings**, on the **Role Management** page, select the administrator role from which you want to remove users.
2. On the role details page, next to **Role Members**, click **Edit**.

**Note**

You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, select a user in the **Assigned Users** list and use the picker arrows to remove them.

**Tip**

Enter a name or part of a name in the search box to filter the list of assigned users.

### 4.7.3 Tamper Protection

You can enable or disable tamper protection for all your servers and users’ computers.

To do this, in **Settings**, open the **Tamper Protection** page.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:

- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
- Disable tamper protection.
- Uninstall the Sophos agent software.

#### Manage tamper protection for a specific device

You can change the tamper protection settings for a specific device or server.

Open the device’s details page and look under **Tamper Protection**. There you can do as follows:

- View the password.
- Generate a new password.
- Temporarily disable tamper protection for that device.
Recover tamper protection passwords

You can recover the tamper protection passwords of devices that you’ve recently deleted.
You might need to do this so that you can uninstall Sophos software that is still on those devices.

4.7.4 API Token Management

You can generate and manage the API token used for secure access to the Security Information and Event Management (SIEM) Integration API. This enables you to pull new event and alert data from Sophos Central. For further information, click the knowledge base article link provided on the page.
To add a token:
1. In Settings, open the API Token Management page.
2. Click Add Token.
3. Give the token a name and click Save.
   This generates the API token. The token is valid for a year.
   Click Renew to extend the validity of the token.
   Click Delete to remove the token.

4.7.5 API credentials

You can manage and add credentials for Sophos Central Admin.

Note
The first time you click API credentials you must read and accept the terms and conditions of use.

To add credentials, do the following:
1. Click Add Credential and give the credential details.
   This generates the credential, together with a Client ID and a Client Secret.
2. Copy the Client ID and Client Secret.
   Note
   You can only see the Client Secret once.

To delete an API credential, select it in API credentials and click Delete.

4.7.6 Website Management

This page is not available if you do not have a Web Control or Web Gateway license.
Note
If an option is locked, global settings have been applied by your partner or Enterprise administrator.

You can extend the website filtering provided by Sophos Central. For more information on how Sophos filters websites see Sophos Web Security and Control Test Site.

In Settings, on the Website Management page, you can use a website list to:
- Control websites not in one of the Sophos categories.
- Tag websites to put them in groups, which are like custom categories. You can then use policies to control these websites for certain users.
- Override the Sophos category for a site. This changes that site’s category for all your users.

Note
If you think Sophos has put a website in the wrong category, you can ask us to change it. To do this, see Open a Support Case. We suggest you try this instead of overriding the category.

To add a site to the website list:
1. Click Add in the upper right of the page.
   The Add Website Customization dialog is displayed.
2. Enter sites.
   Entries in the website list can be single URLs, full domains, TLDs, IP addresses, CIDR ranges, or even top level domains.

   Note
   Managing websites using IP addresses only controls browser-based access. It does not block other applications or interact with rules for a local firewall.

3. Select Enable Category Override if you want to associate a specific category with the sites you have entered. Then select a Category.
4. Select Enable Tags to associate a tag with the sites you have entered. Then type a tag name.
   Tags can be used when creating web control policies for endpoint computers or servers. See the Log web control events section in Web Control Policy.
5. Enter text in the Comments text box.
   It can be helpful to include information about tags you have created and categories you have overridden for troubleshooting policy issues in the future.
6. Click Save.
   Your entry will be added to the website list.

You can also edit entries in the list or delete them.

To edit an entry, click the edit icon . The icon is on the right of the entry.
To delete an entry, select the checkbox to the left of the entry and click Delete.

Related concepts
Web Control Policy (page 220)
4.7.7 Registered Firewall Appliances

In Settings, on the Registered Firewall Appliances page, you can view Sophos XG Firewalls that have been registered with Sophos Central. You can also deregister (or "disconnect") them.

Note
You can only register a Sophos XG Firewall from a Sophos XG Firewall console (Go to Central synchronization).

About registered Firewalls

When a Sophos XG Firewall is registered with Sophos Central, your computers can send regular reports on their security status or "health" to Sophos XG Firewall. These reports are known as "Security Heartbeats".

If more than one Sophos XG Firewall is registered, computers send Security Heartbeats to the nearest one available.

If the Security Heartbeat reports show that a computer might have been compromised, the Sophos XG Firewall can restrict its network access. A Sophos XG Firewall admin and a Sophos Central administrator also receive alerts that tell them what to do to restore the computer’s health.

View Firewalls

The page displays details of Sophos XG Firewalls that are registered with Sophos Central:

- **Name**
- **IP Address**
- **Active**. This indicates whether a Sophos XG Firewall has received Security Heartbeats within the previous hour.

To find a Sophos XG Firewall, start to enter the name in the Search for a Firewall field. As you type, the list is filtered to show only Sophos XG Firewalls that match.

Deregister Firewalls

You can deregister Sophos XG Firewalls from Sophos Central. For example, if you no longer use a Sophos XG Firewall, you could deregister it so that it is no longer shown here.

When you deregister a Sophos XG Firewall, you continue to protect and manage the computers that are associated with it, but the Security Heartbeats feature will no longer work.

1. Select a Sophos XG Firewall you want to deregister.
2. Click the Delete button in the upper-right of the page.
3. When prompted, click OK to confirm that you want to deregister a Sophos XG Firewall.
The selected Sophos XG Firewall is removed from the list. You can deregister more than one Sophos XG Firewall at a time.

If you deregister all the Sophos XG Firewalls, this page will still be displayed and you will still be able to see old events and alerts related to the Security Heartbeat feature.

### 4.7.8 Global Exclusions

You can exclude files, websites and applications from scanning for threats.

**Introduction**

You use exclusions to tune the detection behavior of Sophos Central.

**Related tasks**

- **Exploit Mitigation Exclusions** (page 117)
  You can exclude applications from protection against security exploits.

**Related reference**

- **Website exclusions** (page 116)
  You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.
- **Process exclusions (Windows)** (page 116)
  You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).
- **Malicious Network Traffic Prevention (IPS) (Windows) exclusions** (page 120)
  You can exclude specific network traffic from inspection.
- **Device isolation exclusions (Windows)** (page 117)
  You can allow isolated devices to have limited communications with other devices.
- **Windows Scanning Exclusions: Wildcards and Variables** (page 110)
  When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.
- **macOS Scanning Exclusions** (page 112)
  You can add scanning exclusions for macOS workstations.
- **Virtual Server Scanning Exclusions: Wildcards** (page 114)
  **Virtual Server** exclusions let you exclude items from scanning on Windows guest VMs that are protected by a Sophos security VM.

**Related information**

- **Sophos Threat Center**

**Exclusions**

Global exclusions apply to all your users (and their devices) and servers.

If you want exclusions to apply only to certain users or servers, use policy exclusions instead.

You can set up the following types of exclusion:

- Exclude files or folders from scanning.
  - If you exclude files from scanning, we'll still check the excluded items for exploits.
- Exclude from checking any process that runs from an application.
• Exclude websites from checking.
• Exclude applications from protection against security exploits.
• Exclude applications that are normally detected as spyware and previously detected exploits from scanning and detection.
• Exclude previously detected malicious behavior exploits. This is only available if you are signed up to the Early Access Program.

You can also use exclusions to allow isolated devices to communicate with other devices under restrictions. This feature is available if you have Intercept X Advanced with EDR.

**Warning**
Think carefully before you add global exclusions because doing so may reduce your protection.

**Can’t edit the exclusions?**

If an option is locked global settings have been applied by your partner or Enterprise administrator. You can still stop detecting applications, exploits and ransomware from events.

**Exploit exclusions**

If you exclude files from scanning, we’ll still check the excluded items for exploits. If you want exclusions from exploit checking, do as follows:

• To stop checking for an exploit that has been detected, use a **Detected Exploits** exclusion.
• To exclude certain applications from checking, use Exploit Mitigation Exclusions.
• To stop checking for a malicious behavior exploit that has been detected, use a Behavioral Protection exclusion.

**Set up exclusions**

You can exclude files, websites and applications from scanning for threats.

To set exclusions:

1. Go to **Global Exclusions**.
2. Click **Add Exclusion**.
   The **Add Exclusion** dialog is displayed.
3. In the **Exclusion Type** drop-down list select what you want to exclude.
4. Specify the item or items you want to exclude.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File or folder (Windows)</td>
<td>You can exclude a drive, folder or file by full path. You can use the wildcard * for file name or extension but <em>.</em> is not valid.</td>
</tr>
<tr>
<td>File or folder (Mac/Linux)</td>
<td>You can exclude a folder or file. You can use the wildcards ? and *.</td>
</tr>
<tr>
<td>File or folder (Sophos Security VM)</td>
<td>On Windows guest VMs protected by a Sophos security VM, you can exclude a drive,</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>folder or file by full path. You can use the wildcards * and ? but only for file names.</td>
<td><strong>Process (Windows)</strong> You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process). If possible, enter the full path from the application.</td>
</tr>
<tr>
<td>You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.</td>
<td><strong>Website (Windows/Mac)</strong> You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.</td>
</tr>
<tr>
<td>You can exclude applications that are normally detected as spyware. Specify the exclusion using the same name under which it was detected by the system. Find more information about PUAs in the Sophos Threat Center.</td>
<td><strong>Potentially Unwanted Application (Windows/Mac)</strong> You can exclude applications that are normally detected as spyware. Specify the exclusion using the same name under which it was detected by the system. Find more information about PUAs in the Sophos Threat Center.</td>
</tr>
<tr>
<td>You can exclude any exploit that has already been detected. We’ll no longer detect it for the affected application and no longer block the application.</td>
<td><strong>Detected Exploits (Windows/Mac)</strong> You can exclude any exploit that has already been detected. We’ll no longer detect it for the affected application and no longer block the application.</td>
</tr>
<tr>
<td>You can allow isolated devices to have limited communications with other devices. Choose whether isolated devices will use outbound or inbound communications, or both. You can then restrict communications.</td>
<td><strong>Device isolation (Windows)</strong> You can allow isolated devices to have limited communications with other devices. Choose whether isolated devices will use outbound or inbound communications, or both. You can then restrict communications.</td>
</tr>
<tr>
<td>You can exclude specific network traffic from inspection. Choose whether to exclude outbound or inbound traffic. Then specify the address or ports the traffic uses.</td>
<td><strong>Malicious Network Traffic Prevention (IPS) (Windows)</strong> You can exclude specific network traffic from inspection. Choose whether to exclude outbound or inbound traffic. Then specify the address or ports the traffic uses.</td>
</tr>
<tr>
<td>You can exclude applications from protection against security exploits. For example, you might want to exclude an application that is incorrectly detected as a threat until the problem has been resolved.</td>
<td><strong>Exploit Mitigation (Windows)</strong> You can exclude applications from protection against security exploits. For example, you might want to exclude an application that is incorrectly detected as a threat until the problem has been resolved.</td>
</tr>
<tr>
<td>You can exclude a drive, folder or file by full path. Code in this location is not scanned. You can use the wildcard * for file name or extension.</td>
<td><strong>AMSI Protection (Windows)</strong> You can exclude a drive, folder or file by full path. Code in this location is not scanned. You can use the wildcard * for file name or extension.</td>
</tr>
<tr>
<td>You can exclude applications from protection against behavioral exploits.</td>
<td><strong>Behavioral Protection (Windows)</strong> You can exclude applications from protection against behavioral exploits.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>For example, you might want to exclude an application that has been incorrectly detected as behaving maliciously. You can't edit these exclusions after you create them. This option is only available if you are signed up to the Early Access Program.</td>
</tr>
</tbody>
</table>

5. For File or folder exclusions, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.

6. Click **Add** or **Add Another**. The exclusion is added to the scanning exclusions list.

   To edit an exclusion later, click its name in the exclusions list, enter new settings and click **Update**.

### 4.7.9 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

#### Set the bandwidth used

In **Settings**, on the **Bandwidth Usage** page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.

This helps to ensure that updating does not cause computers to run slowly.

You can specify a custom bandwidth or unlimited bandwidth.

**Note**

This setting is for Windows computers only.

**Note**

This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos. To save bandwidth in this case, see **Manage Update Caches and Message Relays**.

#### Related concepts

**Manage Update Caches and Message Relays** (page 128)

Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos.

### 4.7.10 HTTPS updating

Your computers and servers can get their Sophos updates via HTTPS. We recommend that you use HTTPS for greater security.

To use HTTPS updating:

1. Go to **Settings > HTTPS Updating**.
2. Turn on **HTTPS Updating**.

### 4.7.11 Multi-factor authentication

If you're a Super Admin, you can make some or all of the Sophos Central admins sign in with multi-factor authentication.

**Introduction**

Using multi-factor authentication means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos or Google Authenticator, SMS or email authentication to sign in.

Multi-factor authentication is turned on by default for newly created Sophos Central accounts.

This page tells you how to do the following:

- Set up multi-factor authentication.
- Sign in with multi-factor authentication for the first time.
- Add another method for multi-factor authentication.
- Sign in with email authentication if you don't have Sophos or Google Authenticator.
- Reset an admin's sign-in details, for example if they lose their phone.
- Turn off multi-factor authentication for an admin.

**Set up multi-factor authentication**

If you're a Super Admin, you can choose how your administrators sign in.

To set up multi-factor authentication, do as follows:

1. Go to **Settings > Multi-factor Authentication (MFA)**.
2. Choose how you want admins to sign in:
   - **No MFA needed**.
   - **All admins need MFA**. This is the default for new accounts.
   - **Select admins who will need MFA**. This lets you select individual admins.
3. If you choose **Select admins who will need MFA**, a user list is displayed. Click **Add admins** (on the right of the screen). Move admins to the **Assigned Users** list and click **Add**.
4. Click **Save**.

When admins next sign in, they are prompted to set up a new method of authentication.

**Sign in with multi-factor authentication for the first time**

The first time you sign in with MFA, do as follows:

1. At the sign-in screen, enter your user ID (email address) and password.
   - A **Set Up Your Login Information** dialog explains that signing in needs additional authentication.
2. In the next dialog:
a) Enter the security code that has been sent to you in an email.
b) Create a 4-digit PIN. This enables you to use email as an authentication method.

3. In the next dialog, choose authentication type.

4. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
   You also need to enter a security code to verify a device if you have chosen SMS as your authentication type.
   Sophos Central Admin opens.

   The next time you sign in, you only need to enter a code from Sophos or Google Authenticator when prompted.

Add another authentication option for multi-factor authentication

You can set up multiple authentication options for a Sophos Central Admin account.
You can authenticate with SMS and Sophos or Google Authenticator.
You must have an authentication option already set up.

To set up another authentication option, do as follows:
1. Sign in to Sophos Central Admin.
2. Click your account name and click Manage Login Settings.
3. Click Create New Method.
4. Choose another authentication method.
5. Click Next.
6. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
7. To confirm that the new method has been added, click your account name and click Manage Login Settings.
   An additional authentication method has been added.

Sign in with email authentication

If you don't have access to Sophos or Google Authenticator, you can sign in with email authentication instead.

1. At the sign-in screen, enter the user ID (email address) and password.
2. In Verify Your Login, click Choose Another Method.
3. In Pick Your Challenge, click the email option.
   An email is sent to you.
4. Open the email and find the security code.
5. In Verify Your Login, enter the security code and your 4-digit PIN.

You'll be asked for the security code and PIN each time you sign in from now on, until you switch back to using Sophos or Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can allow them to set up their sign-in again.

1. On the People page, under Users, find the user and click their name to open their details.
2. In the user details, on the left of the screen, you’ll see their MFA status and settings. Click **Reset** and confirm that you want to do a reset.

The next time the admin tries to sign in, they’ll need to go through the setup steps again.

**Turn off multi-factor authentication**

If you’re a Super Admin, you can turn off multi-factor authentication for an administrator.

To turn off multi-factor authentication, do as follows:

1. Go to **Settings > Multi-factor Authentication (MFA)**.
2. Click **Select admins who will need MFA**.
3. Click **Add admins**.
4. Move the administrator from the **Assigned Users** list and to the **Available Users** list.
5. Click **Add**.
6. Click **Save**.

### 4.7.12 Admin Isolated Devices

On the **Settings > Admin Isolated Devices** page you can see which devices you've isolated and remove them from isolation.

**Note**

This list doesn't include devices that have isolated themselves automatically because their health is red, see **Device Isolation** in **Threat Protection Policy**.

You can isolate affected devices while you investigate a threat case, see **Threat Cases**. You can also search for other affected devices and isolate those from your threat search results, see **Threat Searches**.

You can allow isolated devices to communicate with other devices in limited circumstances, see **Global Exclusions**.

After you have cleaned up and blocked any suspicious applications you can remove the affected devices from isolation.

To do this:

1. Select the device and click **Remove from Isolation**.

**Related concepts**

- **Threat Protection Policy** (page 203)
  Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

- **Threat Cases** (page 19)
  Threat cases let you investigate and clean up malware attacks.

- **Threat Searches** (page 31)
  You can search for potential threats on your network.

**Related information**

- **Global Exclusions** (page 240)
You can exclude files, websites and applications from scanning for threats.

### 4.7.13 Encryption Recovery Key Search

You can get a device encryption recovery key by entering a volume or recovery identifier.

#### Retrieve recovery key (Windows computers)

If users are unable to log in to their encrypted computer, you can get a recovery key which is used to unlock the computer. There is a recovery key for each volume of a BitLocker protected computer. It is created and backed up in Sophos Central before the computer is encrypted.

**Note**

When Sophos Device Encryption is installed, existing BitLocker recovery keys are replaced automatically and can no longer be used.

**Note**

Even if a policy has been disabled and the computer's Device Encryption status is shown as "Unmanaged", you can get a recovery key if one is available.

To get the recovery key, go to **Computers**, select the computer you want to recover, and click **More > Retrieve Recovery Key**. If you cannot find the computer in the list, you need the recovery key identifier or the volume identifier and use it in the recovery wizard, as follows:

1. Tell the user to restart the computer and press the Esc key in the **BitLocker** logon screen.
2. Ask the user to provide you with the information displayed in the **BitLocker recovery** screen.
3. In Sophos Central, go to **Computers** and click **More > Retrieve Recovery Key**.
4. Enter at least five characters of the recovery key identifier or the volume identifier provided by the user.
5. Click **Show Key** to display the recovery key.

**Note**

If you enter a volume identifier, Sophos Central displays all available recovery keys for this volume. The latest recovery key is the top one.

6. Make sure that the user is authorized to access the encrypted device before you provide the recovery key.

**Note**

As soon as a recovery key is displayed to you as administrator, it is marked as used and will be replaced at the next synchronization.

7. Give the recovery key to the user.

The user can now unlock the computer. Users of computers running Windows 8 or later are prompted to create a new PIN or password. Instructions for creating the PIN or password are displayed automatically.
After the computer has been recovered, a new recovery key will be created and backed up in Sophos Central. The old one will be deleted from the computer.

Retrieve recovery key (Macs)

If users forget their login password, you can get a recovery key which is used to unlock the computer.

To get the recovery key, go to Computers, select the computer you want to recover, and click More > Retrieve Recovery Key. If you cannot find the computer in the list, you need the recovery key identifier or the volume identifier and use it in the recovery wizard, as follows:

1. Tell the user to switch on their computer and wait until the Recovery Key ID is displayed.

   **Note**
   The recovery key ID is displayed for a short time. To display it again, users must restart their computer.

2. Ask the user to tell you the Recovery Key ID.
3. In Sophos Central, go to Computers and click More > Retrieve Recovery Key.
4. Enter at least five characters of the recovery key identifier.
5. Click Show Key to display the recovery key.
6. Make sure that the user is authorized to access the encrypted device before you provide the recovery key.
7. Give the recovery key to the user.
   - For users imported from Active Directory, continue to step 8.
   - For all other users, go straight to step 10.
8. Reset the existing password in Active Directory. Then generate a preliminary password and give it to the user.
9. Tell the user to click Cancel in the Reset Password dialog and enter the preliminary password instead.
10. Tell the user to do as follows:
    - Create a new password.
    - Click Create New Keychain if prompted.

The user can access the computer again.

On endpoints running macOS 10.12 or earlier, a new recovery key is created and stored in Sophos Central. A recovery key can only be used once. If you need to recover a computer again later, you need to retrieve a new recovery key.

On endpoints running macOS 10.13 and Apple File System (APFS), no new recovery key is created. The existing recovery key remains valid.

### 4.7.14 Allowed applications

On the Settings > Allowed Applications page you can see applications that you have allowed to run on your endpoint computers.
The page shows where the application was originally detected (if applicable) and how it was allowed.

About allowed applications

Our software detects threats that are previously unknown. However, it may sometimes identify an application as a threat, even though you know that it’s safe. When this happens, you can “allow” the application. This does as follows:

- Prevents this detection from happening again.
- Restores all copies that have been cleaned up (removed from computers).

Alternatively, you can allow an application in advance, so that it won’t be detected when you install it for users.

**CAUTION**

Think carefully before you allow applications because it reduces your protection.

**Note**

If an option is locked global settings have been applied by your partner or Enterprise administrator. You can still stop detecting applications, exploits and ransomware by going to the events list.

Allow an application that's been detected

Only allow an application if you know it's safe. For help deciding, see [How to investigate and resolve a potential False Positive or Incorrect Detection](#).

To allow an application that Sophos has detected and removed, do as follows.

**Note that:**

- This allows the application for all computers and users.
- This allows the application to start, but we’ll still check it for threats, exploits and malicious behavior when it’s running.

1. Go to the **Computers** or **Servers** page, depending on where the application was detected.
2. Find the computer where the detection happened and click on it to view its details.
3. On the **Events** tab, find the detection event and click **Details**.
4. In the **Event details** dialog, look under **Allow this application**.
5. Select the method of allowing the application:
   - **Certificate:** This is recommended. It also allows other applications with the same certificate.
   - **SHA-256:** This allows this version of the application. However, if the application is updated, it could be detected again.
   - **Path:** This allows the application as long as it's installed in the path (location) shown. You can edit the path (now or later) and you can use variables if the application is installed in different locations on different computers.
6. Click **Allow**.
Edit the path for an allowed application

You can change the path that you specified when you allowed an application.
1. On the **Allowed Applications** page, find the application. The current path is shown in the details.
2. Click the edit icon (the pen) on the far right of the page.

3. In the **Edit path** dialog, enter the new path.

When you edit a path, details of the original detection (user, computer and path) are removed from the list.

Start detecting an application again

If you want Sophos to start detecting and removing an application again, you remove it from the **Allowed Applications** list.
Select the application and click **Remove** (in the upper right of the page).

**Related information**

*How to investigate and resolve a potential False Positive or Incorrect Detection*

### 4.7.15 Blocked items

This option is available if you have Intercept X Advanced with EDR.

On the **Settings > Blocked Items** page, you can block and clean up suspicious applications.

You can also see applications that you have blocked from running on your computers. You can see who blocked the application and why.

**About blocked applications**

You can block applications using their SHA-256 hash. This prevents suspicious applications from running on your computers.

You can only block applications. SHA-256 hashes for other items, or for files Sophos believes to be safe, are ignored.

When you block an application it’s cleaned up on any devices it’s already on.

You can also clean up and block applications when you investigate a threat case or review the results of a threat search.

**Block an application**

To block and clean up an application:
1. Click **Add**.
2. Enter the application’s SHA-256 hash.
3. Enter a reason for blocking the application.

4. Click **Add**.
   - Click **Add Another** if you want to block more than one application.

5. When you have finished, click **Save** on the **Blocked Items** page.

This blocks the application on all computers and cleans it up on computers it’s already on.

### Remove an application from the block list

You can remove applications from the block list if you’ve decided that they aren’t suspicious. To do this:

1. Select the application in the list and click **Remove**.

### Related concepts

**Threat Cases** (page 19)
Threat cases let you investigate and clean up malware attacks.

**Threat Searches** (page 31)
You can search for potential threats on your network.

**Admin Isolated Devices** (page 246)

### 4.7.16 Controlled updates

By default, computers get the latest Sophos product updates automatically. If you prefer, you can control how your computers update.

For example, you can stop updates on all computers during a busy period, or test updates on selected computers before they are rolled out to the rest of the network.

#### Restriction
You can control updates on Windows and Linux devices, but not Macs.

To control updates, go to **Settings > Controlled Updates**.

You have these options.

- **Pause Updates Now**
- **Pause Updates on a Set Date**
- **Control Updates Manually**

If updates are already controlled, you see a list of computers whose updates are controlled instead of these options.

#### Note
Computers still get automatic security updates to protect them against the latest threats.

You can go back to automatic updating at any time.

### Related concepts

**Pause updates now** (page 252)
You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

Control updates manually (page 252)
You can control product updates manually.

Related tasks
Pause updates on a set date (page 252)
You can choose dates when you want to stop and restart product updates on all computers.

Pause updates now
You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

Restriction
You can control updates on Windows and Linux devices, but not Macs.

On the Settings > Controlled Updates page, click Pause Updates Now. This stops automatic updates on all your computers immediately. Updates start again automatically after 90 days.

Tip
If you want to start updates again earlier, click Resume Automatic Updating.

Pause updates on a set date
You can choose dates when you want to stop and restart product updates on all computers. Automatic updates will stop for 90 days. Your computers will still get security updates.

Restriction
You can control updates on Windows and Linux devices, but not Macs.

1. On the Settings > Controlled Updates page, click Pause Updates on a Set Date.
2. Select a Pause date and a Restart date. Click Apply.

On the restart date, the computers will start updating automatically and get any updates that are available.

Tip
If you want to restart updating earlier, click Resume Automatic Updating.

Control updates manually
You can control product updates manually.

Restriction
You can control updates on Windows and Linux devices, but not Macs.
This stops automatic updating so that you can decide when to test new product versions and roll them out to your computers.

Note
Your computers will still get automatic security updates.

This Help topic tells you how to set up manual updating, and how to test and roll out updates.

How to set up manual updating

On the Settings > Controlled Updates page, click Control Updates Manually.

Note
This stops all automatic updates. You are not asked for confirmation.

Initially, your situation is this:

- All your computers are on the Newest (recommended) version. They’ll be shown as being on this version until Sophos issues a newer version.
- No computers will get any further updates until you update them.

Now you should set up test computers (if you want to).

Set up test computers

You can use test computers to try out new versions.

1. In the Test computers table, click Add.
2. Select computers from the Available Computers list.

You’re now ready to test updates and roll them out manually.

Test and roll out updates

When Sophos releases a new product version:

- You receive an email alert.
- Computers that were on the Newest (recommended) version are now shown as being on the Oldest.

In the table of versions, you can use the buttons in the Action column to update computers when you want to.

Typically, you would want to test the new version on selected computers and then roll it out to all the other computers.

In the Action column, next to Test Computers, click Update test computers to newest version.

When you’re ready to update all your other computers, in the Action column, next to Non-test computers, click Update to match test computers.

This forces the non-test computers to update at the time of the next automatic update, which by default is every 60 minutes. Note that this update will not follow any schedule that you’ve set in the Update Management policy for servers.
Why can I see a 'Previous' version now?

If Sophos releases another product update when you already have test computers on **Newest (recommended)** and the rest on **Oldest**:

- Test computers are now shown as being on the **Previous** version (the version that has just been replaced by a newer one).
- Non-test computers are on **Oldest**.

You can use an action button next to the test computers to **Update test computers to newest version**.
You can use an action button next to non-test computers to **Update to match test computers**.

What happens when a version expires?

Sophos product updates expire after 90 days. When the **Oldest** version expires, computers are forced to update as follows:

- If all computers are on **Oldest**, they resume automatic updating.

  **Note**
  If this happens, all computers get the newest version. You no longer control updates manually.

- If non-test computers are on **Oldest**, but test computers are on a newer version, the non-test computers are updated to the same version as the test computers.

4.7.17 Live Response for computers

Turn on Live Response so that you can connect to computers to investigate and remediate possible security issues.

**Restriction**
You must be a Super Admin to configure Live Response.

1. Go to **Settings > Endpoint Protection > Live Response**.
2. Turn on **Allow Live Response connections to computers**.
3. Click **Save**.

To turn on Live Response for servers, see **Live Response for servers**.

**Related tasks**
**Live Response for servers** (page 390)
Turn on Live Response so that you can connect to servers to investigate and remediate possible security issues.

4.7.18 Data Loss Prevention Rules

You use data loss prevention (DLP) rules to specify conditions to detect, actions to take, and any files to exclude from scanning.

You can use these rules across multiple policies.

There are two types of rules:

- **Content**: A content rule details the action to be taken if a user attempts to transfer data that matches the Content Control Lists (CCLs) in the rule to the specified destination. You use CCLs to match file content.

- **File**: A file rule details the action to be taken if a user tries to transfer a file with the specified file name or file type to the designated destination. For example you can block the transfer of databases to removable storage devices.

When all the conditions listed in a rule are detected, the rule is matched, the action specified in the rule is followed and the event is logged.

If a file matches rules that specify different actions, the rule that specifies the most restrictive action is applied. For example:

- Rules that block file transfer take priority over the rules that allow file transfer on user acceptance.
- Rules that allow file transfer on user acceptance take priority over the rules that allow file transfer.

Manage Data Loss Prevention Rules

This page lists the existing DLP rules and allows you to manage their use across multiple policies. The name, source and type is shown for each rule.

You can create new custom rules, and search existing rules.

You can also filter rules by **Rule Type**.

Click on the name of a rule to edit it.

To view details of a rule, click **Information**.

To clone a rule, click **Clone**.
1. Give a name for the cloned rule.
2. Click **Clone item**. This adds the cloned rule to the list of rules.
3. You can then amend it by clicking its name in the list.

To export custom rules, click **Export**. This creates an xml file containing the rule definition.

To delete a rule, click **Delete**. Click **Delete item** to confirm deletion.

To import rules:
1. Click **Import**.
2. Select the XML file containing the rules.
3. Click **Open**.

Copyright © Sophos Limited 255
The rules are added to the list.

**Related concepts**

**Content Control Lists** (page 257)
A Content Control List (CCL) describes a single type of data (for example, a postal address or social security number) or a combination of data types (for example, a project name near the term “confidential”).

**Related tasks**

**Create a Data Loss Prevention Rule** (page 256)
Follow these instructions to create a DLP rule.

---

**Create a Data Loss Prevention Rule**

Follow these instructions to create a DLP rule.

There are two stages to creating a DLP rule; creation and configuration.

This stage sets up the rule type, the actions taken if the rule is triggered and whether you want to be alerted to the breaches of the rule.

To create a DLP rule:

1. Click **Create New Rule**.
2. Choose from **New Content Rule** or **New File Rule**.
3. Give the rule a **Name** and a **Description**.
4. Click **Send me email alerts** if you want notifying when the rule is breached.

**Note**
You will not get an alert in Sophos Central.

5. For a **File** rule, choose whether you want to match against a file name or a file type as the conditions for the rule. You will give the details when you configure the rule.

**Note**
Conditions are required for a **Content** rule and you cannot set the condition type.

6. Specify if you want to exclude by a file name or by file type. You will give the details when you configure the rule.
7. Specify the actions for the rule. Choose from:
   - **Allow file transfer**.
   - **Allow transfer if user confirms**.
   - **Block transfer**.
8. Click **Next: Rule Configuration**.

**Related tasks**

**Configure a Data Loss Prevention Rule** (page 257)
You can set up the conditions for monitored files, file types or destinations and the exclusions for a DLP rule.

**Configure a Data Loss Prevention Rule**

You can set up the conditions for monitored files, file types or destinations and the exclusions for a DLP rule.

You must have created a DLP rule.

The conditions you set depend on whether you are creating a **File** or **Content** rule.

1. Set up the rule conditions.
   a) To set up conditions for a content rule, click **File Contains** and select the CCLs you want to use.
      You can search the list of CCLs. You can filter the CCLs by **Type**, **Source** (choose from **Sophos Labs** or **Custom**), and **Region**. You can also create a new CCL.
   b) To set up conditions for a file rule, specify the file names or file types for the rule.
2. Click **Destination is** and set the destinations that the rule monitors.
   Destinations include devices (for example, removable storage devices, such as USB flash drives) and applications (for example, internet browsers and email clients).
3. Set the exclusion details for the rule.
4. Click **Finish** to create the rule.

**Related tasks**

* Create a Data Loss Prevention Rule (page 256)

Follow these instructions to create a DLP rule.

**4.7.19 Content Control Lists**

A Content Control List (CCL) describes a single type of data (for example, a postal address or social security number) or a combination of data types (for example, a project name near the term "confidential").

This creates a definition for data that you want to protect. You can then use CCLs in data loss prevention rules to control what happens to this data.

To enable you to quickly define and roll out a data loss prevention policy, SophosLabs maintain a library of sensitive data definitions. SophosLabs CCLs provide expert definitions for common financial and personally identifiable data types, for example, credit card numbers, social security numbers, postal addresses, or email addresses. You cannot edit SophosLabs CCLs, but you can submit a request to Sophos to create a new one.

You can use SophosLabs CCLs in your rules, or create your own CCLs.

You can filter the CCLs.
You also can search the list of CCLs.

To view details of a CCL, click **Information**.
For each custom CCL you can also:

- Click on the name of a CCL to edit it.
- To export a CCL, click **Export**. This creates an XML file containing the definition for the CCL.
To clone a CCL, click **Clone**. Give a name for the cloned CCL and click **Clone item**. This adds the cloned CCL to the list of CCLs. You can then edit it by clicking its name.

To delete a CCL, click **Delete**. Click **Delete item** to confirm deletion.

You can also import CCLs:

1. Click **Import**.
2. Select the XML file containing the CCLs.
3. Click **Open**.
   
The CCLs are added to the list.

**Related concepts**

**Data Loss Prevention Rules** (page 255)

You use data loss prevention (DLP) rules to specify conditions to detect, actions to take, and any files to exclude from scanning.

**Create Custom Content Control List**

Follow these instructions to create a custom CCL.

To create a custom CCL:

1. Click **Add Custom Content Control List**.
2. Give the CCL a **Name** and a **Description**.
3. Click **Select tags** and add the tags you want to use.
4. Specify the matching criteria for the CCL. Choose from:
   
   - **Any of these terms**: Enter a term that you want to match in **Terms** and click **Add** to add another term.
   - **All of these terms**: Enter a term that you want to match in **Terms** and click **Add** to add another term.
   - **Exactly this phrase**: Enter the phrase that you want to match in **Phrase**. This option is not case sensitive.
   - **Advanced Setup**: Use this option to set up an advanced expression.
      
      Set the **Trigger score**.
      
      This is the number of times the regular expression must be matched before the CCL is matched.

5. Click **Save** to create the CCL.

**Related tasks**

**Set up an advanced expression** (page 258)

Follow these instructions to set up an advanced expression for a custom CCL.

**Set up an advanced expression**

Follow these instructions to set up an advanced expression for a custom CCL.

You can only do this as part of creating a custom CCL.

Select **Advanced Setup** as the matching criteria to enter the details for an advanced expression:

1. Set the **Trigger score**.
This is the number of times the regular expression must be matched before the CCL is matched.

2. Enter a Perl 5 regular expression in **Expression**.

For a description of Perl 5 regular expressions, refer to Perl documentation or go to Perl syntax.

3. Set the **Score** for the CCL. This is the number that is added to the total score for a CCL when the regular expression is matched.

**Note**
The **Score** must match the **Trigger score**.

4. Set the **Max count**. This is the maximum number of matches for the regular expression that can be counted towards the total score.

For example, an expression with a **Score** of 5 and a **Max count** of 2 can add the maximum of 10 to the total score of a CCL. If the expression is found 3 times, it still adds 10 to the total score.

5. Click **Add**.
   - To delete an expression, click **Delete**
   - To edit an expression, click **Edit**
   - Once you have finished your edits, click **Save**
   - to save them.

6. Add more expressions, if required.

Adding more expressions expands the scope of the CCL.

For example, the following CCL is matched if Data Loss Prevention finds 2 matches of expression A or 1 match of expression A and 1 match of expression B, or 1 match of expression B and 5 matches of expression C.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Score</th>
<th>Max count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expression A</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Expression B</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Expression C</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

**Related tasks**
Create Custom Content Control List (page 258)
Follow these instructions to create a custom CCL.

**Related information**
Perl syntax

### 4.8 Protect Devices

You can download Sophos installers and use them to protect your devices.

The installers you can see may depend on the license or licenses you have.
Before you start, check which operating systems you can protect with Sophos Central: see the Sophos Central page.

For more details, including what each product does, how you use the installers, and how Sophos Central registers devices and applies policies, read the other topics in this section.

How to use installers

After downloading installers for workstations or servers, you can:

- Run the installer to protect the local computer.
- Transfer the installer to other computers and run it on them.
- Use automated software deployment tools such as System Center Configuration Manager (SCCM) to run the installer on large numbers of computers.

How to find out which data center stores your account

To find out which data center stores your Sophos Central account data, do as follows:

1. Go to Protect Devices.
2. Under Endpoint Protection or Server Protection, hover the mouse pointer over any of the installer download links.

   The data center address is shown in the lower-left corner of the browser:

   ![Data center address](https://api-cloudstation-us-east-2.prod.hydra.sophos.com/api/download/f0ae9d21d7f92d053ab09e932e3a1b1d/SophosSetup.exe)

3. The address shows the geographical location of the data center:

<table>
<thead>
<tr>
<th>Address</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://api-cloudstation-us-east-2.prod.hydra.sophos.com">https://api-cloudstation-us-east-2.prod.hydra.sophos.com</a></td>
<td>US east</td>
</tr>
<tr>
<td><a href="https://api-cloudstation-eu-central-1-prod.hydra.sophos.com">https://api-cloudstation-eu-central-1-prod.hydra.sophos.com</a></td>
<td>EU central</td>
</tr>
</tbody>
</table>

Related information

Sophos Central page

4.8.1 Endpoint Protection

You install an Endpoint Protection agent on workstations to protect them against malware, risky file types and websites, and malicious network traffic.

It also offers peripheral control, web control and more.

Sophos Device Encryption is also installed automatically on Windows workstations (if you have the required license).
Download and run installers

Go to Protect Devices.

Download the installer for your operating system and run it on workstations you want to protect.

- **Download Complete Windows Installer**: Click this for an installer with all endpoint products your license covers.
  
  Alternatively, click **Choose Components...** to choose which products will be included in the installer. The choices are:

  - **Sophos Intercept X Advanced** (protection from ransomware and exploits).
  
  - **Device Encryption**.

- **Download Complete macOS Installer**: Click this for an installer with all endpoint products your license covers.

  Alternatively, click **Choose Components...** to choose which products will be included in the installer. The choices are as for Windows above.

- **Send Installers to Users**: Click this to go to a page where you can add users and send them installers that they can use.

*Note*

For Linux, look for "Server Protection". Sophos Central treats all Linux computers as servers.

What happens when you protect a computer

When you protect a computer:

- Each user who logs in is added to the users list in Sophos Central automatically.
- Default policies are applied to each user.
- Each computer is added to the **Computers** list in Sophos Central.

How we handle Windows usernames and login names

Users are listed with full login name, including the domain if available (for example, `DOMAINNAME\jdoe`).

If there is no domain, and a user logs in to multiple computers, multiple user entries are displayed for this user, for example `MACHINE1\user1` and `MACHINE2\user1`. To merge these entries, delete one and assign the login to the other (and rename the user, if required). See Endpoint protection deployment methods.

**Related information**

Endpoint protection deployment methods
### 4.8.2 Installer command-line options for Windows

You can use the following command-line options with the Sophos Central Endpoint installer for Windows.

#### Command-line options

These options apply to:
- Sophos Endpoint Advanced 11.5.11 and later.
- Sophos Endpoint Standard 11.5.11 and later.

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet</td>
<td>--quiet</td>
<td>Runs the installer without displaying the user interface.</td>
<td></td>
</tr>
<tr>
<td>No proxy detection</td>
<td>--noproxydetection</td>
<td>Doesn't attempt to perform automatic proxy detection.</td>
<td></td>
</tr>
<tr>
<td>No competitor removal</td>
<td>--nocompetitorremoval</td>
<td>Doesn't attempt to automatically remove competitors. (Only on installation of Sophos Anti-Virus.)</td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>--language=&lt;language ID&gt;</td>
<td>Allows you to manually set the installer language. By default the installer uses the system language.</td>
<td>Language ID</td>
</tr>
<tr>
<td>Group</td>
<td>--devicegroup=&lt;Central group&gt;</td>
<td>Specifies the Sophos Central device group to join the endpoint to.</td>
<td>A group to join. If it doesn't exist, it is created.</td>
</tr>
</tbody>
</table>
| CRT catalog path              | --crtcatalogpath=<path to CRT catalog> | Allows you to specify your own catalog of competitors to remove. | Full path and filename to catalog folder. Example:  
  --crtcatalogpath=C:\catalog\productcatalog.xml |
<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Message relays</strong></td>
<td><code>-- messagerelays=&lt;comma-separated message relay list of IPs including the port&gt;</code></td>
<td>Specifies a list of message relays to use.</td>
<td>The IP address of the message relay must be specified along with the port 8190. Example: <code>-- messagerelays=IPADDRESS:8190</code></td>
</tr>
<tr>
<td><strong>Proxy address</strong></td>
<td><code>-- proxyaddress=&lt;custom proxy address&gt;</code></td>
<td>Specifies a custom proxy to use.</td>
<td>URL without protocol (will use HTTPS)</td>
</tr>
<tr>
<td><strong>Proxy username</strong></td>
<td><code>-- proxyusername=&lt;custom proxy user name&gt;</code></td>
<td>If a custom proxy has been specified, set the username with this option.</td>
<td>The username of the proxy.</td>
</tr>
<tr>
<td><strong>Proxy password</strong></td>
<td><code>-- proxypassword=&lt;custom proxy password&gt;</code></td>
<td>If a custom proxy and username have been specified, set the password with this option.</td>
<td>The password for the proxy.</td>
</tr>
<tr>
<td><strong>Computer name override</strong></td>
<td><code>-- computernameoverride=&lt;override for computer name&gt;</code></td>
<td>Overrides the name of the computer to be used in Sophos Central.</td>
<td>Custom computer name.</td>
</tr>
<tr>
<td><strong>Computer description override</strong></td>
<td><code>-- computerdescriptionoverride=&lt;override for description&gt;</code></td>
<td>Overrides the description of the computer to be used in Sophos Central.</td>
<td>Custom computer description.</td>
</tr>
<tr>
<td><strong>Domain name override</strong></td>
<td><code>-- domainnameoverride=&lt;override for domain&gt;</code></td>
<td>Overrides the domain name of the computer to be used in Sophos Central.</td>
<td>Custom domain name.</td>
</tr>
<tr>
<td><strong>Customer token</strong></td>
<td><code>-- customertoken=&lt;the customer token&gt;</code></td>
<td>Specifies the token of the Sophos Central customer to associate the endpoint with.</td>
<td>A UUID which maps to a customer.</td>
</tr>
<tr>
<td><strong>Products to install</strong></td>
<td><code>-- products=&lt;comma-separated list of products&gt;</code></td>
<td>Specifies a list of products to install. If you specify a product that you don't have a license for, then it isn't installed.</td>
<td>A list of products to install, comma-separated. Available options are: antivirus, intercept, mdr, deviceEncryption or all.</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local install source</td>
<td><code>--localinstallsource=&lt;path-to-install-source&gt;</code></td>
<td>Specifies a local install source to use during installation. This allows an installation to occur without having to download the installer files.</td>
<td>It isn't necessary to populate the local install source, but it is necessary to create a <code>SophosLocalInstallSource</code> folder. If an empty folder is provided it is populated during the first installation. If you wish to pre-populate the cache you can take a copy of the files from an already installed endpoint or from your update cache: %ProgramData %\Sophos \AutoUpdate\data \Warehouse %ProgramData %\ Sophos \UpdateCache\www \warehouse Even if a populated local install source is provided, internet access is still required and some files are downloaded. The amount of data downloaded depends on various factors including, for example: Whether the platform of the installation endpoint differs from the files already populated. Whether the warehouse has changes since the local install source was populated. For the purpose of this example <code>SomeContent</code> represents the files and folders within the Warehouse folder. %ProgramData %\ Sophos \AutoUpdate \data\Warehouse</td>
</tr>
</tbody>
</table>
### Option Example usage Description Trailing argument

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message trail logging</td>
<td>--traillogging</td>
<td>Turns on the logging of message content between the endpoint and Sophos Central during installation. You must switch this option off after installing, see Enabling a diagnostic message trail of Sophos MCS.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

There is no command-line option for installation from an update cache. The installer automatically assesses connectivity to any update caches set up in the Sophos Central account and installs from them.

### Windows examples

**Install Sophos Anti-Virus and Intercept X without user interaction:**

```bash
SophosSetup.exe --products=antivirus,intercept --quiet
```

**Install using a proxy:**

```bash
SophosSetup.exe --proxyaddress=<ProxyIP/FQDN>:<Port>
```

**Install using a message relay:**

```bash
SophosSetup.exe --messagerelays=192.168.10.100:8190
```

### Language IDs

<table>
<thead>
<tr>
<th>Language</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>1033</td>
</tr>
<tr>
<td>French</td>
<td>1036</td>
</tr>
<tr>
<td>German</td>
<td>1031</td>
</tr>
<tr>
<td>Japanese</td>
<td>1041</td>
</tr>
<tr>
<td>Spanish</td>
<td>1034</td>
</tr>
<tr>
<td>Italian</td>
<td>1040</td>
</tr>
<tr>
<td>Polish</td>
<td>1045</td>
</tr>
<tr>
<td>Brazilian Portuguese</td>
<td>1046</td>
</tr>
</tbody>
</table>
Sophos Central Admin

<table>
<thead>
<tr>
<th>Language</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korean</td>
<td>1042</td>
</tr>
<tr>
<td>Chinese Simplified (Mandarin)</td>
<td>2052</td>
</tr>
<tr>
<td>Chinese Traditional (Cantonese)</td>
<td>3076</td>
</tr>
<tr>
<td>Chinese Hong Kong</td>
<td>3076</td>
</tr>
<tr>
<td>Chinese Macau</td>
<td>3076</td>
</tr>
<tr>
<td>Chinese Singapore</td>
<td>2052</td>
</tr>
</tbody>
</table>

**Related concepts**

*Endpoint Protection* (page 161)

You install an Endpoint Protection agent on workstations to protect them against malware, risky file types and websites, and malicious network traffic.

**Related information**

*Enabling a diagnostic message trail of Sophos MCS*

*Domains and ports required for communication to and from Sophos Central Admin and the Sophos Central managed endpoint*

*Frequently Asked Questions (FAQs)*

*New endpoint installer frequently asked questions*

*An Internet connection could not be established*

*Installer precheck messages*

### 4.8.3 Installer command-line options for Mac

The Sophos Central Endpoint installer for Mac supports the following command-line options.

**Mac command line options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet</td>
<td>--quiet --install</td>
<td>Runs the installer without displaying the user interface.</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>--devicegroup &lt;Central group&gt;</td>
<td>Specifies the Sophos Central device group to join the endpoint to.</td>
<td>A group to join. If it doesn't exist, it is created.</td>
</tr>
<tr>
<td>Option</td>
<td>Example usage</td>
<td>Description</td>
<td>Trailing argument</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Message relays</td>
<td>--messagerelays &lt;space-separated message relay list of IPs including the port&gt;</td>
<td>Specifies a list of message relays to use.</td>
<td>The IP address of the message relay must be specified along with the port, 8190.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example: --messagerelays IPADDRESS:8190 IPADDRESS:8190</td>
</tr>
<tr>
<td>Proxy address</td>
<td>--proxyaddress &lt;custom proxy address&gt;</td>
<td>Specifies a custom proxy to use.</td>
<td>URL without protocol (uses HTTPS).</td>
</tr>
<tr>
<td>Proxy port</td>
<td>--proxyport &lt;proxy port&gt;</td>
<td>Specifies a port that the proxy uses.</td>
<td>Port for the proxy.</td>
</tr>
<tr>
<td>Proxy username</td>
<td>--proxyusername &lt;custom proxy user name&gt;</td>
<td>If a custom proxy has been specified, set the username with this option.</td>
<td>The username for the proxy.</td>
</tr>
<tr>
<td>Proxy password</td>
<td>--proxypassword &lt;custom proxy password&gt;</td>
<td>If a custom proxy and username have been specified, set the password with this option.</td>
<td>The password for the proxy.</td>
</tr>
<tr>
<td>Computer name override</td>
<td>--computernameoverride &lt;override for computer name&gt;</td>
<td>Overrides the name of the computer to be used in Sophos Central.</td>
<td>Custom computer name.</td>
</tr>
<tr>
<td>Computer description override</td>
<td>--computerdescriptionoverride &lt;override for description&gt;</td>
<td>Overrides the description of the computer to be used in Sophos Central.</td>
<td>Custom computer description.</td>
</tr>
<tr>
<td>Domain name override</td>
<td>--domainnameoverride &lt;override for domain&gt;</td>
<td>Overrides the domain name of the computer to be used in Sophos Central.</td>
<td>Custom domain name.</td>
</tr>
<tr>
<td>Preferred domain name for usernames in Sophos Central</td>
<td>--mcsPreferredDomainName</td>
<td>Sets the client to send usernames as domain\username instead of machine\username.</td>
<td></td>
</tr>
<tr>
<td>Registration server</td>
<td>--mgmtserver &lt;registration server URL&gt;</td>
<td>Specifies the MCS server to connect to.</td>
<td>MCS server URL.</td>
</tr>
</tbody>
</table>
## Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Example usage</th>
<th>Description</th>
<th>Trailing argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer token</td>
<td><code>--customertoken &lt;the customer token&gt;</code></td>
<td>Specifies the token of the Sophos Central customer to associate the endpoint with.</td>
<td>A UUID which maps to a customer.</td>
</tr>
<tr>
<td>Products to install</td>
<td><code>--products &lt;space separated list of products to install&gt;</code></td>
<td>Specifies a list of products to install. If you specify a product that you don’t have a license for, then it isn’t installed.</td>
<td>A list of products to install, space-separated. Available options are: antivirus, intercept, deviceEncryption or all.</td>
</tr>
</tbody>
</table>

**Note**

The Mac installer is aware of all the message relays and update caches when the installation is downloaded. Changes to caches and relays mean that you need to download a new installation. You can specify relays using the command line as well.

**Mac examples**

**Install Sophos Anti-Virus and Intercept X without user interaction:**

```bash
sudo ./Sophos\ Installer.app/Contents/MacOs/Sophos\ Installer --products antivirus intercept --quiet
```

**Install using a proxy:**

```bash
sudo ./Sophos\ Installer.app/Contents/MacOs/Sophos\ Installer --proxyaddress <ProxyIP/FQDN> --proxyport <Port>
```

**Install using a message relay:**

```bash
sudo ./Sophos\ Installer.app/Contents/MacOs/Sophos\ Installer --messagerelays 192.168.10.100:8190
```
5 Encryption

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault on Macs. Encrypting hard disks keeps data safe, even when a device is lost or stolen.

5.1 Dashboard

The Dashboard is the start page of Device Encryption and lets you see the most important information at a glance.

What do you need to do?

Click Set up Device Encryption for on-screen instructions that help you encrypt computers for the first time. Follow the other links to start the most important tasks in Device Encryption.

Encryption status

This shows you how many computers are encrypted and how many can be encrypted (but aren't).

Note

Total computers shows all your computers, including the ones that aren't managed or can't be encrypted.

Licensing

This shows your license usage.

5.2 Logs & Reports

The Logs & Reports page lists the reports that you can generate about security features in Sophos Central.

The page also lists any Saved Reports. These are custom reports that you or other administrators for this account have saved.

To find out how reports work and how you can customize, save and schedule them, see Reports.

Related concepts

Reports (page 269)

5.2.1 Reports

The reports that you can see depend on your license.
You can customize reports, save them and send them out as scheduled emails.

**Note**
A report may not support all the customization or viewing options.

**Limit report data to a specific time range**

In some reports, you can limit report data to a specific date range by entering a **From** and **To** date. In some reports, you can select a time period.

**Filter reports**

In some reports, you can filter the displayed information by clicking on the category tiles. For example in the Computers report you can show all the active computers by clicking on **Active**. You may also be able to filter by groups. You can also use **Search** to filter for specific information.

**Print or export reports**

You can print or export your reports.

- **Print**: Click this to open a printer-friendly view. Then press Ctrl+P to open the printer dialog.
- **Export to CSV**: Click this to export the current view as a comma separated file.
- **Export to PDF**: Click this to export the current view as a PDF file.

**Save and email custom reports**

You can create and save custom reports. A list of the saved reports is shown at the top of the **Logs & Reports** page.

You can also choose to send custom reports by email and set up a schedule for them. You can save as many reports as you like, but you can only schedule up to 25.

1. Set up the report by selecting the appropriate filters.
2. Click **Save as Custom Report**.
   - This opens the **Save Report** dialog.
3. Enter a **Name** for the report.
4. If you want to send the report by email, select one of these options:
   - **Send a link to the report**.
   - **Attach the report to the email**.
   - We recommend that you send a link if the report includes personally identifiable information.
   - You need to enter Sophos Central sign-in credentials to view reports from a link.
5. Select the **Frequency**. You can choose from monthly or weekly.
6. Select the format: **PDF** or **CSV**.
7. Click **Save**.

The email is received by the user who signs in and creates the report.

**Note**

Scheduled emails stop after six months. You can reschedule them if you want to.

### 5.3 People

On the **People** page, you can manage your users and user groups.

#### 5.3.1 Users

On the **Users** tab of the **People** page, you can add or manage users, and get the users’ computers protected.

You can also enable the users to protect their own devices by emailing them a setup link.

The current users are listed with their details.

**Health Status.** An icon shows whether the user has security alerts on any of their devices.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Check Mark" /></td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td><img src="image" alt="Amber Warning Sign" /></td>
<td>Amber warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td><img src="image" alt="Red Warning Sign" /></td>
<td>Red warning sign if there are critical alerts.</td>
</tr>
</tbody>
</table>

**Name** Click the user's name to see details of devices and to see which has an alert.

**Email.**

**Exchange Login.**

**Last Active.** The last time a user reported to Sophos Central.

**Group Name.** This is shown if the user has been added to a user group.

**Role.** This shows what administration role, if any, the user has. This column is only visible if you are an administrator.

Click any column header to sort the users. By default, users are sorted according to the **Last Active** time.

To see full details for a user, click the user's name.

You can add users manually or automatically by protecting their devices. You can also import users in bulk from a CSV file or from Active Directory. You can also protect existing users.

To modify users, click the user's name to open and edit their user details.

You can also delete users and export lists of users.
**Related concepts**

*User Summary* (page 272)

*Administration Roles* (page 302)

**Related tasks**

*Add a user manually* (page 277)

You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

*Add users automatically* (page 278)

You can add users automatically by protecting their devices.

*Import users from a CSV file* (page 278)

You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

*Import users from Active Directory* (page 279)

You can import users and groups from Active Directory.

*Protect existing users* (page 279)

You can protect users that you have already added to Sophos Central.

*Delete users* (page 280)

You can delete users from Sophos Central if you are a Super Admin.

*Export to CSV* (page 280)

You can export lists of users as CSV files.

---

**User Summary**

The **Summary** tab in a user's details page shows a summary of the following:

- The user's security status, administration role, if any, and account details.
- Recent events on the user's devices.
- Mailboxes associated with the user.
- Devices associated with the user.
- Policies that apply to the user.
- Groups that the user belongs to.
- Logins.

You can find details of each below.

The security status and account details are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.

You can click on the other tabs for more on **Devices**, **Events**, and **Policies**.

---

**Health Status**

In the left-hand pane, an icon shows you whether the user has security alerts on any of their devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://example.com/checkmark.png" alt="Green check mark icon" /></td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Orange warning sign" /></td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td><img src="image" alt="Red warning sign" /></td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>

You can see which devices have alerts in the **Devices** tab.

A padlock icon shows that the user has been imported from Active Directory.

A badge shows the user’s assigned administration role. Click on the role name to view the settings for the role.

**Note**
Role information is only displayed for administration roles.

### Account details

In the left-hand pane, you can modify or delete the user’s account.

**Note**
If a user has been imported from Active Directory, you cannot change the account details. However, you can add the user to a new Sophos Central group or add another login.

**Modify the account**

1. Click **Edit** and enter the following settings:
   - **First & Last name**: Enter the name of the user. Do not include a domain name.
   - **Role**: Select a role for the user. Choose from: *Super Admin*, *Admin*, *Help Desk*, *Read-only*, or *User*.

   **Restriction**
   You can only see the **Role** option and assign administrator roles if you are a Super Admin.

   **Note**
   You cannot amend your own administration role.

   **Note**
   Anyone with a **User** role only has access to the Self Service Portal.

   **Email Address**: Enter the email address of the user.

   **Exchange Login** (optional): Enter the Exchange account name of the user.

   **Note**
   In Sophos Mobile policies, you can use the placeholder `%USERNAME%` to refer to this setting.
**Add to groups**: Select one of the available user groups and use the picker arrows to move it to the assigned groups.

**Email Setup Link**: Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs.

**Note**
The user needs administrative privileges and internet access in order to protect their computer.

**Note**
**Web Gateway** provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

2. Click **Save**.

**Delete the account**
To delete the account, click **Delete User** in the left-hand pane. Logins assigned to this user can afterward be assigned to another user.

**Restriction**
You cannot delete users who have an assigned administration role.

**Multi-factor authentication**
If the user is an admin, the left-hand pane shows whether multi-factor authentication (MFA) is enabled for them. If it is enabled, the admin must use another form of authentication, as well as their user name and password, to sign in.

If you’re a Super Admin, you can edit the settings as follows:

- Click **Reset** to let the admin set up their MFA sign-in details again.
- Click **MFA Settings** to go to a page where you can enable or disable multi-factor authentication for the admin.

**Recent Events**
This lists recent events on the user’s devices.
For a full list, click the **Events** tab.

**Mailboxes**
This lists all email addresses, including distribution lists and public folders, associated with the user. Primary indicates the user’s primary email address. Owner indicates the user controls a distribution list or public folder.
For full details, click an email address.
Devices

This shows a summary of the devices associated with the user.
Click the device name to go to the device's details page for more information.
Click **Actions** to carry out any of the same actions that are available on the device's details page (for example, Scan Now and Update Now for a computer).
For full details of the user's devices, click the **Devices** tab.

Policies

This shows a summary of the policies applied to the user.
The list shows the policy name, whether the policy is enabled or not, and icons that indicate the features included in the policy.
Click on a policy name to view and edit the user policy.

**Note**
Editing the policy affects all users to which this policy is applied.

For full details of all the policies applied to this user, click the **Policies** tab.

Groups

This shows the groups the user belongs to.
Click on a group name to see details of the group.
Click **Edit** (on the right) to change the groups the user belongs to.

Logins

This shows the user's logins.
Click **Edit** (on the right) to change the logins assigned to the user.

**Related concepts**

- About Policies (page 293)
- Administration Roles (page 302)

User Devices

The **Devices** tab in a user's details page lets you see the devices associated with the user.
This tab also shows any servers where the user has logged on with Remote Desktop Services.
For each associated device you can see the device type and the operating system. You also have these options:

- **View Details**: This opens the full device details page.
• **Delete**: This removes the device from the list and stops Sophos Central managing it, but it does not uninstall the Sophos software.

• **Actions**: Actions you can take. These depend on the device type.

**User Events**

The **Events** tab in a user's details page lets you see a list of events detected on the user's devices. You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

• **Severity**: Hover over an icon to see what it means.

• **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.

• **Details**: This link (for certain events) lets you get further details and take action.

**View Events Report** shows events arranged by type and a graph of events day by day.

**Stop detecting an application**

If an application is reported as malware but you know it's safe, you can allow it from the events list. For help with deciding whether an application is safe, see *How to investigate and resolve a potential False Positive or Incorrect Detection*.

Click the **Details** link beside the event and then allow the application.

**Note**

This currently applies only to malware events reported by Intercept X.

**Stop detecting an exploit**

If an exploit is detected but you're sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.

2. In **Event details**, look for **Don't detect this again** and select an option:

   • **Exclude this Detection ID from checking**: prevents this detection on this app.

   • **Exclude this application from checking**: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.

3. Click **Exclude**.

We'll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

**Stop detecting ransomware**

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again.
This will apply to all your users and computers.
1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again.
   Select Exclude this Detection ID from checking. This prevents this detection on this app.
3. Click Exclude.
We’ll add your exclusion to the Global Exclusions list.

Related information
How to investigate and resolve a potential False Positive or Incorrect Detection

User Policies

The Policies tab in a user's details page lets you see the policies that are enabled and applied to the user.
Click a policy name to view and edit policy details.
Editing the policy affects all users to which this policy is applied.

Add a user manually

You can add an individual user and protect them. This also gives you the option to let users protect their own devices.
To add a user:
1. Go to Users.
2. Click Add and select Add User.
3. In the Add User dialog, enter the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First and Last Name</td>
<td>Enter the name of the user. Do not include a domain name.</td>
</tr>
<tr>
<td>Role</td>
<td>Select an administration role for the user. A user who is assigned an administration role will receive an email telling them how to set up their administration account. You can only see the Role option and assign administrator roles if you are a Super Admin. Anyone with a User role only has access to the Self Service Portal.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address of the user.</td>
</tr>
<tr>
<td>Add to groups (optional).</td>
<td>Select one of the available user groups and use the picker arrows to move it to the assigned groups. You can start typing a name in the search box to filter the displayed groups.</td>
</tr>
</tbody>
</table>
## Option | Description
--- | ---
### Email Setup Link
Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs.
The user needs administrative privileges and internet access in order to protect their computer.

### Web Gateway
This provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

---

4. Click **Save** or **Save and Add Another**.
The new user is added to the user list.

When the user downloads and installs the software, their device is automatically associated with the user.

### Add users automatically
You can add users automatically by protecting their devices.

To add users:
1. Download an installer from **Protect Devices**.
2. Run the installer on the devices.
This adds the user of each device automatically.

### Related concepts
**Protect Devices** (page 314)
You can download Sophos installers and use them to protect your devices.

### Import users from a CSV file
You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

To import users:
1. Go to **Users**.
2. Click **Add** and click **Import users from CSV**.
3. Click **Browse** and select your CSV file.

**Tip**
You can download template CSV files from the **Import users from CSV** dialog.

The CSV file can include groups a user is assigned to.

4. To create new groups, click **Create new groups**.
5. To send a registration email for the Sophos Central Self Service portal to each imported user, click **Give users access to Sophos Central Self Service**.
6. Click **Add**.

**Note**
The CSV file can include the email address of each user's manager. If there's a manager who isn't already a user in Sophos Central, a user is created. So the number of users imported may exceed the number of rows in the file.

**Note**
If an email address in your CSV file matches an existing user in Sophos Central, the user is updated with the information in your import file.

**Note**
If an email address in your CSV file matches an existing user in Sophos Central that is managed through Active Directory Synchronization, the user is skipped during import and no changes are made to the user account.

**Import users from Active Directory**
You can import users and groups from Active Directory.
To do this:
1. Go to **Users**.
2. Click the **Set up Active Directory Sync** link in the upper right of the page.
3. Follow the set up synchronization process.

**Related tasks**
Set up synchronization with Active Directory (page 299)
Follow these instructions to set up synchronization with Active Directory.

**Protect existing users**
You can protect users that you have already added to Sophos Central.
To protect them you need to email them a setup link. To do this:
1. Go to **Users**.
2. Select the user or users you want to protect.
3. Click **Email Setup Link** in the upper right of the page.
4. In the **Email Setup Link** dialog, select the types of protection the user needs (if your license includes more than one).

**Web Gateway** provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

Users need administrative privileges and internet access to use the setup link.
Delete users

You can delete users from Sophos Central if you are a Super Admin.

**Restriction**
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them.

Under some circumstances, the user may be recreated automatically in future:
- If the user logs in to an associated device that is still managed by Sophos Central, they are added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they are added as a user again the next time that Sophos Central synchronizes with Active Directory.

To delete users:
1. Go to **Users**.
2. Click the checkbox next to each user you want to delete.
3. Click **Delete**.

Deleting a user does not delete devices associated with that user or remove the Sophos software from these devices.

Logins assigned to a deleted user can afterwards be assigned to another user. You can edit logins by clicking the **Edit** link on a user's details page.

**Related concepts**
*User Summary* (page 272)

Export to CSV

You can export lists of users as CSV files.

You can export lists of different types of user.

For example you can export a list of administrators by applying the **Admins only** filter before you click **Export to CSV**.

To export users:
1. Go to **Users**.
2. Click **Export to CSV**.
   
   This creates a file called `users.csv`. Any currently active filters are applied to the list.

5.3.2 Groups

On the **Groups** tab of the **People** page, you can add or manage groups of users.

You can use groups to assign a policy to multiple users at once.

The sections below tell you about the groups list and how to add, modify or delete groups.
About the groups list

The current groups are listed and the number of users in each group is shown.
To see full details for a group, click the group's name.

Add a group

1. Click the Add Group button.
2. In the Add Group dialog, enter the following settings:
   - **Group Name**: Enter the name of the new group.
   - **Available Users**: Select users from the list of available users.
     
     **Tip**
     In the Search box you can start typing a name to filter down the displayed entries.

3. Click Save.

Modify a group

To modify a group, click the group's name to open and edit the group details. For more information, see User Group Details.

Delete a group

To delete a group, select it and click Delete in the upper right of the page.
Deleting a group will not delete its users.

**Related concepts**
User Group Details (page 281)

User Group Details

On a group's details page, you can:

- Add or remove members.
- Delete the group.

Add or remove members

To add or remove members:

1. Click Edit under the group name.

2. In the Edit Group dialog, use the picker arrows to add users to the Assigned Users list or remove them.
3. Click **Save**.

### Delete the group

To delete the group:

1. Click **Delete** under the group name.
2. In the **Confirm Group Deletion** pop-up, click **Yes**.

Deleting a group will not delete its users.

### User Group Policies

The **Policies** tab in a user group's details page lets you see the policies that are enabled and applied to the group.

Click a policy name to view and edit policy details.

Editing the policy affects all groups to which this policy is applied.

### 5.4 Computers

On the **Computers** page, you can manage your protected computers.

They will appear automatically after Sophos agent software has been installed.

You can:

- View details of the computers.
- See the encryption status (if you are using Sophos Device Encryption).
- Delete computers.
- Install or uninstall software.
- Get a recovery key for encrypted computers (if you are using Sophos Device Encryption).
- Export the computers list to CSV.

### View computer details

The computers list shows you the current computers with these details:

- Name.
- IP Address. Hover over the icon to see details of all IPv4 and IPv6 addresses.
- Operating System.
- Products installed. For example, Intercept X or Encryption.
- Last user.
- Last active. This is the last time that the computer contacted Sophos.
- Group. The group that the computer belongs to (if it belongs to one).
- Device Encryption. This shows the encryption status.
- To search for a computer, enter the name in the search field above the list.
To filter computers according to their type, their health status, or their encryption status, use the filters above the list.

You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

See the encryption status

The computers list shows you the **Device Encryption** status. This can be one of the following:

- **Encrypted**: The endpoint is fully encrypted.
- **Encrypting**: The endpoint has an encryption policy, but it is not fully encrypted.
- **Suspended**: Device Encryption has been suspended for at least one volume.
- **Not supported**: The endpoint cannot be encrypted because the operating system is not supported.
- **Unmanaged**: Device Encryption is disabled for the endpoint via policy.
- **Unknown**: The endpoint hasn’t sent an encryption status yet (for example, because Device Encryption isn't installed).

Delete computers

You can delete computers that you no longer need to manage from Sophos Central.

Select the computer or computers you want to delete and click **Delete** (in the upper right of the page).

This deletes the computer and the alerts associated with the computer.

**Warning**

You should uninstall the Sophos software before deleting a computer.

Install or uninstall software

You can select new endpoint software to be installed on computers that are already protected and managed by Sophos Central.

You can also uninstall software.

To do either, do as follows.

1. Click **Manage Endpoint Software** (in the upper right of the page).
2. Select software.
3. Select computers and use the picker arrows to change the software installed, as follows.
   - To install the software, select eligible computers and move them to the assigned list.
   - To uninstall the software, select assigned computers and move them to the eligible list.

The computers will update to the selected software.
Export to CSV

To export a list of computers:
Click **Export to CSV**.

This creates a file called devices.csv. Any currently active filters are applied to the list.

For example you can export a list of Windows computers by applying the **Windows Computers** filter before clicking **Export to CSV**.

Retrieve recovery key

This option is available from **More** on the **Computers** page.

If users are unable to log in to their encrypted computer, you can get a recovery key which is used to unlock the computer.

**Related concepts**
**Encryption Recovery Key Search** (page 312)

5.4.1 Computer Summary

The **Summary** tab in a computer's details page shows you the following information.
The sections you see depend on your license and the features you've set up.

Security status

In the left-hand pane, you can see the security status and take actions.

**Note**
The left-hand pane is always shown, even when you click the other tabs on this page.

An icon shows you whether the computer has any security alerts:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="green-check-mark.png" alt="Green check mark" /></td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td><img src="orange-warning-sign.png" alt="Orange warning sign" /></td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td><img src="red-warning-sign.png" alt="Red warning sign" /></td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>
Actions you can take

The action buttons are in the left-hand pane.

**Update**: This updates your computer with the latest Sophos software.

**Delete**: This deletes the computer from Sophos Central. It also deletes the alerts associated with the computer.

**Warning**
You should uninstall the Sophos software before deleting a computer.

**Isolate**: This isolates the computer from the network.

**Live Response (Beta)**: This enables you to connect to the computer to investigate and remediate possible security issues.

**Change group**: This lets you add it to a group, move it to a different group, or remove it from its current group.

**Scan Now**: This scans the computer for threats.

The scan may take some time. When complete, you can see a “Scan completed” event and any successful cleanup events on the **Logs & Reports > Events** page. You can see alerts about unsuccessful cleanup on the **Alerts** page.

If the computer is offline, it is scanned when it is back online. If a computer scan is already running, the new scan request will be ignored and the earlier scan will carry on.

**Diagnose**: This diagnoses potential issues with the computer.

**Create forensic snapshot**: This gets data from a Sophos log of the device's activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

**Isolate or remove from isolation**

This option is available if you have Intercept X Advanced with EDR.

**Isolate** isolates the computer from the network. You might want to do this if potential threats are found on it. You can still manage the computer from Sophos Central and you can remove it from isolation at any time.

When a computer has been isolated, you see the following under the computer icon and security status.

- The message **Isolated by Admin**.
- A link labeled **Remove from Isolation**. Click it to reconnect the computer to the network.

**Note**
You don't see the **Isolate** option if the computer has already isolated itself automatically. See **Device Isolation in Threat Protection Policy**.

Copyright © Sophos Limited
Live Response (Beta)

This option is available only if you are a Super Admin and you've signed in using multi-factor authentication. You must also turn on Allow Live Response connections to computers in Global Settings, see Live Response for devices.

This enables you to connect to the computer to investigate and remediate possible security issues. You might want to do this if an infection or suspicious activity is identified on the computer. You can connect to the computer even if it’s isolated. To connect to the computer, do as follows:

1. Click Live Response (Beta).
2. In Session purpose, summarize the purpose of your session.
3. Click Start.
   A connection to the computer is opened in another browser tab. The tab shows a terminal window.
4. At the command prompt, type commands to perform your investigation or remediation.
   Use DOS, UNIX, or Linux commands depending on the computer to which you’ve connected.
5. When you finish, click End Session.
   The connection is closed, although the tab remains open. You can browse elsewhere in Sophos Central from here.
   The connection is also closed in the following cases:
   - You close the tab.
   - You refresh the tab.
   - You browse elsewhere in Sophos Central from here.
   - There is no activity for 30 minutes.

To see which Live Response sessions have started or ended, view the Sophos Central audit log.

Create forensic snapshot

You can create a “forensic snapshot” of data from the device. This gets data from a Sophos log of the device’s activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

You'll need a converter (which we provide) to read the data.

Note
You can choose how much data you want in snapshots and where to upload them. To do this, go to Global Settings > Forensic Snapshots. These options may not be available for all customers yet.

To create a snapshot:

1. Go to a threat case's Analyze tab.
   Alternatively, on the details page of the device, open the Status tab.
2. Click Create forensic snapshot.
3. Follow the steps in Upload a forensic snapshot to an AWS S3 bucket.
You can find the snapshots you generated in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Forensic Snapshots\.

Snapshots generated from detections are in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Saved Data\.

Note
You need to be an administrator with access to the tamper protection password and run a command prompt as an administrator to access the saved snapshots.

Recent Events

This lists recent events on the computer. For a full list, click the Events tab.
The icons indicate which Sophos agent reported each event. Hover over an icon to see what it means.

Agent Summary

The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.

The summary shows the following details. It also includes links to let you update the computer, install products, or change the group the computer's in, as needed.

• Last Activity: Shows when the last activity occurred.
• Last Agent Update: Shows whether the computer is up to date.
• Assigned Products: Shows the Sophos products installed (for example, Intercept X or Device Encryption). Shows the license and the version number for each installed product. The version information is only available for Windows computers.
• Installed component versions: Click this to see a full list of the Sophos components and their version numbers. This is only available for Windows computers.
• Group: Shows which group the computer is in (if any).

Device Encryption

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault encryption on Macs.

This summary shows:

• All volumes of the computer.
• The volume ID for each volume.
• The encryption status.
• The authentication type.
• The encryption method.

Volumes can be encrypted with software-based or hardware-based encryption. Device Encryption always uses software-based encryption for new volumes, even if the drive supports hardware-based encryption.
If a drive is already encrypted with hardware-based encryption, it will not be changed.

If a BitLocker group policy setting requires hardware-based encryption, it is used.

**Retrieve Recovery Key**

You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their sign-in credentials.

**Trigger change of password/PIN**

This requires users to immediately change their BitLocker password or PIN. A message is displayed when the request has been sent successfully.

On the endpoint, users are prompted to set a new BitLocker password or PIN. If users close the dialog without entering a new password or PIN, the dialog is shown again after 30 seconds, until they enter a new one. After users have closed the dialog five times without changing the password or PIN an alert is logged.

**Web Gateway summary**

Sophos Web Gateway provides advanced protection against risky or inappropriate web browsing.

The summary shows the last network activity. It also shows the version of the Web Gateway agent (and whether it is up to date).

If you need to update the Web Gateway agent, an **Update** button is displayed.

**Tamper Protection**

This shows whether tamper protection is enabled on the computer or not.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:

- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
- Disable tamper protection.
- Uninstall the Sophos agent software.

Click **Disable Tamper Protection** to manage the tamper protection password for the computer. If tamper protection is switched off we recommend you turn it on.

**Update Cache and Message Relay**

Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos. You can also designate servers to communicate with Sophos Central as message relays.

This shows that a cache has been set up for the computer. It shows which server is being used.

**Windows Firewall**

Windows Firewall is active and being managed on the computer. It also shows:

- Whether Windows Group Policy is being used.
• The active network profiles.
• If other registered firewalls are installed and active.

Related concepts
Encryption Recovery Key Search (page 312)
Threat Protection Policy (page 203)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

5.4.2 Computer Events

The Events tab in a computer’s details page displays events detected on the computer.
You can see details and, in some cases, take action to prevent unwanted detections.
The list includes:
• **Sev**: Hover over an icon to see what it means.
• **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
• **Details**: This link (for certain events) lets you get further details and take action.

**View Events Report**: Shows events arranged by type and a graph of events day by day.

Stop detecting an application

If an application is reported as malware but you know it’s safe, you can allow it from the events list.
For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.
Click the Details link beside the event and then allow the application.

**Note**
This currently applies only to malware events reported by Intercept X.

Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again.
This will apply to all your users and computers.
1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again and select an option:
   • **Exclude this Detection ID from checking**: prevents this detection on this app.
   • **Exclude this application from checking**: prevents any checks for exploits on this app.
   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.
3. Click Exclude.
   We’ll add your exclusion to a list.
Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again.
   Select Exclude this Detection ID from checking. This prevents this detection on this app.
3. Click Exclude.

We’ll add your exclusion to the Global Exclusions list.

Related information
How to investigate and resolve a potential False Positive or Incorrect Detection

5.4.3 Computer Status

The Status tab in a computer’s details page lets you see the computer's security health and details of any alerts.

It also lets you take action against alerts.

Security Health

These status details are only shown if the computer is using the Security Heartbeat feature.

The computer security status is reported by computers running Windows 7 and later.

This shows whether the device has threats detected, has out-of-date software, is not compliant with policy, or is not properly protected. The overall status is the same as that for the highest-priority item listed (red, orange or green).

Alerts

The page lists any alerts on the device. The details include:

- Alert details: For example, the name of the malware.
- When the alert occurred.
- The actions that you can take. These depend on the type of threat or event and are the same as the actions available in the Dashboard.

Related concepts
Alerts (page 4)
The Alerts page lists all the alerts that require your action.

Forensic snapshots (page 138)
Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

**Related information**

Upload a forensic snapshot to an AWS S3 bucket (page 140)

Follow these instructions to upload a forensic snapshot.

### 5.4.4 Computer Policies

The **Policies** tab in a computer’s details page lets you see the policies that are applied to the computer.

You can view and edit policy details by clicking the policy in the list.

**Note**

Editing the policy affects all users to which this policy is applied.

### 5.5 Unmanaged computers

You can view your computers that don’t have Sophos Device Encryption installed.

They will appear automatically after you have synchronized with Active Directory.

You can see the details of the synchronized computers that don’t have Sophos Device Encryption installed. You can then encrypt these computers.

### 5.6 Computer Groups

On the **Computer Groups** tab you can add or manage groups of computers.

You can use groups to assign a policy to multiple computers at once.

The sections below tell you about the groups list and how to add, modify or delete groups.

#### About the groups list

The current groups are listed and the number of computers in each group is shown.

To see full details for a group, click on the group’s name.

#### Add a group

To add a group click **Add Computer Group** in the upper right of the page. Give a name and description and then assign computers to the group.

**Note**

A computer can only be in one group. If you select a computer that’s already in a group, it will be removed from its current group.
Tip
In the Search box you can start typing a name to filter down the displayed entries.

Edit a group
To edit a group, click the group's name to open and edit the group details.

Delete a group
To delete a group, select it and click Delete in the upper right of the page.
Deleting a group will not delete its computers.
You can also delete a group at the group's details page. Click the group's name to open the details.

5.6.1 Computer Group Summary
The Summary tab in a computer group's details lets you add or remove computers from groups. You can also delete groups.
To add or remove computers from a group click Edit in the left-hand pane. Amend the Assigned Computers for the group and click Save.
To delete the group, click Delete in the left-hand pane.
Deleting a group will not delete its computers.

5.6.2 Computer Group Policies
The Policies tab in a computer group's details page lets you see the policies that are enabled and applied to the group.
Click a policy name to view and edit policy details.

Note
Editing the policy affects all groups to which this policy is applied.

5.7 Policies
A policy is a set of options (for example, settings for malware protection) that Sophos Central applies to protected users, devices, servers, or networks.
There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).
To find out how policies work and how you can use them to customize security settings, see About Policies.
To find out how to create and edit policies, see Create or Edit a Policy.
Note
Your assigned administrator role affects what you can do.

5.7.1 About Policies

If you’re new to policies, read this page to find out how policies work.

What is a policy?

A policy is a set of options that Sophos Central applies to protected users, devices or servers.
There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).
Users, devices and servers have separate policies.

What is a Base policy?

Each feature has a Base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.
For some features, like threat protection, Sophos configures the Base policy with the best practice settings. You can leave it unchanged if you want to.
For other features, like application control or peripheral control, which are more specific to your network, you must edit the policy to set up the feature.
The Base policy is always available and is used if you don’t have other policies activated.

Note
You cannot disable or delete the Base policy.

Do I need to add new policies?

You can choose whether to set up your own policies or not.
If you want to apply the same policy to all users or devices or servers, you can simply use the Base policy or adapt it for your needs.
If you want to use different settings for different groups, you can create additional policies.

What can I do with additional policies?

You can set up additional policies to override some or all of the settings in the Base policy.
You can use additional policies to apply different settings to different users, devices or servers. You can also use them to make it easier to switch the settings that are applied quickly.
The order in which you put the policies in the list matters. The policies at the top of the list override the policies at the bottom. See “How do you prioritize policies?” below.
What’s the difference between user policies and computer policies?

A user policy applies to all the devices that a user has.

A “device” or computer policy applies to specific computers or groups of computers, regardless of which user logs on.

Some features let you create either kind of policy. Other features only let you create one kind. For example you can set an updating policy for computers, but not for users.

If you set up a user policy and a computer policy for the same feature, and both could apply to the same computer, the policy that’s higher in your policy list takes priority. See "How are policies prioritized?"

You can check which policy is applied to a computer by looking at the Policies tab on that computer’s details page.

What is in each policy?

A policy lets you:

• Configure one of the features that you have licensed.
• Specify which users, devices or servers the policy applies to.
• Specify whether the policy is enforced and whether it expires.

A policy contains all the settings for a product or feature. For example, you cannot split up the threat protection settings across several different policies in such a way that a user gets one setting from one policy and another setting from a different policy.

How are policies prioritized?

The order in which you arrange the policies determines which is applied to specific users, devices or servers.

Sophos Central looks through the policies from the top down and applies the first policy it finds that applies to those users or devices.

The Base Policy is always at the bottom, and is applied to any users, devices or servers that aren’t covered by policies higher in the list.

Tip
Place the most specific policies at the top and general policies further down. Otherwise, a general policy might apply to a device for which you wanted an individual policy.

To sort policies, grab a policy and drag it to the position where you want to insert it.
5.7.2 Create or Edit a Policy

You can create or edit a policy as follows.

Create a policy

1. If you have more than one Sophos product, select the one where you want to create a policy.

   **Note**
   You can't create policies from the Overview pages.

2. Go to the Policies page.
3. Click Add Policy (in the upper right).
4. If you see an Add Policy dialog, select:
   - The feature you want.
   - The policy type (applies only to Endpoint Protection).
5. On the policy details page, use the tabs to:
   - Assign the policy. For example, assign it to specific users or devices.
   - Enter settings for the policy. See the Help topic for that policy type.
   - Enable or disable the policy.

Edit a policy

1. If you have more than one Sophos product, select the one where you want to edit a policy.

   **Note**
   You can't edit policies from the Overview pages.

2. Go to the Policies page.
3. You see a list of policy types.
4. Click on the policy type to open a list of policies.
5. Find the policy you want to edit and click it.
6. On the policy details page, use the tabs to:
   - Assign the policy. For example, assign it to specific users or devices.
   - Enter settings for the policy. See the Help topic for that policy type.
   - Enable or disable the policy.
5.7.3 Device Encryption Policy

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault on Macs. Encrypting hard disks keeps data safe, even when a device is lost or stolen.

Note
If an option is locked global settings have been applied by your partner or Enterprise administrator.

Encryption is set up as follows:
1. The Device Encryption agent is installed on Windows computers automatically when you use the standard Windows agent installer (if you have the required license). You must manually install the Device Encryption agent on Macs.
2. Create a Device Encryption policy and apply the policy to users as described below.
3. Computers are encrypted when those users log in.

Note
FileVault encryption is user based; every user of an endpoint must have encryption enabled.

For full details of how computers are encrypted, see the Sophos Central Device Encryption administrator guide.

Note
Device Encryption can be applied to boot volumes and fixed data volumes, but not to removable media.

To set up a policy:
• Create a Device Encryption policy. See Create or Edit a Policy.
• Open the policy's Settings tab and configure it as described below. Make sure the policy is enabled.

Settings

Device Encryption is on/off: A computer is encrypted as soon as one of the users the policy is applied to logs in.

A Windows endpoint stays encrypted even if a different user who is not included in the policy logs in.

Warning
You must apply an encryption policy to all users of a specific Mac endpoint to make sure that it is fully protected.

Encrypt boot volume only: This option allows you to encrypt the boot volume only. Data volumes are ignored.
Advanced Windows settings

Require startup authentication: This option is turned on by default. It enforces authentication via TPM+PIN, passphrase, or USB key. If it is turned off, TPM-only logon protection will be installed on supported computers. For more information on authentication methods, see the Sophos Central Device Encryption administrator guide.

Require new authentication password/PIN from users: This option is turned off by default. It forces a change of the BitLocker password or PIN after the specified time. An event is logged when users change their password or PIN.

Note
On the endpoint, the feature is only available in Central Device Encryption 2.0 or later.

If users close the dialog without entering a new password or PIN, the dialog is shown again after 30 seconds, until they enter a new one. After users have closed the dialog five times without changing the password or PIN an alert is logged.

Encrypt used space only: This option is turned off by default. It allows you to encrypt used space only instead of encrypting the whole drive. You can use it to make initial encryption (when the policy is first applied to a computer) much faster.

Warning
If you encrypt used space only, deleted data on the computer might not be encrypted, so you should only use this option for newly set up computers.

Note
This option has no effect on Windows 7 endpoints.

Password protect files for secure sharing (Windows only)

Note
On the endpoint, the feature is only available in Central Device Encryption 2.0 or later.

Enable right-click context menu: If you turn on this option, a Create password-protected file option is added to the right-click menu of files. Users can attach password-protected files to emails when sending sensitive data to recipients outside your corporate network. Files are wrapped in a new HTML file with encrypted content.

Recipients can open the file by double-clicking it and entering the password. They can send the received file back and protect it with the same or a new password or they can create a new password-protected file.

Enable Outlook add-in: This option adds encryption of email attachments to Outlook. Users can protect attachments by selecting Protect Attachments on the Outlook ribbon. All unprotected attachments are wrapped in a new HTML attachment with encrypted content and the email is sent.

Always ask how to proceed with attached files: If you turn on this option, users are prompted to choose how to send attachments whenever the message contains one. They can send them password protected or unprotected.
You can enter excluded domains for which the **Always ask how to proceed with attached files** option does not apply. For example, this can be the domain of your organization. If recipients belong to such a domain, the senders are not asked how they want to handle attachments.

Enter only complete domain names and separate them by commas.

**Related concepts**

Create or Edit a Policy (page 295)

You can create or edit a policy as follows.

**Related information**

Sophos Central Device Encryption administrator guide

---

## 5.8 Settings

The Settings pages are used to specify security settings that apply to all your users and devices. The pages displayed depend on the features included in your license. Some of these pages may also be displayed under **Global Settings** in **Overview**.

**Note**

If you want to apply settings only to certain users, servers, or devices, use the **Policies** pages instead.

---

### 5.8.1 Active Directory Sync

You can import users and user groups from Active Directory to Sophos Central.

In Settings, on the **Active Directory Sync** page, you can select the Active Directory service you want to use.

- There is a download link for the Sophos Central Active Directory synchronization utility.
- In **Endpoint Protection** and **Email Gateway** you can use Azure Active Directory synchronization instead.

**Note**

If you are using Office 365 you must use Azure Active Directory synchronization.

For instructions on setting up the utility, see the Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

**Related concepts**

Active Directory Sync Status (page 299)

On the **Active Directory Sync** page, you can check the sync status and download the installer.

About Active Directory synchronization (page 299)

Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

**Related tasks**

Set up synchronization with Active Directory (page 299)
Follow these instructions to set up synchronization with Active Directory.

**Active Directory Sync Status**

On the **Active Directory Sync** page, you can check the sync status and download the installer. You need to set up Active Directory synchronization before you can see these options. You can download the latest installer for setting up synchronization with Active Directory.

**Sync status**

This shows your synchronization status and the synchronization settings in Active Directory.

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The time of the last synchronization with Active Directory.
- The number of users and groups imported from Active Directory.

You can view Active Directory synchronization alerts on the **Overview > Alerts** page. You can view synchronization events on the **Overview > Logs & Reports > Events** page.

**About Active Directory synchronization**

Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

To synchronize with Active Directory, you need to download and install the Sophos Central Active Directory Sync utility. The utility works as follows.

- It synchronizes active users and user groups.
- It can run automatically on a regular basis, as set up by the Sophos Central administrator.
- It doesn't duplicate existing users or groups when they are matched to an existing Sophos Central user or group. For example, an email address from Active Directory may be added to an existing user in Sophos Central.
- It supports only the Active Directory service.
- It can synchronize multiple Active Directory forests. To do this, you need to install the utility on multiple machines and configure each utility to synchronize a different Active Directory forest. We strongly recommend to synchronize different Active Directory forests at different times of day, so that the synchronizations do not overlap.
- It doesn't help you to deploy the Sophos agent software to your users’ devices. Use other methods of deployment with Active Directory.

**Set up synchronization with Active Directory**

Follow these instructions to set up synchronization with Active Directory.

Before you can set up synchronization, you need .NET Framework 4 on the computer where you will run the Sophos Central AD Sync Utility.

**Warning**

Before you proceed, make sure all your active directory users are set up correctly with an email address. Users without an email address aren't protected and email going to an email address not tied to a user isn't delivered.

You need to use API credentials to synchronize with Active Directory.

To set up synchronization with Active Directory:
1. Set up your API credentials for AD sync. To do this, click **Settings > API credentials**.

2. Add a new credential. Enter the following information:
   - **Credential name**
   - **Description**

3. Copy the **Client ID** and **Client Secret**.

4. Click **Settings > Active Directory Sync**, and click the link to download the Sophos Central AD Synchronization Utility installer. Then run it.

   Alternatively, go to the **Start** menu and click **Sophos > Central > AD Sync**. If you are running Windows 8 or later, in the Apps list, find the app **AD Sync** listed under **Sophos**.

   The **Sophos Central AD Sync Utility Setup** assistant starts.

5. In the setup wizard, enter the information required.

   Follow the instructions in the **Sophos Central AD Sync Utility Setup** assistant.

6. On the last page of the setup assistant, select **Launch Sophos Central AD Sync Utility** and click **Finish**.

7. In the Active Directory Synchronization Setup utility, on the **Sophos Credentials** page, enter your **Client ID** and **Client Secret** instead of your Sophos Central account credentials.

8. On the **AD Configuration** page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the **Use LDAP over an SSL connection (recommended)** checkbox selected. If your LDAP environment doesn’t support SSL, clear the **Use LDAP over an SSL connection (recommended)** checkbox and change the port number. The port number is usually 636 for SSL connections and 389 for insecure connections.

9. If you don’t want to synchronize the entire forest, on the **AD Filters** page, you can specify which domains to include in the synchronization. You can also specify additional search options (search bases and LDAP query filters) for each domain. Distinct options can be specified for users and user groups.

   **Note**
   
   AD Sync will only create groups that have members which include discovered users or devices, regardless of group filter settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Search bases       | You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format:  
OD=Finance,DC=myCompany,DC=com |
| LDAP query filters | To filter users, for example, by group membership, you can define a user query filter in this format:  
memberOf=CN=testGroup, DC=myCompany, DC=com  
The above query limits user discovery to users belonging to “testGroup”. Note that |
## 5.8.2 Role Management

You can use pre-defined administration roles to divide up security tasks according to the administrators’ responsibility level.

In **Settings**, the **Role Management** page shows a list of administration roles and the number of users assigned to each role.

You can only see this option if you are a Super Admin administrator.

Click on a role name to see a detailed description of the role and the names of the people that have that role assigned to them. You can manage the people assigned to a specific role in that role’s page.

### Restriction
An administrator role affects what a user can do.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>if you don't specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter: CN=testGroup</td>
</tr>
</tbody>
</table>

### Note
If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

10. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.

    **Note**
    A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

    If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select **Never. Only sync when manually initiated**.

11. Click **Finished**.

12. To synchronize immediately, in the AD Sync Utility, click **Preview and Sync**. Review the changes that will be made during the synchronization. If you are happy with the changes, click **Approve Changes and Continue**.

    The Active Directory users and groups are imported from the Active Directory to Sophos Central.

    To stop the synchronization in progress, click **Stop**.
Administration Roles

Predefined roles cannot be edited or deleted.

Your assigned administrator role affects what you can do.

A Super Admin can add custom roles. These roles are based on the predefined roles but you can restrict the access for a custom role to a specific product.

Restriction
You can add custom roles only if you are signed up to the Sophos Early Access Program.

Super Admin

Administrators with this role have access to everything in Sophos Central.

They can manage roles and role assignments. In addition, they can create, edit, assign, and delete custom roles.

There must be at least one administrator with the Super Admin role.

Admin

Administrators with this role have access to everything in Sophos Central.

They can't manage roles and role assignments.

Help Desk

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

• Look at sensitive logs or reports.
• Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.
• Update the Sophos agent software on a computer.
• Scan computers.
• Modify co-branding.

They can't see role management options. Also they can't see some options, such as Edit buttons.

Read-only

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

• Look at sensitive logs or reports.
• Receive alerts.

They can't see role management options. Also they can't see some options, such as Edit buttons.
User

Administrators with this role have no administration capabilities. They have access only to the Self Service Portal.

Related concepts
Administration Roles for Intercept X with EDR (page 303)
Administrators can do more if they have Intercept X with EDR.

User Summary (page 272)

Related tasks
Remove administrators (page 307)
You can remove administrators. Removing an administration role from a user does not delete the user.

Add administrators (page 304)
You assign administration roles to users using the Available Users list.

Administration role details
If you click a role on the Role Management page, its details are shown on a separate page.
The sections on that page include the following.

Permissions

This is the access level for a role. The options are Full, Help Desk, or Read-only.

Global Settings

These are the specialized capabilities for a role. The settings are:

- **Access sensitive logs & reports**: This option means that an administrator can view sensitive logs and reports; for example the Audit Logs.
- **Access policy management**: This option means that an administrator can change policy settings.
- **Access policy assignment**: This option means that an administrator can assign policies to users and devices.

Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details.

Administration Roles for Intercept X with EDR

Administrators can do more if they have Intercept X with EDR.

Super Admin and Admin

Administrators with these roles can also:
- View the intelligence report.
- Request the intelligence report
- Add items to the “Clean and Block” list.
- Remove items from the “Clean and Block” list.
- View blocked items.
- Request an on-demand threat case.
- View on-demand threat cases.
- Isolate and un-isolate devices.
- Request a forensic snapshot.
- Request a threat search.
- View a saved threat search.

**Help Desk**

Administrators with this role can also:
- View the intelligence report.
- Request the intelligence report.
- View blocked items.
- Request an on-demand threat case.
- View on-demand threat cases.
- Request a forensic snapshot.
- Request a threat search.
- View a saved threat search.

**Read-only**

Administrators with this role can also:
- View the intelligence report.
- View blocked items.
- View on-demand threat cases.
- View a saved threat search.

**Related concepts**

*Administration Roles* (page 302)

**Add administrators**

You assign administration roles to users using the *Available Users* list.

Existing administration roles, if any, are indicated next to the user's name.

A user can only have one assigned role.
For example if you add a Read-only administrator to the list of Help Desk administrators their assigned role will change to Help Desk administrator. They will no longer be a Read-only administrator.

To add an administrator:

1. In **Settings**, on the **Role Management** page, select the administrator role that you want to assign.
2. On the role details page, next to **Role Members**, click **Edit**.

   **Note**
   You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, select a user in the **Available Users** list and use the picker arrows to add them to the **Assigned Users** list for the role. Select **Save**.

   **Tip**
   Enter a name or part of a name in the search box to filter the list of available users.

**Add a custom role**

You can add custom roles if you are a Super Admin.

Custom roles are based on the predefined roles. You can restrict the access for a custom role to a specific product. You can also create a role that allows an administrator to have full access to one product and read-only access to a second product.

**Restriction**
If a role doesn't have access to both **Endpoint Protection** and **Server Protection** (in some cases **Encryption** as well), the shared settings are read-only.

The shared settings are:

- Tamper protection
- Allowed applications
- Website management
- Proxy configuration
- Blocked item
- Bandwidth usage (Encryption access required)
- HTTPS updating
- DLP rules
- Manage content control list
- Reject network connections
- EDR threat analysis center

To create a custom role:

1. In **Settings**, on the **Role Management** page, select **Add role**.
2. Give the custom role a name and a description.
3. Select the **Base role** you want to use as the basis for the custom role.
For example, if you choose Help Desk as the Base role, administrators with the custom role have Help Desk permissions.

4. Choose the product and access type you want the role to have.
For example, you create a custom role called Endpoint Help Desk. This custom role uses Read-only as its Base role and Endpoint Protection as its selected product with an access type of Help Desk.

This custom role allows any administrators assigned to this role to access Endpoint Protection with Help Desk permissions.

a) Choose more than one product, if required.

You can choose different access types for different products.

For example you can create a custom role that has Help Desk access permissions for Endpoint Protection and Read-only access for Mobile. You can set the permissions for all other products to None. This means that the custom role only has access to Endpoint Protection with Help Desk permissions and Mobile with Read-only permissions.

5. Choose the additional access and management options for the custom role.

- Enable access to logs & reports.
- Enable policy management (add, edit, and delete).
- Enable policy assignment to users, device, etc.. (turn policies on and off; and add users, user groups, devices and device groups to existing policies).

For example, this allows a Super Admin to add these permissions to a Read-only or Help Desk role. You can also use these options to reduce the permissions for an Admin role. For example, you could prevent the custom role from managing policies.

Note
These additional options only apply to the selected products for the custom role.

The additional options are the same for all products and access types for the custom role.

6. Select Save.

You can now assign this role to administrators.

Related concepts
Administration Roles (page 302)

Related tasks
Change roles (page 306)

You can change the assigned roles for administrators if you are a Super Admin.

Delete custom role (page 307)

You can delete custom roles if you are a Super Admin.

Change roles

You can change the assigned roles for administrators if you are a Super Admin.

You can change roles for multiple administrators at the same time.

Restriction
You can't change roles for administrators who are currently signed in.

To change roles:
1. In **Settings**, on the **Role Management** page, select the administrator role that you want to assign to other administrators. For example, select a read-only administrator role if you want to assign that role to other administrators.

2. On the role details page, next to **Role Members**, click **Edit**.

   **Note**
   You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, add users from the **Available Users** list or remove users from the **Assigned Users** list. Select **Save**.

   **Tip**
   Enter a name or part of a name in the search box to filter the list of available users.

### Delete custom role

You can delete custom roles if you are a Super Admin.

You can only delete custom roles. You can't delete roles that have administrators assigned to them. You must change their role first.

1. In **Settings**, on the **Role Management** page, select the role you want to remove and select **Delete**.
   
   To select a role, click anywhere in the row apart from the name.

2. Select **Delete** to confirm role deletion.

**Related concepts**

- Administration Roles (page 302)

**Related tasks**

- Add a custom role (page 305)

You can add custom roles if you are a Super Admin.

### Remove administrators

You can remove administrators. Removing an administration role from a user does not delete the user.

**Note**

You cannot delete a user who has an assigned administration role. You must remove the role from the user before deleting the user.

To delete administrators:

1. In **Settings**, on the **Role Management** page, select the administrator role from which you want to remove users.

2. On the role details page, next to **Role Members**, click **Edit**.

   **Note**
   You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, select a user in the **Assigned Users** list and use the picker arrows to remove them.
Tip
Enter a name or part of a name in the search box to filter the list of assigned users.

5.8.3 API Token Management

You can generate and manage the API token used for secure access to the Security Information and Event Management (SIEM) Integration API. This enables you to pull new event and alert data from Sophos Central. For further information, click the knowledge base article link provided on the page.

To add a token:
1. In Settings, open the API Token Management page.
2. Click Add Token.
3. Give the token a name and click Save.
   This generates the API token. The token is valid for a year.
Click Renew to extend the validity of the token.
Click Delete to remove the token.

5.8.4 API credentials

You can manage and add credentials for Sophos Central Admin.

Note
The first time you click API credentials you must read and accept the terms and conditions of use.

To add credentials, do the following:
1. Click Add Credential and give the credential details.
   This generates the credential, together with a Client ID and a Client Secret.
2. Copy the Client ID and Client Secret.
   Note
   You can only see the Client Secret once.

To delete an API credential, select it in API credentials and click Delete.

5.8.5 Tamper Protection

You can enable or disable tamper protection for all your servers and users' computers.

To do this, in Settings, open the Tamper Protection page.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:
• Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
• Disable tamper protection.
• Uninstall the Sophos agent software.

Manage tamper protection for a specific device

You can change the tamper protection settings for a specific device or server. Open the device's details page and look under Tamper Protection. There you can do as follows:
• View the password.
• Generate a new password.
• Temporarily disable tamper protection for that device.

Recover tamper protection passwords

You can recover the tamper protection passwords of devices that you’ve recently deleted. You might need to do this so that you can uninstall Sophos software that is still on those devices.

5.8.6 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

Set the bandwidth used

In Settings, on the Bandwidth Usage page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.
This helps to ensure that updating does not cause computers to run slowly.
You can specify a custom bandwidth or unlimited bandwidth.

Note
This setting is for Windows computers only.

Note
This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos. To save bandwidth in this case, see Manage Update Caches and Message Relays.

Related concepts
Manage Update Caches and Message Relays (page 128)
Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos.

5.8.7 HTTPS updating

Your computers and servers can get their Sophos updates via HTTPS. We recommend that you use HTTPS for greater security.

To use HTTPS updating:
1. Go to Settings > HTTPS Updating.
2. Turn on HTTPS Updating.

5.8.8 Multi-factor authentication

If you're a Super Admin, you can make some or all of the Sophos Central admins sign in with multi-factor authentication.

Introduction

Using multi-factor authentication means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos or Google Authenticator, SMS or email authentication to sign in.

Multi-factor authentication is turned on by default for newly created Sophos Central accounts.

This page tells you how to do the following:
• Set up multi-factor authentication.
• Sign in with multi-factor authentication for the first time.
• Add another method for multi-factor authentication.
• Sign in with email authentication if you don't have Sophos or Google Authenticator.
• Reset an admin's sign-in details, for example if they lose their phone.
• Turn off multi-factor authentication for an admin.

Set up multi-factor authentication

If you're a Super Admin, you can choose how your administrators sign in.

To set up multi-factor authentication, do as follows:
1. Go to Settings > Multi-factor Authentication (MFA).
2. Choose how you want admins to sign in:
   • No MFA needed.
   • All admins need MFA. This is the default for new accounts.
   • Select admins who will need MFA. This lets you select individual admins.
3. If you choose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). Move admins to the Assigned Users list and click Add.
4. Click Save.
When admins next sign in, they are prompted to set up a new method of authentication.

**Sign in with multi-factor authentication for the first time**

The first time you sign in with MFA, do as follows:

1. At the sign-in screen, enter your user ID (email address) and password.
   
   A *Set Up Your Login Information* dialog explains that signing in needs additional authentication.

2. In the next dialog:
   
   a) Enter the security code that has been sent to you in an email.
   
   b) Create a 4-digit PIN. This enables you to use email as an authentication method.

3. In *Verify Your Device*, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
   
   You also need to enter a security code to verify a device if you have chosen SMS as your authentication type.

   Sophos Central Admin opens.

   The next time you sign in, you only need to enter a code from Sophos or Google Authenticator when prompted.

**Add another authentication option for multi-factor authentication**

You can set up multiple authentication options for a Sophos Central Admin account.

You can authenticate with SMS and Sophos or Google Authenticator.

You must have an authentication option already set up.

To set up another authentication option, do as follows:

1. Sign in to Sophos Central Admin.

2. Click your account name and click *Manage Login Settings*.

3. Click *Create New Method*.

4. Choose another authentication method.

5. Click *Next*.

6. In *Verify Your Device*, scan the QR code and enter the security code that Sophos or Google Authenticator displays.

7. To confirm that the new method has been added, click your account name and click *Manage Login Settings*.
   
   An additional authentication method has been added.

**Sign in with email authentication**

If you don't have access to Sophos or Google Authenticator, you can sign in with email authentication instead.

1. At the sign-in screen, enter the user ID (email address) and password.

2. In *Verify Your Login*, click *Choose Another Method*.

3. In *Pick Your Challenge*, click the email option.
   
   An email is sent to you.

4. Open the email and find the security code.
5. In **Verify Your Login**, enter the security code and your 4-digit PIN. You'll be asked for the security code and PIN each time you sign in from now on, until you switch back to using Sophos or Google Authenticator.

### Reset an admin's sign-in details

If an admin replaces or loses their phone, you can allow them to set up their sign-in again.

1. On the **People** page, under **Users**, find the user and click their name to open their details.
2. In the user details, on the left of the screen, you'll see their MFA status and settings. Click **Reset** and confirm that you want to do a reset.

The next time the admin tries to sign in, they'll need to go through the setup steps again.

### Turn off multi-factor authentication

If you're a Super Admin, you can turn off multi-factor authentication for an administrator.

To turn off multi-factor authentication, do as follows:

1. Go to **Settings > Multi-factor Authentication (MFA)**.
2. Click **Select admins who will need MFA**.
3. Click **Add admins**.
4. Move the administrator from the **Assigned Users** list and to the **Available Users** list.
5. Click **Add**.
6. Click **Save**.

### 5.8.9 Encryption Recovery Key Search

You can get a device encryption recovery key by entering a volume or recovery identifier.

### Retrieve recovery key (Windows computers)

If users are unable to log in to their encrypted computer, you can get a recovery key which is used to unlock the computer. There is a recovery key for each volume of a BitLocker protected computer. It is created and backed up in Sophos Central before the computer is encrypted.

**Note**

When Sophos Device Encryption is installed, existing BitLocker recovery keys are replaced automatically and can no longer be used.

**Note**

Even if a policy has been disabled and the computer's Device Encryption status is shown as "Unmanaged", you can get a recovery key if one is available.

To get the recovery key, go to **Computers**, select the computer you want to recover, and click **More > Retrieve Recovery Key**. If you cannot find the computer in the list, you need the recovery key identifier or the volume identifier and use it in the recovery wizard, as follows:

1. Tell the user to restart the computer and press the Esc key in the **BitLocker** logon screen.
2. Ask the user to provide you with the information displayed in the **BitLocker recovery** screen.
3. In Sophos Central, go to **Computers** and click **More > Retrieve Recovery Key**.
4. Enter at least five characters of the recovery key identifier or the volume identifier provided by the user.
5. Click **Show Key** to display the recovery key.

**Note**
If you enter a volume identifier, Sophos Central displays all available recovery keys for this volume. The latest recovery key is the top one.

6. Make sure that the user is authorized to access the encrypted device before you provide the recovery key.

**Note**
As soon as a recovery key is displayed to you as administrator, it is marked as used and will be replaced at the next synchronization.

7. Give the recovery key to the user.

The user can now unlock the computer. Users of computers running Windows 8 or later are prompted to create a new PIN or password. Instructions for creating the PIN or password are displayed automatically.

After the computer has been recovered, a new recovery key will be created and backed up in Sophos Central. The old one will be deleted from the computer.

### Retrieve recovery key (Macs)

If users forget their login password, you can get a recovery key which is used to unlock the computer.

To get the recovery key, go to **Computers**, select the computer you want to recover, and click **More > Retrieve Recovery Key**. If you cannot find the computer in the list, you need the recovery key identifier or the volume identifier and use it in the recovery wizard, as follows:

1. Tell the user to switch on their computer and wait until the Recovery Key ID is displayed.

**Note**
The recovery key ID is displayed for a short time. To display it again, users must restart their computer.

2. Ask the user to tell you the Recovery Key ID.
3. In Sophos Central, go to **Computers** and click **More > Retrieve Recovery Key**.
4. Enter at least five characters of the recovery key identifier.
5. Click **Show Key** to display the recovery key.
6. Make sure that the user is authorized to access the encrypted device before you provide the recovery key.
7. Give the recovery key to the user.
• For users imported from Active Directory, continue to step 8.
• For all other users, go straight to step 10.

8. Reset the existing password in Active Directory. Then generate a preliminary password and give it to the user.

9. Tell the user to click Cancel in the Reset Password dialog and enter the preliminary password instead.

10. Tell the user to do as follows:
    • Create a new password.
    • Click Create New Keychain if prompted.

The user can access the computer again.

On endpoints running macOS 10.12 or earlier, a new recovery key is created and stored in Sophos Central. A recovery key can only be used once. If you need to recover a computer again later, you need to retrieve a new recovery key.

On endpoints running macOS 10.13 and Apple File System (APFS), no new recovery key is created. The existing recovery key remains valid.

### 5.9 Protect Devices

You can download Sophos installers and use them to protect your devices.

The installers you can see may depend on the license or licenses you have.

Before you start, check which operating systems you can protect with Sophos Central: see the Sophos Central page.

For more details, including what each product does, how you use the installers, and how Sophos Central registers devices and applies policies, read the other topics in this section.

**How to use installers**

After downloading installers for workstations or servers, you can:

• Run the installer to protect the local computer.
• Transfer the installer to other computers and run it on them.
• Use automated software deployment tools such as System Center Configuration Manager (SCCM) to run the installer on large numbers of computers.

**Related concepts**

Encryption (page 315)
Sophos Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers.

**Related tasks**

Add users automatically (page 278)
You can add users automatically by protecting their devices.

**Related information**

Sophos Central page
5.9.1 Encryption

Sophos Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers. Encrypting hard disks keeps data safe, even when a device is lost or stolen.

For full details of how computers are encrypted, see Sophos Central Device Encryption administrator guide.

Download and run installer

Go to Protect Devices.

Download an Endpoint Protection installer and run it on the computers you want to protect. You can choose from:

- **Download Complete Windows Installer**: Click this for an installer with all endpoint products your license covers.
  
  Alternatively, click **Choose Components…** to choose which products will be included in the installer. The choices are:
  
  — **Sophos Intercept X Advanced with EDR** (protection from ransomware and exploits).
  
  — **Device Encryption**.

- **Download Complete macOS Installer**: Click this for an installer with all endpoint products your license covers.
  
  Alternatively, click **Choose Components…** to choose which products will be included in the installer. The choices are as for Windows above.

- **Send Installers to Users**: Click this to go to a page where you can add users and send them installers that they can use.

Related information

Sophos Central Device Encryption administrator guide
6 Server Protection

Server Protection protects servers against malware, risky file types and websites, and malicious network traffic. It also offers peripheral control, web control, and server lockdown, which lets you control the software run on your servers.

6.1 Dashboard

The Dashboard is the start page of Server Protection and lets you see the most important information at a glance.

It consists of these areas.

Devices and users: summary

- **Devices and users: summary** shows details of usage and protection for users or protected devices. It also shows the number of unprotected users or devices.

- Click on the tabs to see information for each device type or for users.

- Click See Report to open a detailed report for the tab you have selected.

Web control

- **Web control** shows statistics for your Web Control protection.

- The figures are for threats blocked, policy violations blocked, and policy warnings. There is also a figure for "policy warnings proceeded", which is the number of users who have bypassed a warning to visit a website.

- Click on a figure to open a detailed report.

Servers on AWS

- **Servers on AWS** shows statistics for your AWS instances in different locations (you see this if you have connected Sophos Central to AWS accounts).

- Click See Map or click anywhere on the map to open a page where you can see details of the AWS instances and s3 storage buckets, and their security health.

6.2 Logs & Reports

The **Logs & Reports** page lists the reports that you can generate about security features in Sophos Central.

The page also lists any **Saved Reports**. These are custom reports that you or other administrators for this account have saved.

To find out more about logs, see Logs.
To find out how reports work and how you can customize, save and schedule them, see Reports.

**Related concepts**
- Logs (page 317)
- Reports (page 318)

### 6.2.1 Logs

The following log is available for Server Protection:

- **Data Loss Prevention.** All events triggered by data loss prevention rules for computers or servers, see Data Loss Prevention Events Log.

**Data Loss Prevention Events Log**

The **Data Loss Prevention Events Log** displays all events triggered by data loss prevention rules for computers or servers.

**Note**

An endpoint computer can send a maximum of 50 data control events per hour to Sophos Central. All events are logged locally on the endpoint computer.

You can find the following features and information on the **Data Loss Prevention Events Log**:

- **Search:** If you want to view events for a certain user, device or rule name, enter the name of the user, device, or rule in the search box.
- **Choose period:** Use the box to select the time period for which you want to view events. If you select **Custom**, use the **From** and **To** fields to select the dates between which you want to view events. You can view events that occurred in the past 90 days or less.
- **Filter by rule name:** You can filter the events by rule name.
- **Filter by file type:** You can filter the events by file type.
- **Update:** Click this to display any new events reported since the page was last opened or refreshed.

**Event table**

The event table provides these event details:

- **Date and time:** Time and date when the event occurred
- **User:** Source that caused the event, for example, the name of a user or system
- **Device:** Device that caused the event
- **Rule name:** Data loss prevention rule that caused the event
- **Rule action:** Data loss prevention action that caused the event
- **File name:** Name of the file that caused the event
- **Destination type:** Name of the destination that caused the event

**Save as Custom Report** lets you save the report settings in the **Saved Reports** table on the **Logs & Reports** page.
The **Export** menu (on the right of the table) lets you export the current view or the report for the past 90 days as a CSV (comma separated value) or PDF file.

### 6.2.2 Reports

The reports that you can see depend on your license.

You can customize reports, save them and send them out as scheduled emails.

**Note**

A report may not support all the customization or viewing options.

#### Limit report data to a specific time range

In some reports, you can limit report data to a specific date range by entering a **From** and **To** date.

In some reports, you can select a time period.

#### Filter reports

In some reports, you can filter the displayed information by clicking on the category tiles. For example in the Computers report you can show all the active computers by clicking on **Active**.

You may also be able to filter by groups.

You can also use **Search** to filter for specific information.

#### Print or export reports

You can print or export your reports.

- **Print**: Click this to open a printer-friendly view. Then press Ctrl+P to open the printer dialog.
- **Export to CSV**: Click this to export the current view as a comma separated file.
- **Export to PDF**: Click this to export the current view as a PDF file.

#### Save and email custom reports

You can create and save custom reports. A list of the saved reports is shown at the top of the **Logs & Reports** page.

You can also choose to send custom reports by email and set up a schedule for them. You can save as many reports as you like, but you can only schedule up to 25.

1. Set up the report by selecting the appropriate filters.
2. Click **Save as Custom Report**.
   
   This opens the **Save Report** dialog.
3. Enter a **Name** for the report.
4. If you want to send the report by email, select one of these options:
   
   - **Send a link to the report**.
• Attach the report to the email.
  
  We recommend that you send a link if the report includes personally identifiable information. You need to enter Sophos Central sign-in credentials to view reports from a link.

5. Select the Frequency. You can choose from monthly or weekly.

6. Select the format: PDF or CSV.

7. Click Save.

The email is received by the user who signs in and creates the report.

Note
Scheduled emails stop after six months. You can reschedule them if you want to.

Recover tamper protection passwords

You can recover the tamper protection passwords of devices that you’ve recently deleted. You might need to do this so that you can uninstall Sophos software that is still on those devices.

1. Go to Logs & Reports.
2. In Reports, under Endpoint & Server Protection, click Recover Tamper Protection passwords. You see a list of deleted devices.
3. Find the device you want.
4. In the Password(s) column, click View password details. This shows you the password (and previous passwords).

6.3 Servers

On the Servers page, you can manage your servers, Azure VMs, and server groups.

6.3.1 Servers

On the Servers page you can view and manage your protected servers. The sections below tell you about the servers list and also how to:

• Add a server.
• View full details of a server and manage it.
• Export the list.

About the servers list

The servers list shows you the current servers with these details:

• Name.
• IP. Hover over the icon to see details of all IPv4 and IPv6 addresses.
• OS. “Sophos Security VM” indicates a host where Sophos protects the guest VMs.
• Last Active. This is the last time that the server contacted Sophos.
- **Group.** The group that the server belongs to (if it belongs to one).
- **Lockdown status.** This shows whether Sophos Lockdown has been installed to prevent unauthorized changes on the server:
  - "Locked Down" shows that Sophos Lockdown has been installed.
  - "Not installed" shows that Sophos Lockdown is not installed. Click **Lock Down** to install it and lock the server.

To search for a server, enter the name in the search field above the list.

To display different types of server, or servers with a specific health status, use the filters above the list.

For example, the **Sophos Security VMs** filter displays instances of Sophos Security VM on a hypervisor.

### Add a server

To add a server (that is to protect and manage a server, so that it appears in the list), click **Add Server** in the upper right of the page.

This takes you to the **Protect Devices** page, where you can download the installers you need to protect your servers. For help with the server installers, see **Server Protection**.

### View full details of a server

For details of a server, click on its entry in the list to open the server details. You can then view full details of the server, and also update, scan, lock, unlock or delete it.

### Export to CSV

To export a list of servers:

Click on **Export to CSV**.

This creates a file called servers.csv. Any currently active filters are applied to the list.

For example you can export a list of Windows servers with a bad health status by applying the **Windows servers** and **Servers with a bad status** filters before clicking **Export to CSV**.

**Related concepts**

- **Server Summary** (page 320)
  The **Summary** tab in a server's details page lets you see server details.
- **Server Protection** (page 396)
  You install a Server Protection agent on servers to protect them against malware, risky file types and websites, and malicious network traffic.

### Server Summary

The **Summary** tab in a server's details page lets you see server details.

You can manage the server from here.

The sections you see depend on your license and the features you've set up.
Security status

In the left-hand pane, you can see the security status and take actions.

Note
The left-hand pane is always shown, even when you click the other tabs on this page.

If you see "Sophos Security VM" under the server name, the server is a host with a Sophos security VM installed. You'll also see additional information in the “Device Status” summary.

Actions you can take

The actions links and buttons are in the left-hand pane.

Restriction
Some actions are only available for Windows servers.

- **Isolate**: This isolates the server from the network.
- **Delete**: Deletes the server from Sophos Central.

Warning
You should uninstall the Sophos software before deleting a server.

- **Scan Now**: Scans the server immediately.
  
  The scan may take some time. When complete, you can see a "Scan ‘Scan my computer’ completed" event and any successful cleanup events on the Logs & Reports > Events page. You can see alerts about unsuccessful cleanup on the Alerts page.

  If the server is offline, it will be scanned when it is back online. If a computer scan is already running, the new scan request will be ignored and the earlier scan will carry on.

- **Lock Down**: Prevents unauthorized software from running on the server.
  
  This option makes a list of the software already installed on the server, checks that it is safe, and allows only that software to run in future.

  If you need to make changes on the server later, either unlock it or use the Server Lockdown preferences in the server policy.

- **Unlock**: Unlocks the server. This button is available if you have previously locked down the server.

- **Diagnose**: Runs the Sophos Diagnostic Utility.

- **Live Response (Beta)**: Enables you to connect to the server to investigate and remediate possible security issues.

Live Response (Beta)

This option is available only if you are a Super Admin and you’ve signed in using multi-factor authentication. Allow Live Response connections to servers must also be turned on in Global Settings: see Live Response for devices.
This enables you to connect to the server to investigate and remediate possible security issues. You might want to do this if an infection or suspicious activity is identified on the server. You can connect to the server even if it’s isolated. To connect to the server, do as follows:

1. Click **Live Response (Beta)**.
2. In **Session purpose**, summarize the purpose of your session.
3. Click **Start**.

   A connection to the server is opened in another browser tab. The tab shows a terminal window.
4. At the command prompt, type commands to perform your investigation or remediation.

   Use DOS, UNIX, or Linux commands depending on the computer to which you’ve connected.
5. When you finish, click **End Session**.

   The connection is closed, although the tab remains open. You can browse elsewhere in Sophos Central from here.

   The connection is also closed in the following cases:
   - You close the tab.
   - You refresh the tab.
   - You browse elsewhere in Sophos Central from here.
   - There is no activity for 30 minutes.

To see which Live Response sessions have started or ended, view the Sophos Central audit log.

**Recent Events**

This lists recent events on the server.

For a full list, click the **Events** tab.

**Agent Summary**

The summary shows the following details.

**Restriction**

Some details are only available for Windows servers.

- **Last Sophos Central Activity**: The last time the server communicated with Sophos Central.
- **Last Agent Update**: The last time the Sophos agent was updated. **Update Now** updates the Sophos agent.
- **Agent Version**: The version number of the Sophos agent.
- **Assigned Products**: Shows the Sophos products installed (for example, Intercept X). Shows the license and the version number for each installed product.
- **Installed component versions**: Click this to see a full list of the Sophos components and their version numbers.
- **IPv4 Address**
- **IPv6 Address**
• **Operating System**: If this is shown as "Sophos Security VM", the server is a host with a Sophos security VM installed.

• **Lockdown Status**: Shows the status of Server Lockdown, which prevents unauthorized software from running on servers.

• **Group**: Shows the group the server belongs to (if any). **Change group** lets you add it to a group, move it to a different group, or remove it from its current group. A server can only be in one group.

• **Connected Guest VMs**: You see this only if the server is a host with a Sophos Security VM. It shows the number of guest VMs connected to the Security VM. Click the number to see a list of the guest VMs.

  If no guest VMs are powered on, or if you’re still installing agents on them, you may see zero guest VMs.

  If you have enabled guest VMs to migrate between Security VMs, this can affect the number of guest VMs connected.

  Usually, a connected guest VM is protected. However, if the agent is newly installed, or there is a problem, scanning for threats may not have started yet.

• **Tamper Protection**: This shows whether **Tamper Protection** is enabled on the server or not. Click **Disable Tamper Protection** to manage the tamper protection password for the server.

### Update Cache and Message Relay Status

If you're using update caches or message relays on your network, you see this status information.

If the server is being used as an update cache or a message relay, you see:

• The status of the cache and when the last update was made. It also shows how many computers are using it as a cache.

• The status of the relay and how many computers are using it.

Alternatively, if the server is getting its updates from a cache (or using a relay) that's been set up elsewhere, you see details of where that cache or relay is.

### Windows Firewall

Windows Firewall is active and being managed on the computer. It also shows:

• Whether Windows Group Policy is being used.

• The active network profiles.

• If other registered firewalls are installed and active.

### Related concepts

**Tamper Protection** (page 371)

**Manage Update Caches and Message Relays** (page 380)

### Related tasks

**Live Response for devices** (page 144)

Turn on Live Response so that you can connect to devices to investigate and remediate possible security issues.

**Recover deleted devices** (page 87)
You can recover devices that you’ve deleted from Sophos Central if they are synced using Active Directory synchronization.

**Server Events**

The **Events** tab in a server’s details page lets you see events detected on the server. You can see details and, in some cases, take action to prevent unwanted detections.

On this tab, you can also see details of events on guest VMs (if you’re using Sophos for Virtual Environments).

**Stop detecting an application**

If an application is reported as malware but you know it's safe, you can allow it from the events list.

For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the **Details** link beside the event and then allow the application.

**Note**

This currently applies only to malware events reported by Intercept X.

**Stop detecting an exploit**

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again** and select an option:
   - **Exclude this Detection ID from checking**: prevents this detection on this app.
   - **Exclude this application from checking**: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.
3. Click **Exclude**.

   We’ll add your exclusion to a list.

   Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

**Stop detecting ransomware**

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again**.
   - Select **Exclude this Detection ID from checking**. This prevents this detection on this app.
3. Click Exclude.
We’ll add your exclusion to the Global Exclusions list.

Events on guest VMs

If the server is a Sophos security VM, click See all events (on the right of the page) to change to a view where you can see which guest VM the event occurred on.

If you have enabled guest VMs to migrate between Security VMs, a threat detection might remain in the events list here even if the guest VM has migrated and the threat has been cleaned up elsewhere.

Related concepts
Allowed applications (page 382)
Related information
How to investigate and resolve a potential False Positive or Incorrect Detection

Server Status

The Status tab in a server's details page lets you see the server's security health and details of any alerts.

It also lets you take action against alerts.

Security Health

Note
These status details are only shown if the server is using the Security Heartbeat feature.

This shows whether the device has threats detected, has out-of-date software, is not compliant with policy, or is not properly protected. The overall status is the same as that for the highest-priority item listed (red, orange or green).

This section also shows which Sophos services are running on the server.

Alerts

The page lists any alerts on the device. The details include:
• Alert details: For example, the name of the malware.
• When the alert occurred.
• The actions that you can take. These depend on the type of threat or event and are the same as the actions available in the Dashboard.

Create forensic snapshot

You can create a "forensic snapshot" of data from the device.
This gets data from a Sophos log of the device's activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

You'll need a converter (which we provide) to read the data (see Convert a forensic snapshot).

**Note**
You can choose how much data you want in snapshots and where to upload them. To do this, go to Global Settings > Forensic Snapshots. These options may not be available for all customers yet.

To create a snapshot:
1. Go to a threat case's Analyze tab.
   Alternatively, on the details page of the device, open the Status tab.
2. Click Create forensic snapshot.
3. Follow the steps in Upload a forensic snapshot to an AWS S3 bucket.

You can find the snapshots you generated in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Forensic Snapshots.\n
Snapshots generated from detections are in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Saved Data.\n
**Note**
You need to be an administrator with access to the tamper protection password and run a command prompt as an administrator to access the saved snapshots.

**Related concepts**

Forensic snapshots (page 138)  
Forensic snapshots get data from a Sophos log of a computer's activity so that you can do your own analysis.

Alerts (page 4)  
The Alerts page lists all the alerts that require your action.

**Related tasks**

Convert a forensic snapshot (page 139)  
Use the SDR Exporter tool to convert forensic snapshots so you can run queries on them.

**Related information**

Upload a forensic snapshot to an AWS S3 bucket (page 140)  
Follow these instructions to upload a forensic snapshot.

**Server Exclusions**

The Exclusions tab in a server's details page lets you see a list of files or applications excluded from scanning for threats.

By default, Sophos Central automatically uses vendor-recommended exclusions for certain widely-used applications. You can also set up your own exclusions in your policy.
Note
Some automatic exclusions shown in the list might not work on servers running Windows Server 2003.

Related concepts
Server Threat Protection Policy (page 335)
Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

Server Applications
The Applications tab on a server’s details page lets you see a list of applications installed on the server.
You can search the installed applications.

Server Lockdown Events
The Lockdown Events tab in a server’s details page lets you see “events” in which Server Lockdown blocked unauthorized activity on the server.
Examples of such events are: a user trying to run an unauthorized program on the server, an unknown updater trying to update files, or a user trying to modify files with a program that isn't authorized for the purpose.
The tab is displayed only for servers that you have locked down.
To see the report, click Update Report. This creates a report on events in the previous twenty-four hours.
The list shows:
• The event type.
• When each event happened.
• The Parent. This is the program, script or parent process that was active.
• The Target. This is the file or program that was the target of the activity.

Server Policies
The Policies tab in a server’s details page lets you see the policies that are applied to the server.
The Type column indicates the security settings (such as threat protection) included in each policy.
You can view and edit policy details by clicking the policy in the table.

Note
Editing the policy affects all servers to which this policy is applied.

6.3.2 Azure VMs
On the Azure VMs page, you can view the Azure VMs in Azure Active Directories associated with your Sophos Central account.
If you can’t see your Azure VMs here, click Connect to Azure for Virtual Machine information (on the right of the screen). For details, see Connect to Microsoft Azure.

The Azure VMs are listed with these details:

- **Virtual Machine Name**: Click the VM name to view details.
- **Sophos Product**: If you see "Agent installed", click it to go to the VM’s server details page.
- **Status**: This shows the state of the VM, for example “Running” or "Stopped".
- **Subscription**: Shows the subscription and Active Directory that the VM is in.
- **Location**
- **Resource Group Name**

**Related tasks**
Connect to Microsoft Azure (page 389)

### 6.3.3 Server Groups

On the Server Groups page you can add or manage groups of servers.

You can use groups to assign a policy to multiple servers at once.

The sections below tell you about the groups list and how to add, modify or delete groups.

**About the groups list**

The current groups are listed and the number of servers in each group is shown.

To see full details for a group, click on the group’s name.

**Add a group**

To add a group click Add Server Group in the upper right of the page. Give a name and description and then assign servers to the group.

**Note**

A server can only be in one group. If you select a server that’s already in a group, it will be removed from its current group.

**Tip**

In the Search box you can start typing a name to filter down the displayed entries.

**Edit a group**

To edit a group, click the group’s name to open and edit the group details.
Delete a group

To delete a group, select it and click **Delete** in the upper right of the page. Deleting a group will not delete its servers.

You can also delete a group at the group's details page. Click the group's name to open the details.

**Related concepts**

Server Group Summary (page 329)

The **Summary** tab in a server group’s details lets you add or remove servers. You can also delete groups.

**Server Group Summary**

The **Summary** tab in a server group’s details lets you add or remove servers. You can also delete groups.

To add or remove computers from a group click **Edit** in the left-hand pane. Amend the **Assigned Servers** for the group and click **Save**.

A server can only be in one group. If you select a server that’s already in a group, it will be removed from its current group.

To delete the group, click **Delete** in the left-hand pane.

Deleting a group will not delete its servers.

**Server Group Policies**

The **Policies** tab in a server group’s details page lets you see the policies that are enabled and applied to the group.

The icons beside a policy indicate the security settings (such as threat protection) included in the policy.

A gray icon indicates that this setting is disabled in the policy.

Click a policy name to view and edit policy details.

**Note**

Editing the policy affects all groups to which this policy is applied.

**6.4 Servers on AWS**

The **Servers on AWS** pages let you see and manage your AWS instances and S3 storage buckets.

**6.4.1 Servers on AWS map**

The **Map** tab on the **Servers on AWS** page lets you see the status of your AWS instances and S3 storage in different locations.
Resource Summary

The **Resource Summary** above the map shows you statistics for AWS instances and S3 storage in the location or region currently shown on the map.

- Instances or storage in good, medium or bad health.
- Instances with no Sophos protection agent installed.
- Instances with a UTM.
- Number of resources, instances or storage.

Connected AWS accounts

If you have any unconnected AWS accounts, a message is shown in the upper right of the page. Click **AWS account connections** to go to a page where you can connect Sophos Central to AWS accounts.

Filters

The **Location**, **Resource type** or **AWS account** filters let you get a closer view of a specific continent, AWS instances, S3 storage or AWS account.

The map

Each location or region is indicated by a donut chart. To see the regions within a continent in more detail, click the donut chart. Hover over the donut chart to see how many resources are in each of these states:

- Bad health
- Medium health
- Good health
- No Sophos agent (instances only)
- UTM (instances only)

To return to a view of the entire globe at any time, click the globe icon.

6.4.2 AWS Instances

On the **AWS Instances** tab on the **Servers on AWS** page, you can view the Amazon Web Services EC2 instances associated with your Sophos Central account.
Note
If you have switched on AWS Security Hub and connected your AWS Account to Sophos Central we will send some alert data to the AWS Security Hub.

If you can't see your AWS instances here, click **AWS account connections** (on the right of the screen). For details, see Amazon Web Services Accounts.

You can filter your AWS instances to display those with no Sophos product, those with Server Protection installed or containing a Sophos UTM, or those with a good, bad or medium agent status. You can also filter by AWS region.

The AWS instances are listed with these details:

- **Instance ID**: Click on the ID to view the details of the instance and to access the server's Summary tab or the UTM web admin.
- **Lifecycle State**: This shows which state of the AWS lifecycle the instance is in. See Instance Lifecycle.
- **Server Name**
- **Sophos Product**: This shows whether the instance has a Sophos agent installed or contains a Sophos UTM. Click on the instance ID to see more information about the instance.
- **AWS Account**
- **AWS Region**
- **Auto Scaling Group**: Click on the group name to view the server group details.

**Related tasks**
Amazon Web Services Accounts (page 144)

**Related information**
Instance Lifecycle

### 6.4.3 AWS S3 storage

On the **S3 storage** tab on the Servers on AWS page, you can view the Amazon Web Services S3 storage buckets associated with your Sophos Central account.

If you can't see your S3 storage buckets here, click **AWS account connections** (on the right of the screen). For details, see Amazon Web Services Accounts.

We assign a health status to your S3 storage buckets based on our security recommendations.

You can filter your S3 storage buckets by health status, including those with acknowledged health, and by AWS region.

**Note**
The buckets with a bad health status are listed first on the page. Health status is indicated in the first column.

You can acknowledge settings with bad health status to prevent them influencing the health status for the bucket. Buckets with acknowledged settings are given an acknowledged health status.

The S3 storage buckets are listed with their settings and an indicator of whether the setting complies with our security recommendations:
6.5 Policies

A policy is a set of options (for example, settings for malware protection) that Sophos Central applies to protected users, devices, servers, or networks.

There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).

To find out how policies work and how you can use them to customize security settings, see About Policies.

To find out how to create and edit policies, see Create or Edit a Policy.

Note
Your assigned administrator role affects what you can do.

Related concepts
Administration Roles (page 365)

6.5.1 About Policies

If you’re new to policies, read this page to find out how policies work.

What is a policy?

A policy is a set of options that Sophos Central applies to protected users, devices or servers.
There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).

Users, devices and servers have separate policies.

What is a Base policy?

Each feature has a Base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.

For some features, like threat protection, Sophos configures the Base policy with the best practice settings. You can leave it unchanged if you want to.

For other features, like application control or peripheral control, which are more specific to your network, you must edit the policy to set up the feature.

The Base policy is always available and is used if you don't have other policies activated.

Note
You cannot disable or delete the Base policy.

Do I need to add new policies?

You can choose whether to set up your own policies or not.

If you want to apply the same policy to all users or devices or servers, you can simply use the Base policy or adapt it for your needs.

If you want to use different settings for different groups, you can create additional policies.

What can I do with additional policies?

You can set up additional policies to override some or all of the settings in the Base policy.

You can use additional policies to apply different settings to different users, devices or servers. You can also use them to make it easier to switch the settings that are applied quickly.

The order in which you put the policies in the list matters. The policies at the top of the list override the policies at the bottom. See “How do you prioritize policies?” below.

What’s the difference between user policies and computer policies?

A user policy applies to all the devices that a user has.

A “device” or computer policy applies to specific computers or groups of computers, regardless of which user logs on.

Some features let you create either kind of policy. Other features only let you create one kind. For example you can set an updating policy for computers, but not for users.

If you set up a user policy and a computer policy for the same feature, and both could apply to the same computer, the policy that’s higher in your policy list takes priority. See “How are policies prioritized?”

You can check which policy is applied to a computer by looking at the Policies tab on that computer’s details page.
What is in each policy?

A policy lets you:

• Configure one of the features that you have licensed.
• Specify which users, devices or servers the policy applies to.
• Specify whether the policy is enforced and whether it expires.

A policy contains all the settings for a product or feature. For example, you cannot split up the threat protection settings across several different policies in such a way that a user gets one setting from one policy and another setting from a different policy.

How are policies prioritized?

The order in which you arrange the policies determines which is applied to specific users, devices or servers.

Sophos Central looks through the policies from the top down and applies the first policy it finds that applies to those users or devices.

The Base Policy is always at the bottom, and is applied to any users, devices or servers that aren’t covered by policies higher in the list.

Tip
Place the most specific policies at the top and general policies further down. Otherwise, a general policy might apply to a device for which you wanted an individual policy.

To sort policies, grab a policy and drag it to the position where you want to insert it.

6.5.2 Create or Edit a Policy

You can create or edit a policy as follows.

Create a policy

1. If you have more than one Sophos product, select the one where you want to create a policy.

   Note
   You can’t create policies from the Overview pages.

2. Go to the Policies page.
3. Click Add Policy (in the upper right).
4. If you see an Add Policy dialog, select:
   • The feature you want.
   • The policy type (applies only to Endpoint Protection).
5. On the policy details page, use the tabs to:
• Assign the policy. For example, assign it to specific users or devices.
• Enter settings for the policy. See the Help topic for that policy type.
• Enable or disable the policy.

Edit a policy

1. If you have more than one Sophos product, select the one where you want to edit a policy.

   Note
   You can't edit policies from the Overview pages.

2. Go to the Policies page.
   You see a list of policy types.
3. Click on the policy type to open a list of policies.
4. Find the policy you want to edit and click it.
5. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users or devices.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.

6.5.3 Server Threat Protection Policy

Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

Note
Some options are only for Windows servers. The columns on the right of the page show you which server type each option is for.

Note
If an option is locked global settings have been applied by your partner or Enterprise administrator. You can still stop detecting applications, exploits and ransomware by going to the events list.

To set up a policy:
• Create a Threat Protection policy.
• Open the policy's Settings tab and configure it as described below. Make sure the policy is enabled.

You can either use the recommended settings or change them.

CAUTION
Think carefully before you change the recommended settings because doing so may reduce your protection.
Note
SophosLabs can independently control which files are scanned. They may add or remove scanning of certain file types in order to provide the best protection.

Intercept X Advanced for Server

If you have this license, your threat protection policy offers protection from ransomware and exploits, signature-free threat detection, and “threat cases” for analysis of threat events.

We recommend that you use these settings for maximum protection.

For full details, see Server Protection: Intercept X Advanced

Note
If you enable any of these features, servers assigned to this policy will use an Intercept X Advanced for Server license.

Server Protection default settings

We recommend that you leave these settings turned on. These provide the best protection you can have without complex configuration.

These settings offer:
• Detection of known malware.
• In-the-cloud checks to enable detection of the latest malware known to Sophos.
• Proactive detection of malware that has not been seen before.
• Automatic cleanup of malware.
• Automatic exclusion of activity by known applications from scanning.

For full details, see Server Protection: Default settings.

Scheduled scanning

Scheduled scanning performs a scan at a time or times that you specify.

This form of scanning is enabled by default for servers.

You can select these options:
• **Enable scheduled scan.** This lets you define a time and one or more days when scanning should be performed.

  **Note**
  The scheduled scan time is the time on the endpoint computers (not a UTC time).

• **Enable deep scanning.** If you select this option, archives are scanned during scheduled scans. This may increase the system load and make scanning significantly slower.
Note
Scanning archives may increase the system load and make scanning significantly slower.

Scanning exclusions

Some applications have their activity automatically excluded from real-time scanning. You can also exclude other items or activity by other applications from scanning. You might do this because a database application accesses many files, and so triggers many scans and impacts a server’s performance.

Tip
To set up exclusions for an application, you can use the option to exclude processes running from that application. This is more secure than excluding files or folders.

We’ll still check excluded items for exploits. However, you can stop checking for an exploit that has already been detected (use a Detected Exploits exclusion).

Exclusions set in a policy are only used for the servers the policy applies to.

Note
If you want to apply exclusions to all your users and servers, set up global exclusions on the Settings > Global Exclusions page.

To create a policy scanning exclusion:

1. Click Add Exclusion (on the right of the page). The Add Exclusion dialog is displayed.
2. In the Exclusion Type drop-down list, select a type of item to exclude (file or folder, process, website, potentially unwanted application).
3. Specify the item or items you want to exclude. The following rules apply:
   - **File or folder (Windows).** On Windows, you can exclude a drive, folder or file by full path. You can use wildcards and variables. Examples:
     - Folder: C:\programdata\adobe\photoshop\ (add a slash for a folder)
     - Entire drive: D:
     - File: C:\program files\program\*.vmg
   - **File or folder (Linux).** On Linux, you can exclude a folder or file. You can use the wildcards ? and *. Example: /mnt/hgfs/excluded.
   - **File or folder (Sophos Security VM).** On Windows guest VMs protected by a Sophos security VM, you can exclude a drive, folder or file by full path, just as you can for other Windows computers. You can use the wildcard * but only for file names.

Note
By default, exclusions apply to all guest VMs protected by the security VM. For exclusions on one or more specific VMs.
• **Process (Windows).** You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process). If possible, enter the full path from the application, not just the process name shown in Task Manager. Example: `%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe

**Note**
To see all processes or other items that you need to exclude for an application, see the application vendor’s documentation.

**Note**
You can use wildcards and variables.

• **Website (Windows).** Websites can be specified as an IP address, IP address range (in CIDR notation), or domain. Examples:
  — IP address: 192.168.0.1
  — IP address range: 192.168.0.0/24 The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range. Thus /24 equals the netmask `11111111.11111111.11111111.00000000`. In our example, the range includes all IP addresses starting with 192.168.0.
  — Domain: google.com

• **Potentially Unwanted Application (Windows).** Here, you can exclude applications that are normally detected as spyware. Specify the exclusion using the same name under which it was detected by the system. Find more information about PUAs in the Sophos Threat Center.

• **Detected Exploits (Windows/Mac).** You can exclude any exploit that has already been detected. We’ll no longer detect it for the affected application and no longer block the application.

**Note**
This turns off CryptoGuard ransomware protection for this exploit for the affected application on your Windows servers.

• **AMSI Protection (Windows).** On Windows, you can exclude a drive, folder or file by its full path. Code in this location is not scanned. You can use the wildcard * for file name or extension.

• **Server isolation (Windows).** Device isolation (by an administrator) is available for servers if you are signed up to the Early Access Program for Intercept X Advanced for Server with EDR. You can allow isolated devices to have limited communications with other devices.

  Choose whether isolated devices will use outbound or inbound communications, or both. Restrict those communications with one or more of these settings:
  — **Local Port:** Any device can use this port on isolated devices.
  — **Remote Port:** Isolated devices can use this port on any device.
  — **Remote Address:** Isolated devices can only communicate with the device with this IP.

  Example 1: You want remote desktop access to an isolated device so that you can troubleshoot.

  — Select **Inbound Connection.**
— In **Local Port**, enter the port number.

Example 2: You want to be able to go to an isolated device and download cleanup tools from a server.

— Select **Outbound Connection**.

— In **Remote Address**, enter the address of the server.

4. For **File or folder** exclusions only, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.

5. Click **Add** or **Add Another**. The exclusion is added to the scanning exclusions list.

To edit an exclusion later, click its name in the exclusions list, enter new settings and click **Update**.

### Desktop Messaging

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

**Desktop Messaging** is on by default.

**Note**

If you switch off **Desktop Messaging** you will not see any notification messages related to Threat Protection.

Click in the message box and enter the text you want to add.

**Related concepts**

**Create or Edit a Policy** (page 334)
You can create or edit a policy as follows.

**Server Protection: Intercept X Advanced** (page 340)
If you have an Intercept X Advanced for Server license, you'll see options in your threat protection policy in addition to the standard Server Protection options.

**Server Protection: Default settings** (page 341)
The server threat protection base policy includes these standard options.

**Related reference**

**Windows Scanning Exclusions: Wildcards and Variables** (page 343)
When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

**Virtual Server Scanning Exclusions: Wildcards** (page 347)
**Virtual Server** exclusions let you exclude items from scanning on Windows guest VMs that are protected by a Sophos security VM.

**Device isolation exclusions (Windows)** (page 350)
You can allow isolated devices to have limited communications with other devices.

**Website exclusions** (page 349)
You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

**Process exclusions (Windows)** (page 349)
You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

**Related information**

Global Exclusions (page 374)
You can exclude files, websites and applications from scanning for threats.

Sophos Threat Center
Antimalware Scan Interface (AMSI)
Automatic Exclusions

**Server Protection: Intercept X Advanced**

If you have an Intercept X Advanced for Server license, you'll see options in your threat protection policy in addition to the standard Server Protection options.

**Runtime Protection**

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

- **Protect document files from ransomware (CryptoGuard):** This protects document files against malware that restricts access to files, and then demands a fee to release them. You can also choose to protect 64-bit computers against ransomware run from a remote location.

- **Protect from master boot record ransomware:** This protects the computer from ransomware that encrypts the master boot record (and so prevents startup) and from attacks that wipe the hard disk.

- **Protect critical functions in web browsers (Safe Browsing):** This protects your web browsers against exploitation by malware.

- **Mitigate exploits in vulnerable applications:** This protects the applications most prone to exploitation by malware. You can select which application types to protect.

- **Advanced exploit mitigation settings:**
  - **Prevent credential theft:** This prevents the theft of passwords and hash information from memory, registry, or hard disk.
  - **Prevent code cave utilisation:** This detects malicious code that's been inserted into another, legitimate application.
  - **Prevent APC violation:** This prevents attacks from using Application Procedure Calls (APC) to run their code.
  - **Prevent privilege escalation:** This prevents attacks from escalating a low-privilege process to higher privileges to access your systems.

We recommend testing these settings before you apply the policy to your servers.

- **Protect processes:** This helps prevent the hijacking of legitimate applications by malware. You can choose to:
  - protect against process replacement attacks (process hollowing attacks).
  - protect against loading .DLL files from untrusted folders.

- **Enable CPU branch tracing:** CPU malicious code detection is a feature of Intel processors that allows tracing of processor activity for detection. We support it on Intel processors with the following architectures: Nehalem, Westmere, Sandy Bridge, Ivy Bridge, Haswell, Broadwell, Goldmont, SkyLake, and Kaby Lake.

We don't support it if there is a (legitimate) hypervisor on the computer.
Deep Learning

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

Remediation

- **Enable Threat Case creation**: Threat cases let you investigate the chain of events in a malware attack and identify areas where you can improve your security.
- **Allow servers to send data on suspicious files, network events and admin tool activity to Sophos Central**: This sends details of potential threats to Sophos. Ensure it's turned on in any policy for servers where you want to do threat searches.

  **Note**
  This option is available if you have Intercept X Advanced with EDR for Server.

  **Restriction**
  You must turn this option on in both Endpoint and Server Protection to use Intercept X Advanced for Server with EDR.

**Related concepts**

- **Threat Cases** (page 19)
  Threat cases let you investigate and clean up malware attacks.
- **Threat Searches** (page 31)
  You can search for potential threats on your network.

**Server Protection: Default settings**

The server threat protection base policy includes these standard options.

We recommend that you leave these settings turned on. These provide the best protection you can have without complex configuration.

**CAUTION**
Think carefully before you change the recommended settings because doing so may reduce your protection.

**Restriction**
Some options are only for Windows servers. The columns on the right of the page show you which server type each option is for.

**Runtime Protection**

Runtime protection protects against threats by detecting suspicious or malicious behavior or traffic.
**Detect malicious connections to command and control servers.** This detects traffic between an endpoint computer and a server that indicates a possible attempt to take control of the endpoint computer (a “command and control” attack).

**Enable Sophos Security Heartbeat:** This sends server “health” reports to each Sophos XG Firewall that is registered with your Sophos Central account. If more than one firewall is registered, reports go to the nearest one available. If a report shows that a server might have been compromised, the firewall can restrict its access.

**AMSI Protection (with enhanced scan for script-based threats).** This protects against malicious code (for example, PowerShell scripts) using the Microsoft Antimalware Scan Interface (AMSI). Code forwarded via AMSI is scanned before it runs and the applications used to run the code are notified of threats by Sophos. If a threat is detected, an event is logged.

**Live Protection**

Live Protection checks suspicious files against the latest malware in the SophosLabs database.

**Use Live Protection to check the latest threat information from SophosLabs online:** This checks files during real-time scanning.

- Use Live Protection during scheduled scans

**Real-time scanning - Local files and network shares**

Real-time scanning scans files as users attempt to access them, and allows access if the file is clean.

**Local and remote:** If you select **local** instead, files in network shares will not be scanned.

**On read:** This scans files when you open them.

**On write:** This scans files when you save them.

**Real-time scanning - Internet**

Real-time scanning scans internet resources as users attempt to access them.

**Scan downloads in progress.**

**Block access to malicious websites:** This denies access to websites that are known to host malware.

**Detect low-reputation files:** This warns if a download has a low reputation. The reputation is based on the file's source, how often it is downloaded and other factors. You can specify:

- **The Action to take on low-reputation downloads:** If you select **Prompt user**, users will see a warning when they attempt to download a low-reputation file. This is the default setting.

- **The Reputation level:** If you select **Strict**, medium-reputation as well as low-reputation files will be detected. The default setting is **Recommended**.

**Remediation**

**Automatic cleanup of malware:** This attempts to clean up detected threats automatically. This option is supported on Windows servers and also on guest VMs protected by a Sophos security VM (but only if you have installed the Sophos Guest VM Agent on them).
Note
We always clean up PE (Portable Executable) files like applications, libraries, and system files, even if you turn off automatic cleanup. PE files are quarantined and can be restored.

Real-time scanning - Options

Automatically exclude activity by known applications: This prevents Sophos Central from scanning files used by certain widely-used applications. For a list of these applications, see Download Reputation. You can manually exclude activity by other applications by using the Exclusions options.

Detect malicious behavior (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.

Advanced Settings

These settings are for testing or troubleshooting only. We recommend that you leave them set to the defaults.

Related information
Antimalware Scan Interface (AMSI)
Download Reputation
Automatic Exclusions

Windows Scanning Exclusions: Wildcards and Variables

When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

Note
Some wildcards or variables cannot be used for exclusions from real-time scanning on Windows XP or Windows Server 2003.

Warning
Scanning exclusions may significantly reduce your protection. Only use them if you understand the risks.

Wildcards

You can use the wildcards shown in this table.

Note
Only * and ? can be used on Windows XP and Windows Server 2003.
<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>* (Star)</td>
<td>Zero or more of any character except \ or /</td>
<td>For example:</td>
</tr>
<tr>
<td>** (Star Star)</td>
<td>Zero or more characters including \ and /, when bracketed by \ or / characters or used at the start or end of an exclusion. Any other use of a ** is treated as a single * and matches zero or more characters excluding \ and /.</td>
<td>For example:</td>
</tr>
<tr>
<td>\ (Backslash)</td>
<td>Either \ or /</td>
<td></td>
</tr>
<tr>
<td>/ (Forward slash)</td>
<td>Either / or \</td>
<td></td>
</tr>
<tr>
<td>? (Question mark)</td>
<td>One single character. If it is at the end of a string it can match zero characters.</td>
<td></td>
</tr>
<tr>
<td>. (Period)</td>
<td>A period OR the empty string at the end of a filename, if the pattern ends in a period and the filename does not have an extension.</td>
<td>Note that:</td>
</tr>
</tbody>
</table>

Example wildcards

Here are some examples of the use of wildcards.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Interpreted as</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo</td>
<td>**\foo</td>
<td>Exclude any file named foo (in any location).</td>
</tr>
<tr>
<td>foo\bar</td>
<td>**\foo\bar</td>
<td>Exclude any file named bar in a folder named foo (in any location).</td>
</tr>
<tr>
<td>*.txt</td>
<td>***.txt</td>
<td>Exclude all files named *.txt (in any location).</td>
</tr>
</tbody>
</table>
### Expression

<table>
<thead>
<tr>
<th>Expression</th>
<th>Interpreted as</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D:\</td>
<td>D:&quot;</td>
<td>Exclude the entire drive D: from scanning. Use with care. PE files (such as applications), including malware, will be able to run on this drive without detection.</td>
</tr>
<tr>
<td>C:\foo\</td>
<td>C:&quot;foo&quot;</td>
<td>All files and folders underneath C:\foo, including C:\foo itself.</td>
</tr>
<tr>
<td>C:\foo*.txt</td>
<td>C:&quot;foo*.txt&quot;</td>
<td>All files or folders contained in C:\foo named *.txt.</td>
</tr>
</tbody>
</table>

### Variables for exclusions

You can use variables when you set up scanning exclusions.

The table below shows the variables and examples of the locations they correspond to on each operating system.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Windows 7 and later</th>
<th>Windows XP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2008 and later</td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>%allusersprofile%</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users</td>
</tr>
<tr>
<td>%appdata%</td>
<td>C:\Users*\AppData \Roaming</td>
<td>C:\Documents and Settings*\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>%commonprogramfiles%</td>
<td>C:\Program Files\Common Files</td>
<td></td>
</tr>
<tr>
<td>%commonprogramfiles(x86)%</td>
<td>C:\Program Files (x86)\Common Files</td>
<td></td>
</tr>
<tr>
<td>%localappdata%</td>
<td>C:\Users*\AppData \Local</td>
<td>C:\Documents and Settings*\Local Settings\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>%programdata%</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users \Application Data</td>
</tr>
<tr>
<td>Variable</td>
<td>Windows 7 and later Windows Server 2008 and later</td>
<td>Windows XP Windows Server 2003</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>%programfiles%</td>
<td>C:\Program Files</td>
<td></td>
</tr>
<tr>
<td>%programfiles(x86)%</td>
<td>C:\Program Files (x86)</td>
<td></td>
</tr>
<tr>
<td>%systemdrive%</td>
<td>C:</td>
<td></td>
</tr>
<tr>
<td>%systemroot%</td>
<td>C:\Windows</td>
<td></td>
</tr>
<tr>
<td>$temp% or %tmp%</td>
<td>C:\Users*\AppData \Local\Temp</td>
<td>C:\Documents and Settings*\Local Settings\Temp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>%userprofile%</td>
<td>C:\Users*</td>
<td>C:\Documents and Settings*</td>
</tr>
<tr>
<td>%windir%</td>
<td>C:\Windows</td>
<td></td>
</tr>
</tbody>
</table>

**Linux scanning exclusions: wildcards**

You can add scanning exclusions for Linux servers.

**CAUTION**  
Think carefully before you add scanning exclusions because doing so may reduce your protection.

**Wildcards**

You can use the wildcards shown in this table.

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>* (Star)</td>
<td>Zero or more of any character including / (slash)</td>
</tr>
<tr>
<td>? (Question mark)</td>
<td>One single character.</td>
</tr>
</tbody>
</table>

**Excluding a specific directory or file**

You can exclude a specific directory or file by its full path. To exclude a directory, add a trailing slash and star. For example:

- `/mnt/hgfs/excluded` excludes the file named `excluded`.
- `/mnt/hgfs/excluded/*` excludes the directory named `excluded` and all directories and files below it in the filesystem.
Excluding a directory or file in any location

You can exclude a directory or file in any location by preceding it with a star and slash. For example:

- */excluded excludes the file named excluded in any location.
- */excluded/* excludes the directory named excluded in any location and all directories and files below it in the filesystem.

Examples

Here are some examples of exclusion expressions.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Items that are excluded</th>
</tr>
</thead>
<tbody>
<tr>
<td>*/data/report</td>
<td>A file named report in a directory named data in any location</td>
</tr>
<tr>
<td>*.txt</td>
<td>Any file whose name ends in .txt in any location</td>
</tr>
<tr>
<td>/mnt/hgfs/data/*.txt</td>
<td>Any file whose name ends in .txt in the directory named /mnt/hgfs/data/</td>
</tr>
<tr>
<td>*/report??2020</td>
<td>Any file whose name begins with report followed by two characters and ends with 2020 in any location</td>
</tr>
<tr>
<td><em>/report20??/</em></td>
<td>Any directory in any location whose name begins with report20 and ends with two characters, and all directories and files below it in the filesystem</td>
</tr>
</tbody>
</table>

Virtual Server Scanning Exclusions: Wildcards

Virtual Server exclusions let you exclude items from scanning on Windows guest VMs that are protected by a Sophos security VM.

CAUTION

Think carefully before you add scanning exclusions because doing so may reduce your protection.

You can exclude a drive, folder or file by full path, just as you can for other Windows computers. However, there are restrictions on specifying items without a full path and also on the use of wildcards. See the details below and the examples.

Items without a full path

You can specify a file without a full path, for example file.com. You must include the extension. The security VM will exclude any file with this name.
You cannot specify folders without a full path.

Wildcards

You can use the wildcards shown in this table.

Note
Only * and ? can be used on Windows XP and Windows Server 2003.

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
<th>For example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>* (Star)</td>
<td>Zero or more of any character except \ or /</td>
<td></td>
<td>* matches:</td>
</tr>
</tbody>
</table>
| ** (Star Star) | Zero or more characters including \ and /, when bracketed by \ or / characters or used at the start or end of an exclusion. | Any other use of a ** is treated as a single * and matches zero or more characters excluding \ and /.
| \ (Backslash) | Either \ or /                                                            |                                                                                                   | ** matches c:\foo\bar                                                                         |
| / (Forward slash) | Either / or \                                                          |                                                                                                   | c:\foo**matches c:\foo\more\bar                                                                |
| ? (Question mark) | One single character. If it is at the end of a string it can match zero characters. |                                                                                                   |                                                                                                   |
| . (Period) | A period OR the empty string at the end of a filename, if the pattern ends in a period and the filename does not have an extension. | Note that:                                                                                         | *.matches all files                                                                             |
                                                                                                           |                                                                                                   | * matches all files without an extension                                                         |
                                                                                                           |                                                                                                   | “foo.” matches “foo” and “foo.”                                                                  |

Exclusions that work

The expressions shown in this table are valid for Virtual Server exclusions.

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>D:</td>
<td>Excludes the entire drive.</td>
</tr>
</tbody>
</table>
### Exclusion

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\programdata\adobe\photoshop\</td>
<td>Excludes the folder (you must include the final slash).</td>
</tr>
<tr>
<td>C:\program files\program*.com</td>
<td>Excludes files with a .com extension in the specified folder.</td>
</tr>
<tr>
<td>file.com</td>
<td>Excludes files with this name in any location (full path not needed).</td>
</tr>
<tr>
<td>file.*</td>
<td>Excludes all files called “file”, with any extension, in all locations.</td>
</tr>
<tr>
<td>*.com</td>
<td>Excludes all files with a .com extension in all locations.</td>
</tr>
<tr>
<td><em>.</em></td>
<td>Excludes all files in all locations.</td>
</tr>
<tr>
<td>C:\file???.docx</td>
<td>Excludes C:\file12.exe (but not C:\file123.exe).</td>
</tr>
</tbody>
</table>

### Process exclusions (Windows)

You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

If possible, enter the full path from the application, not just the process name shown in Task Manager.

**Example:**

```
%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe
```

**Note**
To see all processes or other items that you need to exclude for an application, see the application vendor’s documentation.

**Note**
You can use wildcards and variables.

### Website exclusions

You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

**Examples:**

- IP address: 192.168.0.1
- IP address range: 192.168.0.0/24
- The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range.

Thus /24 equals the netmask:
In our example, the range includes all IP addresses starting with 192.168.0.

- Domain: google.com

**Device isolation exclusions (Windows)**

You can allow isolated devices to have limited communications with other devices. You can choose whether isolated devices will use outbound or inbound communications, or both.

Use the following settings to restrict communications:

- **Local Port**: Any device can use this port on isolated devices.
- **Remote Port**: Isolated devices can use this port on any device.
- **Remote Address**: Isolated devices can only communicate with the device with this IP.

**Example 1**

You want remote desktop access to an isolated device so that you can troubleshoot.

- In **Direction**, select **Inbound Connection**.
- In **Local Port**, enter the port number.

**Example 2**

You want to be able to go to an isolated device and download cleanup tools from a server.

- In **Direction**, select **Outbound Connection**.
- In **Remote Address**, enter the address of the server.

**6.5.4 Server Peripheral Control Policy**

Peripheral control lets you control access to peripherals and removable media. You can also exempt individual peripherals from that control.

**Note**

If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set it up:

- Create a **Peripheral Control** policy. See Create or Edit a Policy.
- Open the policy's **Settings** tab and configure it as described below. Make sure the policy is enabled.

**Manage Peripherals**

In **Manage Peripherals**, select how you want to control peripherals:
• **Monitor but do not block (all peripherals will be allowed).** If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you cannot set access rules for them.

• **Control access by peripheral type and add exemptions.** If you select this, you can go on to set access policies for peripheral types and for individual detected peripherals.

**Set Access Policies**

Set access policies in the table.

The table displays detected peripheral types, the number of each type detected, and the current access policy.

**Note**
The totals include all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent policies for all devices.

**Note**
The [MTP/PTP](#) category includes devices such as phones, tablets, cameras, and media players that connect using the MTP or PTP protocols.

For each peripheral type, you can change the access policy:

• **Allow:** Peripherals are not restricted in any way.

• **Block:** Peripherals are not allowed at all.

• **Read Only:** Peripherals can be accessed only for reading.

**Note**
The Bluetooth, Infrared, and Modem categories do not have the **Read Only** option.

**Note**
The Wireless category has a **Block Bridged** option. This prevents bridging of two networks.

**Peripheral Exemptions**

Click the **Peripheral Exemptions** fold-out if you want to exempt individual peripherals from the control settings, or apply less restrictive controls.

1. Click **Add Exemptions**.

2. In **Add Peripheral Exemptions**, you'll see a list of detected peripherals.

**Note**
Peripherals are detected when you are in monitoring mode or if there is an access restriction for that type of peripheral.
3. Select a peripheral.

4. In the Policy column, you can optionally use the drop-down list to assign a specific access policy to an exempt peripheral.

Restriction
Do not set a stricter access policy for an individual peripheral than for its peripheral type. If you do, the setting for the individual policy is ignored and a warning icon is displayed beside it.

5. In the Enforce By column, you can optionally use the drop-down menu to apply the policy to all peripherals of that model or to ones with the same ID (the list shows you the model and ID).

6. Click Add Exemption(s).

Desktop Messaging

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

Desktop Messaging is on by default.

Note
If you switch off Desktop Messaging you will not see any notification messages related to Peripheral Control.

Click in the message box and enter the text you want to add.

Related concepts
Create or Edit a Policy (page 334)
You can create or edit a policy as follows.

6.5.5 Server Application Control Policy

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.

Note
If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set it up:
• Create an Application Control policy. See Create or Edit a Policy.
• Open the policy's Settings tab and configure the policy as described below. Make sure the policy is enabled.
We recommend that you detect the applications being used on your network and then decide which to block, as follows.

1. In the **Controlled Applications** list, click **Add/Edit List**.
   This opens a dialog where you can see the categories of applications that you can control. Sophos supplies and updates the list.

2. Click an application category, for example **Browser plug-in**.
   A full list of the applications in that category is displayed in the right-hand table.

3. We recommend that you select the option **Select all applications**. You'll refine your selection later.

4. Click **Save to List** and repeat for each category you want to control.

   **Note**
   If you want to control an application that isn't in the list supplied by Sophos, you can ask to have it added. Click the **Application Control Request** link at the bottom of the **Settings** tab.

5. In **Detection Options**:
   a) Select **Detect controlled applications during scheduled and on-demand scans**.
   b) Do not select any other options for now.

   **Note**
   Application control uses the scheduled scans and the scanning options (which file types are scanned) that you set in Threat Protection settings.

6. Allow time for all your computers to run a scheduled scan.

7. Go to the **Overview > Logs & Reports > Events** page.

8. In the list of event types, clear all the checkboxes except **Application Control**.
   Detected applications are now shown in the list of events. Make a note of any you want to continue using.

9. Return to your policy page.

10. In the **Controlled Applications** list, click **Add/Edit List** again. Then:
   a) Find the applications you want to use and clear the checkbox next to them.
   b) Select **New applications added to this category by Sophos** (optional). Any new applications that Sophos adds to this category later will automatically be added to your controlled list. Newer versions of applications already in your list will also be added.

   **CAUTION**
   Only select this if you're sure you want to control applications in this category from now on.

   c) Click **Save to List**.

11. In **Detection Options**:
   a) Select **Detect controlled applications when users access them**.
   b) Select **Block the detected application**.

   **Note**
   If you chose to control any new applications added by Sophos, those new applications will now be blocked.
12. In **Desktop Messaging** you can add a message to the standard notification. If you leave the message box empty only the standard message is shown.

   Desktop messaging is on by default.

   **Note**
   If you switch off desktop messaging you will not see any notification messages related to Application Control.

   a) Click in the message box and enter the text you want to add.

### 6.5.6 Server Web Control Policy

Web Control lets you restrict access to certain categories of website.

**Note**
Web Control settings apply only to Windows servers.

**Note**
All servers to which this policy applies will use a Server Advanced license.

**Note**
If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set up a policy:
- Create a **Web Control** policy. See Create or Edit a Policy.
- Open the policy's **Settings** tab and configure it as described below. Make sure the policy is enabled.

#### Website Controls

Select **Website Controls** to control access to websites that may be inappropriate.

For each website category, you can select:
- **Allow**: Allows all websites in this category.
- **Warn**: Warns the user that a website may be inappropriate.
- **Block**: Blocks all websites in this category.

#### Log web control events

Select **Log web control events** to log attempts to visit blocked websites or websites for which we display a warning.

**Note**
If you do not enable logging, only attempts to visit infected sites will be logged.
Control sites tagged in Website Management

You can put websites into your own custom categories ("tag" them) and then use a Web Control policy to control sites in each category.

To set this up, do as follows.

1. In Endpoint or Server Protection, go to **Settings > Website Management**.
2. Click **Add**.
3. In **Add Website Customization**, enter a website and add a tag. You can either type in a new tag name, or select a tag you've used before (you'll see suggested tags when you start typing). Click **Save**.
4. In Endpoint or Server Protection, go to **Policies > Web Control** and select a policy.
5. Click the **Settings** tab.
6. Turn on **Control sites tagged in Website Management**.
7. Click **Add New** on the right of the page.
8. In **Add Website Tag**, do as follows.
   - Select the website tag you created.
   - Choose the **Action** you want to take against websites.
   - Click **Save**.
9. On the **Settings** tab, click **Save**.

For more information on how Sophos filters websites see [Sophos Web Security and Control Test Site](#).

**Related concepts**
- [Create or Edit a Policy](#) (page 334)
  You can create or edit a policy as follows.

**Related tasks**
- [Website Management](#) (page 372)

**Related information**
- [Sophos Web Security and Control Test Site](#)

### 6.5.7 Server Lockdown Policy

Server Lockdown prevents unauthorized software from running on servers.

To do this, Sophos makes a list of the software already installed, checks it is safe, and allows only that software to run in future.

You lock down a server at its details page.

You can use the Server Lockdown settings in a policy to change what is allowed without the need to unlock the server. For example, you might want to add and run new software.

**Note**
If an option is locked global settings have been applied by your partner or Enterprise administrator.
To set up a policy:

- Create a **Lockdown** policy. See Create or Edit a Policy.
- Open the policy's **Settings** tab and configure it as described below. Make sure the policy is enabled.

## Allowed files/folders

This option lets you allow software (such as updaters) to run and modify other applications. It also lets you add new software to a locked-down server without unlocking it.

**CAUTION**

This option “trusts” the software, so that any files it creates or changes are also allowed. This is different from the process when you lock down a server, which only allows the software itself to run.

You can specify files that are allowed, or a folder in which all the files are allowed.

**Tip**

You can specify a folder where you always download installers for use on the server.

1. Click **Add allowed file/folder**.
2. Select the type of item to allow (file or folder).
3. Enter the path of the file or folder.

**Note**

You can use the wildcard * 

4. Click **Save**.

## Blocked files/folders

This lets you block software that is currently allowed to run.

You can specify files that are blocked, or a folder in which all the files are blocked.

**Tip**

You can block a folder used for applications, such as installers, that you want to make available to other users on the network, but don’t want to run on your server.

1. Click **Add blocked file/folder**.
2. Select the type of item to block (file or folder).
3. Enter the path of the file or folder.

**Note**

You can use the wildcard * 

4. Click **Save**.
You can create or edit a policy as follows.

6.5.8 Server Data Loss Prevention Policy

Data Loss Prevention (DLP) controls accidental data loss. DLP enables you to monitor and restrict the transfer of files containing sensitive data. For example, you can prevent a user sending a file containing sensitive data home using web-based email.

You do this by creating rules, see Data Loss Prevention Rules. You then add the rules to policies, as described below. You can then apply these policies to users, computers and Windows servers, see About Policies.

Data Loss Prevention (DLP) policies include one or more rules that specify conditions and actions to be taken when the rule is matched. When a DLP policy contains several rules, a file that matches any of the rules in the DLP policy violates the policy. A rule can be included in multiple policies. You can add text to the messages shown on protected endpoints or Windows servers when the rules are triggered. There are two types of message:

- A confirmation notification that asks the user to confirm the file transfer.
- A block notification that informs the user that they cannot transfer the file.

You can create custom policies or policies from templates. The templates cover standard data protection for different regions. You can apply these policies to users, computers or Windows servers.

To set up a policy:

- Create a Data Loss Prevention policy. See Create or Edit a Policy.

- Open the policy's Settings tab and configure it as described below. Make sure Use rules for data transfers is enabled.

1. Choose whether you want to create a policy from a template or a custom policy.

   - To use a template, select a region and a template and click Create from Template. This adds a pre-defined rule to the policy.

   **Tip**
   To add more rules, click **Add**.

   - To create a custom policy, click Create Custom Policy and click Add. Choose whether you want to an use existing rule or create a new rule: see Create a Data Loss Prevention Rule. Select the rules you want to add and click Add.

2. Turn on the options in the Messages For End Users area and click the option names to add your own message to the standard confirmation and block notifications. Each message can have a maximum of 100 characters.

   **Note**
   You can turn off either or both of these messages. The standard notification is shown on the endpoint or server. If you leave the message box blank the standard notification is shown.

   a) Enter the message text.
   b) Click **Finish**.

Copyright © Sophos Limited
6.5.9 Server Updating Policy

The Updating policy lets you specify when product updates become available on your network. This ensures that your computers don’t start updating until a time that suits you.

**Note**
If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set it up:
- Create an **Update Management** policy. See Create or Edit a Policy.
- Open the policy's **Settings** tab and configure it as described below. Make sure the policy is enabled.

### Scheduled Updates

Enable **Scheduled Updates** and select the day and time when you want product updates to become available. The time is local to each computer. For example, if you select 9 pm, each computer will get the update at 9 pm local time for the computer. This means that computers in different time zones will not get the update concurrently.

Remember that if computers aren’t on, they won’t get the update until they are next on at the scheduled update time.

6.5.10 Server Windows Firewall Policy

You can monitor and configure Windows Firewall (and monitor other registered firewalls) on your computers and servers using a Windows Firewall policy.

You can apply a Windows Firewall policy to individual devices (computers or servers) or to groups of devices.

**CAUTION**
Other firewalls or your Windows Group Policy settings may affect how the policy is applied on individual computers and servers.

We advise that you test any firewall rules you create (locally or via Group Policy) to make sure that communication with Sophos is allowed.

**Note**
If an option is locked global settings have been applied by your partner or Enterprise administrator.

To set it up:
- Create a **Windows Firewall** policy. See Create or Edit a Policy.
- Open the policy's **Settings** tab and configure it as described below. Make sure the policy is enabled.
Monitor Type

In Monitor Type, select the level of monitoring you want:

- **Monitor Only**. Devices will report their firewall status to Sophos Central. This is the default option.
- **Monitor & Configure Network Profiles**. Devices will report their firewall status to Sophos Central. You can also choose whether to block or allow inbound connections on Domain Networks, Private Networks, and Public Networks.

Choose from:

- **Block All**
- **Block (with exceptions)**. You must set up the exceptions locally on the computer or server. If you don’t set up exceptions all inbound connections are blocked.
- **Allow All**

6.5.11 File Integrity Monitoring Policy

File Integrity Monitoring lets you monitor files, folders, registry keys or registry values for changes. This monitoring helps you comply with security requirements like PCI DSS.

To set up a policy:

2. Create a File Integrity Monitoring policy or edit the Base Policy. See Create or Edit a Policy.
3. Open the policy’s Settings tab.
4. Select Use File Integrity Monitoring.

By default, we monitor critical Windows system files. You can set up custom monitoring if you want to monitor other locations.

**Note**

If you set up custom monitoring, we strongly recommend that you read the section below.

Custom monitoring

To monitor a location, do as follows.

1. Go to Custom monitoring.
2. Click Add location.
3. In Add location, select the item Type.

**Note**

If you select Folder, we monitor the folder and the files in it by default. To monitor only the files in the folder, deselect Monitor changes to the folder as well as the files.
If you select **Registry Key**, we monitor the key but not the values in it. You must use the location type **Registry Value** to monitor values.

You can use variables. See File Integrity Monitoring locations: Variables.

4. Click **Add** or **Add Another**.

To edit a location already in the list, click its path and update the details.

To delete a location from the list, click the cross on the right.

**Monitoring exclusions**

To exclude a location from monitoring, do as follows.

1. Go to **Monitoring exclusions**.
2. Click **Add exclusion**.
3. In **Add exclusion**, select the item **Type**.

**Note**

If you select **Folder**, you exclude the folder and the files in it.

**Note**

If you select **Registry Key**, you exclude the key and the registry values within it.

You can use variables. See File Integrity Monitoring locations: Variables.

4. Click **Add** or **Add Another**.

To edit a location already in the list, click its path and update the details.

To delete a location from the list, click the cross on the right.

**Related concepts**

- Create or Edit a Policy (page 334)
- You can create or edit a policy as follows.
- File Integrity Monitoring locations: Variables (page 360)

**Related information**

- Sophos File Integrity Monitoring: Default monitored locations

### File Integrity Monitoring locations: Variables

You can use variables when you set up custom monitoring locations or exclusions for File Integrity Monitoring.

The table below shows the variables and examples of the locations they correspond to.

These variables can only be used on Windows 7 and later or Windows Server 2008 and later.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>@allusersprofile%</td>
<td>C:\ProgramData</td>
</tr>
</tbody>
</table>
### Variable Location

<table>
<thead>
<tr>
<th>Variable</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>%commonprogramfiles%</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>%commonprogramfiles(x86)%</td>
<td>C:\Program Files (x86)\Common Files</td>
</tr>
<tr>
<td>%programdata%</td>
<td>C:\ProgramData</td>
</tr>
<tr>
<td>%programfiles%</td>
<td>C:\Program Files</td>
</tr>
<tr>
<td>%programfiles(x86)%</td>
<td>C:\Program Files (x86)</td>
</tr>
<tr>
<td>%systemroot%</td>
<td>C:\Windows</td>
</tr>
<tr>
<td>%windir%</td>
<td>C:\Windows</td>
</tr>
</tbody>
</table>

### 6.6 Settings

The Settings pages are used to specify security settings that apply to all your users and devices. The pages displayed depend on the features included in your license. Some of these pages may also be displayed under **Global Settings** in **Overview**.

**Note**
If you want to apply settings only to certain users, servers, or devices, use the **Policies** pages instead.

#### 6.6.1 Active Directory Sync

You can import users and user groups from Active Directory to Sophos Central.

In Settings, on the **Active Directory Sync** page, you can select the Active Directory service you want to use.

- There is a download link for the Sophos Central Active Directory synchronization utility.
- In **Endpoint Protection** and **Email Gateway** you can use Azure Active Directory synchronization instead.

**Note**
If you are using Office 365 you must use Azure Active Directory synchronization.

For instructions on setting up the utility, see the Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

**Related concepts**
- [Active Directory Sync Status](#) (page 362)
- On the **Active Directory Sync** page, you can check the sync status and download the installer.
- About [Active Directory synchronization](#) (page 362)
Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

**Related tasks**
Set up synchronization with Active Directory (page 362)
Follow these instructions to set up synchronization with Active Directory.

### Active Directory Sync Status

On the **Active Directory Sync** page, you can check the sync status and download the installer.

You need to set up Active Directory synchronization before you can see these options.

You can download the latest installer for setting up synchronization with Active Directory.

**Sync status**

This shows your synchronization status and the synchronization settings in Active Directory.

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The time of the last synchronization with Active Directory.
- The number of users and groups imported from Active Directory.

You can view Active Directory synchronization alerts on the **Overview > Alerts** page. You can view synchronization events on the **Overview > Logs & Reports > Events** page.

**About Active Directory synchronization**

Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

To synchronize with Active Directory, you need to download and install the Sophos Central Active Directory Sync utility. The utility works as follows.

It synchronizes active users and user groups.

It can run automatically on a regular basis, as set up by the Sophos Central administrator.

It doesn't duplicate existing users or groups when they are matched to an existing Sophos Central user or group. For example, an email address from Active Directory may be added to an existing user in Sophos Central.

It supports only the Active Directory service.

It can synchronize multiple Active Directory forests. To do this, you need to install the utility on multiple machines and configure each utility to synchronize a different Active Directory forest. We strongly recommend to synchronize different Active Directory forests at different times of day, so that the synchronizations do not overlap.

It doesn't help you to deploy the Sophos agent software to your users’ devices. Use other methods of deployment with Active Directory.

**Set up synchronization with Active Directory**

Follow these instructions to set up synchronization with Active Directory.

Before you can set up synchronization, you need .NET Framework 4 on the computer where you will run the Sophos Central AD Sync Utility.
Warning
Before you proceed, make sure all your active directory users are set up correctly with an email address. Users without an email address aren't protected and email going to an email address not tied to a user isn't delivered.

You need to use API credentials to synchronize with Active Directory.

To set up synchronization with Active Directory:
1. Set up your API credentials for AD sync. To do this, click Settings > API credentials.
2. Add a new credential. Enter the following information:
   - Credential name
   - Description
3. Copy the Client ID and Client Secret.
4. Click Settings > Active Directory Sync, and click the link to download the Sophos Central AD Synchronization Utility installer. Then run it.

   Alternatively, go to the Start menu and click Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.

   The Sophos Central AD Sync Utility Setup assistant starts.
5. In the setup wizard, enter the information required.

   Follow the instructions in the Sophos Central AD Sync Utility Setup assistant.
6. On the last page of the setup assistant, select Launch Sophos Central AD Sync Utility and click Finish.
7. In the Active Directory Synchronization Setup utility, on the Sophos Credentials page, enter your Client ID and Client Secret instead of your Sophos Central account credentials.
8. On the AD Configuration page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the Use LDAP over an SSL connection (recommended) checkbox selected. If your LDAP environment doesn’t support SSL, clear the Use LDAP over an SSL connection (recommended) checkbox and change the port number. The port number is usually 636 for SSL connections and 389 for insecure connections.
9. If you don’t want to synchronize the entire forest, on the AD Filters page, you can specify which domains to include in the synchronization. You can also specify additional search options (search bases and LDAP query filters) for each domain. Distinct options can be specified for users and user groups.

   Note
   AD Sync will only create groups that have members which include discovered users or devices, regardless of group filter settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search bases</td>
<td>You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format:</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OU=Finance,DC=myCompany,DC=com</td>
<td>To filter users, for example, by group membership, you can define a user query filter in this format:</td>
</tr>
<tr>
<td></td>
<td>memberOf=CN=testGroup, DC=myCompany, DC=com</td>
</tr>
<tr>
<td></td>
<td>The above query limits user discovery to users belonging to “testGroup”. Note that if you don't specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter: CN=testGroup</td>
</tr>
</tbody>
</table>

**Note**
If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

10. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.

**Note**
A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select **Never. Only sync when manually initiated.**

11. Click **Finished**.

12. To synchronize immediately, in the AD Sync Utility, click **Preview and Sync**. Review the changes that will be made during the synchronization. If you are happy with the changes, click **Approve Changes and Continue**.

The Active Directory users and groups are imported from the Active Directory to Sophos Central.

To stop the synchronization in progress, click **Stop**.

### 6.6.2 Role Management

You can use pre-defined administration roles to divide up security tasks according to the administrators’ responsibility level.

In **Settings**, the **Role Management** page shows a list of administration roles and the number of users assigned to each role.

You can only see this option if you are a Super Admin administrator.
Click on a role name to see a detailed description of the role and the names of the people that have that role assigned to them. You can manage the people assigned to a specific role in that role’s page.

**Restriction**
An administrator role affects what a user can do.

**Administration Roles**

Predefined roles cannot be edited or deleted.

Your assigned administrator role affects what you can do.

A Super Admin can add custom roles. These roles are based on the predefined roles but you can restrict the access for a custom role to a specific product.

**Restriction**
You can add custom roles only if you are signed up to the Sophos Early Access Program.

**Super Admin**

Administrators with this role have access to everything in Sophos Central.

They can manage roles and role assignments. In addition, they can create, edit, assign, and delete custom roles.

There must be at least one administrator with the Super Admin role.

**Admin**

Administrators with this role have access to everything in Sophos Central.

They can’t manage roles and role assignments.

**Help Desk**

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

- Look at sensitive logs or reports.
- Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.
- Update the Sophos agent software on a computer.
- Scan computers.
- Modify co-branding.

They can’t see role management options. Also they can’t see some options, such as Edit buttons.

**Read-only**

Administrators with this role have read-only access for all settings in Sophos Central. They can also:
Sophos Central Admin

- Look at sensitive logs or reports.
- Receive alerts.

They can’t see role management options. Also they can’t see some options, such as Edit buttons.

User

Administrators with this role have no administration capabilities. They have access only to the Self Service Portal.

Related concepts

Administration Roles for Intercept X with EDR (page 367)
Administrators can do more if they have Intercept X with EDR.

Related tasks

Add administrators (page 368)
You assign administration roles to users using the Available Users list.

Remove administrators (page 371)
You can remove administrators. Removing an administration role from a user does not delete the user.

Administration role details
If you click a role on the Role Management page, its details are shown on a separate page.
The sections on that page include the following.

Permissions

This is the access level for a role. The options are Full, Help Desk, or Read-only.

Global Settings

These are the specialized capabilities for a role. The settings are:

- **Access sensitive logs & reports**: This option means that an administrator can view sensitive logs and reports; for example the Audit Logs.
- **Access policy management**: This option means that an administrator can change policy settings.
- **Access policy assignment**: This option means that an administrator can assign policies to users and devices.

Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details.
Administration Roles for Intercept X with EDR

Administrators can do more if they have Intercept X with EDR.

Super Admin and Admin

Administrators with these roles can also:

• View the intelligence report.
• Request the intelligence report
• Add items to the “Clean and Block” list.
• Remove items from the “Clean and Block” list.
• View blocked items.
• Request an on-demand threat case.
• View on-demand threat cases.
• Isolate and un-isolate devices.
• Request a forensic snapshot.
• Request a threat search.
• View a saved threat search.

Help Desk

Administrators with this role can also:

• View the intelligence report.
• Request the intelligence report.
• View blocked items.
• Request an on-demand threat case.
• View on-demand threat cases.
• Request a forensic snapshot.
• Request a threat search.
• View a saved threat search.

Read-only

Administrators with this role can also:

• View the intelligence report.
• View blocked items.
• View on-demand threat cases.
• View a saved threat search.
Related concepts
Administration Roles (page 365)

Add administrators

You assign administration roles to users using the Available Users list.
Existing administration roles, if any, are indicated next to the user's name.
A user can only have one assigned role.

For example if you add a Read-only administrator to the list of Help Desk administrators their assigned role will change to Help Desk administrator. They will no longer be a Read-only administrator.

To add an administrator:

1. In Settings, on the Role Management page, select the administrator role that you want to assign.
2. On the role details page, next to Role Members, click Edit.

   Note
   You can only see this option if you are a Super Admin.

3. In Edit Role Members, select a user in the Available Users list and use the picker arrows to add them to the Assigned Users list for the role. Select Save.

   Tip
   Enter a name or part of a name in the search box to filter the list of available users.

Add a custom role

You can add custom roles if you are a Super Admin.

Custom roles are based on the predefined roles. You can restrict the access for a custom role to a specific product. You can also create a role that allows an administrator to have full access to one product and read-only access to a second product.

Restriction
If a role doesn't have access to both Endpoint Protection and Server Protection (in some cases Encryption as well), the shared settings are read-only.

The shared settings are:
- Tamper protection
- Allowed applications
- Website management
- Proxy configuration
- Blocked item
- Bandwidth usage (Encryption access required)
- HTTPS updating
- DLP rules
To create a custom role:

1. In Settings, on the Role Management page, select Add role.
2. Give the custom role a name and a description.
3. Select the Base role you want to use as the basis for the custom role.
   For example, if you choose Help Desk as the Base role, administrators with the custom role have Help Desk permissions.
4. Choose the product and access type you want the role to have.
   For example, you create a custom role called Endpoint Help Desk. This custom role uses Read-only as its Base role and Endpoint Protection as its selected product with an access type of Help Desk.
   This custom role allows any administrators assigned to this role to access Endpoint Protection with Help Desk permissions.
   a) Choose more than one product, if required.
      You can choose different access types for different products.
      For example you can create a custom role that has Help Desk access permissions for Endpoint Protection and Read-only access for Mobile. You can set the permissions for all other products to None. This means that the custom role only has access to Endpoint Protection with Help Desk permissions and Mobile with Read-only permissions.
5. Choose the additional access and management options for the custom role.
   • Enable access to logs & reports.
   • Enable policy management (add, edit, and delete).
   • Enable policy assignment to users, device, etc.. (turn policies on and off; and add users, user groups, devices and device groups to existing policies).
   For example, this allows a Super Admin to add these permissions to a Read-only or Help Desk role. You can also use these options to reduce the permissions for an Admin role. For example, you could prevent the custom role from managing policies.

   Note
   These additional options only apply to the selected products for the custom role.

   The additional options are the same for all products and access types for the custom role.
6. Select Save.

You can now assign this role to administrators.

Related concepts
Administration Roles (page 365)

Related tasks
Delete custom role (page 370)
You can delete custom roles if you are a Super Admin.
Remove administrators (page 371)
You can remove administrators. Removing an administration role from a user does not delete the user.

**Change roles**

You can change the assigned roles for administrators if you are a Super Admin.
You can change roles for multiple administrators at the same time.

**Restriction**

You can't change roles for administrators who are currently signed in.

To change roles:

1. In **Settings**, on the **Role Management** page, select the administrator role that you want to assign to other administrators. For example, select a read-only administrator role if you want to assign that role to other administrators.
2. On the role details page, next to **Role Members**, click **Edit**.

**Note**

You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, add users from the **Available Users** list or remove users from the **Assigned Users** list. Select **Save**.

**Tip**

Enter a name or part of a name in the search box to filter the list of available users.

**Delete custom role**

You can delete custom roles if you are a Super Admin.
You can only delete custom roles. You can't delete roles that have administrators assigned to them. You must change their role first.

1. In **Settings**, on the **Role Management** page, select the role you want to remove and select **Delete**.
   
   To select a role, click anywhere in the row apart from the name.
   
2. Select **Delete** to confirm role deletion.

**Related concepts**

Administration Roles (page 365)

**Related tasks**

Add a custom role (page 368)
You can add custom roles if you are a Super Admin.

Change roles (page 370)
You can change the assigned roles for administrators if you are a Super Admin.

Remove administrators (page 371)
You can remove administrators. Removing an administration role from a user does not delete the user.

**Remove administrators**

You can remove administrators. Removing an administration role from a user does not delete the user.

**Note**

You cannot delete a user who has an assigned administration role. You must remove the role from the user before deleting the user.

To delete administrators:

1. In **Settings**, on the **Role Management** page, select the administrator role from which you want to remove users.
2. On the role details page, next to **Role Members**, click **Edit**.

   **Note**

   You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, select a user in the **Assigned Users** list and use the picker arrows to remove them.

   **Tip**

   Enter a name or part of a name in the search box to filter the list of assigned users.

---

**6.6.3 Tamper Protection**

You can enable or disable tamper protection for all your servers and users’ computers.

To do this, in **Settings**, open the **Tamper Protection** page.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:

- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
- Disable tamper protection.
- Uninstall the Sophos agent software.

**Manage tamper protection for a specific device**

You can change the tamper protection settings for a specific device or server.

Open the device’s details page and look under **Tamper Protection**. There you can do as follows:

- View the password.
- Generate a new password.
- Temporarily disable tamper protection for that device.
Recover tamper protection passwords

You can recover the tamper protection passwords of devices that you’ve recently deleted.
You might need to do this so that you can uninstall Sophos software that is still on those devices.

6.6.4 API Token Management

You can generate and manage the API token used for secure access to the Security Information and Event Management (SIEM) Integration API. This enables you to pull new event and alert data from Sophos Central. For further information, click the knowledge base article link provided on the page.

To add a token:
1. In Settings, open the API Token Management page.
2. Click Add Token.
3. Give the token a name and click Save.
   This generates the API token. The token is valid for a year.
Click Renew to extend the validity of the token.
Click Delete to remove the token.

6.6.5 API credentials

You can manage and add credentials for Sophos Central Admin.

Note
The first time you click API credentials you must read and accept the terms and conditions of use.

To add credentials, do the following:
1. Click Add Credential and give the credential details.
   This generates the credential, together with a Client ID and a Client Secret.
2. Copy the Client ID and Client Secret.

   Note
   You can only see the Client Secret once.

To delete an API credential, select it in API credentials and click Delete.

6.6.6 Website Management

This page is not available if you do not have a Web Control or Web Gateway license.
Note
If an option is locked, global settings have been applied by your partner or Enterprise administrator.

You can extend the website filtering provided by Sophos Central. For more information on how Sophos filters websites see Sophos Web Security and Control Test Site.

In Settings, on the Website Management page, you can use a website list to:

- Control websites not in one of the Sophos categories.
- Tag websites to put them in groups, which are like custom categories. You can then use policies to control these websites for certain users.
- Override the Sophos category for a site. This changes that site’s category for all your users.

Note
If you think Sophos has put a website in the wrong category, you can ask us to change it. To do this, see Open a Support Case. We suggest you try this instead of overriding the category.

To add a site to the website list:
1. Click Add in the upper right of the page.
   The Add Website Customization dialog is displayed.
2. Enter sites.
   Entries in the website list can be single URLs, full domains, TLDs, IP addresses, CIDR ranges, or even top level domains.

   Note
   Managing websites using IP addresses only controls browser-based access. It does not block other applications or interact with rules for a local firewall.

3. Select Enable Category Override if you want to associate a specific category with the sites you have entered. Then select a Category.
4. Select Enable Tags to associate a tag with the sites you have entered. Then type a tag name.
   Tags can be used when creating web control policies for endpoint computers or servers. See the Log web control events section in Web Control Policy.
5. Enter text in the Comments text box.
   It can be helpful to include information about tags you have created and categories you have overridden for troubleshooting policy issues in the future.
6. Click Save.
   Your entry will be added to the website list.

You can also edit entries in the list or delete them.

To edit an entry, click the edit icon . The icon is on the right of the entry.
To delete an entry, select the checkbox to the left of the entry and click Delete.

Related concepts
Server Web Control Policy (page 354)
6.6.7 Global Exclusions

You can exclude files, websites and applications from scanning for threats.

Introduction

You use exclusions to tune the detection behavior of Sophos Central.

Related tasks

Exploit Mitigation Exclusions (page 117)
You can exclude applications from protection against security exploits.

Related reference

Website exclusions (page 116)
You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

Process exclusions (Windows) (page 116)
You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

Malicious Network Traffic Prevention (IPS) (Windows) exclusions (page 120)
You can exclude specific network traffic from inspection.

Device isolation exclusions (Windows) (page 117)
You can allow isolated devices to have limited communications with other devices.

Windows Scanning Exclusions: Wildcards and Variables (page 110)
When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

macOS Scanning Exclusions (page 112)
You can add scanning exclusions for macOS workstations.

Virtual Server Scanning Exclusions: Wildcards (page 114)
Virtual Server exclusions let you exclude items from scanning on Windows guest VMs that are protected by a Sophos security VM.

Related information

Sophos Threat Center

Exclusions

Global exclusions apply to all your users (and their devices) and servers.

If you want exclusions to apply only to certain users or servers, use policy exclusions instead.

You can set up the following types of exclusion:

- Exclude files or folders from scanning.
  - If you exclude files from scanning, we'll still check the excluded items for exploits.
- Exclude from checking any process that runs from an application.
- Exclude websites from checking.
- Exclude applications from protection against security exploits.
- Exclude applications that are normally detected as spyware and previously detected exploits from scanning and detection.
- Exclude previously detected malicious behavior exploits. This is only available if you are signed up to the Early Access Program.

You can also use exclusions to allow isolated devices to communicate with other devices under restrictions. This feature is available if you have Intercept X Advanced with EDR.

**Warning**
Think carefully before you add global exclusions because doing so may reduce your protection.

Can’t edit the exclusions?

If an option is locked global settings have been applied by your partner or Enterprise administrator. You can still stop detecting applications, exploits and ransomware from events.

**Exploit exclusions**

If you exclude files from scanning, we'll still check the excluded items for exploits. If you want exclusions from exploit checking, do as follows:

- To stop checking for an exploit that has been detected, use a **Detected Exploits** exclusion.
- To exclude certain applications from checking, use Exploit Mitigation Exclusions.
- To stop checking for a malicious behavior exploit that has been detected, use a Behavioral Protection exclusion.

**Set up exclusions**

You can exclude files, websites and applications from scanning for threats.

To set exclusions:

1. Go to **Global Exclusions**.
2. Click **Add Exclusion**.
   The **Add Exclusion** dialog is displayed.
3. In the **Exclusion Type** drop-down list select what you want to exclude.
4. Specify the item or items you want to exclude.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File or folder (Windows)</strong></td>
<td>You can exclude a drive, folder or file by full path. You can use the wildcard * for file name or extension but <em>.</em> is not valid.</td>
</tr>
<tr>
<td><strong>File or folder (Mac/Linux)</strong></td>
<td>You can exclude a folder or file. You can use the wildcards ? and *.</td>
</tr>
<tr>
<td><strong>File or folder (Sophos Security VM)</strong></td>
<td>On Windows guest VMs protected by a Sophos security VM, you can exclude a drive,</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>folder or file by full path. You can use the</td>
<td>folder or file by full path. You can use the wildcards * and ? but only for file names.</td>
</tr>
<tr>
<td>wildcards * and ? but only for file names.</td>
<td></td>
</tr>
<tr>
<td><strong>Process (Windows)</strong></td>
<td>You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process). If possible, enter the full path from the application.</td>
</tr>
<tr>
<td><strong>Website (Windows/Mac)</strong></td>
<td>You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.</td>
</tr>
<tr>
<td><strong>Potentially Unwanted Application</strong> (Windows/Mac)</td>
<td>You can exclude applications that are normally detected as spyware. Specify the exclusion using the same name under which it was detected by the system. Find more information about PUAs in the Sophos Threat Center.</td>
</tr>
<tr>
<td><strong>Detected Exploits (Windows/Mac)</strong></td>
<td>You can exclude any exploit that has already been detected. We’ll no longer detect it for the affected application and no longer block the application.</td>
</tr>
<tr>
<td><strong>Device isolation (Windows)</strong></td>
<td>You can allow isolated devices to have limited communications with other devices. Choose whether isolated devices will use outbound or inbound communications, or both. You can then restrict communications.</td>
</tr>
<tr>
<td><strong>Malicious Network Traffic Prevention (IPS)</strong> (Windows)</td>
<td>You can exclude specific network traffic from inspection. Choose whether to exclude outbound or inbound traffic. Then specify the address or ports the traffic uses.</td>
</tr>
<tr>
<td><strong>Exploit Mitigation (Windows)</strong></td>
<td>You can exclude applications from protection against security exploits. For example, you might want to exclude an application that is incorrectly detected as a threat until the problem has been resolved.</td>
</tr>
<tr>
<td><strong>AMSI Protection (Windows)</strong></td>
<td>You can exclude a drive, folder or file by full path. Code in this location is not scanned. You can use the wildcard * for file name or extension.</td>
</tr>
<tr>
<td><strong>Behavioral Protection (Windows)</strong></td>
<td>You can exclude applications from protection against behavioral exploits.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For example, you might want to exclude an application that has been incorrectly detected as behaving maliciously.</td>
</tr>
<tr>
<td></td>
<td>You can't edit these exclusions after you create them.</td>
</tr>
<tr>
<td></td>
<td>This option is only available if you are signed up to the Early Access Program.</td>
</tr>
</tbody>
</table>

5. For File or folder exclusions, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.

6. Click **Add** or **Add Another**. The exclusion is added to the scanning exclusions list.

To edit an exclusion later, click its name in the exclusions list, enter new settings and click **Update**.

### 6.6.8 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

**Set the bandwidth used**

In **Settings**, on the **Bandwidth Usage** page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.

This helps to ensure that updating does not cause computers to run slowly.

You can specify a custom bandwidth or unlimited bandwidth.

**Note**

This setting is for Windows computers only.

**Note**

This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos. To save bandwidth in this case, see **Manage Update Caches and Message Relays**.

**Related concepts**

- **Create or Edit a Policy** (page 334)
  You can create or edit a policy as follows.
- **Manage Update Caches and Message Relays** (page 380)

### 6.6.9 HTTPS updating

Your computers and servers can get their Sophos updates via HTTPS. We recommend that you use HTTPS for greater security.

To use HTTPS updating:
1. Go to **Settings > HTTPS Updating**.
2. Turn on **HTTPS Updating**.

### 6.6.10 Multi-factor authentication

If you're a Super Admin, you can make some or all of the Sophos Central admins sign in with multi-factor authentication.

#### Introduction

Using multi-factor authentication means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos or Google Authenticator, SMS or email authentication to sign in.

Multi-factor authentication is turned on by default for newly created Sophos Central accounts.

This page tells you how to do the following:

- Set up multi-factor authentication.
- Sign in with multi-factor authentication for the first time.
- Add another method for multi-factor authentication.
- Sign in with email authentication if you don't have Sophos or Google Authenticator.
- Reset an admin's sign-in details, for example if they lose their phone.
- Turn off multi-factor authentication for an admin.

#### Set up multi-factor authentication

If you're a Super Admin, you can choose how your administrators sign in.

To set up multi-factor authentication, do as follows:

1. Go to **Settings > Multi-factor Authentication (MFA)**.
2. Choose how you want admins to sign in:
   - **No MFA needed**.
   - **All admins need MFA**. This is the default for new accounts.
   - **Select admins who will need MFA**. This lets you select individual admins.
3. If you choose **Select admins who will need MFA**, a user list is displayed. Click **Add admins** (on the right of the screen). Move admins to the **Assigned Users** list and click **Add**.
4. Click **Save**.

When admins next sign in, they are prompted to set up a new method of authentication.

#### Sign in with multi-factor authentication for the first time

The first time you sign in with MFA, do as follows:

1. At the sign-in screen, enter your user ID (email address) and password.
   
   A **Set Up Your Login Information** dialog explains that signing in needs additional authentication.
2. In the next dialog:
a) Enter the security code that has been sent to you in an email.
b) Create a 4-digit PIN. This enables you to use email as an authentication method.
3. In the next dialog, choose authentication type.
4. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
   You also need to enter a security code to verify a device if you have chosen SMS as your authentication type.
   Sophos Central Admin opens.
   The next time you sign in, you only need to enter a code from Sophos or Google Authenticator when prompted.

Add another authentication option for multi-factor authentication

You can set up multiple authentication options for a Sophos Central Admin account.
You can authenticate with SMS and Sophos or Google Authenticator.
You must have an authentication option already set up.
To set up another authentication option, do as follows:
1. Sign in to Sophos Central Admin.
2. Click your account name and click Manage Login Settings.
3. Click Create New Method.
4. Choose another authentication method.
5. Click Next.
6. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
7. To confirm that the new method has been added, click your account name and click Manage Login Settings.
   An additional authentication method has been added.

Sign in with email authentication

If you don't have access to Sophos or Google Authenticator, you can sign in with email authentication instead.
1. At the sign-in screen, enter the user ID (email address) and password.
2. In Verify Your Login, click Choose Another Method.
3. In Pick Your Challenge, click the email option.
   An email is sent to you.
4. Open the email and find the security code.
5. In Verify Your Login, enter the security code and your 4-digit PIN.

You'll be asked for the security code and PIN each time you sign in from now on, until you switch back to using Sophos or Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can allow them to set up their sign-in again.
1. On the People page, under Users, find the user and click their name to open their details.
2. In the user details, on the left of the screen, you’ll see their MFA status and settings. Click Reset and confirm that you want to do a reset.

The next time the admin tries to sign in, they’ll need to go through the setup steps again.

**Turn off multi-factor authentication**

If you’re a Super Admin, you can turn off multi-factor authentication for an administrator.

To turn off multi-factor authentication, do as follows:

1. Go to **Settings > Multi-factor Authentication (MFA).**
2. Click **Select admins who will need MFA.**
3. Click **Add admins.**
4. Move the administrator from the **Assigned Users** list and to the **Available Users** list.
5. Click **Add.**
6. Click **Save.**

**6.6.11 Manage Update Caches and Message Relays**

This saves you bandwidth, as updates are downloaded only once, by the server.

You can also enable computers to communicate with Sophos Central through a message relay on a server on your network.

A message relay server must also have an update cache set up on it.

This help page tells you how caches and relays work and how you set them up.

**Tip**

Computers can get the latest Sophos agent from a cache the first time you run the Sophos installer on them. You need to set up your caches before installation. If you have endpoints that can’t connect to Sophos directly, you also need to set up your update caches as message relays.

**Note**

If you use the **Reject network connections** feature (for customers with Sophos XG Firewall), it could prevent a cache server from delivering updates. To avoid this, see **Reject network connections**.

**How caches and relays work**

When you set up a cache (and optionally relay) on a server, Sophos Central does as follows:

- Installs Sophos caching software (and relay software).
- Fetches updates from Sophos and puts them in a cache.
- Automatically configures computers in your network to update from a cache (and use a relay).

You can also assign computers to use a specific cache or relay.

Using caches doesn't affect how often or when computers are updated.
Computers that can use caches and relays

You can install caches and relays on Windows Server 2008 or later (2008 R2 for relays).

The following computers can use caches or relays:

- Windows 7 and later (including servers), Macs and Linux computers can use a cache.
- Windows 7 and later (including servers) and Linux computers can use a relay.

Set up a cache/relay

You can set up a cache and a relay at the same time, or a cache only. You can also set up a relay on a server that already has a cache.

Before you set up a cache or a relay, ensure that:

- The server is running Windows Server 2008 or later.
- The server has at least 5GB free disk space.
- Port 8190 and 8191 are available and accessible to computers that will update from the cache and use the relays.

  The installers will open ports 8190 and 8191 in Windows Firewall. When Update Cache or Message Relay are uninstalled, the ports are closed again.

If you use the Reject network connections feature (for customers with Sophos XG Firewall), you might need to add the server to the exclusions. See Reject network connections.

To set up a cache or a relay:

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. In the filter above the table, click the drop-down arrow and select Cache Capable Servers to see which servers are suitable for a cache and a relay. If you have already set up a cache on some servers, to hide them from view, select Servers without Update Cache. If you want to set up a relay on a server with a cache, select Servers with Update Cache.
3. Select the server or servers where you want to set up a cache or relay.

Sophos Central automatically configures computers in your network to use a cache or relay. You can also manually assign computers to use a specific cache or relay.

Assign computers to a cache/relay

You can manually assign computers to use a specific cache or relay.

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. For the server on which the cache or relay is installed, click the link displaying the number of computers using the Update Cache or Message Relay, in the Updated from cache column or the Using Relay column, respectively.
3. Click Manual assignment.
4. Select the computers.
5. Click Save.
See which computers use caches and relays

On the Manage Update Caches and Message Relays page you can view which servers have update caches and message relays. You can see how many computers are using them as caches or relays and the activity of the update caches.

Click a server to see the details of the computers using its update cache or message relay.

Remove a cache/relay

**Note**
If you want to remove a cache that has computers manually assigned to it you must reassign them first.

When you remove a cache, Sophos Central does as follows:

- Uninstalls caching software, removes the cache of downloaded updates, and closes port 8191 in Windows Firewall.
- Also uninstalls the message relay software (if installed) and closes port 8190 in Windows Firewall.
- Reconfigures computers that update from this server to update from another update cache, if you have one.
- Reconfigures computers that use the relay to use another message relay, if you have one.

If you remove all your caches, computers will update directly from Sophos.

If you remove all of your message relays, computers will communicate directly with Sophos Central.

To remove a cache/relay:

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. In the filter above the table, click the drop-down arrow and select Servers with Update Cache to see which servers have a cache set up. You can also select Servers with Message Relay to see which servers have a message relay set up.
3. Select the server or servers you want to remove a cache/relay from.
4. Click Remove Cache/Relay.

**Related concepts**
Reject network connections (page 136)
You can configure devices to reject connections from other devices on the network that may be unsafe.

### 6.6.12 Allowed applications

On the Settings > Allowed Applications page you can see applications that you have allowed to run on your endpoint computers.

The page shows where the application was originally detected (if applicable) and how it was allowed.
About allowed applications

Our software detects threats that are previously unknown. However, it may sometimes identify an application as a threat, even though you know that it’s safe. When this happens, you can “allow” the application. This does as follows:

• Prevents this detection from happening again.
• Restores all copies that have been cleaned up (removed from computers).

Alternatively, you can allow an application in advance, so that it won’t be detected when you install it for users.

CAUTION
Think carefully before you allow applications because it reduces your protection.

Note
If an option is locked global settings have been applied by your partner or Enterprise administrator. You can still stop detecting applications, exploits and ransomware by going to the events list.

Allow an application that's been detected

Only allow an application if you know it's safe. For help deciding, see How to investigate and resolve a potential False Positive or Incorrect Detection.

To allow an application that Sophos has detected and removed, do as follows.

Note that:
• This allows the application for all computers and users.
• This allows the application to start, but we’ll still check it for threats, exploits and malicious behavior when it’s running.

1. Go to the Computers or Servers page, depending on where the application was detected.
2. Find the computer where the detection happened and click on it to view its details.
3. On the Events tab, find the detection event and click Details.
4. In the Event details dialog, look under Allow this application.
5. Select the method of allowing the application:
   • Certificate: This is recommended. It also allows other applications with the same certificate.
   • SHA-256: This allows this version of the application. However, if the application is updated, it could be detected again.
   • Path: This allows the application as long as it's installed in the path (location) shown. You can edit the path (now or later) and you can use variables if the application is installed in different locations on different computers.
6. Click Allow.
Edit the path for an allowed application

You can change the path that you specified when you allowed an application.
1. On the **Allowed Applications** page, find the application. The current path is shown in the details.
2. Click the edit icon (the pen) on the far right of the page.

3. In the **Edit path** dialog, enter the new path.
When you edit a path, details of the original detection (user, computer and path) are removed from the list.

Start detecting an application again

If you want Sophos to start detecting and removing an application again, you remove it from the **Allowed Applications** list.
Select the application and click **Remove** (in the upper right of the page).

**Related information**
**How to investigate and resolve a potential False Positive or Incorrect Detection**

### 6.6.13 Blocked items

This option is available if you have Intercept X Advanced with EDR.

On the **Settings > Blocked Items** page, you can block and clean up suspicious applications.
You can also see applications that you have blocked from running on your computers. You can see who blocked the application and why.

**About blocked applications**

You can block applications using their SHA-256 hash. This prevents suspicious applications from running on your computers.

You can only block applications. SHA-256 hashes for other items, or for files Sophos believes to be safe, are ignored.

When you block an application it's cleaned up on any devices it's already on.

You can also clean up and block applications when you investigate a threat case or review the results of a threat search.

**Block an application**

To block and clean up an application:

1. **Click Add**.
2. Enter the application's SHA-256 hash.
3. Enter a reason for blocking the application.
4. Click **Add**.
   - Click **Add Another** if you want to block more than one application.
5. When you have finished, click **Save** on the **Blocked Items** page.

This blocks the application on all computers and cleans it up on computers it’s already on.

### Remove an application from the block list

You can remove applications from the block list if you’ve decided that they aren’t suspicious. To do this:

1. Select the application in the list and click **Remove**.

### Related concepts

- **Threat Cases** (page 19)
- **Threat Searches** (page 31)
- **Admin Isolated Devices** (page 137)

### 6.6.14 Controlled updates

By default, computers get the latest Sophos product updates automatically. If you prefer, you can control how your computers update.

For example, you can stop updates on all computers during a busy period, or test updates on selected computers before they are rolled out to the rest of the network.

**Restriction**

You can control updates on Windows and Linux devices, but not Macs.

To control updates, go to **Settings > Controlled Updates**.

You have these options.

- **Pause Updates Now**
- **Pause Updates on a Set Date**
- **Control Updates Manually**

If updates are already controlled, you see a list of computers whose updates are controlled instead of these options.

**Note**

Computers still get automatic security updates to protect them against the latest threats.

You can go back to automatic updating at any time.

### Related concepts

- **Pause updates now** (page 386)
You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

Control updates manually (page 386)
You can control product updates manually.

Related tasks
Pause updates on a set date (page 386)
You can choose dates when you want to stop and restart product updates on all computers.

Pause updates now
You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

Restriction
You can control updates on Windows and Linux devices, but not Macs.

On the Settings > Controlled Updates page, click Pause Updates Now.
This stops automatic updates on all your computers immediately.
Updates start again automatically after 90 days.

Tip
If you want to start updates again earlier, click Resume Automatic Updating.

Pause updates on a set date
You can choose dates when you want to stop and restart product updates on all computers.
Automatic updates will stop for 90 days. Your computers will still get security updates.

Restriction
You can control updates on Windows and Linux devices, but not Macs.

1. On the Settings > Controlled Updates page, click Pause Updates on a Set Date.
2. Select a Pause date and a Restart date. Click Apply.
On the restart date, the computers will start updating automatically and get any updates that are available.

Tip
If you want to restart updating earlier, click Resume Automatic Updating.

Control updates manually
You can control product updates manually.

Restriction
You can control updates on Windows and Linux devices, but not Macs.
This stops automatic updating so that you can decide when to test new product versions and roll them out to your computers.

**Note**
Your computers will still get automatic security updates.

This Help topic tells you how to set up manual updating, and how to test and roll out updates.

### How to set up manual updating

On the **Settings > Controlled Updates** page, click **Control Updates Manually**.

**Note**
This stops all automatic updates. You are not asked for confirmation.

Initially, your situation is this:

- All your computers are on the **Newest (recommended)** version. They'll be shown as being on this version until Sophos issues a newer version.
- No computers will get any further updates until you update them.

Now you should set up test computers (if you want to).

#### Set up test computers

You can use test computers to try out new versions.

1. In the **Test computers** table, click **Add**.
2. Select computers from the **Available Computers** list.

You’re now ready to test updates and roll them out manually.

#### Test and roll out updates

When Sophos releases a new product version:

- You receive an email alert.
- Computers that were on the **Newest (recommended)** version are now shown as being on the **Oldest**.

In the table of versions, you can use the buttons in the **Action** column to update computers when you want to.

Typically, you would want to test the new version on selected computers and then roll it out to all the other computers.

In the **Action** column, next to Test Computers, click **Update test computers to newest version**.

When you’re ready to update all your other computers, in the **Action** column, next to **Non-test computers**, click **Update to match test computers**.

This forces the non-test computers to update at the time of the next automatic update, which by default is every 60 minutes. Note that this update will not follow any schedule that you’ve set in the Update Management policy for servers.
Why can I see a 'Previous' version now?

If Sophos releases another product update when you already have test computers on Newest (recommended) and the rest on Oldest:

• Test computers are now shown as being on the Previous version (the version that has just been replaced by a newer one).
• Non-test computers are on Oldest.

You can use an action button next to the test computers to Update test computers to newest version.

You can use an action button next to non-test computers to Update to match test computers.

What happens when a version expires?

Sophos product updates expire after 90 days. When the Oldest version expires, computers are forced to update as follows:

• If all computers are on Oldest, they resume automatic updating.

Note
If this happens, all computers get the newest version. You no longer control updates manually.

• If non-test computers are on Oldest, but test computers are on a newer version, the non-test computers are updated to the same version as the test computers.

6.6.15 Amazon Web Services Accounts

On the Settings > Connect AWS Accounts page, you can associate your AWS accounts with your Sophos Central account. This gives you improved management of Sophos Server Protection on AWS EC2 instances and S3 storage buckets.

When you add an AWS account on this page, Sophos Central will do as follows:

• Display AWS instance details.
• Remove terminated AWS instances from the list automatically.
• Let you apply server policies to Auto Scaling Groups.
• Assess the security of your S3 storage buckets.

To associate an AWS Account with Sophos Central:

1. Click Add (on the right of the page).
2. In the Connect to AWS dialog:
   a) Enter a Friendly Connection Name. This will be used to refer to the account in Sophos Central.
   b) Add a new IAM Role in your AWS console.
   c) Enter the Amazon Resource Name (ARN) for the AWS account that you want to connect to.
   d) Select Connect.
Sophos Central attempts to verify the credentials. While this happens, the account connection health shows a refresh icon.

3. When the page is refreshed, the account has either connected successfully, is still attempting connection or has failed.

   If the connection fails see Troubleshooting Sophos Central connections to AWS and Creating an IAM Role for Sophos Central.

When you have added the AWS account:

- AWS instances are listed on the Servers on AWS page, on the AWS Instances tab. Instances without a Sophos Agent installed are only shown here.
- AWS instances with a Sophos agent installed are listed on the Servers page.
- AWS Auto Scaling Groups are listed on the Server Groups page. The number of instances with an installed Sophos agent is indicated for the group.
- Policies assigned to AWS AutoScaling Groups are automatically assigned to instances that are in that group and have a Sophos agent installed.
- Your S3 storage buckets are assessed and assigned a health status.

6.6.16 Connect to Microsoft Azure

In Settings, on the Azure Active Directories page, you can associate your Azure Active Directories with your Sophos Central account. This gives you improved management of Sophos Server Protection on Azure Virtual Machines (VMs).

When you add Azure Active Directories on this page, Sophos Central will do as follows:

- Display Azure Active Directories’ details.
- Remove deleted VMs automatically.

To add an Azure Active Directory:

1. Click Add (on the right of the page).
2. In the Connect a directory dialog:
   a) Enter the Active Directory ID. You can find this in the Active Directory properties in the Azure Portal.
   b) Enter the Application ID from the Azure Portal along with the Application Secret Key that was set up with the App secret key.
   c) Click Add.

Sophos Central tries to verify the credentials. While this happens, the account Connection Status shows a refresh icon.

3. When the page is refreshed, you can see that the account has connected, is still trying to connect, or has failed.

   If the connection fails, see Troubleshooting Sophos Central connections to Azure.

When you have added the Azure Active Directory, the page shows:

- The Azure Active Directory along with any associated Subscriptions.
- Total VMs. Click on the total to see a list of VMs on the Azure VMs page.
- Sophos Agent Installed. The number of VMs protected with a Sophos Server Protection agent.

To modify or delete the connection to an Azure Active Directory, select the directory and use the buttons in the upper right of the page.
6.6.17 Live Response for servers

Turn on Live Response so that you can connect to servers to investigate and remediate possible security issues.

**Restriction**
You must be a Super Admin to configure Live Response.

1. Go to Settings > Server Protection > Live Response.
2. Turn on Allow Live Response connections to servers.
3. Click Save.

To turn on Live Response for computers, see Live Response for computers.

**Related tasks**
Live Response for computers (page 254)
Turn on Live Response so that you can connect to computers to investigate and remediate possible security issues.

6.6.18 Data Loss Prevention Rules

You use data loss prevention (DLP) rules to specify conditions to detect, actions to take, and any files to exclude from scanning.

You can use these rules across multiple policies.

There are two types of rules:

- **Content:** A content rule details the action to be taken if a user attempts to transfer data that matches the Content Control Lists (CCLs) in the rule to the specified destination.
  
  You use CCLs to match file content.

- **File:** A file rule details the action to be taken if a user tries to transfer a file with the specified file name or file type to the designated destination. For example, you can block the transfer of databases to removable storage devices.

When all the conditions listed in a rule are detected, the rule is matched, the action specified in the rule is followed and the event is logged.

If a file matches rules that specify different actions, the rule that specifies the most restrictive action is applied. For example:

- Rules that block file transfer take priority over the rules that allow file transfer on user acceptance.
- Rules that allow file transfer on user acceptance take priority over the rules that allow file transfer.

**Manage Data Loss Prevention Rules**

This page lists the existing DLP rules and allows you to manage their use across multiple policies. The name, source and type is shown for each rule.

You can create new custom rules, and search existing rules.

You can also filter rules by Rule Type.
Click on the name of a rule to edit it.

To view details of a rule, click Information.

To clone a rule, click Clone.
1. Give a name for the cloned rule.
2. Click Clone item. This adds the cloned rule to the list of rules.
3. You can then amend it by clicking its name in the list.

To export custom rules, click Export. This creates an xml file containing the rule definition.

To delete a rule, click Delete. Click Delete item to confirm deletion.

To import rules:
1. Click Import.
2. Select the XML file containing the rules.
3. Click Open.

The rules are added to the list.

Related concepts
Content Control Lists (page 393)
A Content Control List (CCL) describes a single type of data (for example, a postal address or social security number) or a combination of data types (for example, a project name near the term "confidential").

Related tasks
Create a Data Loss Prevention Rule (page 391)
Follow these instructions to create a DLP rule.

Create a Data Loss Prevention Rule

Follow these instructions to create a DLP rule.

There are two stages to creating a DLP rule; creation and configuration.

This stage sets up the rule type, the actions taken if the rule is triggered and whether you want to be alerted to the breaches of the rule.

To create a DLP rule:
1. Click Create New Rule.
2. Choose from New Content Rule or New File Rule.
3. Give the rule a Name and a Description.
4. Click Send me email alerts if you want notifying when the rule is breached.

Note
You will not get an alert in Sophos Central.

5. For a File rule, choose whether you want to match against a file name or a file type as the conditions for the rule. You will give the details when you configure the rule.
Note
Conditions are required for a Content rule and you cannot set the condition type.

6. Specify if you want to exclude by a file name or by file type. You will give the details when you configure the rule.
7. Specify the actions for the rule. Choose from:
   - Allow file transfer.
   - Allow transfer if user confirms.
   - Block transfer.
8. Click Next: Rule Configuration.

Related tasks
Configure a Data Loss Prevention Rule (page 392)
You can set up the conditions for monitored files, file types or destinations and the exclusions for a DLP rule.

Configure a Data Loss Prevention Rule
You can set up the conditions for monitored files, file types or destinations and the exclusions for a DLP rule.
You must have created a DLP rule.
The conditions you set depend on whether you are creating a File or Content rule.
1. Set up the rule conditions.
   a) To set up conditions for a content rule, click File Contains and select the CCLs you want to use.
      You can search the list of CCLs. You can filter the CCLs by Type, Source (choose from Sophos Labs or Custom), and Region. You can also create a new CCL.
   b) To set up conditions for a file rule, specify the file names or file types for the rule.
2. Click Destination is and set the destinations that the rule monitors.
   Destinations include devices (for example, removable storage devices, such as USB flash drives) and applications (for example, internet browsers and email clients).
3. Set the exclusion details for the rule.
4. Click Finish to create the rule.

Related tasks
Create a Data Loss Prevention Rule (page 391)
Follow these instructions to create a DLP rule.

6.6.19 Content Control Lists

A Content Control List (CCL) describes a single type of data (for example, a postal address or social security number) or a combination of data types (for example, a project name near the term "confidential").

This creates a definition for data that you want to protect. You can then use CCLs in data loss prevention rules to control what happens to this data.

To enable you to quickly define and roll out a data loss prevention policy, SophosLabs maintain a library of sensitive data definitions. SophosLabs CCLs provide expert definitions for common financial and personally identifiable data types, for example, credit card numbers, social security numbers, postal addresses, or email addresses. You cannot edit SophosLabs CCLs, but you can submit a request to Sophos to create a new one.

You can use SophosLabs CCLs in your rules, or create your own CCLs.

You can filter the CCLs.

You also can search the list of CCLs.

To view details of a CCL, click Information.

For each custom CCL you can also:

• Click on the name of a CCL to edit it.

• To export a CCL, click Export. This creates an XML file containing the definition for the CCL.

• To clone a CCL, click Clone. Give a name for the cloned CCL and click Clone item. This adds the cloned CCL to the list of CCLs. You can then edit it by clicking its name.

• To delete a CCL, click Delete. Click Delete item to confirm deletion.

You can also import CCLs:

1. Click Import.

2. Select the XML file containing the CCLs.

3. Click Open.

The CCLs are added to the list.

Create Custom Content Control List

Follow these instructions to create a custom CCL.

To create a custom CCL:

1. Click Add Custom Content Control List.

2. Give the CCL a Name and a Description.

3. Click Select tags and add the tags you want to use.

4. Specify the matching criteria for the CCL. Choose from:

• Any of these terms: Enter a term that you want to match in Terms and click Add to add another term.

• All of these terms: Enter a term that you want to match in Terms and click Add to add another term.
**Sophos Central Admin**

- **Exactly this phrase**: Enter the phrase that you want to match in Phrase. This option is not case sensitive.

- **Advanced Setup**: Use this option to set up an advanced expression.
  
  Set the **Trigger score**.
  
  This is the number of times the regular expression must be matched before the CCL is matched.

5. Click **Save** to create the CCL.

**Related tasks**

Set up an advanced expression (page 394)

Follow these instructions to set up an advanced expression for a custom CCL.

**Set up an advanced expression**

Follow these instructions to set up an advanced expression for a custom CCL.

You can only do this as part of creating a custom CCL.

Select **Advanced Setup** as the matching criteria to enter the details for an advanced expression:

1. Set the **Trigger score**.
   
   This is the number of times the regular expression must be matched before the CCL is matched.

2. Enter a Perl 5 regular expression in **Expression**.
   
   For a description of Perl 5 regular expressions, refer to Perl documentation or go to Perl syntax.

3. Set the **Score** for the CCL. This is the number that is added to the total score for a CCL when the regular expression is matched.

   **Note**
   
   The **Score** must match the **Trigger score**.

4. Set the **Max count**. This is the maximum number of matches for the regular expression that can be counted towards the total score.
   
   For example, an expression with a **Score** of 5 and a **Max count** of 2 can add the maximum of 10 to the total score of a CCL. If the expression is found 3 times, it still adds 10 to the total score.

5. Click **Add**.
   
   To delete an expression, click **Delete**

   X

   To edit an expression, click **Edit**

   
   Once you have finished your edits, click **Save**

   to save them.

6. Add more expressions, if required.

   Adding more expressions expands the scope of the CCL.

   For example, the following CCL is matched if Data Loss Prevention finds 2 matches of expression A or 1 match of expression A and 1 match of expression B, or 1 match of expression B and 5 matches of expression C.

394 Copyright © Sophos Limited
## Expression Score Max count

<table>
<thead>
<tr>
<th>Expression</th>
<th>Score</th>
<th>Max count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expression A</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Expression B</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Expression C</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

### Related tasks

- Create Custom Content Control List (page 393)
  Follow these instructions to create a custom CCL.

### Related information

- Perl syntax

## 6.7 Protect Devices

You can download Sophos installers and use them to protect your devices.

The installers you can see may depend on the license or licenses you have.

**Before you start, check which operating systems you can protect with Sophos Central:** see the Sophos Central page.

For more details, including what each product does, how you use the installers, and how Sophos Central registers devices and applies policies, read the other topics in this section.

### How to use installers

After downloading installers for workstations or servers, you can:

- Run the installer to protect the local computer.
- Transfer the installer to other computers and run it on them.
- Use automated software deployment tools such as System Center Configuration Manager (SCCM) to run the installer on large numbers of computers.

### How to find out which data center stores your account

To find out which data center stores your Sophos Central account data, do as follows:

1. Go to **Protect Devices**.
2. Under **Endpoint Protection** or **Server Protection**, hover the mouse pointer over any of the installer download links.
   
   The data center address is shown in the lower-left corner of the browser:

   ![Final Gateway](https://spr-cloudstation-us-east-2.prodhydra.sophos.com/api/download/f0ae9d21d7792e053ab89e932e1ac1d/SophosSetup.exe)

3. The address shows the geographical location of the data center:
Sophos Central Admin

<table>
<thead>
<tr>
<th>Address</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://api-cloudstation-us-east-2.prod.hydra.sophos.com">https://api-cloudstation-us-east-2.prod.hydra.sophos.com</a></td>
<td>US east</td>
</tr>
<tr>
<td><a href="https://api-cloudstation-eu-central-1prod.hydra.sophos.com">https://api-cloudstation-eu-central-1prod.hydra.sophos.com</a></td>
<td>EU central</td>
</tr>
</tbody>
</table>

Related concepts
Server Protection (page 170)
You install a Server Protection agent on servers to protect them against malware, risky file types and websites, and malicious network traffic.

Virtual Environment Protection (page 172)
Sophos for Virtual Environments lets you protect your virtual machines (VMs) and manage them from Sophos Central.

Related tasks
Server Protection on Microsoft Azure (page 171)
You can protect Azure VMs with Intercept X Advanced for Server as you create them.

Related information
Sophos Central page

6.7.1 Server Protection

You install a Server Protection agent on servers to protect them against malware, risky file types and websites, and malicious network traffic.

To protect a server, download the installer for your operating system and run it on the server.

Download and run the Windows installer

1. Go to Protect Devices.
2. Click Download Windows Server Installer.
3. Go to the Downloads folder and run the installer.

Download and run the Linux EDR or Linux MTR installer

If you have a license for Linux EDR (Endpoint Detection and Response) or Linux MTR (Managed Threat Response), you see a link to the appropriate installer.

1. Go to Protect Devices.
2. To download the installer from your browser, click Download Linux MTR Installer or Download Linux EDR Installer.
   Alternatively, to download the installer from a command line or script, do as follows:
   a) Right-click the installer link and copy the link address.
b) On the Linux server, at a command prompt or in a script, use `wget` with the link address:

```
wget Linux installer link
```

c) Move the installer to the `Downloads` directory.

3. Run the installer as follows:
   a) Change to the `Downloads` directory.
   b) Change the file permissions to include “execute”:

```
chmod +x SophosSetup.sh
```

c) Run the installer:

```
./SophosSetup.sh
```

If you are not signed in as root, run the installer with the `sudo` command:

```
sudo ./SophosSetup.sh
```

### Download and run the Linux Server installer

The Linux Server installer provides anti-virus protection. It doesn't provide the more advanced features of Linux EDR or Linux MTR.

1. Go to Protect Devices.

2. To download the installer from your browser, click Download Linux Server Installer.

   Alternatively, to download the installer from a command line or script, do as follows:

   a) Right-click Download Linux Server Installer and copy the link address.

   b) On the Linux server, at a command prompt or in a script, use `wget` with the link address:

```
wget Linux installer link
```

c) Move the installer to the `Downloads` directory.

3. Run the installer as follows:

   a) Change to the `Downloads` directory.

   b) Change the file permissions to include “execute”:

```
chmod +x SophosInstall.sh
```

c) Run the installer:

```
./SophosInstall.sh
```

If you are not signed in as root, run the installer with the `sudo` command:

```
sudo ./SophosInstall.sh
```

### What happens when you protect a server

When you protect a server:

- The server is added to the Servers list in Sophos Central.
- Default policies are applied to the server.
6.7.2 Server Protection on Microsoft Azure

You can protect Azure VMs with Intercept X Advanced for Server as you create them. This involves downloading a custom extension script and using it.

1. Go to Protect Devices.
2. Find Server Protection on Microsoft Azure.
3. Click Get your VM extension script. Then click Download Script.
   You’ll need an API token so that the script can find and access the installer. If you don’t have a token, we’ll create one for you.
4. Click Deploy Server Protection to a new Azure VM. This displays a link to an article on how to use a custom extension script.
5. Follow the steps in the article to deploy the new VM.

6.7.3 Virtual Environment Protection

Sophos for Virtual Environments lets you protect your virtual machines (VMs) and manage them from Sophos Central.

To set up protection for VMs, you do as follows:
• Install Sophos Security VM on your host. This provides central anti-virus scanning for guest VMs.
• Install Sophos Guest VM Agent on your guest VMs. This is required for each guest VM that you want to protect. The agent enables communication between the guest VM and Sophos Security VM as well as automatic cleanup of threats.

Download the installer

Go to Protect Devices.

To get started, you only need to download the Sophos Security VM installer. You’ll be prompted to get the installer for the agent later.

Select the installer for the environment you want to protect: Hyper-V and/or ESXi.

We recommend you read the startup guide.

Note
If you’ve been managing Sophos for Virtual Environments from Sophos Enterprise Console until now, or if you’re migrating from Sophos Anti-Virus for vShield, see “Migrate to Sophos for Virtual Environments” in the startup guide.

What happens after installation

After you install Sophos Security VM on your host:
• This instance of Sophos Security VM is added to the Servers list in Sophos Central.
• Server policies are applied to the security VM (by default, these are the Base policies).
• Remember you must have installed Sophos Guest VM Agent on each guest VM and checked it is connected.
7 Wireless

Configure and manage access points, wireless networks, and devices.

Network requirements

To use any access point with Sophos Wireless, the access point has to be able to communicate with Sophos Central. Therefore, the following requirements have to be fulfilled:

- DHCP and DNS servers are configured to provide an IP address to the access point and answer its DNS requests (IPv4 only).
- Access point can reach Sophos Central without requiring a VLAN to be configured on the access point for this connection.
- Communication on ports 443, 123, 80 to any internet server is possible.
- There is no HTTPS proxy on the communication path.

Warning

Don’t disconnect your access point from the power outlet when the lights blink rapidly. This means that a firmware flash is in progress. For example, a firmware flash after a scheduled firmware update.

7.1 Wireless Dashboard

See the most important information about your wireless environment at a glance.

Network Security

Click on the circles in the legend to include or exclude information from a graph.

You can see information on your access points.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>Access point is up and working.</td>
</tr>
<tr>
<td>Issues</td>
<td>Access point is up but has some problems.</td>
</tr>
<tr>
<td>Critical</td>
<td>Access point is up but is in a critical state.</td>
</tr>
<tr>
<td>Offline</td>
<td>Access point is offline.</td>
</tr>
<tr>
<td>Unconfigured</td>
<td>Access point is up but isn't configured.</td>
</tr>
</tbody>
</table>

You can review threats.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>Network that belongs to your account.</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Network that doesn't belong to your account.</td>
</tr>
</tbody>
</table>
### Rogue
Untrusted network that is connected to your secured wired access point network.

### SSID Impersonate
Network that spoofs the network name of your access point.

### BSSID Impersonate
Network that spoofs the hardware address of your access point.

### Evil Twin
Network that spoofs the network name and the hardware address of your access point.

### Advanced Impersonate
Network that spoofs the network name and unique protection code of your access point.

### Adhoc
A peer-to-peer network.

You can see the security status of your devices using Security Heartbeat.

<table>
<thead>
<tr>
<th>Client at risk</th>
<th>Active malware detected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client might be at risk</td>
<td>Potentially unwanted application (PUA) or inactive malware detected.</td>
</tr>
<tr>
<td>Client is protected</td>
<td>No malware detected.</td>
</tr>
<tr>
<td>Missing Security Heartbeat™</td>
<td>Device is connected but the endpoint is not sending heartbeat.</td>
</tr>
<tr>
<td>No Security Heartbeat™</td>
<td>Sophos Endpoint or Sophos Mobile Control is not installed.</td>
</tr>
</tbody>
</table>

### Device Profiles
You can view all, managed or unmanaged devices.

**Tip**
Device type filtering is currently a beta feature. You must turn it on by clicking **Device Classification and Visibility** in **Settings**. You can then see the device profiles on this page.

### Most Recent Alerts
- **All**: Shows all alerts.
- **Warnings**: Shows access points that are offline or not broadcasting.
- **Info**: Shows updates or information.

Click **Details** for more information.
Devices
Number of devices connected.
Click Details for more information.

Usage Insight
Traffic generated by the wireless devices connected to access points.
Click Details for more information.

7.2 Wireless Alerts
View access point generated wireless alerts.

High
Access Point has bad health: The load on the access point is too high. There are too many devices connected. Check you have enough access points to cover the area.

Medium
Access Point is offline: The access point has no internet connection, no power, or has experienced a software error. You can try restarting. Restarts can resolve software errors.
Access Point is not broadcasting any network: The access point isn't configured. To configure the access point click Wireless > Access Points.
Access Point command done: The restart is complete.
Restarting the access point may resolve the following alerts:
• Access Point configuration failed
• Access Points failed to update to the new firmware
If the problem continues, contact Sophos Support. They will need remote access to investigate the issue. Go to Wireless > Settings > Diagnostics > Remote Login to Access Points for Sophos Support to allow remote access.

Low
Access Point will be updated with new firmware: Wireless will be turned off for approximately 5 minutes.
All Access Points will be updated with new firmware: Wireless will be turned off for approximately 5 minutes.
Access Point has been successfully updated with new firmware
All Access Points have been successfully updated
7.3 Devices

View information about the connected devices.

Connected devices are listed with name, MAC address, IP address, vendor, access point, SSID, Security Heartbeat, connection speed, and band.

Security Heartbeat categorizes devices by their security status. Devices are protected by Sophos Endpoint Protection or Sophos Mobile as appropriate. Administrators can set up rules to manage the devices. If these rules are broken the software reports the threat and the device's security heartbeat status reflects this.

You can also search for a specific device by using name, MAC address, IP address, or vendor details.

You can filter devices by selecting Online, Offline, and Online and Offline.

**Client at risk**: Indicates that active malware or ransomware has been found. This blocks all internet traffic and only traffic from the secured browsing environment (walled garden or safe URL list) is allowed.

---

**Note**

If an endpoint or mobile is in the red (high risk) state, you need to refresh the browser twice to access the walled garden. You can also download or update Sophos Anti-Virus from here.

**No Security Heartbeat™**: Indicates that Sophos Endpoint or Sophos Mobile Control is not installed on the listed devices.

Security Heartbeat categorizes devices based on the following:

**Client might be at risk**: Indicates that a potentially unwanted application (PUA) or inactive malware has been detected. All traffic is allowed.

**Client is protected**: Indicates that the endpoint is healthy and all traffic is allowed.

**Missing Security Heartbeat™**: (applicable only for endpoint) Indicates that the device is connected but the endpoint has not been sending heartbeat for 90 seconds.

---

**Device Details**

Click on a device to see more information.

- **Static details**: Shows MAC address, current access point, current site, current network, signal quality, band, state, hostname, IP address, and vendor details.
- **Usage details**: Shows the device's external and total traffic.
- **Signal quality**: Shows signal strength over a period of time.
- **Connectivity**: Shows connectivity details over a period of time.

---

7.4 Usage Insight

View traffic from your devices in categories such as search engines, social media, or advertisements.

Click on a category to obtain more information in the category details list.
To show the traffic generated by users, in categories, you must switch on **Usage Insight**.

**Related concepts**

**Settings** (page 430)
The Settings pages are used to specify security settings that apply to all your access points.

## 7.5 Wireless Diagnostics

Diagnose and view events, system logs, audit logs, and capture packets for troubleshooting.

You can review all wireless related events.

Check the audit log to see all activities monitored by Sophos Central.

You can capture wireless packets and syslog data generated from access points.

**Related concepts**

**Events** (page 404)
View access point generated wireless events.

**Audit Logs** (page 47)
You can view and export a record of all activities that are monitored by Sophos Central using the Audit Log report.

**Packet Capture** (page 407)
Capture wireless packets from remote access points to diagnose and troubleshoot network issues.

**Syslog** (page 409)
Capture syslog data from access points to debug device’s connection-related issues.

### 7.5.1 Events

View access point generated wireless events.

You can filter events and generate reports.

The events list shows you the severity, time the event occurred and the type of event.

There are the following event types.

**High**: Events with high severity are generated when the connected device load on access points is high or an administrative action is required.

**Medium**: Events with medium severity are generated when access points are not configured, offline, or have latency issues.

**Low**: Events with low severity give information about access points. No action required.

Events that require action are also displayed on the **Alerts** page. After you have taken action or ignored the alert they are no longer displayed but events are retained in the event list.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Events</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Access point has bad health.</td>
<td>Number of connected devices is high and needs to be reduced.</td>
</tr>
<tr>
<td>Severity</td>
<td>Events</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Security Heartbeat is enabled in Sophos XG Firewall and Sophos Central Wireless.</td>
<td>Use either Sophos XG Firewall or Sophos Central to turn on Security Heartbeat.</td>
</tr>
<tr>
<td></td>
<td>Ethernet LAN speed is low.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS gateway is unreachable.</td>
<td>Attempt to reach the DNS server failed.</td>
</tr>
<tr>
<td>Medium</td>
<td>Access point is offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access point is not broadcasting any network.</td>
<td>Access point is online but is not broadcasting data packets.</td>
</tr>
<tr>
<td></td>
<td>Access points failed to update to the new firmware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access point configuration failed.</td>
<td>Access point is sending an hostapd event.</td>
</tr>
<tr>
<td></td>
<td>Access point has a DNS timeout.</td>
<td>Access point attempted to reach the DNS server but failed.</td>
</tr>
<tr>
<td></td>
<td>Access point has high data packet retries</td>
<td>Access point is retrying with more data packets.</td>
</tr>
<tr>
<td></td>
<td>Access point has high DNS latency.</td>
<td>Access point is taking more than 250 milliseconds to establish connection.</td>
</tr>
<tr>
<td></td>
<td>RADIUS server is unreachable.</td>
<td>Attempt to reach the RADIUS server failed.</td>
</tr>
<tr>
<td></td>
<td>Access Point channel has been changed.</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Access point will be updated with new firmware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access point has been successfully updated with new firmware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All access points will be updated with new firmware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All access points have been successfully updated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access point command done.</td>
<td>All commands are complete.</td>
</tr>
</tbody>
</table>
### Severity | Events | Description
---|---|---
| | Ethernet LAN speed is high. |
| | RADIUS server is reachable. |

You can export the event report in a CSV (comma separated value) or a PDF file. You can export the current view or for the past 90 days.

You can filter events by the access point name.

Use **From** and **To** to filter information. You can view events that occurred in the past 90 days or less.

**Related concepts**
- Wireless Alerts (page 11)
  View access point generated wireless alerts.

## 7.5.2 Audit Logs

You can view and export a record of all activities that are monitored by Sophos Central using the Audit Log report.

To find the Audit Log reports, go to the **Logs & Reports** page and select **Audit Logs**.

All activities for the past 7 days are shown in the Audit Log by default. You can view all activities for up to 90 days. You can export an Audit Log report containing a record of all activities.

The Audit Log lists the following for each activity:

- **Date**: Date and time when the activity or change occurred.
- **Modified by**: The Sophos Central Admin account that made the change or signed in.
- **Item type**: The type of activity or change. For example Users and Groups were changed.
- **Item modified**: What was added, changed or deleted. For example the name of a new user that was added.
- **Description**: More details about the activity or change. For example a successful authentication by a Sophos Central account.
- **IP address**: The IP Address from where activity or change was carried out.

You can filter the Audit Log by date range and by search results. You must click **Update** to apply the filters.

- **From** and **To**: Use these options to set the date range for the activities you want to view. You can select any date within the last 90 days. The date range works with the **Search** field and the Audit Log shows the items related to your selected date range and search term. If you do not enter a search term the Audit Log shows all activities for your selected date range.

- **Search**: There is a limited search available. The Audit Log shows the items related to your search term and the selected date range. If you do not set a date range the Audit Log shows the items related to your search term for the last 7 days, by default. You can search by:
  - **IP address**: Shows all changes and activity from an IP Address over the selected date range.
  - **Modified By**: Shows all changes and actions made by a Sophos Central account over the selected date range.
Export

You can export an Audit Log report that contains a record of activities for a selected date range or the last 90 days. You can filter the Audit Log before exporting. Search filtering applies to all export options. The date range does not.

To export an audit report:

1. Filter the Audit Log, if required. Click Update to apply the filters to the Audit Log.
2. Click Export on the right-hand side of the Audit Log page and choose an option from the drop-down list.
   - CSV of current view or PDF of current view: Exports the current view as a comma separated file or as a PDF file. If you select one of these options all currently selected filters are applied to the exported file.
   - CSV of past 90 days or PDF of past 90 days: Exports activities from the past 90 days as a comma separated file or as a PDF file. If you select one of these options only search filtering is applied to the exported file.
3. Review the audit report to check that it contains the information you require.
4. Change the audit report name.
   Audit reports are exported as audit.csv or audit.pdf.

7.5.3 Packet Capture

Capture wireless packets from remote access points to diagnose and troubleshoot network issues.

The access point acts as a distributed sniffer, and captures packets on the configured channel and configured channel width from remote access points. If you have configured Autochannel, the access points will capture packets on the channel picked by Autochannel.

The access point can’t capture its own transmitted packets. It can only capture received (rx) packets.

Table 1: Packet capture across all access points

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AP15C</td>
<td>All packets received by the access point in the channel are captured.</td>
<td>Packets intended for the access point and broadcasts are captured.</td>
<td>All packets received by the access point in the channel are captured.</td>
<td>All packets received by the access point in the channel are captured.</td>
</tr>
<tr>
<td>AP100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The access point uses TaZmen Sniffer Protocol (TZSP) as an encapsulation protocol that runs over User Datagram Protocol (UDP). The access point encapsulates the wireless packets with TZSP and sends it to the configured server (running Wireshark) on UDP port 37008.

If the UDP port 37008 is not open, an Internet Control Message Protocol (ICMP) packet with the error "destination port unreachable" is generated for every packet sent by the access point.
You can use a display filter in your capture tool such as Wireshark to see only wireless packets. For example, you can use `wlan or tzsp && !(icmp)` as a filter.

You can search access points either by name or serial number. You can also filter access points based on the sites. By default, all the access points are displayed.

**Configuration Prerequisites**

Before you start you need to check the following:

- Make sure the IP address configured for the packet capture is reachable.
- Install Wireshark on the server or PC.
- The server might have multiple interfaces and so run Wireshark on the interface which has the configured IP address.
- To check only the wireless traffic sent by access point, apply the filter `wlan or tzsp && !(icmp)`.
- You can save packets on the server using **Save** in Wireshark.

**Configuration**

Use the configured server IP address and port number to start capturing network packets. You need to set the following options.

**Status**: You can capture packets only when the access point status is green.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Access point is online.</td>
</tr>
<tr>
<td>🟦</td>
<td>Access point is offline.</td>
</tr>
</tbody>
</table>

**Access Point Name**: Access point hostname.

**Serial Number**: Serial number of the access point.

**Client MAC**: (Optional). Access point will capture packets from this MAC address.

**Server IP**: Access point sends packets to this server on UDP port 37008. You must run a packet capture tool such as Wireshark on the server to see the packets. We recommend that you use a server in the same subnet as the access point. If the server is in a different subnet or in the cloud, you must allow the UDP port in the firewall.

**Duration (sec)**: Time interval for the packet capture.

**Action**: Start or stop the packet capture.

**Status**: Status of the packet capture.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started</td>
<td>Packet capture has started.</td>
</tr>
<tr>
<td>Completed</td>
<td>Packet capture is complete.</td>
</tr>
</tbody>
</table>
### Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Supported</td>
<td>The firmware on the access point doesn’t support packet capture.</td>
</tr>
<tr>
<td>Server not reachable</td>
<td>Access point is unable to reach the IP address.</td>
</tr>
</tbody>
</table>

### Related concepts

- **Access Point Details** *(page 414)*
  Configure, restart, or manage your access points.

- **Frequently asked questions** *(page 410)*
  These are the most frequently asked questions about packet capture and syslog data capture.

### 7.5.4 Syslog

Capture syslog data from access points to debug device’s connection-related issues.

The syslog data also captures system anomalies over a period of time.

You must have a configured syslog server in place. You can only configure a syslog server for access points that are online in Sophos Central.

You can configure syslog servers at each access point.

We recommend that you don’t setup a syslog server for more than two access points to avoid data intermixing. This keeps debugging simple.

### Configuration Prerequisites

Before you start you need to check the following:

- Install a syslog server on the PC or server. There are various syslog servers available for different operating systems.
- Make sure you allow ICMP on the syslog server. When you start sending logs to the syslog server, the APX tries to ping the server. If the server is not responding, no UDP packets are sent.
- By default, syslog runs on UDP port 514. If you have configured syslog to listen on a different port, add this information to Sophos Central.
- Make sure the access point is connected to the syslog server.
- The logs are stored under the location configured in the syslog software. You can use a graphical user interface or a text editor to view logs.
- Make sure that you have enough space on the syslog server to store new logs.

### Configuration

Use the configured server IP address and port number to capture syslog data. You can use **Start** to capture system generated logs for a specific access point. You need to set the following options.

**Status**: Indicates whether the access point is offline or online. You can capture syslog data only when the access point status is green.
**Icon** | **Status**
---|---
[ ] | Access point is online.
[ ] | Access point is offline.

**Access Point Name**: Access point hostname.

**Serial Number**: Serial number of the access point.

**Server IP**: Access point sends packets to this server. You must run a syslog analyzer tool on the server to see the packets.

**Server Port**: Access points send packets to this port on the server.

**Action**: Start or stop the syslog data capture.

**Status**: Status of the syslog data capture.

<table>
<thead>
<tr>
<th><strong>Status</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Started</td>
<td>Syslog data capture has started.</td>
</tr>
<tr>
<td>Completed</td>
<td>Syslog data capture is complete.</td>
</tr>
<tr>
<td>Server not reachable</td>
<td>Access point is unable to reach the IP address provided by the user.</td>
</tr>
</tbody>
</table>

**Related concepts**

Frequently asked questions (page 410)

These are the most frequently asked questions about packet capture and syslog data capture.

### 7.5.5 Frequently asked questions

These are the most frequently asked questions about packet capture and syslog data capture.

**Packet capture**

<table>
<thead>
<tr>
<th><strong>Questions</strong></th>
<th><strong>Solution</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Why don't I see packets in Wireshark?</td>
<td>Check if the server IP is configured properly.</td>
</tr>
<tr>
<td></td>
<td>Check if Wireshark is running on the right interface.</td>
</tr>
<tr>
<td></td>
<td>Check if there is an incorrect filter in the Wireshark.</td>
</tr>
<tr>
<td></td>
<td>Check if the access point is offline while running the packet capture.</td>
</tr>
<tr>
<td></td>
<td>Check if firewall allows port 37008 if the server IP is in different subnet.</td>
</tr>
</tbody>
</table>
### Questions

<table>
<thead>
<tr>
<th>Question</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>What happens when Wireshark isn't running on the server?</td>
<td>The access point will still send the packets to configured server. You must start Wireshark to see the packets.</td>
</tr>
<tr>
<td>Can I capture packets on multiple access points?</td>
<td>Yes, you can capture packets on multiple access points.</td>
</tr>
<tr>
<td>Can I capture packets without assigning SSIDs.</td>
<td>Yes, you can capture packets without assigning SSIDs. The access point will capture packets either on the manually configured channel or on the channel picked by <strong>Autochannel</strong>.</td>
</tr>
<tr>
<td>Is Packet capture feature supported on all access point firmwares?</td>
<td>Packet capture is supported on v2.1.0-1 or later.</td>
</tr>
<tr>
<td>Why can't I start packet capture when access point status is gray?</td>
<td>The access point is offline. You cannot capture packets when the access point is offline.</td>
</tr>
</tbody>
</table>

### Syslog data capture

<table>
<thead>
<tr>
<th>Question</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why I cannot see any syslog data in my configured syslog server?</td>
<td>Check if your syslog server is reachable from the access point.</td>
</tr>
<tr>
<td>Why has my syslog server stopped receiving data?</td>
<td>Check if the access point is up and running. Also, check the connectivity between the access point and the syslog server.</td>
</tr>
</tbody>
</table>

### 7.6 Access points

View all wireless access points and their details.

A wireless access point (WAP) is a networking hardware device that allows a Wi-Fi enabled device to connect to a wired network. To configure an access point from Sophos Central, you need to connect it to the internet and register it on Sophos Central using the serial number available on the package.

The registered access points are listed with the following details:

- **Name**: Access point name.
- **MAC**: Access point's MAC address.
- **Serial number**: Access point's serial number.
- **Internal IP**: Access point's assigned internal IP address.
- **Model**: Access point model.
- **Access point state**: Access point's status such as online or offline.
• **Workload**: Connected device load on an access point. The workload is calculated based on memory and CPU usage. Memory usage up to 60% or CPU usage up to 50% is shown as green. Memory usage of 60% to 80% or CPU usage 50% to 80% is shown as yellow. Memory or CPU usage above 80% is shown as red.

• **Band**: Configured radio bands on an access point.

• **Mode**: Channel operating mode such as autochannel (AO), dynamic channel (AC), or manual channel (M).

• **Channels**: Displays configured and operating channels. It is displayed as configured channel (operating channel). The operating channel might differ if radar is detected on the configured Dynamic Frequency Selection (DFS) channel.

• **Firmware**: Firmware version installed on an access point.

• **Uptime**: Displays the uptime for an access point.

• **Mesh Role**: Displays the role of access point in a mesh network. An access point can either have a root role or a mesh role. You can view the role, radio band (used for the mesh network), and the last four letters of the serial number.

**Note**

You need the ports 443 (HTTPS), 80 (HTTP) and 123 (NTP) open to all internet servers. Otherwise the access points are not able to connect.

The country setting of an access point regulates the available channels to be compliant with the local law. For more information on access points, see the operating instructions.

### Register an access point

You can register access points individually or in bulk.

You can register a single access point. To do this click **Register** and enter the serial number. The access point is validated after you click **Register** again.

To register multiple access points you need a comma separated value (CSV) file containing serial numbers in the first column. Each row must have a unique serial number. To do this click **Register**, click **Bulk Provisioning** and upload your CSV file. The access points are validated.

You can then enter and save the hostname. The access points are displayed in the list once registration is complete.

### LED behavior

**Table 2: LED behavior with APX series**

<table>
<thead>
<tr>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Access point is turned off.</td>
</tr>
<tr>
<td>Green (blinking during restart)</td>
<td>Restart is taking place.</td>
</tr>
<tr>
<td></td>
<td>Configuration is being pushed from the cloud.</td>
</tr>
</tbody>
</table>
LED

<table>
<thead>
<tr>
<th>Color (solid)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Normal operation. After configuration has been pushed.</td>
</tr>
<tr>
<td>Red</td>
<td>Ethernet is unplugged. Cloud is not reachable. Hardware reset is taking place (hardware reset button has been pressed for 15-20 seconds).</td>
</tr>
<tr>
<td>Amber (solid APX 320 only)</td>
<td>Restart is taking place (hardware reset button has been pressed for 3-5 seconds).</td>
</tr>
</tbody>
</table>

Related information

Access point operating instructions

7.6.1 Supported Access Points

View all supported access points with details.

Dedicated access points

<table>
<thead>
<tr>
<th>Name</th>
<th>Standards</th>
<th>Band</th>
<th>Band for Mesh Networks</th>
<th>FCC regulatory domain (mainly US)</th>
<th>ETSI regulatory domain (mainly Europe)</th>
<th>Client capacity per radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP 15</td>
<td>802.11b/g/n</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>Channels 1-11</td>
<td>Channels 1-13</td>
<td>120</td>
</tr>
<tr>
<td>AP 15C</td>
<td>802.11b/g/n</td>
<td>2.4 /5 GHz dual-band or single-radio</td>
<td>2.4 GHz</td>
<td>Channels 1-11, 36-48, 149-165</td>
<td>Channels 1-13, 36-48</td>
<td>120</td>
</tr>
<tr>
<td>AP 55</td>
<td>802.11a/b/g/n/ac</td>
<td>2.4 /5 GHz dual-band or dual-radio</td>
<td>2.4 GHz and 5 GHz</td>
<td>Channels 1-11, 36-64, 100-140, 149-165</td>
<td>Channels 1-13, 36-64, 100-116, 132-140</td>
<td>120</td>
</tr>
<tr>
<td>AP 55C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP 100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP 100C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>APX 120</td>
<td>802.11a/b/g/n/ac</td>
<td>2.4 /5 GHz dual-band or dual-radio</td>
<td>2.4 GHz and 5 GHz</td>
<td>Channels 1-11, 36-64, 100-140, 149-165</td>
<td>Channels 1-13, 36-64, 100-116, 132-140</td>
<td>120</td>
</tr>
</tbody>
</table>
### 7.6.2 Access Point Details

Configure, restart, or manage your access points.

**Restart access point**: Click to restart your access point. Any configuration will be kept.
**Name:** The default name of an access point is its serial number. You can change the name.

**Bands:** Depending on the access point, 2.4 GHz and 5 GHz are available. Configure the bands separately. For AP15 and APX 320 models, you can also configure the 5 GHz from the 2.4 GHz band.

**TX Power**: Controls the power of outbound transmissions from the router to the antenna. Adjusting the power can help with coverage and data rate. Reducing the power means reducing the operating distance. For example, if you want to minimize the interference, you need to reduce the power. This reduces the operating distance and interference. Default: 100 %.

<table>
<thead>
<tr>
<th>TX Power (%)</th>
<th>Absolute TX Power - RSSI (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 %</td>
<td>0 dBm</td>
</tr>
<tr>
<td>75 %</td>
<td>1 dBm</td>
</tr>
<tr>
<td>50 %</td>
<td>3 dBm</td>
</tr>
<tr>
<td>25 %</td>
<td>6 dBm</td>
</tr>
<tr>
<td>10 %</td>
<td>10 dBm</td>
</tr>
</tbody>
</table>

**Table 3: TX power reference**

**Allow mesh:** Enables the access point to create a mesh network. It is available only when you select the 5 GHz frequency band on the first radio. Available only for APX 320 and AP15C.

**Channel width:** The lower the channel width, the higher the number of individual channels. With more channels, more data can be transmitted, which results in faster wireless speed. If there are lots of neighboring wireless networks, a higher channel width may cause too much interference. Default: 20 MHz.

**Autochannel:** This will automatically select the least used channel for transmission.

**Dynamic Background Channel Selection:** The access point automatically changes the channel on a regular basis to optimize the network.

**MU-MIMO Support:** Enable multi-user, multiple-input, multiple-output technology to establish communication between multiple devices simultaneously. For devices that do not support MU-MIMO, MIMO feature is available. Also, if you disable MU-MIMO, the MIMO feature is restored.

**Assign SSIDs:** Use this option to make separate SSIDs accessible in different parts of your building. For example, a company SSID that is available in your offices and a guest SSID available in the public parts of your building. Each access point can have a maximum of eight SSIDs per band.

**Tip**
You can also add an access point to a network when you create an SSID.

**Airtime Fairness:** Access points distribute transmission airtime equally to all devices according to their traffic needs.

We recommend that you turn on this option if you have several devices connected to your network or if you offer public wireless.

Disabling the option makes sense if you want to have better performance on a slower device.

**Comment:** You can save additional information about your access point.
7.7 SSIDs

Configure and manage your Service Set Identifiers (SSIDs).

An SSID is a unique identifier for a wireless network. It differentiates one WLAN from another. Multiple access points within a network can use the same SSID to broadcast the same network. You can also have multiple SSIDs on an access point. This allows you to have SSIDs with different bands or other configurations like separate guest networks or a mesh network.

7.7.1 Settings

Configure, assign, and save your settings.

Configure basic settings for your SSID.

**SSID**: Enter a name. SSIDs are case-sensitive and must satisfy the following criteria:

- A minimum of 1 printable character.
- A maximum of 32 printable characters.
- No space at the beginning or end of name.

We recommend that you use ASCII printable characters to avoid display errors on client devices.

**Encryption Mode**: Select the encryption mode. When using an enterprise authentication method, you also need to configure a Remote Authentication Dial-In User Service (RADIUS) server for your local network.

We recommend that you use WPA2 instead of WPA as it doesn't use TKIP (Temporal Key Integrity Protocol).

**Encryption Algorithm**: Select the encryption algorithm. The default algorithm is Advanced Encryption Standard (AES).

We recommended that you use this as it is a quick and strong cipher and is widely accepted.

**Passphrase**: Enter a passphrase to protect the SSID from unauthorized access. Your passphrase can have up to 63 ASCII printable characters and it must have at least 8 characters.

**Frequency Band**: Select the frequency band. The access points assigned to this SSID will transmit on the selected frequency band(s).

We recommend that you use the 5 GHz frequency band for Voice over IP (VoIP) communication. It has higher performance, lower latency, and less interference.

**Enable mesh mode**: You can create a mesh network between access points for a single hop. If you wish to disable the mesh network, you must delete the SSID.

**Note**

Only one mesh network per SSID is allowed.

Assign Network

Assign one or more access points to your SSID. Each access point can have a maximum of eight SSIDs per band.

**Multiple Access Points**: Assign the available and registered access points.
Add Access Points later: Assign the access points later by editing the SSID.

Save configuration

Save your basic settings.

**Enable SSID:** You can enable the SSID that you just created. If you wish to disable the SSID, deactivate after saving your configuration.

Related concepts

SSID advanced settings (page 420)
Configure security, backend authentication, client connection, quality of service (QoS), network availability, and captive portal.

Access points (page 411)
View all wireless access points and their details.

Mesh Networks (page 417)
View deployment scenarios for configuring access points as root, repeater, or bridge.

Related tasks

Create a Mesh Network (page 419)
Create a mesh network to form a WPA2-Personal network with a random passphrase.

Mesh Networks

View deployment scenarios for configuring access points as root, repeater, or bridge.

An access point which is configured to use the mesh network turns into a repeater and scans for the mesh network, if it fails to connect. If a mesh network is found, the access point joins it as a client. An access point can be configured as root, repeater (mesh), or bridge. The role of access points gets determined on the network.

We recommend that you set the root access point to 5 GHz and client to 2.4 GHz. The maximum throughput of a mesh client, configured with 5 GHz, gets reduced by 50% per hop. This happens because data packets sent to the access point are forwarded to other access points which adds up to the airtime.

Deployment possibilities

In mesh mode, you can configure multiple mesh (repeater) access points with one root access point. There can be multiple root access points. A mesh access point can broadcast the SSID from the root access point to cover a larger area without using cables.
A mesh network can also be used to bridge Ethernet networks without laying cables. To run a wireless bridge, you have to plug in your second Ethernet segment into the Ethernet interface of the mesh access point. The first Ethernet segment is the one on which the root access point connects to Sophos Central.

**Good to know**

There are some things you should know about mesh networks:

- You can create a mesh network only with Sophos access points.
- For setting up a mesh network, you must create a new SSID.
- You can have only one mesh SSID.
- At least one access point must have a LAN connection.
- Mesh access points must be on the same channel.
- Avoid using dynamic channel selection as channels of access points may differ after a restart.
- The mesh network may need up to five minutes to be available after configuration.
- There is no automatic takeover of the root access point. The connection to a mesh occurs during a boot.
- For APX access points, there is no need to specify the mesh role. If the mesh-enabled SSID is pushed to 2 APXs, the one with the existing ethernet connection becomes the root AP. Once the mesh-enabled SSIDs are pushed to the APXs, we recommend that you reboot them. During the boot sequence, if the AP has ethernet connectivity, then it becomes the root and the one without ethernet becomes the mesh client.
Mesh networks can only be created between access points of the same series. For example, APX access points can only create a mesh network with other APX access points.

Create a Mesh Network

Create a mesh network to form a WPA2-Personal network with a random passphrase.

A mesh network passphrase is shared among all access points that are configured to broadcast the mesh SSID. The mesh ID is not visible to the administrator. A mesh network can implement a wireless bridge or a wireless repeater.

1. Connect all access points you want to have in the mesh network to the required LAN network.
2. Register them under **Wireless > Access Points > Register**.
3. Ensure that the access points are connected to an SSID.
4. Set the same channel on all access points to the 5 GHz band.
   - You can set **Autochannel** but we recommend that you statically set a non-DFS channel to avoid connectivity issues or latency in forming a mesh network.
   - **Note**
     - Do not use **Dynamic Background Channel Selection**, as then the channel could change after a reboot.
5. Create a new SSID (**Wireless > SSIDs > Create**).
   - a) Enter a name for the **SSID**.
   - b) Select a frequency band.
     - **Note**
       - We recommend you to use the 5 GHz band when the access points are close as the throughput is higher. For longer distances between the access points you should use the 2.4 GHz band.
     - c) Click **Next** and assign the access points by selecting them in the list.
     - d) Go to **SSID > Basic Settings** and select **Enable mesh mode**.
     - e) Save your settings.
6. Navigate to the access points list and wait until the status of the access points is **up to date**.
7. Disconnect the mesh access point from the LAN network and place it at the intended location.
8. Reboot the access points (power off and on).

The mesh network is available after a few minutes. It is not visible to end users.

To disable the mesh network, delete the SSID.

**Related concepts**

- **Access Point Details** (page 414)
  - Configure, restart, or manage your access points.
- **Settings** (page 416)
  - Configure, assign, and save your settings.
- **Troubleshooting mesh networks** (page 420)
This tells you how to fix common issues with mesh networks.

**Troubleshooting mesh networks**

This tells you how to fix common issues with mesh networks.

If **Enable mesh mode** is not displayed create a new SSID.

If a second mesh SSID does not work. You can only have one SSID with mesh mode enabled.

The mesh network is not coming up. Try the following:

- Wait a few minutes for it to appear.
- Check if the Spanning Tree Protocol (STP) blocks your mesh configuration.
- Test the connection by broadcasting only mesh on the root access point and a visible SSID on the repeater access point. If it is visible, mesh works.

The mesh network is not visible to end users. This is normal behavior. Make it visible by creating a separate SSID and adding the same access points as to the mesh network.

The mesh network is not usable. Try the following:

- Check if you have at least two access points in the mesh network.
- Ensure that at least one access point is connected to the network via LAN (cable).
- Check if your mesh access points are on the same channel.
- Ensure that access points which are not part of the mesh network are on a different channel.

Not all the access points are showing in the mesh network. Try the following:

- Ensure that all access points got the configuration (had been connected via LAN until all configurations were saved and the access point was restarted)
- Ensure that the LAN cable of the repeater access point is unplugged.

**7.7.2 SSID advanced settings**

Configure security, backend authentication, client connection, quality of service (QoS), network availability, and captive portal.

**Security**

Define settings to make your network more secure.

**Synchronized Security**: Enable to ensure that clients with Sophos Endpoint Protection and Sophos Mobile Protection can communicate with Sophos Central Wireless access points. If Synchronized Security is enabled on both Sophos XG Firewall and Sophos Central Wireless, the settings on Sophos XG Firewall will take precedence.

To use this feature, you need to have an Endpoint Advanced Protection license for your endpoints. For mobile protection, go to **Mobile > Setup > System setup > Network Access Control**, and select **Sophos Wireless**.

**Note**

Available only for APX 320, APX 530, and APX 740.

**Security Heartbeat green**: Indicates that the endpoint is healthy and all traffic is allowed.
**Security Heartbeat yellow**: Indicates that a potentially unwanted application (PUA) or inactive malware has been detected. All traffic is allowed.

**Security Heartbeat red**: Indicates that active malware or ransomware has been detected or the access point is unable to receive Security Heartbeat messages from the endpoint’s Sophos Endpoint Services. The access point blocks all internet traffic. Only traffic from the secured browsing environment (walled garden or safe URLs list) is allowed.

**Sophos Mobile (UEM)**: Turned on by default. Allows heartbeat information to be sent from Sophos managed mobile devices. You can also manage policies for these devices in Sophos Central.

**Sophos Central Endpoint Protection**: Turn on if you want to manage endpoint policies in Sophos Central. Alternatively you can manage endpoint policies in XG Firewall.

**Restrict SSID to Sophos Managed Devices**: When an unmanaged device connects to the SSID, after authentication, we determine that the device is unmanaged and display a landing page, which you have to configure. The device is put behind a walled garden. The behavior of this device is similar to having a red security heartbeat status. The device is allowed to access only Sophos websites or those URLs and IPs that are on the allowed list.

A managed device is a mobile or endpoint device protected by Sophos.

When you enable this option the landing page configuration is shown. Enter the following information:

- **Page Title**
- **Welcome Text**
- **Message to appear**
- **Company logo**

**Whitelisted Domains**: Enter domains here that you still want clients to access, along with any .sophos.com domains, when they have a red **Synchronized Security** status. These domains will also be accessible by unmanaged devices if you have turned on **Restrict SSID to Sophos Managed Devices**. Both IP addresses and domain names are supported.

**Hidden SSID**: Hides the SSID for network scans. When hidden, the SSID is still available and you need to know the SSID name for a direct connection. Even if an SSID is hidden, you can assign the SSID to an access point.

**Note**
This is not a security feature. You still need to protect hidden SSIDs.

**Client isolation**: Blocks communication between clients within the same radio frequency. This is useful in a guest or hotspot network.

**MAC Filtering**: Provides minimal security by restricting Media Access Control (MAC) address connections.
- **None**: No restriction on MAC addresses.
- **Blocked List**: All MAC addresses are allowed except those that you enter here.
- **Allowed List**: All MAC addresses are prohibited except those that you enter here.

**Client Connection**

**LAN**: Bridges a wireless network onto the network of an access point. The wireless clients share the same IP address range.
**VLAN**: Directs the client traffic to specific VLANs. The uplink switch must be configured to accept VLAN packets.

**RADIUS VLAN Assignment**: Separates users without having multiple SSIDs. Available with encryption mode **WPA/WPA2 Enterprise**.

Users will be tagged to a VLAN provided by a RADIUS server. Traffic is untagged if the RADIUS server does not provide VLAN.

**Note**
IPv6 is blocked in SSIDs if dynamic VLAN is enabled. If IPv6 is not blocked, devices may end up with multiple IPv6 addresses and gateways from multiple VLANs.

**Enable Guest Network**: Enables a guest network. A guest network provides an isolated network for the clients with some traffic restrictions. Access points can have one guest network at a given time. The following modes are available:

- **Bridge Mode**: Uses the DHCP server from the same subnet.
  It filters all traffic and only allows communication to the gateway, DNS server, and external networks. You can add a guest network to an environment without VLAN and still have an isolation. As the DHCP server is still on your network, roaming between access points will work.

**Note**
By using VLAN for your guest network, you can have a separate guest VLAN additional to the guest network.

- **NAT Mode**: Uses the on-board DHCP server on the access point. This provides local isolated IPs to the guest network clients. Clients are unaware of the internal IP scheme.
  In NAT mode, a DNS server is optional for a client address. If a DNS address is not assigned to the client by the DNS server, they will be assigned the same DNS address as of the access point.
  Bridge mode has a higher throughput, whereas NAT mode has more isolation.

**Network Availability**
Define SSIDs which are only available for a certain time of a day or certain days in a week. The SSIDs are not visible in the meantime.

- **Always**: Select to make SSID available at all times.
- **Scheduled**: Select the weekdays and timeframes for the network to be available.

**Quality of Service**
Configure settings to optimize your network.

- **Multicast to unicast conversion**: Optimizes the multicast packets to unicast packets. The access point converts multicast packets to unicast packets individually for each client based on the Internet Group Management Protocol (IGMP).
  It works best when fewer clients are connected to one access point.
  The conversion to unicast is preferred for media streaming as it can operate at higher throughput rates.
**Proxy ARP**: Enables the access point to answer Address Resolution Protocol (ARP) requests intended for the connected wireless clients.

**Fast roaming**: Optimizes the roaming times when switching between different access points. SSIDs with WPA2 encryption use the IEEE 802.11r standard to reduce roaming times (with enterprise authentication). It applies when the same SSID is assigned to different access points. Clients also need to support the IEEE 802.11r standard.

**Keep broadcasting**: Ensures that the access point keeps broadcasting when it is not able to reconnect to Sophos Central after a restart. If this is turned on, clients will still be able to connect to the access point and (or) to the internet and the access point works with its old configuration.

**Note**
The SSID will be broadcasted in all cases of connection loss to Sophos Central, regardless if this function is turned on or not.

**Band Steering**: Distributes clients based on the load on two radio bands and the client's capability between the 2.4 GHz and 5 GHz bands. Dual-band capable wireless clients will be routed to 5 GHz, if possible, to improve the client experience. This is done by rejecting the initial association request sent by the client in the 2.4 GHz band. This will cause a dual-band client to then attempt to negotiate at 5 GHz. If it does not associate in the 5 GHz band, it will be marked as “steering unfriendly” and will not be routed again. If a client is too far away from the access point, routing will not be attempted. This prevents routing clients to 5 GHz when the range is usually less than in the 2.4 GHz band. Band Steering is done on a per access point level and will affect all SSIDs on that access point.

**Captive Portal**
Activate and configure a hotspot.

**Enable hotspot**: Turns the SSID into a hotspot. This allows cafés, hotels, or companies to provide time and traffic restricted internet access to guests.

**CAUTION**
In many countries, operating a public hotspot is subject to specific national laws, restricting access to websites of legally questionable content. For example, file sharing sites or extremist websites.

**Page Title**: You can define a title for the landing page. It is visible to the users when they accept terms of service.

**Welcome Text**: You can define welcome text for the landing page.

**Terms of Service**: Users have to accept the terms of service before authentication.

**Backend Authentication**: With this authentication type, users can authenticate via Remote Authentication Dial-In User Service (RADIUS).

**Note**
Backend authentication requires PAP (Password Authentication Protocol) policy on the RADIUS server. All user credentials transmitted to the RADIUS server will be encrypted with HTTPS by Sophos Central.

**Password schedule**: You can create a new password automatically on a fixed schedule. If the schedule is set to weekly or monthly, you can also select a weekday or week. The old password expires when the scheduled time is reached and current sessions are cut off. The new password is sent as a notification to the specified email addresses.
Voucher: With this hotspot type, vouchers with time limitations can be generated, printed, and given to customers. After entering the code, users can directly access the internet.

Social Login: You can allow your users to authenticate using their social media accounts. You can let them use their Facebook or Google accounts. To set up Google authentication, go to the Google Developer Console and get the Client ID and Secret for Google. Enter this information here. To set up Facebook authentication, go to Facebook Developer Account and get the Application ID and Secret for Facebook. Enter this information here.

To retrieve the Google client ID from the Google developer console you will need to do as follows:
1. Create a new project.
2. Go to the OAuth Consent screen and enter the application name. You can enter anything in this field. Then enter the authorized domain, which has to be "myapsophos.com".
3. Go to credentials > create credentials > OAuth client ID.
4. Choose application type as web application.
5. Under the restrictions, enter the authorized javascript origins and authorized redirect URIs as given below.
   Authorized JavaScript origins: https://www.myapsophos.com:8443
   Authorized redirect URIs: https://www.myapsophos.com:8443/hotspot.cgi

Note
If a user signs in with a social media account they are asked to accept the certificate and continue. They must click the Google button to do this.

Note
If a user authenticates with a social media account, we don't store personal information from that account.

Session Timeout: Restricts the users internet access time.
Re-Login Timeout: Enabling this will prevent the user from re-logging into the network for 24 hours from the time of initial connection to social login.

Note
A maximum of 8 devices can connect using the same email ID.

Redirect URL: You can define the URL to which users will be redirected from the landing page. Users can be redirected to the default website of the mobile device or a specific website of your choice. For example, your company page.

Related tasks
Create a hotspot (page 426)
Create a secured hotspot to generate a wireless node that provides internet and VPN access.
Create a voucher (page 428)
Create a voucher for the hotspot.
Create a guest network (page 425)
Create a guest network to allow clients to connect to the internet. A guest network is an isolated network that uses the same access point but has some traffic restrictions.

**Create a guest network**

Create a guest network to allow clients to connect to the internet. A guest network is an isolated network that uses the same access point but has some traffic restrictions.

You can either use an existing SSID or create a new SSID to enable a guest network. This procedure describes how to set up a guest network with an existing SSID.

1. Go to SSIDs and click the SSID for which you want to enable a guest network.
2. Go to Advanced Settings > Client Connection.
3. Choose the required connection type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>Bridges the client traffic into the same network the access point is connected to.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Bridges the client traffic into a specific VLAN where the client traffic is isolated from the rest of the network.</td>
</tr>
</tbody>
</table>

4. Click Enable Guest Network.
5. Choose the client addressing.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Mode</td>
<td>Clients receive DHCP leases from the customer's DHCP server either on same LAN or VLAN based on the connection type, LAN or VLAN. Clients are allowed to access the internet, but not the private IP addresses. Roaming between access points works flawlessly.</td>
</tr>
</tbody>
</table>
| NAT Mode     | Clients receive IP addresses from the DHCP server running on Access Point. The traffic is NATed to the LAN or VLAN based on the connection type, LAN or VLAN. Clients cannot communicate with each other, but can access the internet.  
**Primary DNS Server**: Specify the DNS server IP address to be used by clients when connected to the guest network.  
**Secondary DNS Server**: Specify the secondary DNS server IP address to be used by clients when connected to the guest network.  
If primary and secondary DNS server IP addresses are not specified, then clients receive Access Point's DNS server IP address. |
6. Save your settings.
7. Give the passphrase to guest network clients.

**Captive Portals and Hotspots**

View information on turning an access point into a hotspot.

Turning an access point into a hotspot allows you to provide time and traffic restricted internet access to guests. The hotspot feature restricts traffic which is allowed by the firewall. Ensure that a firewall rule exists which allows the traffic to be managed by the hotspots. We recommend that you test the traffic with the hotspot feature disabled. Enable the hotspots if the test is successful.

**CAUTION**

In many countries, operating a public hotspot is subject to specific national laws, restricting access to websites of legally questionable content (for example, file sharing sites, extremist websites). Legal regulations may require you to register your hotspot with the national regulatory body.

**Landing Page**

Sophos Central intercepts HTTP traffic and redirects users to a predefined page, the so-called hotspot or captive portal. There, users have to use one of the configured authentication methods before they can access the allowed networks, for example, the Internet. The landing page is the first page users will see after connecting to the hotspot.

**Create a hotspot**

Create a secured hotspot to generate a wireless node that provides internet and VPN access.

Ensure that you have an existing SSID that can be turned into a hotspot.

You need to set up authentication with Google and Facebook if you want to allow your users to use their social media accounts to authenticate themselves. You need to set this up in the Advanced Settings for the SSID.

You can create a hotspot with or without a voucher.

1. Click on an existing SSID (*Wireless > SSID*).
2. Go to *Advanced Settings > Captive Portal* and click *Enable hotspot*.
3. Enter the information you want to provide on the landing page.

   **Note**
   The hotspot can be customized using the template drop-down menu at the top of the page. When selecting a custom template you can upload a company logo and change background color. For more information please see *Customize hotspot*.

4. Select an authentication type to define how users can access the hotspot.

   **Note**
   It is more secure to use authentication.

5. Select *Custom URL* if you want to redirect users to a specific landing page after authentication.
6. Preview your customization if you want to.
7. Save your settings.
The hotspot is available after a few seconds.

**Troubleshooting**
The backend authentication fails:
- Check your server logs for anomalies.

HTTPS traffic is not redirected:
- HTTPS redirect for hotspot sign-in is not supported.

LED on the access point is amber:
- There is no connection from the access point to Sophos Central. Try to reconnect.

**Note**
Passwords and vouchers will not expire.

**Related concepts**
- **SSIDs** (page 416)
  Configure and manage your Service Set Identifiers (SSIDs).
- **Settings** (page 416)
  Configure, assign, and save your settings.
- **SSID advanced settings** (page 420)
  Configure security, backend authentication, client connection, quality of service (QoS), network availability, and captive portal.

**Related tasks**
- **Customize hotspot** (page 427)
The below steps describe how to create a custom template for wifi hotspots.

**Related information**
- Google Developer Console
- Facebook Developer Account

**Customize hotspot**
The below steps describe how to create a custom template for wifi hotspots.

You must have already created an SSID and enabled the hotspot on it.

You can create a custom hotspot to show your company logo and change background color.

1. Click on an existing SSID (**Wireless > SSID**).
2. Click the template drop down at the top of the page and select **Custom**. The customization preview page appears.

   **Note**
   The default template is used unless it is customized.

3. Under company logo select the folder icon to upload a logo file from your local computer.
4. To change the background color, either select a color from the menu or enter the hex code in the field to the right of the menu.

Note
Maximum file size is 1MB and the recommended dimensions of the image are 200x200 pixels.

5. Save your settings.

Create a voucher

Create a voucher for the hotspot.

To create a voucher:
1. Click on the newly created hotspot (Wireless > SSID).
2. Go to Advanced Settings > Captive Portal and click Create Voucher. The voucher creation dialog opens.
3. Define the following:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter a name</td>
</tr>
<tr>
<td>Access time</td>
<td>Use the start and end date to set a time period for access. You can also make it always accessible.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Set the timezone.</td>
</tr>
<tr>
<td>Amount of vouchers</td>
<td>Set the number of vouchers.</td>
</tr>
<tr>
<td>Valid for</td>
<td>Set the period the voucher is valid for.</td>
</tr>
</tbody>
</table>

4. Save your settings.
The voucher appears in the list.
5. Click Show PDF and save the file or print it directly.
Hand the voucher out to users.

7.8 Sites

Specify locations to easily manage your access points.

Create multiple floor plans for sites to see where the best places are to mount access points or to get an overview of where access points are installed.
Neighborhood Networks

The **Neighborhood Networks** tab shows every network within the range of the selected site's access points. This also includes networks which are not provided by Sophos Central. You can filter the scanned networks to show All, Rogue, Trusted, Untrusted, Advanced Impersonate, Evil Twin, BSSID Impersonate, SSID Impersonate, or Adhoc. Use the following options:

**Scan:** You can scan all online networks in the supported channels of an access point. Devices connected to the network will experience network interruption for three to five minutes during a scan.

**Select Classification:** You can customize or mark a scanned network as Rogue, Trusted, Untrusted, Advanced Impersonate, Evil Twin, BSSID Impersonate, SSID Impersonate, or Adhoc.

**Clear Custom Classification** You can clear or undo the custom classification.

**Neighborhood SSIDs** are classified as shown in the table.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted</td>
<td>Network that belongs to your account.</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Network that doesn't belong to your account.</td>
</tr>
<tr>
<td>Rogue</td>
<td>Untrusted network that is connected to your secured wired access point network.</td>
</tr>
<tr>
<td>SSID Impersonate</td>
<td>Network that spoofs the network name of your access point.</td>
</tr>
<tr>
<td>BSSID Impersonate</td>
<td>Network that spoofs the hardware address of your access point.</td>
</tr>
<tr>
<td>Evil Twin</td>
<td>Network that spoofs the network name and the hardware address of your access point.</td>
</tr>
<tr>
<td>Advanced Impersonate</td>
<td>Network that spoofs the network name and unique protection code of your access point.</td>
</tr>
<tr>
<td>Adhoc</td>
<td>A peer-to-peer network.</td>
</tr>
</tbody>
</table>

Every access point scans for neighborhood SSIDs once during the startup process. For example, when you restart an access point or install a new firmware update. If you activate dynamic background channel selection, access points scan for neighborhood SSIDs on a regular basis.

To show neighborhood SSIDs, you must enable **Rogue Access Point detection** in **Settings**.

**Floor plans**

Use floor plans to set detailed locations for access points. Upload a floor plan as an image file (PDF, PNG, JPEG, BMP, GIF or WBMP) and position the access points.
7.8.1 Create a Site

Create a site to add your access point.

To create a site:
1. Go to Sites and click Create.
2. Type the location.
   Sophos Central uses Google maps. You must enter a real address.
3. Select access points you want to add to the site.
   An access point can be added to one site only.
4. Save your settings.

7.8.2 Create a Floorplan

Create a floorplan to place your access points.

To create a floorplan:
1. Go to Sites and click on a site.
2. Click Create a floor.
3. Add a floorplan.
   The floorplan must be an image file (PDF, PNG, JPEG, BMP, GIF or WBMP).
4. Upload the floorplan to Sophos Central.
5. Crop the image or proceed without changes.
6. Assign the dimensions.
   Measured dimensions are required to correctly show the network range of access points.
7. Drag and drop an access point from the available tab and place it on the floorplan.
   Delete access points from the floorplan in the placed tab.
8. Save your settings.

The floorplan with the positions of the access points has been added to the site.

7.9 Settings

The Settings pages are used to specify security settings that apply to all your access points.

7.9.1 Wireless System Settings

Manage the firmware and wireless system settings.

**Sophos Unique Customer ID:** You can show or hide your unique ID. This ID helps Sophos Support if you have an issue.

**Firmware Update:** You can update the firmware version immediately or schedule it on a daily, weekly, or monthly basis. To schedule an update, ensure that you convert your local time to the UTC standard.
**Update Version** `<version>` is displayed if a new version is available. If you update, all access points under your account will be updated to the selected version. You can view the information about the installed firmware version, release, and installation date.

**Note**
During an update, access points along with the configured SSIDs are temporarily unavailable. We recommend that you schedule firmware updates during off-peak hours to avoid service interruption.

The event and audit logs are also generated during a firmware update.

**Diagnostics**

**Forward access points logs:** You can forward the access point logs to Sophos Support. We recommend that you turn on this option for debugging purposes.

**Remote Login to Access Points for Sophos Support:** Sophos Support can connect to access points remotely. You can turn this on for 5 hours to 30 days. It is turned off at the end.

**Analysis**

**Usage Insight:** The traffic generated by the user is categorized and shown.

The access point uses SophosLabs to categorize traffic. This option is turned off by default. Turning this feature on results in performance issues. For more information, see [Web category descriptions](#).

**Rogue Access Point detection**

**Detect and report rogue access points:** The access point scans for the neighborhood networks in all the channels defined by the regulatory domain. You can scan neighboring SSIDs on the Sites page.

**AdvancedRF Management**

**Roaming assist:** Sticky clients can connect to your other access points within a site. A sticky client is a client that remains connected to an access point even if it is far away.

**Discovery Protocol**

**Link layer discovery protocol (LLDP):** Access points advertise their identity by using link layer discovery protocol (LLDP) Ethernet frames.

Network switches that support IEEE 802.1ab LLDP can discover access points. This helps you manage the access point if there is a Layer 2 connectivity issue with the switch.

The access point shows MAC address, model, serial number, management port, and management IP address in the LLDP packet. Access points send LLDP packets only on the wired interface as a security measure.

**Note**
Available only for APX 320, APX 530, and APX 740.
8 Email Gateway

Email Gateway provides protection against spam, spoofing, viruses and advanced threats.

Introduction

Restriction
This option is only available if your license includes Sophos Email.

Set up Email Gateway to protect your domains and mailboxes. To do this:

• Add mailboxes you want to protect.
• Add email domains you want to protect.
• Configure Policies and Settings.

Related concepts
Email Security Policy (page 458)
You can apply security settings to your mailboxes using Email Security policies.

Data Loss Prevention policy (page 467)
Data Loss Prevention (DLP) stops data from being leaked by email.

Related tasks
Set up synchronization with Active Directory (page 471)
Follow these instructions to set up synchronization with Active Directory.

Set up synchronization with Azure Active Directory (page 474)
Add a mailbox manually (page 452)
Sophos Email allows you to add single mailboxes manually via the user interface.

Import Mailboxes (page 453)
Sophos Email allows you to import mailboxes in bulk.

Add mailboxes to Email Gateway

You can add mailboxes to Email Gateway.

You can add mailboxes in the following ways:

1. Automatically using Active Directory Sync. You can choose from the following Active Directory services:
   • AD Sync
   • Azure Sync
2. Manually using the UI.
Domains Settings/Status

Configure and manage email domains protected by Email Gateway.

Go to Settings > Domain Settings/Status.

Add a domain

Tip
Instructions on how to set up your domain for common providers are available online. Example: Office 365.

To view the instructions:
1. Expand Configure External Dependencies.
2. Under Inbound Settings, click the link for your chosen provider.
3. Use the information to help you configure your email domain.
   - Click Outbound Settings to view your outbound relay host.

To add a domain:
1. Click Add Domain.
2. In the Email Domain text field enter your email domain. Example: example.com.
   - Domain ownership must be verified before mail will be delivered through Sophos Central. To verify domain ownership, you need to add a TXT record to your domain. Adding this record will not affect your email or other services.
3. Click Verify Domain Ownership.
4. Use the details given in Verify Domain Ownership to add the TXT record to your Domain Name Server (DNS).
   - This can take up to ten minutes to take effect.
5. Click Verify.
   - CAUTION
     You cannot save an unverified domain. You must correct any issues with the domain ownership verification.
6. Select the direction you want to configure the domain for. If you select Inbound and Outbound you will need to select an outbound gateway from the drop-down list. If you select Custom Gateway, at least one IP/CIDR (subnet range) is required. Enter the IP and CIDR and click Add. You can add multiple IP addresses/ranges.
7. Select whether you wish to use a mail host or a mail exchange (MX) record in the Inbound destination drop-down list.
Note
You must use a mail exchange record if you want to use multiple destinations.

a) If you selected Mail Host enter an IP address or an FQDN (fully-qualified domain name) in the IP/FQDN text field. Example: 111.111.11.111 or mymail@example.com.
b) If you selected MX enter an FQDN in the MX text field. Example: mymail@example.com.

8. In the Port text field enter the port information for your email domain.

9. Expand Information to configure External Dependencies.

   The Mail Routing Settings tab shows the Sophos delivery IP addresses and MX record values used for configuring mail flow for your region.

   a) Make a note of the appropriate settings so that you know where to allow SMTP traffic from.
   b) Ensure that you configure your mail flow for Email Security.

10. Click Save to validate your settings.

11. Click the Base Policy link to configure spam protection.

Note
Spam protection applies to all protected mailboxes by default. You must review the settings to check that they are appropriate.

You can add extra domains at any time.

Delete a domain

To delete a domain, click on the gray cross to the right of the domain you wish to remove.

Edit a domain

To edit a domain, click on the domain name in the list, change the settings and click Save.

Policies and Settings

Configure Policies and Settings.

- Go to Policies to configure, edit or delete Email Security and Data Loss Prevention policies.
- Go to Settings to configure, edit or delete Email Gateway settings.
8.1 Email Gateway Dashboard

The Email Gateway Dashboard is the start page of Sophos Email and lets you see the most important information at a glance. It consists of these areas.

**Restriction**
This option is only available if your license includes Sophos Email.

### Inbound Activity Summary

**Inbound Activity Summary** shows the total number of inbound email messages and mailboxes scanned by Sophos Email for the last 30 days. It also shows the number of legitimate messages processed, the number of threats you have been protected from, and which categories they belong to.

Click **See Report** to open the **Message Summary** report, and review the details of the processed messages.

### Outbound Activity Summary

**Outbound Activity Summary** shows the total number of outbound email messages and mailboxes scanned by for the last 30 days. It also shows the number of legitimate messages processed, the number of threats you have been protected from, and which categories they belong to.

Click **See Report** to open the **Message Summary** report, and review the details of the processed messages.

### Sandstorm activity summary

**Restriction**
This option is only available with an **Email Advanced** license.

**Sandstorm Activity Summary** shows the number of mailboxes monitored by Sandstorm, and the number of emails checked by Sandstorm in the last 30 days. It also shows the number of legitimate messages processed, and the number of messages containing advanced threats detected.

Click **See Report** to open the **Sandstorm Activity Summary** report, and review the details of the processed messages.

**Note**
Sandstorm only checks messages from mailboxes where you've enabled it in the policy.

### At risk users

**At risk users** shows the users that have clicked the most malicious links within the last 30 days.
Sophos Central Admin

Click See Report to open the At risk users report, and review the details of the most at risk users. Click Create phish threat campaign for these users to create a Phish Threat campaign which automatically includes the top at risk users.

Related concepts
Message Summary Report  (page 52)
The Message Summary report details the email messages processed by Email Gateway for your protected mailboxes.

At risk users  (page 54)
This report lists users who are most at risk.

Data loss prevention policy violations  (page 54)
This shows all the emails that have violated email Data Loss Prevention (DLP) policies.

8.2 Message History Report

The Message History report details the emails processed by Email Gateway for your protected mailboxes.

Restriction
This option is only available if your license includes Sophos Email.

You can search emails by Subject, Sender or Recipient.

You can select the time period for which you want to view the email processing history. By default the report displays the emails that have been processed during the current day.

You can order messages by Direction or Date. You can filter emails by Status.

Click Update to refresh the report if you have changed the date range, entered a search term or filtered the emails. This shows the results of the changes you selected.

Report Details

For each message the report shows:

The Status of the email message.

• Delivered Successfully: The email was processed successfully and is being sent for delivery.
• Quarantined: The email was marked as spam due to its content or block list configuration. You can view quarantined emails on the Quarantined Messages page.
• Deleted: The email was deleted due to its content or block list configuration. When you select Deleted, you can select a Reason for deletion from the drop-down menu.
• Processing: The email is temporarily still being processed. This applies to emails in the Sandbox environment and emails that have been queued for delivery.
• Accepted: The email has been received successfully and is being processed by our system.
• Delivery Failed: Delivery of the email was attempted several times but it could not be delivered and the request timed out.
• Queued for Delivery: The initial delivery attempt failed, so the email will be re-queued for delivery. We will attempt to deliver the email for up to 5 days. Possible reasons for the initial delivery attempt failing are the recipient mail server being offline and issues retrieving the DNS records for the
recipient. Emails that have been queued for delivery and are now in the processing phase will show up as Processing.

- **Processing Encryption**: The email is still in the process of being encrypted, or the encrypted email is waiting to be delivered after the recipient sets their password.

**Note**
Whether an email is quarantined or deleted depends on the spam protection settings you have chosen.

**Message Details**

To view **Message Details**, click the **Subject** line. You can click on the following tabs for more information about the message.

- **Message Details**: shows general information about the message.

Select **Block IP** if you want to add the IP to the **Inbound Allow/Block** list then click **Block** to confirm your choice. Any sender using this IP address is blocked. Click **Cancel** to cancel the action.

Select the **show more** icon to see message events with timestamps. If an email is queued for delivery, you will see a Delivery Status Notification (DSN) error code underneath the **Queued for Delivery** status. This is the code returned by the recipient's mail server when you have attempted to deliver an email and the email isn't delivered. The code is helpful for troubleshooting the reason the email isn't delivered.

- **Raw Header**: shows the email header details.
- **Attachments**: shows the name and size of attachments.

**Related concepts**

- **Email Security Policy** (page 458)
  You can apply security settings to your mailboxes using **Email Security** policies.

- **Inbound Allow/Block** (page 482)
  You can create a list of email domains and addresses that you trust or don't trust.

- **Quarantined Messages** (page 454)
  The **Quarantined Messages** page lists the email messages that have been quarantined for all your protected mailboxes.

**Related information**

- **Enhanced Mail System Status Codes**

**8.3 Message Summary Report**

The **Message Summary** report details the email messages processed by **Email Gateway** for your protected mailboxes.

**Restriction**
This option is only available if your license includes **Sophos Email**.

You can view messages that occurred in the past 365 days or less. Messages for the last 30 days are shown by default.
Direction: Select **Inbound** or **Outbound** from the drop-down menu to view messages that have been received or sent.

All scanned messages are shown in the report by default. The messages are classified as follows:

- **Scanned**: All messages processed by **Email Gateway**.
- **Legitimate**: Messages that have been allowed.
- **Spam**: Messages classified as spam.
- **Virus**: Messages classified as containing viruses.
- **DLP policy violations**: Messages that violated Data Loss Prevention policies.
- **Advanced threat**: Messages classified as containing advanced threats.
- **Realtime blocklist**: Messages detected due to a blacklisted sending IP.
- **Company blocklist**: Messages sent from an address that has already been added to the company blocklist (inbound allow/block).
- **Authentication failures**: Messages that failed authentication by DMARC, SPF or DKIM.

The graph shows you at a glance the number of messages that were processed per day.

The message table shows the number of email messages processed for each date listed. It reflects the selected date and all message types.

8.4 Advanced Threat Report

The **Advanced Threat Report** details all emails submitted to Sophos Labs Intelix for advanced threat analysis.

You can view messages that occurred in the past 365 days or less. Messages for the last 30 days are shown by default.

The report shows clean, likely clean, suspicious, and malicious emails in graph form and in a list. They are categorized by the level of threat and you can filter the graph by **Scan result**. You can export the list in CSV or PDF format. Any emails that encounter errors are quarantined.

You can click the subject of any email to see **Message Details**. This shows you more information about the contents of a specific email and the results of the analysis. There are the following sections:

- **Summary**: Details of the email and whether it was delivered.
- **Threat prevalence**: How many times this malware has been received at your organization and other organizations.
- **Static analysis**: Details of machine learning analysis.
- **Dynamic analysis**: Results from tests run in a sandboxed environment.

If analysis is still in progress, you can't click the subject.

Use this information to determine the severity of the threat in an email.
8.5 Time of Click Summary

The **Time of Click Summary** report details the email messages processed by Time of Click URL Protection for your protected mailboxes.

**Restriction**
This option is only available with an **Email Advanced** license.

You can view messages that occurred in the past 365 days or less. Messages for the last 30 days are shown by default. All scanned messages are shown in the report by default. The messages are classified as follows:

- **Total Clicks**: All links that were clicked.
- **# Clicks Allowed**: All links that were allowed.
- **# Clicks Warned**: All links that generated a warning.
- **# Clicks Blocked**: All links that were blocked.

The graph shows you at a glance the number of messages that were processed per day. The message table shows the number of email messages processed for each date listed. It reflects the date range selected and all message types.

8.6 At risk users

This report lists users who are most at risk.

**Restriction**
This option is only available with an **Email Advanced** license.

This report uses information from the Time of Click URL Protection and **Impersonation Protection** features. Details for the last 30 days are shown by default.

To educate high-risk users there are direct links to **Phish Threat** training from the report. The **Phish Threat** campaign wizard automatically includes the at risk users for the date range you have selected. You can also add and remove users manually.

**Related tasks**
[Create a Phish Threat Campaign](#) (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

8.7 Data loss prevention policy violations

This shows all the emails that have violated email Data Loss Prevention (DLP) policies.

**Restriction**
This option is only available with an Email Advanced license.

Select the time period for which you want to view details of policy violations. Details for the last 30 days are shown by default.

You can see the following information:

- **Direction**: You can choose to view all processed emails, all inbound or all outbound.
- **Category**: You can filter the report by the type of information affected, for example financial information (FI).
- **Action**: You can filter the report by the action taken.

You can also click Create Phish Threat campaign to create training for your users.

**Restriction**
This option is only available with a Sophos Phish Threat license.

The users who have been logged by the data loss prevention policies for the date range you have selected are automatically included in the campaign. You can also add and remove users manually.

**Related concepts**
Data Loss Prevention policy (page 467)
Data Loss Prevention (DLP) stops data from being leaked by email.
Phish Threat (page 596)

8.8 People

On the People page, you can manage your users and user groups.

8.8.1 Users

On the Users tab of the People page, you can add or manage users, and get the users’ computers protected.

You can also enable the users to protect their own devices by emailing them a setup link.

The current users are listed with their details.

**Health Status**. An icon shows whether the user has security alerts on any of their devices.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>🟡</td>
<td>Amber warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>🟥</td>
<td>Red warning sign if there are critical alerts.</td>
</tr>
</tbody>
</table>

**Name** Click the user’s name to see details of devices and to see which has an alert.

**Email.**

**Exchange Login.**

**Last Active.** The last time a user reported to Sophos Central.

**Group Name.** This is shown if the user has been added to a user group.

**Role.** This shows what administration role, if any, the user has. This column is only visible if you are an administrator.

Click any column header to sort the users. By default, users are sorted according to the **Last Active** time.

To see full details for a user, click the user’s name.

You can add users manually or automatically by protecting their devices. You can also import users in bulk from a CSV file or from Active Directory. You can also protect existing users.

To modify users, click the user’s name to open and edit their user details.

You can also delete users and export lists of users.

**Related concepts**

- User Summary (page 442)
- Administration Roles (page 475)
- Mailboxes (page 451)

On the Mailboxes page you can manage your mailboxes for users, distribution lists and public folders. All protected mailboxes are listed.

**Related tasks**

- Add a user manually (page 447)
- Import users from a CSV file (page 448)
- Import users from Active Directory (page 448)
- Protect existing users (page 449)
- Delete users (page 449)
- Export to CSV (page 449)
You can export lists of users as CSV files.

**User Summary**

The **Summary** tab in a user’s details page shows a summary of the following:

- The user’s security status, administration role, if any, and account details.
- Recent events on the user’s devices.
- Mailboxes associated with the user.
- Devices associated with the user.
- Policies that apply to the user.
- Groups that the user belongs to.
- Logins.

You can find details of each below.

The security status and account details are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.

You can click on the other tabs for more on **Devices**, **Events**, and **Policies**.

**Health Status**

In the left-hand pane, an icon shows you whether the user has security alerts on any of their devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green check mark]</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>![Orange warning sign]</td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>![Red warning sign]</td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>

You can see which devices have alerts in the **Devices** tab.

A padlock icon shows that the user has been imported from Active Directory.

A badge shows the user’s assigned administration role. Click on the role name to view the settings for the role.

**Note**

Role information is only displayed for administration roles.

**Account details**

In the left-hand pane, you can modify or delete the user’s account.
Note
If a user has been imported from Active Directory, you cannot change the account details. However, you can add the user to a new Sophos Central group or add another login.

Modify the account
1. Click Edit and enter the following settings:

   **First & Last name**: Enter the name of the user. Do not include a domain name.

   **Role**: Select a role for the user. Choose from: **Super Admin, Admin, Help Desk, Read-only, or User**.

   **Restriction**
   You can only see the **Role** option and assign administrator roles if you are a Super Admin.

   **Note**
   You cannot amend your own administration role.

   **Note**
   Anyone with a **User** role only has access to the Self Service Portal.

   **Email Address**: Enter the email address of the user.

   **Exchange Login** (optional): Enter the Exchange account name of the user.

   **Note**
   In Sophos Mobile policies, you can use the placeholder $USERNAME$ to refer to this setting.

   **Add to groups**: Select one of the available user groups and use the picker arrows to move it to the assigned groups.

   **Email Setup Link**: Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs.

   **Note**
   The user needs administrative privileges and internet access in order to protect their computer.

   **Note**
   **Web Gateway** provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

2. Click **Save**.

Delete the account
To delete the account, click **Delete User** in the left-hand pane. Logins assigned to this user can afterward be assigned to another user.
Restriction
You cannot delete users who have an assigned administration role.

Multi-factor authentication
If the user is an admin, the left-hand pane shows whether multi-factor authentication (MFA) is enabled for them. If it is enabled, the admin must use another form of authentication, as well as their user name and password, to sign in.

If you're a Super Admin, you can edit the settings as follows:
Click Reset to let the admin set up their MFA sign-in details again.
Click MFA Settings to go to a page where you can enable or disable multi-factor authentication for the admin.

Recent Events
This lists recent events on the user's devices.
For a full list, click the Events tab.

Mailboxes
This lists all email addresses, including distribution lists and public folders, associated with the user.
Primary indicates the user's primary email address. Owner indicates the user controls a distribution list or public folder.
For full details, click an email address.

Devices
This shows a summary of the devices associated with the user.
Click the device name to go to the device's details page for more information.
Click Actions to carry out any of the same actions that are available on the device's details page (for example, Scan Now and Update Now for a computer).
For full details of the user's devices, click the Devices tab.

Policies
This shows a summary of the policies applied to the user.
The list shows the policy name, whether the policy is enabled or not, and icons that indicate the features included in the policy.
Click on a policy name to view and edit the user policy.
Note
Editing the policy affects all users to which this policy is applied.

For full details of all the policies applied to this user, click the Policies tab.

Groups
This shows the groups the user belongs to.
Click on a group name to see details of the group.
Click Edit (on the right) to change the groups the user belongs to.

Logins
This shows the user’s logins.
Click Edit (on the right) to change the logins assigned to the user.

Related concepts
About Policies (page 455)
Administration Roles (page 475)

User Devices
The Devices tab in a user’s details page lets you see the devices associated with the user.
This tab also shows any servers where the user has logged on with Remote Desktop Services.
For each associated device you can see the device type and the operating system. You also have these options:
• View Details: This opens the full device details page.
• Delete: This removes the device from the list and stops Sophos Central managing it, but it does not uninstall the Sophos software.
• Actions: Actions you can take. These depend on the device type.

User Events
The Events tab in a user’s details page lets you see a list of events detected on the user’s devices.
You can see details and, in some cases, take action to prevent unwanted detections.
The list includes:
• Severity: Hover over an icon to see what it means.
• Type: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
• Details: This link (for certain events) lets you get further details and take action.
View Events Report shows events arranged by type and a graph of events day by day.
Stop detecting an application

If an application is reported as malware but you know it’s safe, you can allow it from the events list.
For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.
Click the Details link beside the event and then allow the application.

Note
This currently applies only to malware events reported by Intercept X.

Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again.
This will apply to all your users and computers.
1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again and select an option:
   • Exclude this Detection ID from checking: prevents this detection on this app.
   • Exclude this application from checking: prevents any checks for exploits on this app.
   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.
3. Click Exclude.
We’ll add your exclusion to a list.
Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again.
This will apply to all your users and computers.
1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again.
   Select Exclude this Detection ID from checking. This prevents this detection on this app.
3. Click Exclude.
We’ll add your exclusion to the Global Exclusions list.

Related information
How to investigate and resolve a potential False Positive or Incorrect Detection
User Policies

The Policies tab in a user's details page lets you see the policies that are enabled and applied to the user.

Click a policy name to view and edit policy details.

Editing the policy affects all users to which this policy is applied.

Add a user manually

You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

To add a user:

1. Go to Users.
2. Click Add and select Add User.
3. In the Add User dialog, enter the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First and Last Name</td>
<td>Enter the name of the user. Do not include a domain name.</td>
</tr>
<tr>
<td>Role</td>
<td>Select an administration role for the user.</td>
</tr>
<tr>
<td></td>
<td>A user who is assigned an administration role will receive an email telling</td>
</tr>
<tr>
<td></td>
<td>them how to set up their administration account.</td>
</tr>
<tr>
<td></td>
<td>You can only see the Role option and assign administrator roles if you are</td>
</tr>
<tr>
<td></td>
<td>a Super Admin.</td>
</tr>
<tr>
<td></td>
<td>Anyone with a User role only has access to the Self Service Portal.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address of the user.</td>
</tr>
<tr>
<td>Add to groups (optional).</td>
<td>Select one of the available user groups and use the picker arrows to move it to the assigned groups. You can start typing a name in the search box to filter the displayed groups.</td>
</tr>
<tr>
<td>Email Setup Link (optional).</td>
<td>Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs. The user needs administrative privileges and internet access in order to protect their computer.</td>
</tr>
<tr>
<td>Web Gateway</td>
<td>This provides more advanced web security for computers than Endpoint Protection. You can</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>install it alongside Endpoint Protection or on its own.</td>
</tr>
</tbody>
</table>

4. Click **Save** or **Save and Add Another**. The new user is added to the user list.

When the user downloads and installs the software, their device is automatically associated with the user.

### Import users from a CSV file

You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

To import users:

1. Go to **Users**.
2. Click **Add** and click **Import users from CSV**.
3. Click **Browse** and select your CSV file.

   **Tip**
   You can download template CSV files from the **Import users from CSV** dialog.

   The CSV file can include groups a user is assigned to.

4. To create new groups, click **Create new groups**.
5. To send a registration email for the Sophos Central Self Service portal to each imported user, click **Give users access to Sophos Central Self Service**.
6. Click **Add**.

**Note**
The CSV file can include the email address of each user's manager. If there's a manager who isn't already a user in Sophos Central, a user is created. So the number of users imported may exceed the number of rows in the file.

**Note**
If an email address in your CSV file matches an existing user in Sophos Central, the user is updated with the information in your import file.

**Note**
If an email address in your CSV file matches an existing user in Sophos Central that is managed through Active Directory Synchronization, the user is skipped during import and no changes are made to the user account.

### Import users from Active Directory

You can import users and groups from Active Directory.

To do this:

1. Go to **Users**.
2. Click the **Set up Active Directory Sync** link in the upper right of the page.
3. Follow the set up synchronization process.

Related tasks
Set up synchronization with Active Directory (page 471)
Follow these instructions to set up synchronization with Active Directory.

Protect existing users

You can protect users that you have already added to Sophos Central.
To protect them you need to email them a setup link. To do this:
1. Go to Users.
2. Select the user or users you want to protect.
3. Click Email Setup Link in the upper right of the page.
4. In the Email Setup Link dialog, select the types of protection the user needs (if your license includes more than one).
   - Web Gateway provides more advanced web security for computers than Endpoint Protection.
   - You can install it alongside Endpoint Protection or on its own.
   - Users need administrative privileges and internet access to use the setup link.

Delete users

You can delete users from Sophos Central if you are a Super Admin.

Restriction
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them.

Under some circumstances, the user may be recreated automatically in future:
- If the user logs in to an associated device that is still managed by Sophos Central, they are added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they are added as a user again the next time that Sophos Central synchronizes with Active Directory.

To delete users:
1. Go to Users.
2. Click the checkbox next to each user you want to delete.
3. Click Delete.
Deleting a user does not delete devices associated with that user or remove the Sophos software from these devices.
Logins assigned to a deleted user can afterwards be assigned to another user. You can edit logins by clicking the Edit link on a user's details page.

Export to CSV

You can export lists of users as CSV files.
You can export lists of different types of user.
For example you can export a list of administrators by applying the **Admins only** filter before you click **Export to CSV**.

To export users:
1. Go to **Users**.
2. Click **Export to CSV**.
   This creates a file called `users.csv`. Any currently active filters are applied to the list.

### 8.8.2 Groups

On the **Groups** tab of the **People** page, you can add or manage groups of users.

You can use groups to assign a policy to multiple users at once.

The sections below tell you about the groups list and how to add, modify or delete groups.

#### About the groups list

The current groups are listed and the number of users in each group is shown.

To see full details for a group, click the group's name.

#### Add a group

1. Click the **Add Group** button.
2. In the **Add Group** dialog, enter the following settings:
   - **Group Name**: Enter the name of the new group.
   - **Available Users**: Select users from the list of available users.

   **Tip**
   In the **Search** box you can start typing a name to filter down the displayed entries.

3. Click **Save**.

#### Modify a group

To modify a group, click the group's name to open and edit the group details. For more information, see **User Group Details**.

#### Delete a group

To delete a group, select it and click **Delete** in the upper right of the page.

Deleting a group will not delete its users.

#### User Group Details

On a group's details page, you can:
Add or remove members

To add or remove members:

1. Click **Edit** under the group name.
2. In the **Edit Group** dialog, use the picker arrows to add users to the **Assigned Users** list or remove them.
3. Click **Save**.

Delete the group

To delete the group:

1. Click **Delete** under the group name.
2. In the **Confirm Group Deletion** pop-up, click **Yes**.

Deleting a group will not delete its users.

User Group Policies

The **Policies** tab in a user group's details page lets you see the policies that are enabled and applied to the group.

Click a policy name to view and edit policy details.

Editing the policy affects all groups to which this policy is applied.

8.9 Mailboxes

On the **Mailboxes** page you can manage your mailboxes for users, distribution lists and public folders. All protected mailboxes are listed.

**Restriction**

This option is only available if your license includes **Sophos Email**.

You can manually add mailboxes or import mailboxes and aliases.

You can also use **Active Directory Sync** to import users and groups into Sophos Central.

- If you haven't used it yet, there is a link to get you started.
- If you've already used it, a message here shows you issues, such as users without email addresses. Click on the link to fix the issue.

Click on a mailbox name to see its user, aliases, and the **Email Gateway** policies the user belongs to.

You can edit the aliases for a mailbox and ask Sophos to give **Bulk email sender privileges** to a user.
Related concepts
Add mailboxes to Email Gateway (page 452)
You can add mailboxes to Email Gateway.

Email sending limits and privileges (page 453)
Administrators can request privileges for users who need to send large numbers of emails.

Related tasks
Add a mailbox manually (page 452)
Sophos Email allows you to add single mailboxes manually via the user interface.

Import Mailboxes (page 453)
Sophos Email allows you to import mailboxes in bulk.

Related information
Email Gateway (page 432)
Email Gateway provides protection against spam, spoofing, viruses and advanced threats.

8.9.1 Add mailboxes to Email Gateway

You can add mailboxes to Email Gateway.

You can add mailboxes in the following ways:

1. Automatically using Active Directory Sync. You can choose from the following Active Directory services:
   - AD Sync
   - Azure Sync
2. Manually using the UI.

Related tasks
Set up synchronization with Active Directory (page 471)
Follow these instructions to set up synchronization with Active Directory.

Set up synchronization with Azure Active Directory (page 474)
Add a mailbox manually (page 452)
Sophos Email allows you to add single mailboxes manually via the user interface.

Import Mailboxes (page 453)
Sophos Email allows you to import mailboxes in bulk.

Add a mailbox manually

Sophos Email allows you to add single mailboxes manually via the user interface.

To add a mailbox manually:

1. Click Mailboxes.
2. On the Mailboxes screen, click Add.
3. Select Add Mailbox.

   There are three types of mailbox:
   - **User Email**: a mailbox for a person. Example: firstname.lastname@companyname.com.
**Tip**
For a User Email mailbox you can click on the mailbox name to view the user's details.

- **Distribution List**: a mailbox for a group of people. Example: support@companyname.com.
- **Public Folder**: a mailbox for collecting information such as surveys or feedback. Example: survey@companyname.com.

4. Select a mailbox type.
5. Enter a name for the mailbox.
6. Enter the SMTP address for the mailbox.
7. Click **Save** to create a single mailbox and exit, or **Save and Add Another** to create additional mailboxes.

**Import Mailboxes**

**Sophos Email** allows you to import mailboxes in bulk.

To import mailboxes:

1. Create your import .csv file using the following format:

<table>
<thead>
<tr>
<th>Name</th>
<th>Email Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Alamar</td>
<td><a href="mailto:robert.alamar@test.com">robert.alamar@test.com</a></td>
<td>User</td>
</tr>
<tr>
<td>Support DL</td>
<td><a href="mailto:support@test.com">support@test.com</a></td>
<td>DL</td>
</tr>
<tr>
<td>Vacation Calendar</td>
<td><a href="mailto:vacation@test.com">vacation@test.com</a></td>
<td>PF</td>
</tr>
</tbody>
</table>

2. Click **Add Mailbox** and select **Import Mailboxes**.
3. Click **Browse** and navigate to your import file.
4. Click **Add** to start the import process.

Import will run and display results after it completes.

To verify mailbox creation, you can search for new users in the **People** section or browse the list of mailboxes under the **Mailboxes** section for Distribution Lists and Public Folders.

**8.9.2 Email sending limits and privileges**

Administrators can request privileges for users who need to send large numbers of emails.

The number of emails that users can send is restricted by default to prevent the unregulated sending of large numbers of emails. If an email account is hacked it can be used to send large amounts of spam, which could damage your organization's reputation. Your organization could be blocked or otherwise constrained by external internet organizations.

When an account reaches its sending limit it is blocked until its average sending rate drops below the limit. While it is blocked, attempts to send further emails fail and the sent emails are returned with an error. These measures are applied to the affected account, not the whole organization. This prevents interruption to the whole organization.

Where there is a genuine need for users to send large numbers of emails, you can ask Sophos to give bulk email sender privileges to a user.
Bulk email sending limits

Standard users can send a maximum of 400 emails in a 10 minute period or 2,000 emails in 24 hours. A user with bulk email privileges can send up to 3,000 emails in a 10 minute period or 30,000 in 24 hours.

You can only give bulk email sender privileges to a maximum of 5% of your organization's users.

Applying for bulk sender privileges

In Email Gateway > Mailboxes select a user and click Request bulk sender privileges. If bulk sender privileges have already been asked for or granted for that user, a status message appears.

Note

If Bulk email sender privileges does not appear, click on Settings > Domains settings/status and check that the domain is set to Inbound and Outbound.

Fill in and submit the form with the required information. The request will be reviewed by Sophos within 72 hours.

You can also remove bulk sender privileges, without a Sophos review.

Monitoring bulk sending privileges

Mailboxes have a Bulk email sender privileges section in Email Gateway > Mailboxes. This shows the status of a privilege application.

In Alerts you can see users that have reached their email sending limits. You can also change the frequency of alerts for a user.

8.10 Quarantined Messages

The Quarantined Messages page lists the email messages that have been quarantined for all your protected mailboxes.

Restriction

This option is only available if your license includes Sophos Email.

Search: You can search emails by Subject, Sender or Recipient.

By default the report displays the emails that have been processed during the current day.

You can order messages by Date, Sender, Recipient and Reason. You can also view the message Subject.

Message Details

To view the message details, click the Subject line. You can click on the following tabs for more information about the message:
• **Details**: shows general information about the message.

   Click **Add to blocklist** if you want to add the IP to the **Inbound Allow/Block** list then click **Ok** to confirm your choice. Any sender using this IP address is blocked. Click **Cancel** to cancel the action.

• **Raw Header**: shows the email header details.

• **Message**: shows the body of the email.

• **Attachments**: shows the name and size of attachments.

You can also:

• Release messages from quarantine and send them to users. Select the messages and click **Release**.

• Delete quarantined messages. Select the messages and click **Delete**.

**Related concepts**

*Inbound Allow/Block* (page 482)

You can create a list of email domains and addresses that you trust or don’t trust.

Policies and Settings

### 8.11 Policies

You can create multiple email security policies which can be applied to users, groups and domains.

A policy is a set of options that Sophos Central applies to protected mailboxes.

Policies will be applied from the top down, for example, if a user is added to the policy at the top of the list, those settings will take precedence over any settings in other policies the user is a part of.

You can add a combination of users, groups and domains to a single policy. When an email comes through, Sophos Email will check whether the address corresponds to a single user, a member of a group or a member of a domain. It will then apply the policy settings if the address matches any of them.

To find out how policies work and how you can use them to customize security settings, see *About Policies*.

To find out how to create and edit policies, see *Create or Edit Policies*.

**Related concepts**

*Email Security Policy* (page 458)

You can apply security settings to your mailboxes using *Email Security* policies.

### 8.11.1 About Policies

If you’re new to policies, read this page to find out how policies work.

**What is a policy?**

A policy is a set of options that Sophos Central applies to protected users, devices or servers.

There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).
Users, devices and servers have separate policies.

What is a Base policy?

Each feature has a Base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.

For some features, like threat protection, Sophos configures the Base policy with the best practice settings. You can leave it unchanged if you want to.

For other features, like application control or peripheral control, which are more specific to your network, you must edit the policy to set up the feature.

The Base policy is always available and is used if you don't have other policies activated.

Note

You cannot disable or delete the Base policy.

Do I need to add new policies?

You can choose whether to set up your own policies or not.

If you want to apply the same policy to all users or devices or servers, you can simply use the Base policy or adapt it for your needs.

If you want to use different settings for different groups, you can create additional policies.

What can I do with additional policies?

You can set up additional policies to override some or all of the settings in the Base policy.

You can use additional policies to apply different settings to different users, devices or servers. You can also use them to make it easier to switch the settings that are applied quickly.

The order in which you put the policies in the list matters. The policies at the top of the list override the policies at the bottom. See “How do you prioritize policies?” below.

What’s the difference between user policies and computer policies?

A user policy applies to all the devices that a user has.

A “device” or computer policy applies to specific computers or groups of computers, regardless of which user logs on.

Some features let you create either kind of policy. Other features only let you create one kind. For example you can set an updating policy for computers, but not for users.

If you set up a user policy and a computer policy for the same feature, and both could apply to the same computer, the policy that’s higher in your policy list takes priority. See “How are policies prioritized?”

You can check which policy is applied to a computer by looking at the Policies tab on that computer’s details page.
What is in each policy?

A policy lets you:

• Configure one of the features that you have licensed.
• Specify which users, devices or servers the policy applies to.
• Specify whether the policy is enforced and whether it expires.

A policy contains all the settings for a product or feature. For example, you cannot split up the threat protection settings across several different policies in such a way that a user gets one setting from one policy and another setting from a different policy.

How are policies prioritized?

The order in which you arrange the policies determines which is applied to specific users, devices or servers.

Sophos Central looks through the policies from the top down and applies the first policy it finds that applies to those users or devices.

The Base Policy is always at the bottom, and is applied to any users, devices or servers that aren’t covered by policies higher in the list.

Tip
Place the most specific policies at the top and general policies further down. Otherwise, a general policy might apply to a device for which you wanted an individual policy.

To sort policies, grab a policy and drag it to the position where you want to insert it.

8.11.2 Create or Edit a Policy

You can create or edit a policy as follows.

Create a policy

1. If you have more than one Sophos product, select the one where you want to create a policy.

   Note
   You can’t create policies from the Overview pages.

2. Go to the Policies page.
3. Click Add Policy (in the upper right).
4. If you see an Add Policy dialog, select:
   • The feature you want.
   • The policy type (applies only to Endpoint Protection).
5. On the policy details page, use the tabs to:
Edit a policy

1. If you have more than one Sophos product, select the one where you want to edit a policy.

   **Note**
   You can't edit policies from the **Overview** pages.

2. Go to the **Policies** page.
   You see a list of policy types.
3. Click on the policy type to open a list of policies.
4. Find the policy you want to edit and click it.
5. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users or devices.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.

### 8.11.3 Email Security Policy

You can apply security settings to your mailboxes using **Email Security** policies.

**Restriction**
This option is only available if your license includes **Sophos Email**.

Email Security provides protection against spam. Set up **Email Security**, if you have not already done so.

1. Edit the **Email Security** policy.
2. Open the policy's **Settings** tab and configure it. Make sure the policy is enabled.

   The following settings only apply to inbound messages with the exception of **Enhanced content and file property scan**, which applies to both inbound and outbound messages.

   **Note**
   If an option is locked global settings have been applied by your partner or Enterprise administrator.

**Related concepts**
**About Policies** (page 455)
**Spam Filtering** (page 459)
Each email message is analyzed and given a spam score. The higher the score the more likely the message is to be spam.

**Smart banners** (page 460)
When you turn on **Smart banners**, a banner is displayed at the top of inbound email messages to show if the email is trusted.

**Sender Checks** (page 461)
Sender checks allow you to verify whether an email originates from where it claims to come from. Email Security uses **DMARC**, **SPF**, **DKIM**, and **Header anomalies** checks to do this.

**Enhanced Email Malware Scan** (page 464)
You can apply enhanced email content scanning.

**Related tasks**
**Quarantine Settings** (page 460)
You can choose to send a quarantine summary message to each protected mailbox.

**Related information**
**Email Gateway** (page 432)
Email Gateway provides protection against spam, spoofing, viruses and advanced threats.

**Information on the Sophos Extensible List**

### Spam Filtering

Each email message is analyzed and given a spam score. The higher the score the more likely the message is to be spam.

Messages with the highest spam scores are rated as **Spam**.

Messages are categorized based on their spam score and you can choose how the categories are processed. Messages are split into:

- **Spam**: These are messages that conform to known and verified spam patterns.
- **Bulk**: These are solicited messages sent using mass mailing, for example newsletters sent to a mailing list.
- **Suspected Spam**: These are messages that have been identified as suspicious.

For each category choose an action from:

- **Quarantine**
- **Deliver**
- **Delete**
- **Tag subject line**: The message is tagged and delivered. The tag appears at the start of the subject line in the message. You can customize the tag, using up to 30 characters.

The default settings are:

- **Spam**: Quarantine
- **Bulk**: Quarantine
- **Suspected Spam**: Tag subject line
Smart banners

When you turn on **Smart banners**, a banner is displayed at the top of inbound email messages to show if the email is trusted.

**Note**
Smart banners are only inserted when emails are received from outside the organization. If an internal employee forwards such an email to another internal employee, the banner remains in the forwarded email.

Email recipients can add senders to their allow and block lists from within the email if you have enabled this option in Sophos Central Self Service.

To do this, go to **Self Service Settings** and turn the **Allow / Block List** option on.

If a sender is already allowed, no allow or block links are displayed in the banner.

Emails from Sophos, for example **Quarantine Summary** emails, will not display banners.

**CAUTION**
We strongly recommend that you route outbound email through Sophos Central before you turn on smart banners. If you don’t, external recipients see the banner in replies or forwarded email and can modify end-user allow and block lists.

You can turn on and off the following banner types:

- **Trusted**: The email was sent from an allowed sender and passed DNS authentication (SPF, DKIM, or DMARC).
- **Unknown**: The email was sent from outside your organization.
- **Untrusted**: The email was sent from outside your organization and failed DNS authentication (SPF, DKIM, or DMARC).

**Related concepts**
- **Domains Settings/Status** (page 484)
  Configure and manage email domains protected by **Email Gateway**.

Quarantine Settings

You can choose to send a quarantine summary message to each protected mailbox.

The message contains a table containing spam messages that were quarantined since the last summary message was sent. You can schedule when the messages are sent.

Users can release or delete quarantined spam messages by clicking the appropriate link in the quarantine summary message.

To set up quarantine summary messages:

1. Turn on **Send a quarantine summary email**.
2. Select when you want the messages sent.

**Tip**
All days are selected by default. Click a day to deselect it.
3. One time slot is shown by default. You can add up to three more by clicking **Add another time**. To delete a time slot, click the delete icon next to it.

   **Note**
   The default time slot can't be deleted.

### Sender Checks

Sender checks allow you to verify whether an email originates from where it claims to come from. Email Security uses **DMARC**, **SPF**, **DKIM** and **Header anomalies** checks to do this.

**Restriction**
This option is only available if your license includes **Sophos Email**.

**Note**
If an option is locked global settings have been applied by your partner or Enterprise administrator.

Sender checks are performed in the order they appear in the UI. If an email fails the first sender check, the other checks are not carried out.

You can override the sender checks by allowing domains and email addresses in the **Inbound allow list**.

### DMARC

**DMARC** (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication policy and reporting protocol. It builds on the DKIM and SPF protocols to detect and prevent email spoofing. You can control what happens to messages that fail DMARC checks.

Select from:

- **Conform to sender policy**: What happens to the message depends on what the sender stated in their DMARC policy. (This is the default value.)
- **Tag subject line**: Email Security adds a tag to the message's subject line indicating that it is a spoofed message.
- **Quarantine**: Message is quarantined.
- **Reject**: Message is rejected.
- **Deliver**: Sends the message to the mail server for delivery.

### SPF

**SPF** (Sender Policy Framework) allows you to verify that incoming email comes from an IP address authorized by the sending domain’s administrators.

Emails from IP addresses marked as "fail" by the sending domain's administrators are rejected.

Spam and phishing emails often use forged addresses. This results in an SPF check rejecting the email.
DKIM

DKIM (DomainKeys Identified Mail) is an authentication framework used to sign and validate a message based on the domain of the sender. You can control what happens to messages that fail DKIM checks.

Select from:

- **Tag subject line**: Email Security adds a tag to the message’s subject line indicating that it is a spoofed message. (This is the default value.)
- **Quarantine**: Message is quarantined.
- **Reject**: Message is rejected.
- **Deliver**: Sends the message to the mail server for delivery.

Header anomalies

The **Header anomalies** check identifies email that appears to come from your own domain but originates from an external domain by checking the from header of the email against the recipient domain, and the from address in the envelope.

- If the domain in the from address matches the recipient's domain, the mail is considered to be spoofed.
- If the from address in the header is different to the from address in the envelope, the mail is considered to be spoofed.

**Note**
The header needs to match both the criteria above to trigger the **Header anomalies** check.

You can control what happens to messages that fail the **Header anomalies** check.

Select from:

- **Tag subject line**: Email Security adds a tag to the message's subject line indicating that it is a spoofed message. (This is the default value.)
- **Quarantine**: Message is quarantined.
- **Reject**: Message is rejected.
- **Deliver**: Sends the message to the mail server for delivery.

**Related concepts**

How Sender Checks work (page 462)

Sender checks are used to verify the authenticity of an email's origin.

**Related information**

Information on the Sophos Extensible List

**How Sender Checks work**

Sender checks are used to verify the authenticity of an email’s origin.

This topic addresses the types of sender checks Sophos Email uses to protect you from illegitimate emails.
Note
This topic provides a brief explanation about how the sender checks work, however it does not include detailed information such as setting up DNS records (DMARC, DKIM, SPF) as we are focusing on what happens to incoming mail.

SPF

Sender Policy Framework (SPF) allows you to verify that incoming email comes from an IP address or sending host authorized by the sending domain's administrators.

The sender creates a SPF record which specifies the hosts, IP addresses and subnets that are authorized to send mail for their domain.

When an email is received by Sophos Email, it looks at the address of the sending mail server then compares it to the authorized senders in the SPF record. If these do not match, the SPF check will fail.

DKIM

DomainKeys Identified Mail (DKIM) is used to authorize an email by verifying its digital signature, which associates a domain name with the email.

The sender decides which part of the email they want signed (header and/or body) and then they configure their mail server to create a hash of those parts. The hash is then encrypted by their private key. They also publish a DKIM record which contains the public key used to decrypt the signature.

When Sophos Email sees that an email has a DKIM signature, it does a DNS lookup to find the DKIM record associated with the sending domain. It uses the public key to decrypt the digital signature back to the hash value. It then takes the elements of the message that were signed and creates it's own hash that it compares it to the decrypted hash. If these do not match, the DKIM check will fail.

DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) utilizes both DKIM and SPF to validate the authenticity of an email.

The sender creates a DMARC record which instructs the receiver to carry out DMARC checks and contains information about what to do when DMARC fails.

When an email is received, Sophos Email carries out a DNS check to find the DMARC record for the domain specified in the emails' from (header) address. The DMARC record tells the receiver (in this case, Sophos Email) to check for DMARC and specifies what to do with email that fails DMARC checks. The Sophos Email default option for messages that fail DMARC checks is Conform to sender policy, meaning that what happens to the message depends on what is defined in the DMARC record. The domain specified in the from address is checked against the information in the SPF and DKIM records to verify that the domains match. To pass a DMARC check, the message needs to pass validation and alignment checks for SPF or DKIM:

- For SPF, the domain specified in the MAIL FROM (envelope) address must match one of the IP addresses or subnets specified in the SPF record. DMARC then checks the MAIL FROM address against the from address to make sure they align.
For **DKIM**, the signature must be validated and the domain specified in the **from** address must match the domain used to create the signature specified in the DNS record.

**Header anomalies**

The **Header anomalies** check protects you from senders spoofing emails from your own domain. It identifies email that appears to come from your own domain but originates from an external domain by checking the **from** header of the email against the recipient domain, and the MAIL FROM address in the envelope.

- If the domain in the **from** address belongs to the same customer as the recipient domain, the mail is considered to be spoofed.
- If the **from** address in the header is different to the MAIL FROM address in the envelope, the mail is considered to be spoofed.

**Note**

The header needs to match both the criteria above to trigger the **Header anomalies** check.

**Related information**

- **DKIM**
- **DMARC**
- **SPF: Sender Policy Framework**

**Enhanced Email Malware Scan**

You can apply enhanced email content scanning.

**Restriction**

This option is only available if your license includes **Sophos Email**.

**Note**

If an option is locked global settings have been applied by your partner or Enterprise administrator.

**Enhanced content and file property scan**

This is our highest level of protection against email malware. It is on by default.

This setting applies to inbound and outbound messages.

**Note**

If malware is detected in a message, it is always discarded.

**Un-scanned emails**

You can choose what happens to messages that cannot be scanned. The available actions are:

- **Quarantine**
• **Delete**
• **Tag subject line**

This setting applies to inbound messages only.

There are various reasons we may not be able to scan specific messages:

• **Inability to access the file:** The file is identified correctly, but the software can't access the file to decompress or scan it.
• **Corrupt file:** The file is corrupt, which means it cannot be accessed.
• **Correct identification of a file, but unexpected content is encountered:** The file is correctly identified and access is granted, however unexpected content is found. The antivirus scan process produces an error.
• **Scanner times out:** The antivirus scanner times out when attempting to scan. There are several reasons this can occur. Some examples are, when a file is compressed in lots of nested levels and when the antivirus scanner exceeds the scan time limit.
• **Large compressed attachment:** If a compressed attachment is too large, it cannot be scanned. It may be that the attachment is nested within too many levels of compression, the compressed files included are too large or there are too many compressed files within the attachment.

These are just some examples. There may be other reasons.

Email addresses and domains that you add to the **Inbound Allow/Block** list and Sophos encrypted emails won't be scanned.

### Time of Click URL Protection

This is available with an **Email Advanced** license only and is turned on by default.

When Time of Click URL Protection is enabled, URLs contained within inbound messages are rewritten so that they point to Sophos Email instead of the original destination.

When the link is clicked, Sophos Email performs an SXL lookup, and if it is malicious it is blocked. If the URL is clean, the action taken when you click the link will depend on what you have specified in the policy. For example, if you have set medium risk websites as allowed, once the link has been checked and has been classified as not malicious, the link will take you to the original link destination.

The domain name will be displayed at the start of the rewritten URL so that you can see where the link will send you, if allowed. For example `d=domain.com`.

You can select the action you want to take for websites with the following reputation levels:

• **High risk:** Includes illegal sites, sites containing malware and phishing sites.
• **Medium risk:** Includes sites associated with spam and anonymizing proxies.
• **Unverified:** The reputation of the website can't be verified.

You can't allow high risk websites.

**Note**

URLs you add to the Time of Click allow list are never rewritten at time of click.

You can also control whether URLs are rewritten in plain text messages and within securely signed messages:
Plain text messages: refers to emails with no HTML formatting. Without HTML formatting, when URL rewriting is enabled, the entire encoded URL will display in the email. You can bypass URL re-writing in these messages by deselecting the Re-write URLs in plain text messages. option.

Securely signed messages: URL rewriting may break the signatures of S/MIME, PGP, and DKIM signed messages. You can bypass URL re-writing in these messages by deselecting the Re-write URLs within securely signed messages. option.

**CAUTION**
Please use caution if you choose to bypass URL re-writes, as URLs in these messages will not be protected.

Sandstorm

This is available with an Email Advanced license only and is turned on by default.

Sandstorm sends emails that may contain active malicious content to an isolated virtual environment where they are opened and checked. If emails are found to be malicious, they are removed.

When Sandstorm is enabled, you can select your preferred sandbox location.

**Tip**
Select Let Sophos decide (recommended) to automatically route messages for optimal performance.

Messages that may be malicious will run in a virtual environment for closer inspection. Messages that are clean are delivered as normal. Messages that contain advanced threats are discarded.

Impersonation Protection

This is available with an Email Advanced license only and is turned on by default.

This feature detects emails that pretend to be from well-known brands, or from very important people (VIPs) in your organization.

Choose the action taken when emails are detected by this feature.

In summary reports, these emails are labeled as advanced threat.

You can add email addresses for VIPs in VIP management.

**Related concepts**

URL allow list (page 158)
You can add domains to the allow list so that URLs from those domains are neither rewritten nor scanned by Time of Click protection.

Impersonation Protection and VIP Management (page 159)
Impersonation Protection detects phishing emails that pretend to come from well-known brands or from important people within your organization.

8.11.4 Data Loss Prevention policy

Data Loss Prevention (DLP) stops data from being leaked by email.

Restriction
This option is only available with an Email Advanced license.

In email Data Loss Prevention policies you add rules to restrict the information that can be included in emails. Rules can be applied to inbound or outbound emails and you can add up to 25 rules to a policy.

You can apply rules to different users, groups of users and domains. For example, you could set up a rule to prevent any financial information going out of the organization for most users. You could then apply a less strict rule to accounting staff.

To add Data Loss Prevention to emails, create a Data Loss Prevention policy.

When you create a policy, the action is set to the Sophos default. You can change this when you create or edit the rule.

In Settings, you can see the rules for inbound or outbound emails that are associated with a policy. You can change the order of the rules, and turn them on or off. To view or edit rule settings, click on the rule name. You can also create new rules for a Data Loss Prevention policy.

When you create a rule you can use templates provided by Sophos to protect your data. You can also customize rules. You can choose the action you want to take when sensitive information is found in an email.

Note
The encryption option is only available when encryption is turned on. It applies to outbound messages only.

Templates

You can use templates to filter emails for financial, confidential, health and personally identifiable information. You can also filter emails by their attachment file types.

Custom

You can customize Data Loss Prevention rules using content control lists (CCL), keywords or phrases.

A CCL defines data that you can use to filter emails to prevent data loss. Sophos provides expert definitions for common data types. You can also build CCLs to make customized definitions.

You can specify keywords or phrases you want to use to filter emails. You can add a maximum of 200. Keywords and phrases aren't case sensitive.

Related concepts
Create or Edit a Policy (page 457)
You can create or edit a policy as follows.

**Sophos default blocked email attachment types** (page 469)
The following files will be blocked when you select **Use Sophos list** in the **Attachment file types** rule:

**Related tasks**

Create an email data loss prevention rule (page 468)
Add email **Data Loss Prevention** (DLP) rules to control information allowed in emails.

### Create an email data loss prevention rule

Add email **Data Loss Prevention** (DLP) rules to control information allowed in emails.

To create a new rule, you must edit an existing policy, or create a new policy.

Email **Data Loss Prevention** policies contain rules that describe what information to look for in emails and the action to take when matched. To create a rule:

1. Click **Settings**.
2. Click either **Inbound** or **Outbound** to set the direction of emails this rule checks.
3. Click **Add rule**.
4. Give the rule a **Name** and **Description**.
5. Choose the rule type.
   
   You can use templates provided by Sophos to protect your data. Templates protect common types of sensitive information. You can also customize rules using content control lists (CCLs), keywords or phrases.
   
   Choose from:
   
   • **Protect financial information (FI)**
   • **Protect confidential information (CI)**
   • **Protect health information (HI)**
   • **Protect personally identifiable information (PII)**
   • **Protect using attachment file types**
   • **Protect using Sophos content control lists (CCLs)**
   • **Protect using keywords**.
6. Click **Next**.
7. Choose the lists for the rule.
   
   For most rule types you can use lists provided by Sophos or build custom lists specific to your needs.
   
   a) If you chose **Protect using attachment file types**, we recommend you use the default Sophos list. You can also use a custom list, and select the file types you want to filter emails by.
   
   b) If you chose **Protect using keywords**, enter strings to search for. You can also import keywords.
8. Click **Next**.
9. Choose the actions to take when the rule is triggered, who to notify and additional options.
   
   Options change depending on the rule type and direction (**Inbound** or **Outbound**).
   
   For example, if you select **Inbound** the **Bounce** action doesn't appear in the list of actions.
10. Turn the rule on or off.
11. Click **Save**.
Related concepts
Create or Edit a Policy (page 457)
You can create or edit a policy as follows.

Data Loss Prevention policy (page 467)
Data Loss Prevention (DLP) stops data from being leaked by email.

Sophos default blocked email attachment types

The following files will be blocked when you select Use Sophos list in the Attachment file types rule:

Files with these extensions (not case-sensitive):

- apk
- bat
- chm
- cmd
- com
- cpl
- crt
- exe
- hlp
- hta
- inf
- ins
- isp
- js
- jse
- lnk
- mdb
- pcd
- pif
- reg
- scr
- sct
- shs
- vbe
- vbs
- wsf

Files of the following types:

- ELF: executable files for many non-Windows systems
- Mach-O: object files used in macOS and iOS
- MS-DOS
8.12 Settings

The Settings pages are used to specify security settings that apply to all your protected mailboxes. The pages displayed depend on the features included in your license. Some of these pages may also be displayed under Global Settings in Overview.

Note
If you want to apply settings only to certain users, servers, or devices, use the Policies pages instead.

8.12.1 Active Directory Sync

You can import users and user groups from Active Directory to Sophos Central.

In Settings, on the Active Directory Sync page, you can select the Active Directory service you want to use.

- There is a download link for the Sophos Central Active Directory synchronization utility.
- In Endpoint Protection and Email Gateway you can use Azure Active Directory synchronization instead.

Note
If you are using Office 365 you must use Azure Active Directory synchronization.

For instructions on setting up the utility, see the Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

For instructions on configuring Azure Active Directory synchronization, see the Azure Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

Note
Azure Active Directory synchronization does not support Azure Active Directories that contain data migrated from on-premise Active Directories.

Note
Sophos Azure Active Directory synchronization can be used with Sophos Endpoint Protection and Sophos Email. It has not been tested with other Sophos products.

Related concepts
Active Directory Sync Status (page 471)
On the Active Directory Sync page, you can check the sync status and download the installer.

Azure AD Sync Status (page 473)
About Active Directory synchronization (page 471)
Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

Related tasks
Set up synchronization with Active Directory (page 471)
Follow these instructions to set up synchronization with Active Directory.

Set up synchronization with Azure Active Directory (page 474)

Active Directory Sync Status
On the Active Directory Sync page, you can check the sync status and download the installer.

You need to set up Active Directory synchronization before you can see these options.

You can download the latest installer for setting up synchronization with Active Directory.

Sync status
This shows your synchronization status and the synchronization settings in Active Directory.
- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The time of the last synchronization with Active Directory.
- The number of users and groups imported from Active Directory.

You can view Active Directory synchronization alerts on the Overview > Alerts page. You can view synchronization events on the Overview > Logs & Reports > Events page.

About Active Directory synchronization
Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

To synchronize with Active Directory, you need to download and install the Sophos Central Active Directory Sync utility. The utility works as follows.

It synchronizes active users and user groups.

It can run automatically on a regular basis, as set up by the Sophos Central administrator.

It doesn’t duplicate existing users or groups when they are matched to an existing Sophos Central user or group. For example, an email address from Active Directory may be added to an existing user in Sophos Central.

It supports only the Active Directory service.

It can synchronize multiple Active Directory forests. To do this, you need to install the utility on multiple machines and configure each utility to synchronize a different Active Directory forest. We strongly recommend to synchronize different Active Directory forests at different times of day, so that the synchronizations do not overlap.

It doesn’t help you to deploy the Sophos agent software to your users’ devices. Use other methods of deployment with Active Directory.

Set up synchronization with Active Directory
Follow these instructions to set up synchronization with Active Directory.

Before you can set up synchronization, you need .NET Framework 4 on the computer where you will run the Sophos Central AD Sync Utility.
Warning
Before you proceed, make sure all your active directory users are set up correctly with an email address. Users without an email address aren't protected and email going to an email address not tied to a user isn't delivered.

You need to use API credentials to synchronize with Active Directory.

To set up synchronization with Active Directory:

1. Set up your API credentials for AD sync. To do this, click Settings > API credentials.
2. Add a new credential. Enter the following information:
   - Credential name
   - Description
3. Copy the Client ID and Client Secret.
4. Click Settings > Active Directory Sync, and click the link to download the Sophos Central AD Synchronization Utility installer. Then run it.
   Alternatively, go to the Start menu and click Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.
   The Sophos Central AD Sync Utility Setup assistant starts.
5. In the setup wizard, enter the information required.
   Follow the instructions in the Sophos Central AD Sync Utility Setup assistant.
6. On the last page of the setup assistant, select Launch Sophos Central AD Sync Utility and click Finish.
7. In the Active Directory Synchronization Setup utility, on the Sophos Credentials page, enter your Client ID and Client Secret instead of your Sophos Central account credentials.
8. On the AD Configuration page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.
   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the Use LDAP over an SSL connection (recommended) checkbox selected. If your LDAP environment doesn’t support SSL, clear the Use LDAP over an SSL connection (recommended) checkbox and change the port number. The port number is usually 636 for SSL connections and 389 for insecure connections.
9. If you don’t want to synchronize the entire forest, on the AD Filters page, you can specify which domains to include in the synchronization. You can also specify additional search options (search bases and LDAP query filters) for each domain. Distinct options can be specified for users and user groups.

   Note
   AD Sync will only create groups that have members which include discovered users or devices, regardless of group filter settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search bases</td>
<td>You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format:</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OU=Finance,DC=myCompany,DC=com</td>
<td>To filter users, for example, by group membership, you can define a user query filter in this format: memberOf=CN=testGroup, DC=myCompany, DC=com The above query limits user discovery to users belonging to “testGroup”. Note that if you don't specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter: CN=testGroup</td>
</tr>
</tbody>
</table>

Note
If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

10. On the Sync Schedule page, define the times at which the synchronization will be performed automatically.

Note
A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select Never. Only sync when manually initiated.

11. Click Finished.

12. To synchronize immediately, in the AD Sync Utility, click Preview and Sync. Review the changes that will be made during the synchronization. If you are happy with the changes, click Approve Changes and Continue.

The Active Directory users and groups are imported from the Active Directory to Sophos Central.

To stop the synchronization in progress, click Stop.

Azure AD Sync Status

In Settings, on the Azure Sync Settings/Status page, once you configure Azure Active Directory synchronization, you can view:

- The status of Azure Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Azure Active Directory.
- The time of the last synchronization with Azure Active Directory.
Note
Auto synchronization happens every 6 hours. You cannot change this interval.

• The configuration settings for Azure Active Directory synchronization.
  You can amend these by selecting Edit. See Set up synchronization with Azure Active Directory.
Select Sync to run the synchronization process.
You can validate the Azure Active Directory synchronization connection by selecting Test Connection.
You can view Azure Active Directory synchronization alerts on the Alerts page. You can view synchronization events on the Logs & Reports > Events page.

Set up synchronization with Azure Active Directory
You need:
• A Microsoft Azure subscription.
• Azure Active Directory.

CAUTION
You can use either Azure Active Directory synchronization or Active Directory Sync. You can't set up Azure Active Directory synchronization if you are already using Active Directory Sync.

To configure Azure Active Directory synchronization:
1. Set up your Azure applications. To do this follow the instructions in Prerequisites to access the Azure Active Directory reporting API and the instructions in the next two steps.
2. In To register an Azure AD application, do as follows:
   a) Enter a Name.
   b) Enter https://central.sophos.com in Redirect URI.
3. In Get your application’s client secret, do as follows:
   a) Enter a description and expiry date.
   b) Make a note of your Client secret and Secret expiration date.
   c) Make a note of your Application (client) ID and Primary Domain.
4. In Sophos Central, in the left-hand pane, select Settings.
5. On the Settings page, under Administration, select Azure AD Sync Settings/Status.
7. In the Edit Azure AD Sync dialog box, enter the following information, which you obtained when you set up your Azure applications:
   • Client ID
   • Tenant Domain
   • Application Key (client secret)
   • Application Key Expiration
   You do not have to set the expiration date. We recommend that you do enter it so that Sophos Central can send you notifications of when your key is about to expire.
8. Select Test Connection to validate the Azure Sync connection.
9. Select Save.
10. On the next menu, select **Sync** to import users.

   Synchronization starts. This process may take some time.

**Related information**
Prerequisites to access the Azure Active Directory reporting API

### 8.12.2 Role Management

You can use pre-defined administration roles to divide up security tasks according to the administrators’ responsibility level.

In **Settings**, the **Role Management** page shows a list of administration roles and the number of users assigned to each role.

You can only see this option if you are a Super Admin administrator.

Click on a role name to see a detailed description of the role and the names of the people that have that role assigned to them. You can manage the people assigned to a specific role in that role’s page.

**Restriction**
An administrator role affects what a user can do.

**Administration Roles**

Predefined roles cannot be edited or deleted.

Your assigned administrator role affects what you can do.

A Super Admin can add custom roles. These roles are based on the predefined roles but you can restrict the access for a custom role to a specific product.

**Restriction**
You can add custom roles only if you are signed up to the Sophos Early Access Program.

**Super Admin**

Administrators with this role have access to everything in Sophos Central.

They can manage roles and role assignments. In addition, they can create, edit, assign, and delete custom roles.

There must be at least one administrator with the Super Admin role.

**Admin**

Administrators with this role have access to everything in Sophos Central.

They can't manage roles and role assignments.
Help Desk

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

- Look at sensitive logs or reports.
- Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.
- Update the Sophos agent software on a computer.
- Scan computers.
- Modify co-branding.

They can't see role management options. Also they can't see some options, such as Edit buttons.

Read-only

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

- Look at sensitive logs or reports.
- Receive alerts.

They can't see role management options. Also they can't see some options, such as Edit buttons.

User

Administrators with this role have no administration capabilities. They have access only to the Self Service Portal.

Related concepts
User Summary (page 442)

Related tasks
Create an Enterprise Admin (page 629)
Remove administrators (page 481)

You can remove administrators. Removing an administration role from a user does not delete the user.

Add administrators (page 478)
You assign administration roles to users using the Available Users list.

Administration role details
If you click a role on the Role Management page, its details are shown on a separate page.

The sections on that page include the following.

Permissions
This is the access level for a role. The options are Full, Help Desk, or Read-only.

Global Settings
These are the specialized capabilities for a role. The settings are:
• **Access sensitive logs & reports**: This option means that an administrator can view sensitive logs and reports; for example the Audit Logs.

• **Access policy management**: This option means that an administrator can change policy settings.

• **Access policy assignment**: This option means that an administrator can assign policies to users and devices.

**Role Members**

This is a list of the administrators that are assigned to the role. Click on a name to see their full details.

**Administration Roles for Intercept X with EDR**

Administrators can do more if they have Intercept X with EDR.

**Super Admin and Admin**

Administrators with these roles can also:

• View the intelligence report.
• Request the intelligence report
• Add items to the “Clean and Block” list.
• Remove items from the “Clean and Block” list.
• View blocked items.
• Request an on-demand threat case.
• View on-demand threat cases.
• Isolate and un-isolate devices.
• Request a forensic snapshot.
• Request a threat search.
• View a saved threat search.

**Help Desk**

Administrators with this role can also:

• View the intelligence report.
• Request the intelligence report.
• View blocked items.
• Request an on-demand threat case.
• View on-demand threat cases.
• Request a forensic snapshot.
• Request a threat search.
• View a saved threat search.
Read-only

Administrators with this role can also:
- View the intelligence report.
- View blocked items.
- View on-demand threat cases.
- View a saved threat search.

Related concepts
Administration Roles (page 475)

Add administrators

You assign administration roles to users using the Available Users list.

Existing administration roles, if any, are indicated next to the user's name.

A user can only have one assigned role.

For example if you add a Read-only administrator to the list of Help Desk administrators their assigned role will change to Help Desk administrator. They will no longer be a Read-only administrator.

To add an administrator:

1. In Settings, on the Role Management page, select the administrator role that you want to assign.
2. On the role details page, next to Role Members, click Edit.
   
   Note
   
   You can only see this option if you are a Super Admin.

3. In Edit Role Members, select a user in the Available Users list and use the picker arrows to add them to the Assigned Users list for the role. Select Save.
   
   Tip
   
   Enter a name or part of a name in the search box to filter the list of available users.

Add a custom role

You can add custom roles if you are a Super Admin.

Custom roles are based on the predefined roles. You can restrict the access for a custom role to a specific product. You can also create a role that allows an administrator to have full access to one product and read-only access to a second product.

Restriction

If a role doesn't have access to both Endpoint Protection and Server Protection (in some cases Encryption as well), the shared settings are read-only.
The shared settings are:

- Tamper protection
- Allowed applications
- Website management
- Proxy configuration
- Blocked item
- Bandwidth usage (Encryption access required)
- HTTPS updating
- DLP rules
- Manage content control list
- Reject network connections
- EDR threat analysis center

To create a custom role:

1. In **Settings**, on the **Role Management** page, select **Add role**.
2. Give the custom role a name and a description.
3. Select the **Base role** you want to use as the basis for the custom role.
   For example, if you choose **Help Desk** as the **Base role**, administrators with the custom role have **Help Desk** permissions.
4. Choose the product and access type you want the role to have.
   For example, you create a custom role called Endpoint Help Desk. This custom role uses **Read-only** as its **Base role** and **Endpoint Protection** as its selected product with an access type of **Help Desk**.

   This custom role allows any administrators assigned to this role to access **Endpoint Protection** with **Help Desk** permissions.

   a) Choose more than one product, if required.
      You can choose different access types for different products.
      For example, you can create a custom role that has **Help Desk** access permissions for **Endpoint Protection** and **Read-only** access for **Mobile**. You can set the permissions for all other products to **None**. This means that the custom role only has access to **Endpoint Protection** with **Help Desk** permissions and **Mobile** with **Read-only** permissions.

5. Choose the additional access and management options for the custom role.
   - **Enable access to logs & reports**.
   - **Enable policy management (add, edit, and delete)**.
   - **Enable policy assignment to users, device, etc.** (turn policies on and off; and add users, user groups, devices and device groups to existing policies).

   For example, this allows a Super Admin to add these permissions to a Read-only or Help Desk role. You can also use these options to reduce the permissions for an Admin role. For example, you could prevent the custom role from managing policies.

   **Note**
   These additional options only apply to the selected products for the custom role.

   The additional options are the same for all products and access types for the custom role.

6. Select **Save**.
You can now assign this role to administrators.

**Related concepts**
Administration Roles (page 475)

**Related tasks**
Delete custom role (page 480)
You can delete custom roles if you are a Super Admin.
Change roles (page 480)
You can change the assigned roles for administrators if you are a Super Admin.

**Change roles**
You can change the assigned roles for administrators if you are a Super Admin.
You can change roles for multiple administrators at the same time.

**Restriction**
You can't change roles for administrators who are currently signed in.

To change roles:
1. In Settings, on the Role Management page, select the administrator role that you want to assign to other administrators. For example, select a read-only administrator role if you want to assign that role to other administrators.
2. On the role details page, next to Role Members, click Edit.

  **Note**
  You can only see this option if you are a Super Admin.

3. In Edit Role Members, add users from the Available Users list or remove users from the Assigned Users list. Select Save.

  **Tip**
  Enter a name or part of a name in the search box to filter the list of available users.

**Delete custom role**
You can delete custom roles if you are a Super Admin.
You can only delete custom roles. You can't delete roles that have administrators assigned to them. You must change their role first.
1. In Settings, on the Role Management page, select the role you want to remove and select Delete.
   To select a role, click anywhere in the row apart from the name.
2. Select Delete to confirm role deletion.

**Related concepts**
Administration Roles (page 475)

**Related tasks**
Remove administrators (page 481)
You can remove administrators. Removing an administration role from a user does not delete the user.

**Change roles (page 480)**
You can change the assigned roles for administrators if you are a Super Admin.

**Add a custom role (page 478)**
You can add custom roles if you are a Super Admin.

### Remove administrators

You can remove administrators. Removing an administration role from a user does not delete the user.

**Note**
You cannot delete a user who has an assigned administration role. You must remove the role from the user before deleting the user.

To delete administrators:

1. In **Settings**, on the **Role Management** page, select the administrator role from which you want to remove users.
2. On the role details page, next to **Role Members**, click **Edit**.

**Note**
You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, select a user in the **Assigned Users** list and use the picker arrows to remove them.

**Tip**
Enter a name or part of a name in the search box to filter the list of assigned users.

### 8.12.3 User access

You can automatically give your users access to the Sophos Central Self Service Portal (SSP).

To do this go to **Settings > User Access**.

Turn on **Sophos Central Self Service Portal access**.

New users will now have access to the SSP when you add them to Sophos Central. They will receive an email with sign-in instructions.

Any existing users without access will also be given access and sent an email.

If you turn off automatic access, any users that have access at that point can still sign in to the SSP. Only users added after you turn it off won't have access.
8.12.4 Synchronized Security

Synchronized Security monitors outbound mail, and takes action if 5 or more emails that are classified as spam, or contain viruses are sent from a mailbox within a 10 minute period.

Note
Synchronized Security is only available if you have a Sophos Endpoint license and a Sophos Email license.

You can turn the Synchronized Security feature on and off from Settings > General > Synchronized Security.

The blocking process works like this:

1. The originating mailbox is identified.
2. The owner of the mailbox is identified, along with any devices assigned to the owner of the mailbox.
3. The mailbox is blocked from sending emails for 1 hour. After 1 hour, the mailbox is unblocked automatically. You can't unblock it any sooner.
   
   Lockout periods increase every time the blocking process is triggered. The amount of time the mailbox is blocked for is doubled every time the spam threshold is reached. The previous block period needs to end before another can start. These timed blocks can't be removed and you have to let them expire.
   
   After 6 times, the mailbox will be blocked permanently, and the owner will not be able to send any email from that mailbox. If you believe a permanently blocked mailbox should be unblocked, please contact Sophos support.
4. Sophos Anti-Virus runs an on-demand scan on the devices linked to the mailbox.
5. An alert is sent to the administrator saying that the sender has been blocked.
6. The events report is updated to show that the mailbox has been blocked.

Note
If Synchronized Security is turned off, this will only disable the endpoint scan. The senders of outgoing spam and virus emails will still be blocked.

Related information
Sophos Support

8.12.5 Inbound Allow/Block

You can create a list of email domains and addresses that you trust or don't trust.

Restriction
This option is only available if your license includes Sophos Email.

A list of domains and addresses that are allowed to connect with your email system, or are blocked from it, helps you to control spam. This setting only applies to inbound messages.
You can block or allow entire domain names, IP addresses, or specific email addresses. The domain or email address is added to the list and shown as either allowed or blocked. This list is global and applies to all protected mailboxes.

Wildcards are supported for email addresses and domains. For example, *@domain.com would include any addresses that are part of domain.com. Subnet masks are supported from /16 to /32 (inclusive).

You can also use wildcards to block whole top level domains (TLDs). For example, *.top would block every email from the .top TLD. This is useful for blocking email from generic or geographic TLDs that you do not communicate with, and are common sources of spam.

If you add the same address or domain to both the allow and block lists, select Override duplicates to ensure your most recent choice is used.

You can view email domains and addresses that you have already blocked, including IPs that you have blocked, through the Message History and Quarantined Messages settings.

Go to Settings > Inbound Allow/Block to do as follows:
- Add an allowed domain or address.
- Add a blocked domain or address.
- Import a list of domains to block or allow.
- Delete a domain or address.

Related concepts
Message History Report (page 436)
The Message History report details the emails processed by Email Gateway for your protected mailboxes.

Quarantined Messages (page 454)
The Quarantined Messages page lists the email messages that have been quarantined for all your protected mailboxes.

Email Security Policy (page 458)
You can apply security settings to your mailboxes using Email Security policies.

Related tasks
Import allow/block list (page 483)
You can import lists of email domains and addresses to block or allow.

Import allow/block list

You can import lists of email domains and addresses to block or allow.

You can import a list of domains and addresses into the Inbound Allow/Block list. When you import, you can download template files that show you the import list format.

1. Select Add.
2. Select Import allow/block list from the drop-down list.
3. Download the template files.
4. Create your import list in the same format as the template.
5. When you've finished creating your file, return to Import allow/block list to import it.
8.12.6 Manage settings for Sophos Central Self Service

You can manage self service settings for your users.

**Restriction**
This option is only available if your license includes **Sophos Email**.

You can:
- Turn **Emergency Inbox** on or off. This controls whether your users can access their email from Sophos Central Self Service.
- Turn **Allow/Block list** on or off. This controls whether your users can create their own allow and block rules for email addresses and domains.

8.12.7 Domains Settings/Status

Configure and manage email domains protected by **Email Gateway**.
Go to **Settings > Domain Settings/Status**.

Add a domain

**Tip**
Instructions on how to set up your domain for common providers are available online. Example: Office 365.

To view the instructions:
1. Expand **Configure External Dependencies**.
2. Under **Inbound Settings**, click the link for your chosen provider.
3. Use the information to help you configure your email domain.
   - Click **Outbound Settings** to view your outbound relay host.

To add a domain:
1. Click **Add Domain**.
2. In the **Email Domain** text field enter your email domain. Example: `example.com`.
   - Domain ownership must be verified before mail will be delivered through Sophos Central. To verify domain ownership, you need to add a TXT record to your domain. Adding this record will not affect your email or other services.
3. Click **Verify Domain Ownership**.
4. Use the details given in **Verify Domain Ownership** to add the TXT record to your Domain Name Server (DNS).

**Note**
This can take up to ten minutes to take effect.
5. Click **Verify**.

**CAUTION**
You cannot save an unverified domain. You must correct any issues with the domain ownership verification.

6. Select the direction you want to configure the domain for. If you select **Inbound and Outbound** you will need to select an outbound gateway from the drop-down list. If you select **Custom Gateway**, at least one IP/CIDR (subnet range) is required. Enter the IP and CIDR and click **Add**. You can add multiple IP addresses/ranges.

7. Select whether you wish to use a mail host or a mail exchange (MX) record in the **Inbound destination** drop-down list.

    **Note**
    You must use a mail exchange record if you want to use multiple destinations.

    a) If you selected **Mail Host** enter an IP address or an FQDN (fully-qualified domain name) in the **IP/FQDN** text field. Example: `111.111.11.111` or `mymail@example.com`.

    b) If you selected **MX** enter an FQDN in the **MX** text field. Example: `mymail@example.com`.

8. In the **Port** text field enter the port information for your email domain.

9. Expand **Information to configure External Dependencies**.

    The **Mail Routing Settings** tab shows the Sophos delivery IP addresses and MX record values used for configuring mail flow for your region.

    a) Make a note of the appropriate settings so that you know where to allow SMTP traffic from.

    b) Ensure that you configure your mail flow for **Email Security**.

10. Click **Save** to validate your settings.

11. Click the **Base Policy** link to configure spam protection.

    **Note**
    Spam protection applies to all protected mailboxes by default. You must review the settings to check that they are appropriate.

    You can add extra domains at any time.

### Delete a domain

To delete a domain, click on the gray cross to the right of the domain you wish to remove.

### Edit a domain

To edit a domain, click on the domain name in the list, change the settings and click **Save**.
**DKIM keys**

Manage your DKIM keys to sign and authenticate outbound emails.

**Introduction**

DomainKeys Identified Mail (DKIM) is used to authorize an email by verifying its digital signature, which associates a domain name with the email.

**Related information**

**DKIM**

**Outbound DKIM signing**

To set up outbound DKIM signing, you need to generate a DKIM key in [Sophos Email](https://www.sophos.com). A public key is generated which you use to create and publish a DKIM TXT record, and a private key is generated in the background.

When you send an email, [Sophos Email](https://www.sophos.com) applies policy settings to the email and then creates a hash of the mail content and adds a new header.

**Note**

The hash is encrypted by your private key.

When the receiving mail server sees that an email has a DKIM signature, it does a DNS lookup to find the DKIM TXT record associated with the sending domain. It uses the public key to decrypt the digital signature back to the hash value. It then takes the elements of the message that were signed and creates its own hash that it compares it to the decrypted hash. If these do not match, the DKIM check will fail.

**Add a DKIM key**

Add a DKIM record to your domain so that outgoing mail will be signed and authenticated against your domain.

Generate a DKIM key in [Sophos Email](https://www.sophos.com) and create a DNS TXT record for your domain.

**CAUTION**

If you have smart banners turned on, we strongly recommend that you sign emails with a DKIM key. We remove the banners on outbound replies, which modifies the emails.

1. Go to **Email Gateway > Settings > Domains settings/status** and click on the domain you want to add a DKIM key to.
2. Click **Add key**.
3. Copy the DKIM information that is generated automatically and use it to create a DNS TXT record for your domain.
   
   You will need to speak to your third party DNS provider about setting this up.

**Note**

A key pair is generated by Sophos Central. The private key is generated in the background and is stored in Sophos Central. The public key is visible in the DKIM information and is used to create your DNS TXT record.
4. Wait for the DNS TXT record to propagate. This may take up to an hour.
5. Once your DNS TXT record has been published, click on **Test record** to check that your DNS TXT record matches the information in Sophos Central.

**Note**
If the test fails, check your DNS TXT record, correct any mistakes, and click **Test record**.

6. Click the box at the bottom of the window to activate the DKIM key then click **Save**.
The DKIM key is activated. Note that this deactivates any other active DKIM key for that domain. You can now add DKIM keys for your other domains.

### 8.12.8 Email Encryption

You can encrypt emails.

**Restriction**
This option is only available with an **Email Advanced** license.

The encryption type Sophos Email uses is push based email encryption using AES 256.

To turn encryption on or off, go to **Settings > Encryption settings**.

**Note**
Make sure TLS (Transport Layer Security) v1.2 is enabled on your email gateway before enabling encryption here, otherwise the connection with Sophos will break, and you will not be able to send or receive email. The ciphers required are 'TLSv1.2+FIPS:kRSA+FIPS:eNULL!aNULL'. For more information, see [FIPS mode and TLS](#).

### General settings

**Warning**
- Microsoft Office documents, ZIP files and PDF files are encrypted natively.
- Multiple attachments may be generated from files that have been encrypted natively.
- All other files, for example plain text and HTML will be encrypted as PDFs. Email content will be encrypted as a PDF.
- You need to install Adobe Reader to view encrypted emails and attachments that have been encrypted as PDFs.
- You can view and reply to messages on mobile devices.

- You can select the following encryption options:
  - **Send via TLS if available**
    - TLS prevents eavesdropping and tampering with the message in transit.
Note
If TLS is not available, the entire message will be encrypted as a PDF.

— Encrypt entire message
The email and attachments are encrypted with a password.

The first time an encrypted email is sent to you, an email is sent from Sophos asking you to click on a link to set a Sophos Secure Message password. You need to do this within 30 days, otherwise the email expires. When you click on the link, you are directed to Sophos Secure Message where you can set your password.

Note
The password can only be used for emails within the region that the original email came from. If you receive an email from another region, you need to set another password.

After setting the password, you receive an email from Sophos including the encrypted email and any encrypted attachments. To access them, open them and type in the password you created.

You can reply to encrypted emails securely by clicking Reply on the encrypted PDF.

— Encrypt attachments only
The steps are the same as above, however only attachments are encrypted.

— You can also change the language used for notification and registration messages. Select a language from the list.

• End-user options

— Allow your users to send encrypted messages with a subject line tag.
Enter your preferred subject line tag. The tag is not case sensitive.

— Outlook Add-in (for Office 365 users only)
You can allow users to encrypt emails using the Outlook Add-in by downloading and installing the Outlook Add-in relevant for the user’s Outlook client. An Outlook Add-in is available for the Windows client and another Outlook Add-in is available for both Web and Mac clients.

Note
The Outlook Add-in used for Mac clients will only work if you have turned on the Allow your users to send encrypted messages with a subject line tag option. When the subject line tag is changed, the Outlook Add-in must be downloaded and re-installed on Mac clients.

To download an Outlook Add-in, click Download Windows Outlook Add-in or Download Web/Mac Outlook Add-in.

For installation instructions, see Installing the Sophos Outlook Add-in for Encryption.

When you compose an email, to encrypt it with the Outlook Client, click Encrypt. You can deselect Encrypt if you change your mind and do not want to encrypt the email.

In the Web Client and the Windows Client, clicking Encrypt will flag the email for encryption (add a header to the email).
In the Mac client, clicking **Encrypt** will tag the message subject for encryption.

**Addresses and domains**

Add recipient addresses and domains for which you want to encrypt messages. Text is not case sensitive and wildcards are not supported.

**Related concepts**

- Installing the Sophos Outlook Add-in for Encryption (page 489)
  Sophos Outlook Add-in allows users to encrypt messages with one click from within Outlook.

**Related information**

- FIPS mode and TLS

**Installing the Sophos Outlook Add-in for Encryption**

Sophos Outlook Add-in allows users to encrypt messages with one click from within Outlook.

Sophos Outlook Add-in is available for Outlook (Windows or macOS version) and Outlook Web Access, and is compatible with some Office 365 and Exchange environments.

**Is my environment compatible with the Sophos Outlook Add-in?**

Sophos Outlook Add-in works for mail accounts in the following environments:

- Exchange Server 2013 or later (on-premise Exchange).

  **Note**
  Exchange Server 2013 API version 1.4 or older is not supported.

- Office 365 Business subscription (Exchange online).

  **Note**
  Non-Microsoft mail providers (such as Gmail or other POP/IMAP accounts) are not supported.

**Compatible mail clients**

- Outlook for Mac 2016.
- Outlook Web Access (Office 365 only).

**Download the Sophos Outlook Add-in**

**Note**
If you are using macOS make sure encryption is turned on in **Settings** before you download and install the add-in.
• Web/Mac users must download the XML manifest file. To do this, click the **Download Web/Mac Outlook Add-in** link under **Settings > Encryption settings**. Save this file in a location where you will be able to access it during the deployment step.

• Windows users must download the msi installer. To do this, click the **Download Windows Outlook Add-in** link under **Settings > Encryption settings**. Save this file in a location where you will be able to access it during the deployment step.

### Deploy the Sophos Outlook Add-in

• Sideload is recommended for proof of concept and testing purposes only. It refers to the process of installing Sophos Outlook Add-in on an individual end-user system.

• If you want to use Office 365 Centralized Deployment, check if centralized deployment of add-ins will work in your environment.

• If you are ready to begin centralized deployment of Sophos Outlook Add-in, see the "Manage deployment" instructions to get started.

• For customers in an on-premise environment without a connection to Office 365, use the Exchange Admin Center to install Sophos Outlook Add-in for your organization.

#### Related information

- Sideload installation instructions
- Determine if centralized deployment of add-ins works for your Office 365 organization
- Manage deployment of Office 365 add-ins in the Office 365 Admin Center
- Install or remove add-ins for Outlook for your organization

### 8.12.9 Multi-factor authentication

If you’re a Super Admin, you can make some or all of the Sophos Central admins sign in with multi-factor authentication.

#### Introduction

Using multi-factor authentication means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos or Google Authenticator, SMS or email authentication to sign in.

Multi-factor authentication is turned on by default for newly created Sophos Central accounts.

This page tells you how to do the following:

• Set up multi-factor authentication.

• Sign in with multi-factor authentication for the first time.

• Add another method for multi-factor authentication.

• Sign in with email authentication if you don’t have Sophos or Google Authenticator.

• Reset an admin’s sign-in details, for example if they lose their phone.

• Turn off multi-factor authentication for an admin.
Set up multi-factor authentication

If you're a Super Admin, you can choose how your administrators sign in.

To set up multi-factor authentication, do as follows:

1. Go to Settings > Multi-factor Authentication (MFA).
2. Choose how you want admins to sign in:
   - **No MFA needed.**
   - **All admins need MFA.** This is the default for new accounts.
   - **Select admins who will need MFA.** This lets you select individual admins.
3. If you choose **Select admins who will need MFA**, a user list is displayed. Click **Add admins** (on the right of the screen). Move admins to the **Assigned Users** list and click **Add**.
4. Click **Save**.

When admins next sign in, they are prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

The first time you sign in with MFA, do as follows:

1. At the sign-in screen, enter your user ID (email address) and password.
   - A **Set Up Your Login Information** dialog explains that signing in needs additional authentication.
2. In the next dialog:
   a) Enter the security code that has been sent to you in an email.
   b) Create a 4-digit PIN. This enables you to use email as an authentication method.
3. In the next dialog, choose authentication type.
4. In **Verify Your Device**, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
   - You also need to enter a security code to verify a device if you have chosen SMS as your authentication type.

Sophos Central Admin opens.

The next time you sign in, you only need to enter a code from Sophos or Google Authenticator when prompted.

Add another authentication option for multi-factor authentication

You can set up multiple authentication options for a Sophos Central Admin account.

You can authenticate with SMS and Sophos or Google Authenticator.

You must have an authentication option already set up.

To set up another authentication option, do as follows:

1. Sign in to Sophos Central Admin.
2. Click your account name and click **Manage Login Settings**.
3. Click **Create New Method**.
4. Choose another authentication method.
5. Click **Next**.
6. In **Verify Your Device**, scan the QR code and enter the security code that Sophos or Google Authenticator displays.

7. To confirm that the new method has been added, click your account name and click **Manage Login Settings**.
   An additional authentication method has been added.

**Sign in with email authentication**

If you don’t have access to Sophos or Google Authenticator, you can sign in with email authentication instead.

1. At the sign-in screen, enter the user ID (email address) and password.

2. In **Verify Your Login**, click **Choose Another Method**.

3. In **Pick Your Challenge**, click the email option.
   An email is sent to you.

4. Open the email and find the security code.

5. In **Verify Your Login**, enter the security code and your 4-digit PIN.

You’ll be asked for the security code and PIN each time you sign in from now on, until you switch back to using Sophos or Google Authenticator.

**Reset an admin’s sign-in details**

If an admin replaces or loses their phone, you can allow them to set up their sign-in again.

1. On the **People** page, under **Users**, find the user and click their name to open their details.

2. In the user details, on the left of the screen, you’ll see their MFA status and settings. Click **Reset** and confirm that you want to do a reset.

The next time the admin tries to sign in, they’ll need to go through the setup steps again.

**Turn off multi-factor authentication**

If you’re a Super Admin, you can turn off multi-factor authentication for an administrator.

To turn off multi-factor authentication, do as follows:

1. Go to **Settings > Multi-factor Authentication (MFA)**.

2. Click **Select admins who will need MFA**.

3. Click **Add admins**.

4. Move the administrator from the **Assigned Users** list and to the **Available Users** list.

5. Click **Add**.

6. Click **Save**.

**8.12.10 Time of Click Block/Warn Pages**

You can add suspicious sites to the **Time of Click Block/Warn Pages**.

**Restriction**

This option is only available with an **Email Advanced** license.

To manage Time of Click URL Protection settings for suspicious sites, go to **Settings > Time of Click Block/Warn Pages**.
Turn on **Custom Block & Warn Pages** to enable customization.

You can enter your own message to be displayed when a URL is either blocked or warned. Click **Preview** to view the page.

You can also upload a custom logo by entering the path where the logo is stored. Click **Save** when you are satisfied with your changes.

### 8.12.11 URL allow list

You can add domains to the allow list so that URLs from those domains are neither rewritten nor scanned by **Time of Click** protection.

**Restriction**

This option is only available with an **Email Advanced** license.

Click **Add** and enter the URL you want to allow, for example *domain.com*, then click **Save**.

**Note**

Wildcards are supported, for example *domain.com*.

To delete a URL from the allow list, select it and click **Delete**. You can select single, multiple or all URLs.

### 8.12.12 Enforced TLS connections

You can force specific external domains to use Transport Layer Security (TLS) connections for email.

**Restriction**

This option is only available with an **Email Advanced** license.

To manage domain names with TLS connections, go to **Settings > Enforced TLS Connections**. You can:

- Add domain names (wildcards are supported).
- Search the list of domains that already have TLS connection enforced.
- Change the settings for a domain.
- Delete domain names from the list.

If you have issues with TLS connections, check that TLS is enabled, with the correct version and correct ciphers (see below). If you still have problems, contact Sophos Email Support.

**Adding a new domain name**

When you add a new domain name to the list, servers connect to and from that domain with TLS. The email gateway connects with servers using TLS 1.2 or later, and with ciphers consistent with our email encryption product. The connection is valid if a STARTTLS ping returns successfully.
Note
Make sure TLS 1.2 is enabled on your email gateway before enforcing it on any domains. Otherwise the connection with Sophos breaks and you cannot send or receive email. The ciphers required are 'TLSv1.2+FIPS:kRSA+FIPS:!eNULL:!aNULL'.

TLS failures

If Sophos Email can't make a TLS connection, email isn't sent. Email is queued for redelivery for 7 days. After this it is deleted.

Logging of TLS connection errors

Each time Sophos Email can't send email due to TLS failures it makes an entry in the history log. After the final failure, an entry saying that the email was deleted because of TLS policy is added to the log. The entries have this format: "Processing: Check TLS".

Related concepts
Email Encryption (page 487)
You can encrypt emails.

Related information
FIPS mode and TLS

8.12.13 Impersonation Protection and VIP Management

Impersonation Protection detects phishing emails that pretend to come from well-known brands or from important people within your organization.

Restriction
This option is only available with an Email Advanced license.

Impersonation Protection looks for two types of impersonation:
1. Imitation of a well-known brand, often a financial organization or online shopping site.
2. Use of the names of important people in phishing emails.

Impersonation Protection is turned on by default and controlled by Email Security policy settings.

VIP management

On the VIP management page you can enter up to 200 email addresses of very important people (VIPs) in your organization. Emails are monitored for signs of impersonation of these addresses.

You can manually add email addresses with the Add VIP function.

The Help me find VIPs function searches a connected Active Directory (AD) service for high-risk users. The more information you've added to your AD entries (for example job titles) the better the results are. You then select users from the search results.
8.13 Integrate Sophos Email with external services

You can configure external mail services to route mail through Sophos Email.

For Office 365, see How to configure Sophos Email for Office 365 and Set up outbound email handling with Microsoft Office 365.

For Google, see Set up Sophos Email for G Suite and Set up outbound email handling with Google G Suite.

For other services, see How to configure Sophos Email for Exchange and all other clients and Set up outbound email handling with Exchange and other clients.

Related concepts
Set up outbound email handling with Microsoft Office 365 (page 502)
This section describes how to set up outbound scanning from your Office 365 account.

Related tasks
Set up outbound email handling with Exchange and other clients (page 517)
This document guides you through the process of directing all outbound email via Sophos Email. For Exchange, this requires an SMTP Connector to be configured on your Exchange Server.

Set up outbound email handling with Google G Suite (page 511)
You can set up email handling with Google G Suite.

Related information
How to configure Sophos Email for Office 365 (page 495)
This topic explains how to set up Microsoft Office 365 to route email through Sophos Email.

How to configure Sophos Email for G Suite (page 504)
This topic explains how to set up Google G Suite to route email through Sophos Email.

How to configure Sophos Email for Exchange and all other clients (page 512)
This topic explains how to set up Microsoft Exchange and all other email clients to route email through Sophos Email.

8.13.1 How to configure Sophos Email for Office 365

This topic explains how to set up Microsoft Office 365 to route email through Sophos Email.

Related information
Office 365
Add your domain and verify ownership

You need to add your domain.

Note
You will need to provide the following information when configuring Sophos Email to process and deliver email for your domain:

- Your email domain name
- Your mail delivery destination host as a Fully Qualified Domain Name (FQDN) or IP address
- The port number that is used to listen for SMTP traffic on the mail delivery destination host

To find your FQDN for Office 365:

- Log into the office portal.
- Select Domains.
- Copy the value displayed for the expected MX record.

Note
The format is normally <yourdomain-com>.mail.protection.outlook.com

To add a domain in Sophos Central:

1. Click Email Gateway > Settings.
2. Click Domain Settings/Status.
3. Click Add Domain.
4. Enter your email domain details, direction of traffic and delivery destination details.
5. Next, click Verify Domain Ownership.
6. Copy the TXT value presented in the Verify Domain Ownership dialog.
   This value is specific to your email domain.
7. Create a TXT DNS record in the root level of the domain name (entered in step 5) and paste the TXT value that was copied in the last step. You can give it the same TXT name as shown or use @. If you are not sure how to do this, contact the organization that registered your domain name.
8. Once the new TXT DNS record entry has been saved, click Verify.

Once the DNS update with the correct TXT value has been propagated, a message will be returned indicating that the domain verification was successful.

If the DNS update has not yet propagated, or if the value entered is incorrect, a failure message will be returned. Confirm that the value entered is correct.

Note
The domain verification process may take some time to complete, so it may be worth waiting to check that it is successful.
Add mailboxes to Email Gateway

You can add mailboxes to Email Gateway.

You can add mailboxes in the following ways:

1. Automatically using Active Directory Sync. You can choose from the following Active Directory services:
   - AD Sync
   - Azure Sync
2. Manually using the UI.

Add users or mailboxes using AD Sync

You can add mailboxes using AD Sync.

Before you can set up synchronization, you need .NET Framework 4.5 or higher installed on the computer where you will run the Sophos Central Active Directory Synchronization Utility.

To set up synchronization with Active Directory:

1. On the Active Directory Sync Status page, click the link to download the Sophos Central Active Directory Synchronization Utility installer, then run it.
2. In the setup wizard, enter the information required. On the last page, select Launch Sophos Central AD Sync Utility and click Finish.
   Alternatively, go to the Windows Start menu > All Programs > Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.

   Follow the instructions in the Sophos Central Active Directory Synchronization Setup wizard.
3. On the Central Credentials page, enter your Sophos Central account credentials.
4. On the AD Configuration page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the Use LDAP over an SSL connection checkbox selected. If, however, your LDAP environment doesn't support SSL, clear the Use LDAP over an SSL connection checkbox and change the port number accordingly. Usually, the port number is 636 for SSL connections and 389 for insecure connections.
5. If you don't want to synchronize the entire forest, on the AD Filters page, you can specify which domains to include in the synchronization. You can also specify additional search options—search bases and LDAP query filters—for each domain. Distinct options can be specified for users and groups.

   **Note**
   AD Sync will only create groups that have members which include discovered users, regardless of group filter settings.

   a) **Searchbases**: You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format:
OU=Finance,DC=myCompany,DC=com

b) **LDAP query filters**
To filter users, for example, by group membership, you can define a user query filter in this format:

```
memberOf=CN=testGroup,DC=myCompany,DC=com
```

The above query will limit user discovery to users belonging to “testGroup”. Note that if you don't also specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter:

```
CN=testGroup
```

**Note**
If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

6. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.

**Note**
A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select **Never. Only sync when manually initiated**.

7. To synchronize immediately, click **Preview and Sync**. Review the changes that will be made during the synchronization. If you are happy with the changes, click **Approve Changes and Continue**.

The Active Directory users and groups are imported from the Active Directory to the Sophos Central Admin console.

a) To stop the synchronization in progress, click **Stop**.

**Add a mailbox manually**

**Sophos Email** allows you to add single mailboxes manually via the user interface.

To add a mailbox manually:

1. Click **Mailboxes**.
2. On the **Mailboxes** screen, click **Add**.
3. Select **Add Mailbox**.

There are three types of mailbox:

- **User Email**: a mailbox for a person. Example: firstname.lastname@companyname.com.

  **Tip**
  For a User Email mailbox you can click on the mailbox name to view the user’s details.
- **Distribution List**: a mailbox for a group of people. Example: support@companyname.com.
- **Public Folder**: a mailbox for collecting information such as surveys or feedback. Example: survey@companyname.com.

4. Select a mailbox type.
5. Enter a name for the mailbox.
6. Enter the SMTP address for the mailbox.
7. Click **Save** to create a single mailbox and exit, or **Save and Add Another** to create additional mailboxes.

**Import Mailboxes**

**Sophos Email** allows you to import mailboxes in bulk.

To import mailboxes:
1. Create your import .csv file using the following format:

<table>
<thead>
<tr>
<th>Name</th>
<th>Email Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Alamar</td>
<td><a href="mailto:robert.alamar@test.com">robert.alamar@test.com</a></td>
<td>User</td>
</tr>
<tr>
<td>Support DL</td>
<td><a href="mailto:support@test.com">support@test.com</a></td>
<td>DL</td>
</tr>
<tr>
<td>Vacation Calendar</td>
<td><a href="mailto:vacation@test.com">vacation@test.com</a></td>
<td>PF</td>
</tr>
</tbody>
</table>

2. Click **Add Mailbox** and select **Import Mailboxes**.
3. Click **Browse** and navigate to your import file.
4. Click **Add** to start the import process.

Import will run and display results after it completes.

To verify mailbox creation, you can search for new users in the **People** section or browse the list of mailboxes under the **Mailboxes** section for Distribution Lists and Public Folders.

**Bypass Exchange Online Protection in Office 365**

If you are using **Sophos Email** for your spam filtering and clean email is delivered to Office 365, you need to bypass Exchange Online Protection (EOP) to ensure smooth delivery of your mail.

To bypass Exchange Online Protection:
1. Log in to the office portal.
2. Under Admin Centers, choose **Exchange**.
3. Under **Mailflow**, select **Rules**.
4. Click the + to add a new rule and choose **Bypass Spam Filtering** from the menu.
5. Set the following values:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Sophos Central EOP Bypass</td>
</tr>
<tr>
<td>Apply this rule if</td>
<td>Apply to all messages</td>
</tr>
<tr>
<td>Do the following</td>
<td>Set the spam confidence level (SCL) to...</td>
</tr>
</tbody>
</table>
6. Click **Save** to add the rule.

### Restrict delivery to Sophos IP addresses

To add an additional level of security to the integration between **Sophos Email** and your mail host, we recommend that you configure the connection to your mail host to be restricted to our delivery IPs.

**Note**

Before you proceed, we strongly recommend testing mail flow and domain configuration in a non-production/test environment prior to making any changes to the mail flow for your company.

The specific delivery IP that you will need to use is tied to the region in which your Sophos Central account is hosted. When your Sophos Central account was created, you would have chosen to store your data in the United States, Germany, or Ireland.

<table>
<thead>
<tr>
<th>Region</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>US (West)</td>
<td>52.41.236.76</td>
</tr>
<tr>
<td></td>
<td>50.112.39.248</td>
</tr>
<tr>
<td>US (East)</td>
<td>18.220.12.142</td>
</tr>
<tr>
<td></td>
<td>18.216.7.10</td>
</tr>
<tr>
<td>Germany</td>
<td>52.58.166.242</td>
</tr>
<tr>
<td></td>
<td>52.29.100.147</td>
</tr>
<tr>
<td>Ireland</td>
<td>52.208.126.243</td>
</tr>
<tr>
<td></td>
<td>52.31.106.198</td>
</tr>
</tbody>
</table>

**Note**

Using an IP other than the one specified for your region will prevent mail from flowing properly.

### Configure a Secure Connector between Office 365 and Sophos Email

You need to configure a secure connector to **Sophos Email**.

To configure the secure connector:

1. Log in to your Office 365 Admin Portal.
2. Click **Exchange** then go to **Exchange Admin Center**.
3. Click **mail flow** then click **connectors**.
4. Click the + to add a new connector.
5. Select **Partner Organization** in the **From** field.
6. Select **Office 365** in the **To** field.
7. Click **Next**.
8. Enter a name for the connector. **Sophos Email Connector** is recommended.
9. Enter a description (optional).
10. If you want to turn the connector on immediately after saving, leave the box labeled, **Turn it on** checked. Otherwise, uncheck the box to turn it on later.
11. Click **Next**.
12. Select **Use the sender's domain**.
13. Click the + to add a sender domain.
14. Enter * to apply the settings to all sender domains.
15. Click **Next**.
16. Select **Reject email messages if they aren't sent over TLS** and **Reject email messages if they aren't sent from within this IP address range**.
17. Click the + to add sender IP addresses.
18. Enter the Sophos Email Delivery IP address for your region here. To find out which IP address to use, see **Restrict delivery to Sophos IP addresses**.
19. Click **Next**.
20. Verify the new connector settings and click **Save**.

When you configure a connector this way, only mail coming from Sophos Central IPs will be accepted by Office 365.

**Modify MX records to point to Sophos Email**

Modifying your domain’s MX records to point to **Sophos Email** is crucial to the successful deployment of the solution and ensures all email is filtered and delivered.

If you can’t make these changes yourself, contact your IT department, hosting provider, ISP or Domain Name Service provider and arrange for the MX records for your domain(s) to be modified.

When you created your Sophos Central account, you selected a region in which you wanted to store your data. Your MX records are dependent on this region.

Modify your MX records to include the record names associated to the region that you chose to store your data in.

<table>
<thead>
<tr>
<th>Region</th>
<th>MX Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States (West)</td>
<td>10, mx-01-us-west-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-us-west-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>United States (East)</td>
<td>10, mx-01-us-east-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-us-east-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>Germany</td>
<td>10, mx-01-eu-central-1.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-eu-central-1.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>Ireland</td>
<td>10, mx-01-eu-west-1.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-eu-west-1.prod.hydra.sophos.com</td>
</tr>
</tbody>
</table>
Notes

Please take care with all options to ensure that the spelling and numbers are correct.

Using MX record names other than those provided will prevent mail from flowing properly.

It is always recommended when changing DNS entries like MX records to lower the TTL (to 600 ms or less) on the records well in advance of updating the entries. This will allow the change to propagate in minimum time and provides a quick way to revert the change should there be any issues encountered during testing.

Test and confirm mail flow

Once you have updated your MX records, send a test message to any of your mailboxes protected by Sophos Email. For a true test, you should send your test message from an address outside of your email domain.

To confirm that the message flowed through Sophos Email, you can view the Message History Report.

To access the report:
1. In Sophos Central, click Logs and Reports.
2. Click Message History.
   If messages are flowing through the system, you will see entries in this report.

   If mail is not flowing, meaning you are not receiving email to your test inbox, take the following steps:
1. Verify that your MX records are correct for your region.
2. Verify that you set up the Sophos Delivery IPs correctly in your gateway, firewall or connector.
3. Verify that the mailbox that you are sending to exists in Sophos Email.

If you have taken all these steps and mail is still not flowing for your domain, you should contact Sophos Email Support.

8.13.2 Set up outbound email handling with Microsoft Office 365

This section describes how to set up outbound scanning from your Office 365 account.

You need to:
1. Update your SPF record for your domain(s) to include Sophos Email.
2. Configure routing so that outbound mail is sent through Sophos Email.

Related tasks
Updating the SPF record for your domain (page 503)
Your organization should already have a SPF record for your domains registered with Microsoft Office 365. You need to update this record in the DNS zone for the relevant domain.

Configuring outbound routing (page 503)
You need to configure outbound routing.

### Updating the SPF record for your domain

Your organization should already have a SPF record for your domains registered with Microsoft Office 365. You need to update this record in the DNS zone for the relevant domain.

To update your record:

1. Remove `v=spf1 include:spf.protection.outlook.com -all`.
2. Replace with or add `v=spf1 include:_spf.prod.hydra.sophos.com -all`.

If your outbound email is being routed through Sophos Email and Office 365 simultaneously for a period, you can leave the original SPF record, and add an include statement for Sophos Email. However, we recommend you replace it with the Sophos Email SPF record once all your outbound email is routed through us.

If you are certain that you do not have any third parties sending mail on your behalf, and all your outbound mail is routed through Sophos Email, you can add a hard fail instead: `v=spf1 include:_spf.prod.hydra.sophos.com -all`.

**Note**

This means that your mail needs to be sent from Sophos Email to be accepted by the receiver's mail servers (if they carry out SPF checks).

### Configuring outbound routing

You need to configure outbound routing.

To configure routing:

1. Sign in to Sophos Central.
2. Click Email Gateway > Settings > Domain Settings/Status.
3. Select your domain.
4. Select Inbound and Outbound as the direction under Configure Domain.
5. In the Outbound Gateway drop down list, select Microsoft Office 365 and click Save.
6. Then click Configure External Dependencies.
7. Click Outbound Settings and copy the Outbound Relay Host address.
8. Log in to the Office 365 Admin Center.
The Exchange Admin Center is displayed.
10. Select Mail Flow > Connectors and create a new Connector:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Select Office 365 from the drop down list.</td>
</tr>
<tr>
<td>To</td>
<td>Select Partner Organization from the drop down list.</td>
</tr>
</tbody>
</table>

11. Click Next.
12. Enter the following:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the Connector.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally, enter a description for the Connector.</td>
</tr>
<tr>
<td>Turn It On</td>
<td>Select this option to enable the Connector.</td>
</tr>
</tbody>
</table>

13. Click **Next**.
14. Select **Only when email messages are sent to these domains**.
15. Click the + icon to add the recipient domains that should use this connector.
16. Enter a value of * to route all outbound emails through Sophos.
17. Click **OK** and **Next**.
18. Select **Route Email Through These Smart Hosts**.
19. Click the + icon to add the smart hosts.
20. To retrieve the text you need to insert into the smart host, sign in to Sophos Central.
21. Click **Email Gateway > Settings > Domain Settings/Status**.
   a) Copy and paste the text in **Outbound Relay Host**. This is the text you will need to enter into the smart host webpage. For example, relay-us-east-2.prod.hydra.sophos.com.
   b) Paste the text into the field and click **Save**.
22. Click **Next**.
23. Select the following options:
   • **Always use Transport Layer Security (TLS) to Secure the Connection**
   • **Any digital certificate, including self-signed certificates**.
24. Click **Next** to verify your settings.
25. Click **Next** and add an email address of a recipient from a domain external to your organization.
26. Click **Validate**.
27. Once Office 365 has successfully validated your settings, click **Save**.

Disable or remove any other Outbound Send Connectors that were previously used. Failure to do this means your outbound email still uses these older send connectors, and is not routed through **Sophos Email**. Any send connectors used for other purposes (e.g archiving) may still be required to be enabled. If in doubt, consult Sophos Support.

**Note**
It may take up to 24 hours for the changes to propagate.

### 8.13.3 How to configure Sophos Email for G Suite

This topic explains how to set up Google G Suite to route email through Sophos Email.

**Related tasks**
Set up synchronization with Azure Active Directory (page 474)

**Related information**
G Suite MX record values
Set up an inbound mail gateway
Add your domain and verify ownership

You need to add your domain.

Note
You will need to provide the following information when configuring Sophos Email to process and deliver email for your domain:

- Your email domain name
- The MX records for Google Apps.
- The port number that is used to listen for SMTP traffic on the mail delivery destination host

To add a domain in Sophos Central:

1. Click Email Gateway > Settings.
2. Click Domain Settings/Status.
3. Click Add Domain.
4. Enter your email domain details.
5. Configure your delivery destination.
   a) For delivery destination and port, enter MX, and the value routing-mx.<yourdomain.com> on Port 25. You will configure your routing MX values after you verify domain ownership.
6. Next, click Verify Domain Ownership.
7. Copy the TXT value presented in the Verify Domain Ownership dialog.
   This value is specific to your email domain.
8. Create a TXT DNS record in the root level of the domain name (entered in step 5) and paste the TXT value that was copied in the last step. You can give it the same TXT name as shown or use @.
9. Once the new TXT DNS record entry has been saved, click Verify.

Once the DNS update with the correct TXT value has been propagated, a message will be returned indicating that the domain verification was successful.

If the DNS update has not yet propagated, or if the value entered is incorrect, a failure message will be returned. Confirm that the value entered is correct.

Note
The domain verification process may take some time to complete, so it may be worth waiting to check that it is successful.

Configure routing-mx values to deliver to G Suite

To provide failover for the inbound connection between Sophos Email and G Suite you need to setup new MX records on a new subdomain of your mail domain.

In this example, we recommend using routing-mx.<yourdomain.com>.

Note
This is different to configuring the MX records for mail delivery on your domain itself. Adding these records will have no impact on mailflow at this point, as we are just using these records for the delivery destination configured within Sophos Email.
How this is configured will vary with different DNS providers, but typically you would enter the type as MX, the hostname as routing-mx, and the destination and priority as per the Google URLs in the screenshot below. The key point is to have ASPMX.L.GOOGLE.COM as the highest priority record.

![DNS Configuration Screenshot](image)

Note
If you prefer, you can skip this step, and configure the delivery destination to point directly to ASPMX.L.GOOGLE.COM. However, if there is an issue contacting ASPMX.L.GOOGLE.COM, mail will not be delivered to Google’s alternate MX server.

Add mailboxes to Email Gateway
You can add mailboxes to Email Gateway.
You can add mailboxes in the following ways:
1. Automatically using Active Directory Sync. You can choose from the following Active Directory services:
   - AD Sync
   - Azure Sync
2. Manually using the UI.

Add users or mailboxes using AD Sync
You can add mailboxes using AD Sync.

Before you can set up synchronization, you need .NET Framework 4.5 or higher installed on the computer where you will run the Sophos Central Active Directory Synchronization Utility.

To set up synchronization with Active Directory:
1. On the Active Directory Sync Status page, click the link to download the Sophos Central Active Directory Synchronization Utility installer, then run it.
2. In the setup wizard, enter the information required. On the last page, select Launch Sophos Central AD Sync Utility and click Finish.
   Alternatively, go to the Windows Start menu > All Programs > Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.
   Follow the instructions in the Sophos Central Active Directory Synchronization Setup wizard.
3. On the **Central Credentials** page, enter your Sophos Central account credentials.

4. On the **AD Configuration** page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the **Use LDAP over an SSL connection** checkbox selected. If, however, your LDAP environment doesn’t support SSL, clear the **Use LDAP over an SSL connection** checkbox and change the port number accordingly. Usually, the port number is 636 for SSL connections and 389 for insecure connections.

5. If you don’t want to synchronize the entire forest, on the **AD Filters** page, you can specify which domains to include in the synchronization. You can also specify additional search options—search bases and LDAP query filters—for each domain. Distinct options can be specified for users and groups.

   **Note**
   
   AD Sync will only create groups that have members which include discovered users, regardless of group filter settings.

   a) **Searchbases**: You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format:
   
   \text{OU=Finance,DC=myCompany,DC=com}

   b) **LDAP query filters** To filter users, for example, by group membership, you can define a user query filter in this format:
   
   \text{memberOf=CN=testGroup,DC=myCompany,DC=com}

   The above query will limit user discovery to users belonging to “testGroup”. Note that if you don’t also specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter:
   
   \text{CN=testGroup}

   **Note**
   
   If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

6. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.

   **Note**
   
   A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

   If you want to synchronize manually by running the AD Sync utility and don’t want the synchronization to run automatically on a regular basis, select **Never. Only sync when manually initiated.**

7. To synchronize immediately, click **Preview and Sync**. Review the changes that will be made during the synchronization. If you are happy with the changes, click **Approve Changes and Continue**.
The Active Directory users and groups are imported from the Active Directory to the Sophos Central Admin console.

a) To stop the synchronization in progress, click **Stop**.

### Add a mailbox manually

**Sophos Email** allows you to add single mailboxes manually via the user interface.

To add a mailbox manually:

1. Click **Mailboxes**.
2. On the **Mailboxes** screen, click **Add**.
3. Select **Add Mailbox**.

There are three types of mailbox:

- **User Email**: a mailbox for a person. Example: firstname.lastname@companyname.com.

  **Tip**
  For a User Email mailbox you can click on the mailbox name to view the user’s details.

- **Distribution List**: a mailbox for a group of people. Example: support@companyname.com.

- **Public Folder**: a mailbox for collecting information such as surveys or feedback. Example: survey@companyname.com.

4. Select a mailbox type.
5. Enter a name for the mailbox.
6. Enter the SMTP address for the mailbox.
7. Click **Save** to create a single mailbox and exit, or **Save and Add Another** to create additional mailboxes.

### Add Mailboxes via Import

**Sophos Email** allows you to add mailboxes in bulk mailbox import.

To add import mailboxes:

1. Create your import .csv file using the following format:

<table>
<thead>
<tr>
<th>Name</th>
<th>Email Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Alamar</td>
<td><a href="mailto:robert.alamar@test.com">robert.alamar@test.com</a></td>
<td>User</td>
</tr>
<tr>
<td>Support DL</td>
<td><a href="mailto:support@test.com">support@test.com</a></td>
<td>DL</td>
</tr>
<tr>
<td>Vacation Calendar</td>
<td><a href="mailto:vacation@test.com">vacation@test.com</a></td>
<td>PF</td>
</tr>
</tbody>
</table>

2. Click **Add Mailbox** and select **Import mailboxes**.
3. Click **Browse** and navigate to your import file.
4. Click **Add** to start the import process.

Import will run and display results after it completes.

To verify mailbox creation, you can search for new users in the **People** section or browse the list of mailboxes under the **Mailboxes** section for Distribution Lists and Public Folders.
Restrict delivery to Sophos IP addresses

To add an additional level of security to the integration between Sophos Email and your mail host, we recommend that you configure the connection to your mail host to be restricted to our delivery IPs.

Note
Before you proceed, we strongly recommend testing mail flow and domain configuration in a non-production/test environment prior to making any changes to the mail flow for your company.

The specific delivery IP that you will need to use is tied to the region in which your Sophos Central account is hosted. When your Sophos Central account was created, you would have chosen to store your data in the United States, Germany, or Ireland.

<table>
<thead>
<tr>
<th>Region</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>US (West)</td>
<td>52.41.236.76  50.112.39.248</td>
</tr>
<tr>
<td>US (East)</td>
<td>18.220.12.142  18.216.7.10</td>
</tr>
<tr>
<td>Germany</td>
<td>52.58.166.242  52.29.100.147</td>
</tr>
<tr>
<td>Ireland</td>
<td>52.208.126.243 52.31.106.198</td>
</tr>
</tbody>
</table>

Note
Using an IP other than the one specified for your region will prevent mail from flowing properly.

Create an Inbound Gateway in G Suite

Because you are using Sophos Email to filter your mail and have your MX records pointed directly to us, you will want to restrict delivery to G Suite to only Sophos Delivery IPs.

To configure this setting:
1. Log in to your G Suite Admin Console.
2. Navigate to Apps > G Suite > Settings for Gmail > Advanced settings.
3. On the General Settings tab, scroll down to Inbound Gateway.
4. Click Configure.
5. Describe the Inbound Gateway – “Sophos Email Inbound Gateway.”
6. Click Add and enter the gateway IPs that correspond to your region. You will need to save after each entry.
7. Turn on:
   • Automatically detect external IP (recommended).
   • Reject all mail not from gateway IPs.
• Require TLS connections from the email gateways listed above.

8. Click Add Setting.

You should then see your settings applied after save.

Modify MX records to point to Sophos Email

Modifying your domain's MX records to point to Sophos Email is crucial to the successful deployment of the solution and ensures all email is filtered and delivered.

If you can't make these changes yourself, contact your IT department, hosting provider, ISP or Domain Name Service provider and arrange for the MX records for your domain(s) to be modified.

When you created your Sophos Central account, you selected a region in which you wanted to store your data. Your MX records are dependent on this region.

Modify your MX records to include the record names associated to the region that you chose to store your data in.

<table>
<thead>
<tr>
<th>Region</th>
<th>MX Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States (West)</td>
<td>10, mx-01-us-west-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-us-west-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>United States (East)</td>
<td>10, mx-01-us-east-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-us-east-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>Germany</td>
<td>10, mx-01-eu-central-1.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-eu-central-1.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>Ireland</td>
<td>10, mx-01-eu-west-1.prod.hydra.sophos.com</td>
</tr>
<tr>
<td></td>
<td>20, mx-02-eu-west-1.prod.hydra.sophos.com</td>
</tr>
</tbody>
</table>

Notes

Please take care with all options to ensure that the spelling and numbers are correct.

Using MX record names other than those provided will prevent mail from flowing properly.

It is always recommended when changing DNS entries like MX records to lower the TTL (to 600 ms or less) on the records well in advance of updating the entries. This will allow the change to propagate in minimum time and provides a quick way to revert the change should there be any issues encountered during testing.

Test and confirm mail flow

Once you have updated your MX records, send a test message to any of your mailboxes protected by Sophos Email. For a true test, you should send your test message from an address outside of your email domain.

To confirm that the message flowed through Sophos Email, you can view the Message History Report.

To access the report:
1. In Sophos Central, click **Logs and Reports**.
2. Click **Message History**.
   
   If messages are flowing through the system, you will see entries in this report.

If mail is not flowing, meaning you are not receiving email to your test inbox, take the following steps:
1. Verify that your MX records are correct for your region.
2. Verify that you set up the Sophos Delivery IPs correctly in your gateway, firewall or connector.
3. Verify that the mailbox that you are sending to exists in **Sophos Email**.

If you have taken all these steps and mail is still not flowing for your domain, you should contact Sophos Email Support.

### 8.13.4 Set up outbound email handling with Google G Suite

You can set up email handling with Google G Suite.

To configure outbound scanning from your G Suite account:

1. Sign in to Sophos Central.
2. Click **Email Gateway** > **Settings** > **Domain Settings /Status**.
3. Select your domain.
4. Select **Inbound and Outbound** as the direction under **Configure Domain**.
5. In the **Outbound Gateway** drop down list, select **Google Apps Gmail**.
6. Click **Save**.
7. Then click **Configure External Dependencies**.
8. Click **Outbound Settings**.
9. Copy the Outbound Relay Host address.
10. Log on to the Google Admin Console.
11. Go to **Apps** > **G Suite** > **Gmail** > **Settings For Gmail**.
12. Click on **Advanced Settings**.
13. Scroll down to the **Routing** section.
14. In **Outbound Gateway**, paste the outbound relay host address you copied earlier.
15. Click on the **Save** button.

#### Note
Changes may take several minutes to propagate.

- If you authenticate outgoing email using an SPF record or DKIM, you may need to update your configuration.
- Replace with or add the SPF record: `v=spf1 include:_spf.prod.hydra.sophos.com -all`

If you are certain that you do not have any third parties sending mail on your behalf, and all your outbound mail is routed through **Sophos Email**, you can add a hard fail instead: `v=spf1 include:_spf.prod.hydra.sophos.com -all`. 

Copyright © Sophos Limited
Note
This means that your mail needs to be sent from Sophos Email to be accepted by the receiver’s mail servers (if they carry out SPF checks).

8.13.5 How to configure Sophos Email for Exchange and all other clients

This topic explains how to set up Microsoft Exchange and all other email clients to route email through Sophos Email.

Related tasks
Set up synchronization with Azure Active Directory (page 474)

Add your domain and verify ownership

You need to add your domain details.

Note
You will need to provide the following information when configuring Sophos Email to process and deliver email for your domain:
- Your email domain name
- Your mail delivery destination host as a Fully Qualified Domain Name (FQDN) or IP address
- The port number that is used to listen for SMTP traffic on the mail delivery destination host

To add a domain in Sophos Central:
1. Click Email Gateway > Settings.
2. Click Domain Settings/Status.
3. Click Add Domain.
4. Enter your email domain details, direction of traffic and delivery destination details.
5. Next, click Verify Domain Ownership.
6. Copy the TXT value presented in the Verify Domain Ownership dialog.
   This value is specific to your email domain.
7. Create a TXT DNS record in the root level of the domain name (entered in step 5) and paste the TXT value that was copied in the last step. You can give it the same TXT name as shown or use @.
8. Once the new TXT DNS record entry has been saved, click Verify.

Once the DNS update with the correct TXT value has been propagated, a message will be returned indicating that the domain verification was successful.

If the DNS update has not yet propagated, or if the value entered is incorrect, a failure message will be returned. Confirm that the value entered is correct.

Note
The domain verification process may take some time to complete, so it may be worth waiting to check that it is successful.
Add mailboxes to Email Gateway

You can add mailboxes to Email Gateway.

You can add mailboxes in the following ways:

1. Automatically using Active Directory Sync. You can choose from the following Active Directory services:
   - AD Sync
   - Azure Sync
2. Manually using the UI.

Add users or mailboxes using AD Sync

You can add mailboxes using AD Sync.

Before you can set up synchronization, you need .NET Framework 4.5 or higher installed on the computer where you will run the Sophos Central Active Directory Synchronization Utility.

To set up synchronization with Active Directory:

1. On the Active Directory Sync Status page, click the link to download the Sophos Central Active Directory Synchronization Utility installer, then run it.
2. In the setup wizard, enter the information required. On the last page, select Launch Sophos Central AD Sync Utility and click Finish.

   Alternatively, go to the Windows Start menu > All Programs > Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.

   Follow the instructions in the Sophos Central Active Directory Synchronization Setup wizard.
3. On the Central Credentials page, enter your Sophos Central account credentials.
4. On the AD Configuration page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the Use LDAP over an SSL connection checkbox selected. If, however, your LDAP environment doesn’t support SSL, clear the Use LDAP over an SSL connection checkbox and change the port number accordingly. Usually, the port number is 636 for SSL connections and 389 for insecure connections.
5. If you don’t want to synchronize the entire forest, on the AD Filters page, you can specify which domains to include in the synchronization. You can also specify additional search options—search bases and LDAP query filters—for each domain. Distinct options can be specified for users and groups.

   Note
   AD Sync will only create groups that have members which include discovered users, regardless of group filter settings.

   a) Searchbases: You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format:
b) LDAP query filters To filter users, for example, by group membership, you can define a user query filter in this format:

```
memberOf=CN=testGroup,DC=myCompany,DC=com
```

The above query will limit user discovery to users belonging to “testGroup”. Note that if you don't also specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter:

```
CN=testGroup
```

Note
If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

6. On the Sync Schedule page, define the times at which the synchronization will be performed automatically.

Note
A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select Never. Only sync when manually initiated.

7. To synchronize immediately, click Preview and Sync. Review the changes that will be made during the synchronization. If you are happy with the changes, click Approve Changes and Continue.

The Active Directory users and groups are imported from the Active Directory to the Sophos Central Admin console.

a) To stop the synchronization in progress, click Stop.

Add a mailbox manually

**Sophos Email** allows you to add single mailboxes manually via the user interface.

To add a mailbox manually:

1. Click Mailboxes.
2. On the Mailboxes screen, click Add.
3. Select Add Mailbox.

There are three types of mailbox:

- **User Email**: a mailbox for a person. Example: firstname.lastname@companyname.com.

**Tip**
For a User Email mailbox you can click on the mailbox name to view the user’s details.
• **Distribution List**: a mailbox for a group of people. Example: support@companyname.com.

• **Public Folder**: a mailbox for collecting information such as surveys or feedback. Example: survey@companyname.com.

4. Select a mailbox type.
5. Enter a name for the mailbox.
6. Enter the SMTP address for the mailbox.
7. Click **Save** to create a single mailbox and exit, or **Save and Add Another** to create additional mailboxes.

### Add Mailboxes via Import

**Sophos Email** allows you to add mailboxes in bulk mailbox import.

To add import mailboxes:

1. Create your import .csv file using the following format:

<table>
<thead>
<tr>
<th>Name</th>
<th>Email Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Alamar</td>
<td><a href="mailto:robert.alar@t.com">robert.alar@t.com</a></td>
<td>User</td>
</tr>
<tr>
<td>Support DL</td>
<td><a href="mailto:support@test.com">support@test.com</a></td>
<td>DL</td>
</tr>
<tr>
<td>Vacation Calendar</td>
<td><a href="mailto:vacation@test.com">vacation@test.com</a></td>
<td>PF</td>
</tr>
</tbody>
</table>

2. Click **Add Mailbox** and select **Import Mailboxes**.
3. Click **Browse** and navigate to your import file.
4. Click **Add** to start the import process.

Import will run and display results after it completes.

To verify mailbox creation, you can search for new users in the **People** section or browse the list of mailboxes under the **Mailboxes** section for Distribution Lists and Public Folders.

### Restrict delivery to Sophos IP addresses

To add an additional level of security to the integration between **Sophos Email** and your mail host, we recommend that you configure the connection to your mail host to be restricted to our delivery IPs.

**Note**

Before you proceed, we strongly recommend testing mail flow and domain configuration in a non-production/test environment prior to making any changes to the mail flow for your company.

The specific delivery IP that you will need to use is tied to the region in which your Sophos Central account is hosted. When your Sophos Central account was created, you would have chosen to store your data in the United States, Germany, or Ireland.

<table>
<thead>
<tr>
<th>Region</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>US (West)</td>
<td>52.41.236.76</td>
</tr>
<tr>
<td></td>
<td>50.112.39.248</td>
</tr>
</tbody>
</table>
Note
Using an IP other than the one specified for your region will prevent mail from flowing properly.

Modify MX records to point to Sophos Email

Modifying your domain's MX records to point to Sophos Email is crucial to the successful deployment of the solution and ensures all email is filtered and delivered.

If you can't make these changes yourself, contact your IT department, hosting provider, ISP or Domain Name Service provider and arrange for the MX records for your domain(s) to be modified.

When you created your Sophos Central account, you selected a region in which you wanted to store your data. Your MX records are dependent on this region.

Modify your MX records to include the record names associated to the region that you chose to store your data in.

<table>
<thead>
<tr>
<th>Region</th>
<th>MX Records</th>
</tr>
</thead>
</table>
| United States (West) | 10, mx-01-us-west-2.prod.hydra.sophos.com  
                     | 20, mx-02-us-west-2.prod.hydra.sophos.com       |
| United States (East) | 10, mx-01-us-east-2.prod.hydra.sophos.com     
                     | 20, mx-02-us-east-2.prod.hydra.sophos.com      |
| Germany          | 10, mx-01-eu-central-1.prod.hydra.sophos.com  
                     | 20, mx-02-eu-central-1.prod.hydra.sophos.com   |
| Ireland          | 10, mx-01-eu-west-1.prod.hydra.sophos.com      
                     | 20, mx-02-eu-west-1.prod.hydra.sophos.com      |

Notes
Please take care with all options to ensure that the spelling and numbers are correct.
Using MX record names other than those provided will prevent mail from flowing properly.
It is always recommended when changing DNS entries like MX records to lower the TTL (to 600 ms or less) on the records well in advance of updating the entries. This will allow the change to
propagate in minimum time and provides a quick way to revert the change should there be any issues encountered during testing.

**Test and confirm mail flow**

Once you have updated your MX records, send a test message to any of your mailboxes protected by Sophos Email. For a true test, you should send your test message from an address outside of your email domain.

To confirm that the message flowed through Sophos Email, you can view the Message History Report.

To access the report:

1. In Sophos Central, click Logs and Reports.
2. Click Message History.
   
   If messages are flowing through the system, you will see entries in this report.

If mail is not flowing, meaning you are not receiving email to your test inbox, take the following steps:

1. Verify that your MX records are correct for your region.
2. Verify that you set up the Sophos Delivery IPs correctly in your gateway, firewall or connector.
3. Verify that the mailbox that you are sending to exists in Sophos Email.

If you have taken all these steps and mail is still not flowing for your domain, you should contact Sophos Email Support.

---

**8.13.6 Set up outbound email handling with Exchange and other clients**

This document guides you through the process of directing all outbound email via Sophos Email. For Exchange, this requires an SMTP Connector to be configured on your Exchange Server.

To set up outbound email handling:

1. To set up an SMTP connector, follow the instructions for your version of Exchange on Microsoft's website.
2. When prompted, select Route mail through smart hosts and click + Add.
3. In the Add smart host dialog that appears, enter the corresponding smart host for your region.
   a) To find the smarthost for your region, sign in to Sophos Central.
   b) Go to Email Gateway > Settings > Domain Settings > Configure External Dependencies.
   c) Click on the outbound settings tab. You will see the Outbound Relay Host associated with your account. (This will be dependent on the region you chose when you signed up for Sophos Email.)

<table>
<thead>
<tr>
<th>Region</th>
<th>Outbound Relay Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States (West)</td>
<td>relay-us-west-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>United States (East)</td>
<td>relay-us-east-2.prod.hydra.sophos.com</td>
</tr>
<tr>
<td>Germany</td>
<td>relay-eu-central-1.prod.hydra.sophos.com</td>
</tr>
</tbody>
</table>
4. Turn off or remove any other **Outbound Send Connectors** that were previously used for mail filtering.

**Note**
Failure to do this means your outbound email will still use the older send connectors, and is not routed through **Sophos Email**. If in doubt, consult Sophos Support.

If you authenticate outgoing email using an SPF record or DKIM, you may need to update your configuration. Replace with or add the SPF record:

```
v=spf1
include:_spf.prod.hydra.sophos.com ~all.
```

If you are certain that you do not have any third parties sending mail on your behalf, and all your outbound mail is routed through **Sophos Email**, you can add a hard fail instead:

```
v=spf1
include:_spf.prod.hydra.sophos.com -all.
```

**Note**
This means that your mail needs to be sent from **Sophos Email** to be accepted by the receiver’s mail servers (if they carry out SPF checks).

Confirm that outbound mail is flowing by sending a outbound mail to an external address.

1. Sign in to Sophos Central.
2. Go to **Email Gateway > Logs and Reports > Message History**.
3. Change the direction to outbound.
4. Refresh the screen until you can see the details of the test email you have sent.

**Related information**

* Exchange 2016
* Exchange 2013
9 Web Gateway

Sophos Web Gateway protects your network against risky or inappropriate web browsing. It can also prevent the loss of confidential data, trust certain networks, and report on all your users’ web browsing.

To use Web Gateway:
1. Create or edit a Web Gateway policy.
2. Install the Sophos Web Gateway agent on devices. See the Protect Devices page.

9.1 Dashboard

The Web Gateway Dashboard is the start page of Web Gateway and lets you see the most important information at a glance. It consists of these areas.

Usage Summary

Usage Summary shows details of usage and protection for users or protected devices. It also shows the number of unprotected users or devices.

Click on the tabs to see information for each device type or for users.

Click See Report to open a detailed report for the tab you have selected.

Blocked Summary

Blocked Summary shows statistics for your Web Gateway protection (you see this only if you have a Web Gateway license).

The figures are for malware blocked and websites blocked.

Click on a figure to open a detailed report.

Network Usage

Network Usage shows statistics for data downloaded and uploaded by users and apps.

Click See Report to open a detailed report for the tab you have selected.

Top Blocked

Top Blocked shows statistics for the users, devices, or apps with the most blocked attempts to access websites.

Click See Report to open a detailed report for the tab you have selected.
9.2 Logs

The Web Gateway Network Activity page lets you see all the network activity logs associated with your Web Gateway protection.

You can filter logs by:

- **Action** (Allow, Audit, Block)
- **Filter type** (Category, Malware, Phishing, URL, Data)
- **Website Category** and/or
- **User**.

The Search box for users will attempt to auto-complete as you type.

You can limit report data to a specific date range by entering a From and To date. Once you have a date range specified you can:

- **Update**: Update the data displayed in the report for the specified date range.
- **Export**: Export the data to XSLX, ODS, CSV, or XML format.

9.3 Reports

The Web Gateway Reports page lets you see all the reports for your Web Gateway protection.

Please note that reports update about once an hour.

You can limit report data to a specific date range by entering a From and To date. You can also filter the report using the filters shown.

Once you have set the date range and filters, you can:

- **Update**: Update the data displayed in the report for the specified date range.
- **Print**: Send a copy of the report to the printer.
- **Export**: Export the data to XSLX, ODS, CSV or XML format.

9.4 People

On the People page, you can manage your users and user groups.

9.4.1 Users

On the Users tab of the People page, you can add or manage users, and get the users’ computers protected.

You can also enable the users to protect their own devices by emailing them a setup link.

The current users are listed with their details.

**Health Status.** An icon shows whether the user has security alerts on any of their devices.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>🚨</td>
<td>Amber warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>🚨</td>
<td>Red warning sign if there are critical alerts.</td>
</tr>
</tbody>
</table>

**Name** Click the user's name to see details of devices and to see which has an alert.

**Email.**

**Exchange Login.**

**Last Active.** The last time a user reported to Sophos Central.

**Group Name.** This is shown if the user has been added to a user group.

**Role.** This shows what administration role, if any, the user has. This column is only visible if you are an administrator.

Click any column header to sort the users. By default, users are sorted according to the **Last Active** time.

To see full details for a user, click the user's name.

You can add users manually or automatically by protecting their devices. You can also import users in bulk from a CSV file or from Active Directory. You can also protect existing users.

To modify users, click the user’s name to open and edit their user details.

You can also delete users and export lists of users.

**Related concepts**

- **User Summary** (page 522)
- **Administration Roles** (page 551)

**Related tasks**

- **Add a user manually** (page 527)
  You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

- **Add users automatically** (page 528)
  You can add users automatically by protecting their devices.

- **Import users from a CSV file** (page 528)
  You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

- **Import users from Active Directory** (page 529)
  You can import users and groups from Active Directory.

- **Protect existing users** (page 529)
  You can protect users that you have already added to Sophos Central.

- **Delete users** (page 529)
  You can delete users from Sophos Central if you are a Super Admin.

- **Export to CSV** (page 530)
You can export lists of users as CSV files.

**User Summary**

The **Summary** tab in a user's details page shows a summary of the following:
- The user's security status, administration role, if any, and account details.
- Recent events on the user's devices.
- Mailboxes associated with the user.
- Devices associated with the user.
- Policies that apply to the user.
- Groups that the user belongs to.
- Logins.

You can find details of each below.

The security status and account details are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.

You can click on the other tabs for more on **Devices**, **Events**, and **Policies**.

**Health Status**

In the left-hand pane, an icon shows you whether the user has security alerts on any of their devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>🚨</td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>⚠</td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>

You can see which devices have alerts in the **Devices** tab.

A padlock icon shows that the user has been imported from Active Directory.

A badge shows the user's assigned administration role. Click on the role name to view the settings for the role.

**Note**

Role information is only displayed for administration roles.

**Account details**

In the left-hand pane, you can modify or delete the user's account.
If a user has been imported from Active Directory, you cannot change the account details. However, you can add the user to a new Sophos Central group or add another login.

**Modify the account**

1. Click **Edit** and enter the following settings:
   - **First & Last name**: Enter the name of the user. Do not include a domain name.
   - **Role**: Select a role for the user. Choose from: **Super Admin, Admin, Help Desk, Read-only, or User**.

   **Restriction**
   You can only see the **Role** option and assign administrator roles if you are a Super Admin.

   **Note**
   You cannot amend your own administration role.

   **Note**
   Anyone with a **User** role only has access to the Self Service Portal.

   **Email Address**: Enter the email address of the user.

   **Exchange Login** (optional): Enter the Exchange account name of the user.

   **Note**
   In Sophos Mobile policies, you can use the placeholder `%USERNAME%` to refer to this setting.

   **Add to groups**: Select one of the available user groups and use the picker arrows to move it to the assigned groups.

   **Email Setup Link**: Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs.

   **Note**
   The user needs administrative privileges and internet access in order to protect their computer.

   **Note**
   **Web Gateway** provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

2. Click **Save**.

**Delete the account**

To delete the account, click **Delete User** in the left-hand pane. Logins assigned to this user can afterward be assigned to another user.
Restriction
You cannot delete users who have an assigned administration role.

Multi-factor authentication
If the user is an admin, the left-hand pane shows whether multi-factor authentication (MFA) is enabled for them. If it is enabled, the admin must use another form of authentication, as well as their user name and password, to sign in.
If you're a Super Admin, you can edit the settings as follows:
Click Reset to let the admin set up their MFA sign-in details again.
Click MFA Settings to go to a page where you can enable or disable multi-factor authentication for the admin.

Recent Events
This lists recent events on the user's devices.
For a full list, click the Events tab.

Mailboxes
This lists all email addresses, including distribution lists and public folders, associated with the user.
Primary indicates the user’s primary email address. Owner indicates the user controls a distribution list or public folder.
For full details, click an email address.

Devices
This shows a summary of the devices associated with the user.
Click the device name to go to the device’s details page for more information.
Click Actions to carry out any of the same actions that are available on the device’s details page (for example, Scan Now and Update Now for a computer).
For full details of the user's devices, click the Devices tab.

Policies
This shows a summary of the policies applied to the user.
The list shows the policy name, whether the policy is enabled or not, and icons that indicate the features included in the policy.
Click on a policy name to view and edit the user policy.
Note

Editing the policy affects all users to which this policy is applied.

For full details of all the policies applied to this user, click the Policies tab.

Groups

This shows the groups the user belongs to.

Click on a group name to see details of the group.

Click Edit (on the right) to change the groups the user belongs to.

Logins

This shows the user’s logins.

Click Edit (on the right) to change the logins assigned to the user.

Related concepts

Administration Roles (page 551)
About Policies (page 540)

User Devices

The Devices tab in a user’s details page lets you see the devices associated with the user.

This tab also shows any servers where the user has logged on with Remote Desktop Services.

For each associated device you can see the device type and the operating system. You also have these options:

- **View Details**: This opens the full device details page.
- **Delete**: This removes the device from the list and stops Sophos Central managing it, but it does not uninstall the Sophos software.
- **Actions**: Actions you can take. These depend on the device type.

User Events

The Events tab in a user's details page lets you see a list of events detected on the user’s devices.

You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

- **Severity**: Hover over an icon to see what it means.
- **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
- **Details**: This link (for certain events) lets you get further details and take action.

View Events Report shows events arranged by type and a graph of events day by day.
Stop detecting an application

If an application is reported as malware but you know it’s safe, you can allow it from the events list.

For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the Details link beside the event and then allow the application.

Note
This currently applies only to malware events reported by Intercept X.

Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again.

This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again and select an option:
   • Exclude this Detection ID from checking: prevents this detection on this app.
   • Exclude this application from checking: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.
3. Click Exclude.

We’ll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again.

This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again.

   Select Exclude this Detection ID from checking. This prevents this detection on this app.
3. Click Exclude.

We’ll add your exclusion to the Global Exclusions list.

Related information
How to investigate and resolve a potential False Positive or Incorrect Detection
**User Policies**

The **Policies** tab in a user's details page lets you see the policies that are enabled and applied to the user.

Click a policy name to view and edit policy details.

Editing the policy affects all users to which this policy is applied.

**Add a user manually**

You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

To add a user:

1. Go to Users.
2. Click Add and select Add User.
3. In the Add User dialog, enter the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First and Last Name</strong></td>
<td>Enter the name of the user. Do not include a domain name.</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>Select an administration role for the user. A user who is assigned an administration role will receive an email telling them how to set up their administration account. You can only see the Role option and assign administrator roles if you are a Super Admin. Anyone with a User role only has access to the Self Service Portal.</td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
<td>Enter the email address of the user.</td>
</tr>
<tr>
<td><strong>Add to groups</strong> (optional).</td>
<td>Select one of the available user groups and use the picker arrows to move it to the assigned groups. You can start typing a name in the search box to filter the displayed groups.</td>
</tr>
<tr>
<td><strong>Email Setup Link</strong></td>
<td>Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs. The user needs administrative privileges and internet access in order to protect their computer.</td>
</tr>
<tr>
<td><strong>Web Gateway</strong></td>
<td>This provides more advanced web security for computers than Endpoint Protection. You can</td>
</tr>
</tbody>
</table>
### Add users automatically

You can add users automatically by protecting their devices.

To add users:

1. Download an installer from **Protect Devices**.
2. Run the installer on the devices.

This adds the user of each device automatically.

### Import users from a CSV file

You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

To import users:

1. Go to **Users**.
2. Click **Add** and click **Import users from CSV**.
3. Click **Browse** and select your CSV file.

**Tip**

You can download template CSV files from the **Import users from CSV** dialog.

The CSV file can include groups a user is assigned to.

4. To create new groups, click **Create new groups**.
5. To send a registration email for the Sophos Central Self Service portal to each imported user, click **Give users access to Sophos Central Self Service**.
6. Click **Add**.

**Note**

The CSV file can include the email address of each user's manager. If there's a manager who isn't already a user in Sophos Central, a user is created. So the number of users imported may exceed the number of rows in the file.
Note
If an email address in your CSV file matches an existing user in Sophos Central, the user is updated with the information in your import file.

Note
If an email address in your CSV file matches an existing user in Sophos Central that is managed through Active Directory Synchronization, the user is skipped during import and no changes are made to the user account.

Import users from Active Directory
You can import users and groups from Active Directory.

To do this:
1. Go to Users.
2. Click the Set up Active Directory Sync link in the upper right of the page.
3. Follow the set up synchronization process.

Protect existing users
You can protect users that you have already added to Sophos Central.

To protect them you need to email them a setup link. To do this:
1. Go to Users.
2. Select the user or users you want to protect.
3. Click Email Setup Link in the upper right of the page.
4. In the Email Setup Link dialog, select the types of protection the user needs (if your license includes more than one).
   - Web Gateway provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.
   - Users need administrative privileges and internet access to use the setup link.

Delete users
You can delete users from Sophos Central if you are a Super Admin.

Restriction
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them.

Under some circumstances, the user may be recreated automatically in future:
- If the user logs in to an associated device that is still managed by Sophos Central, they are added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they are added as a user again the next time that Sophos Central synchronizes with Active Directory.

To delete users:
1. Go to **Users**.
2. Click the checkbox next to each user you want to delete.
3. Click **Delete**.

Deleting a user does not delete devices associated with that user or remove the Sophos software from these devices.

Logins assigned to a deleted user can afterwards be assigned to another user. You can edit logins by clicking the **Edit** link on a user's details page.

**Related concepts**

*User Summary* (page 522)

**Export to CSV**

You can export lists of users as CSV files.

You can export lists of different types of user.

For example you can export a list of administrators by applying the **Admins only** filter before you click **Export to CSV**.

To export users:

1. Go to **Users**.
2. Click **Export to CSV**.

   This creates a file called `users.csv`. Any currently active filters are applied to the list.

**9.4.2 Groups**

On the **Groups** tab of the **People** page, you can add or manage groups of users.

You can use groups to assign a policy to multiple users at once.

The sections below tell you about the groups list and how to add, modify or delete groups.

**About the groups list**

The current groups are listed and the number of users in each group is shown.

To see full details for a group, click the group's name.

**Add a group**

1. Click the **Add Group** button.
2. In the **Add Group** dialog, enter the following settings:
   - **Group Name**: Enter the name of the new group.
   - **Available Users**: Select users from the list of available users.

   **Tip**

   In the **Search** box you can start typing a name to filter down the displayed entries.
3. Click **Save**.

**Modify a group**

To modify a group, click the group's name to open and edit the group details. For more information, see User Group Details.

**Delete a group**

To delete a group, select it and click **Delete** in the upper right of the page.
Deleting a group will not delete its users.

**Related concepts**

User Group Details (page 531)

**User Group Details**

On a group's details page, you can:

- Add or remove members.
- Delete the group.

**Add or remove members**

To add or remove members:

1. Click **Edit** under the group name.
2. In the **Edit Group** dialog, use the picker arrows to add users to the **Assigned Users** list or remove them.
3. Click **Save**.

**Delete the group**

To delete the group:

1. Click **Delete** under the group name.
2. In the **Confirm Group Deletion** pop-up, click **Yes**.
Deleting a group will not delete its users.

**User Group Policies**

The **Policies** tab in a user group's details page lets you see the policies that are enabled and applied to the group.

Click a policy name to view and edit policy details.
Editing the policy affects all groups to which this policy is applied.
9.5 Computers

On the Computers page, you can manage your protected computers. They will appear automatically after Sophos agent software has been installed.

You can:

- View details of the computers.
- See the encryption status (if you are using Sophos Device Encryption).
- Delete computers.
- Install or uninstall software.
- Get a recovery key for encrypted computers (if you are using Sophos Device Encryption).
- Export the computers list to CSV.

View computer details

The computers list shows you the current computers with these details:

- Name.
- IP Address. Hover over the icon to see details of all IPv4 and IPv6 addresses.
- Operating System.
- Products installed. For example, Intercept X or Encryption.
- Last user.
- Last active. This is the last time that the computer contacted Sophos.
- Group. The group that the computer belongs to (if it belongs to one).

To search for a computer, enter the name in the search field above the list.

To filter computers according to their type, their health status, or their encryption status, use the filters above the list.

You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

Delete computers

You can delete computers that you no longer need to manage from Sophos Central.

Select the computer or computers you want to delete and click Delete (in the upper right of the page).

This deletes the computer and the alerts associated with the computer.

**Warning**
You should uninstall the Sophos software before deleting a computer.
Install or uninstall software

You can select new endpoint software to be installed on computers that are already protected and managed by Sophos Central.
You can also uninstall software.
To do either, do as follows.
1. Click Manage Endpoint Software (in the upper right of the page).
2. Select software.
3. Select computers and use the picker arrows to change the software installed, as follows.
   • To install the software, select eligible computers and move them to the assigned list.
   • To uninstall the software, select assigned computers and move them to the eligible list.
The computers will update to the selected software.

Export to CSV

To export a list of computers:
Click Export to CSV.
This creates a file called devices.csv. Any currently active filters are applied to the list.
For example you can export a list of Windows computers by applying the Windows Computers filter before clicking Export to CSV.

Retrieve recovery key

This option is available from More on the Computers page.
If users are unable to log in to their encrypted computer, you can get a recovery key which is used to unlock the computer.

9.5.1 Computer Summary

The Summary tab in a computer's details page shows you the following information.
The sections you see depend on your license and the features you've set up.

Security status

In the left-hand pane, you can see the security status and take actions.

Note
The left-hand pane is always shown, even when you click the other tabs on this page.
An icon shows you whether the computer has any security alerts:
### Actions you can take

The action buttons are in the left-hand pane.

**Update:** This updates your computer with the latest Sophos software.

**Delete:** This deletes the computer from Sophos Central. It also deletes the alerts associated with the computer.

**Warning:**
You should uninstall the Sophos software before deleting a computer.

**Isolate:** This isolates the computer from the network.

**Live Response (Beta):** This enables you to connect to the computer to investigate and remediate possible security issues.

**Change group:** This lets you add it to a group, move it to a different group, or remove it from its current group.

**Scan Now:** This scans the computer for threats.

The scan may take some time. When complete, you can see a "Scan completed" event and any successful cleanup events on the **Logs & Reports > Events** page. You can see alerts about unsuccessful cleanup on the **Alerts** page.

If the computer is offline, it is scanned when it is back online. If a computer scan is already running, the new scan request will be ignored and the earlier scan will carry on.

**Diagnose:** This diagnoses potential issues with the computer.

**Create forensic snapshot:** This gets data from a Sophos log of the device’s activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

### Isolate or remove from isolation

This option is available if you have Intercept X Advanced with EDR.

**Isolate** isolates the computer from the network. You might want to do this if potential threats are found on it. You can still manage the computer from Sophos Central and you can remove it from isolation at any time.

When a computer has been isolated, you see the following under the computer icon and security status.

- The message **Isolated by Admin.**
• A link labeled **Remove from Isolation**. Click it to reconnect the computer to the network.

**Note**  
You don't see the **Isolate** option if the computer has already isolated itself automatically. See Device Isolation in Threat Protection Policy.

**Live Response (Beta)**

This option is available only if you are a Super Admin and you’ve signed in using multi-factor authentication. You must also turn on **Allow Live Response connections to computers** in **Global Settings**, see Live Response for devices.

This enables you to connect to the computer to investigate and remediate possible security issues. You might want to do this if an infection or suspicious activity is identified on the computer. You can connect to the computer even if it’s isolated. To connect to the computer, do as follows:

1. Click **Live Response (Beta)**.
2. In **Session purpose**, summarize the purpose of your session.
3. Click **Start**.  
   A connection to the computer is opened in another browser tab. The tab shows a terminal window.
4. At the command prompt, type commands to perform your investigation or remediation.  
   Use DOS, UNIX, or Linux commands depending on the computer to which you’ve connected.
5. When you finish, click **End Session**.  
   The connection is closed, although the tab remains open. You can browse elsewhere in Sophos Central from here.
   
   The connection is also closed in the following cases:
   • You close the tab.
   • You refresh the tab.
   • You browse elsewhere in Sophos Central from here.
   • There is no activity for 30 minutes.

To see which Live Response sessions have started or ended, view the Sophos Central audit log.

**Create forensic snapshot**

You can create a "forensic snapshot" of data from the device. This gets data from a Sophos log of the device's activity and saves it on that device. You can also save it in the Amazon Web Services (AWS) S3 bucket you specify. You can then do your own analysis.

You’ll need a converter (which we provide) to read the data.

**Note**  
You can choose how much data you want in snapshots and where to upload them. To do this, go to **Global Settings > Forensic Snapshots**. These options may not be available for all customers yet.

To create a snapshot:
1. Go to a threat case's Analyze tab. Alternatively, on the details page of the device, open the Status tab.

2. Click Create forensic snapshot.

3. Follow the steps in Upload a forensic snapshot to an AWS S3 bucket.

You can find the snapshots you generated in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Forensic Snapshots\.

Snapshots generated from detections are in %PROGRAMDATA%\Sophos\Endpoint Defense \Data\Saved Data\.

Note
You need to be an administrator with access to the tamper protection password and run a command prompt as an administrator to access the saved snapshots.

Recent Events
This lists recent events on the computer. For a full list, click the Events tab.
The icons indicate which Sophos agent reported each event. Hover over an icon to see what it means.

Agent Summary
The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.
The summary shows the following details. It also includes links to let you update the computer, install products, or change the group the computer's in, as needed.

- **Last Activity**: Shows when the last activity occurred.
- **Last Agent Update**: Shows whether the computer is up to date.
- **Assigned Products**: Shows the Sophos products installed (for example, Intercept X or Device Encryption). Shows the license and the version number for each installed product. The version information is only available for Windows computers.
- **Installed component versions**: Click this to see a full list of the Sophos components and their version numbers. This is only available for Windows computers.
- **Group**: Shows which group the computer is in (if any).

Device Encryption
Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers and FileVault encryption on Macs.

This summary shows:

- All volumes of the computer.
- The volume ID for each volume.
- The encryption status.
- The authentication type.
• The encryption method.

Volumes can be encrypted with software-based or hardware-based encryption. Device Encryption always uses software-based encryption for new volumes, even if the drive supports hardware-based encryption.

If a drive is already encrypted with hardware-based encryption, it will not be changed.

If a BitLocker group policy setting requires hardware-based encryption, it is used.

Retrieval Recovery Key

You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their sign-in credentials.

Trigger change of password/PIN

This requires users to immediately change their BitLocker password or PIN. A message is displayed when the request has been sent successfully.

On the endpoint, users are prompted to set a new BitLocker password or PIN. If users close the dialog without entering a new password or PIN, the dialog is shown again after 30 seconds, until they enter a new one. After users have closed the dialog five times without changing the password or PIN an alert is logged.

Web Gateway summary

Sophos Web Gateway provides advanced protection against risky or inappropriate web browsing. The summary shows the last network activity. It also shows the version of the Web Gateway agent (and whether it is up to date).

If you need to update the Web Gateway agent, an Update button is displayed.

Tamper Protection

This shows whether tamper protection is enabled on the computer or not.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:

• Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
• Disable tamper protection.
• Uninstall the Sophos agent software.

Click Disable Tamper Protection to manage the tamper protection password for the computer. If tamper protection is switched off we recommend you turn it on.

Update Cache and Message Relay

Sophos Update Cache enables your computers to get their Sophos Central updates from a cache on a server on your network, rather than directly from Sophos. You can also designate servers to communicate with Sophos Central as message relays.

This shows that a cache has been set up for the computer. It shows which server is being used.
Windows Firewall

Windows Firewall is active and being managed on the computer. It also shows:

- Whether Windows Group Policy is being used.
- The active network profiles.
- If other registered firewalls are installed and active.

9.5.2 Computer Events

The Events tab in a computer’s details page displays events detected on the computer.

You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

- **Sev**: Hover over an icon to see what it means.
- **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
- **Details**: This link (for certain events) lets you get further details and take action.

**View Events Report**: Shows events arranged by type and a graph of events day by day.

Stop detecting an application

If an application is reported as malware but you know it’s safe, you can allow it from the events list.

For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the Details link beside the event and then allow the application.

**Note**

This currently applies only to malware events reported by Intercept X.

Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again.

This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don’t detect this again and select an option:
   - Exclude this Detection ID from checking: prevents this detection on this app.
   - Exclude this application from checking: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.
3. Click Exclude.

   We’ll add your exclusion to a list.
Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the Events tab, find the detection event and click Details.
2. In Event details, look for Don't detect this again.
   Select Exclude this Detection ID from checking. This prevents this detection on this app.
3. Click Exclude.
   We’ll add your exclusion to the Global Exclusions list.

Related information
How to investigate and resolve a potential False Positive or Incorrect Detection

9.5.3 Computer Status

The Status tab in a computer’s details page lets you see the computer’s security health and details of any alerts.

It also lets you take action against alerts.

Security Health

These status details are only shown if the computer is using the Security Heartbeat feature.

The computer security status is reported by computers running Windows 7 and later.

This shows whether the device has threats detected, has out-of-date software, is not compliant with policy, or is not properly protected. The overall status is the same as that for the highest-priority item listed (red, orange or green).

Alerts

The page lists any alerts on the device. The details include:

- Alert details: For example, the name of the malware.
- When the alert occurred.
- The actions that you can take. These depend on the type of threat or event and are the same as the actions available in the Dashboard.

Related concepts
Forensic snapshots (page 138)
Forensic snapshots get data from a Sophos log of a computer’s activity so that you can do your own analysis.

9.5.4 Computer Policies

The Policies tab in a computer’s details page lets you see the policies that are applied to the computer.

You can view and edit policy details by clicking the policy in the list.

Note
Editing the policy affects all users to which this policy is applied.

9.6 Policies

A policy is a set of options (for example, settings for malware protection) that Sophos Central applies to protected users, devices, servers, or networks.

There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).

To find out how policies work and how you can use them to customize security settings, see About Policies.

To find out how to create and edit policies, see Create or Edit a Policy.

Note
Your assigned administrator role affects what you can do.

9.6.1 About Policies

If you’re new to policies, read this page to find out how policies work.

What is a policy?

A policy is a set of options that Sophos Central applies to protected users, devices or servers.

There is a policy for each product, or for a feature that’s part of a product (for example, there is a policy for the application control feature).

Users, devices and servers have separate policies.

What is a Base policy?

Each feature has a Base policy. Sophos provides this policy and initially it applies to all users (and devices) or all servers.

For some features, like threat protection, Sophos configures the Base policy with the best practice settings. You can leave it unchanged if you want to.
For other features, like application control or peripheral control, which are more specific to your network, you must edit the policy to set up the feature.

The Base policy is always available and is used if you don't have other policies activated.

**Note**
You cannot disable or delete the Base policy.

**Do I need to add new policies?**

You can choose whether to set up your own policies or not.

If you want to apply the same policy to all users or devices or servers, you can simply use the Base policy or adapt it for your needs.

If you want to use different settings for different groups, you can create additional policies.

**What can I do with additional policies?**

You can set up additional policies to override some or all of the settings in the Base policy.

You can use additional policies to apply different settings to different users, devices or servers. You can also use them to make it easier to switch the settings that are applied quickly.

The order in which you put the policies in the list matters. The policies at the top of the list override the policies at the bottom. See “How do you prioritize policies?” below.

**What’s the difference between user policies and computer policies?**

A user policy applies to all the devices that a user has.

A “device” or computer policy applies to specific computers or groups of computers, regardless of which user logs on.

Some features let you create either kind of policy. Other features only let you create one kind. For example you can set an updating policy for computers, but not for users.

If you set up a user policy and a computer policy for the same feature, and both could apply to the same computer, the policy that’s higher in your policy list takes priority. See "How are policies prioritized?"

You can check which policy is applied to a computer by looking at the Policies tab on that computer’s details page.

**What is in each policy?**

A policy lets you:

- Configure one of the features that you have licensed.
- Specify which users, devices or servers the policy applies to.
- Specify whether the policy is enforced and whether it expires.

A policy contains all the settings for a product or feature. For example, you cannot split up the threat protection settings across several different polices in such a way that a user gets one setting from one policy and another setting from a different policy.
How are policies prioritized?

The order in which you arrange the policies determines which is applied to specific users, devices or servers.

Sophos Central looks through the policies from the top down and applies the first policy it finds that applies to those users or devices.

The Base Policy is always at the bottom, and is applied to any users, devices or servers that aren’t covered by policies higher in the list.

**Tip**
Place the most specific policies at the top and general policies further down. Otherwise, a general policy might apply to a device for which you wanted an individual policy.

To sort policies, grab a policy and drag it to the position where you want to insert it.

### 9.6.2 Create or Edit a Policy

You can create or edit a policy as follows.

#### Create a policy

1. If you have more than one Sophos product, select the one where you want to create a policy.

   **Note**
   You can’t create policies from the **Overview** pages.

2. Go to the **Policies** page.
3. Click **Add Policy** (in the upper right).
4. If you see an **Add Policy** dialog, select:
   * The feature you want.
   * The policy type (applies only to Endpoint Protection).
5. On the policy details page, use the tabs to:
   * Assign the policy. For example, assign it to specific users or devices.
   * Enter settings for the policy. See the Help topic for that policy type.
   * Enable or disable the policy.

#### Edit a policy

1. If you have more than one Sophos product, select the one where you want to edit a policy.
Note
You can't edit policies from the Overview pages.

2. Go to the Policies page.
   You see a list of policy types.
3. Click on the policy type to open a list of policies.
4. Find the policy you want to edit and click it.
5. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users or devices.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.

9.6.3 Web Gateway Policy

Sophos Web Gateway protects your network against risky or inappropriate web browsing. It can also prevent the loss of confidential data, trust certain networks, and report on all your users’ web browsing.

To set it up, do as follows:
• Create a Web Gateway policy. See Create or Edit a Policy.
• Open the policy's Settings tab and configure it.
• Make sure the policy is enabled.
• Install the Sophos Web Gateway agent on devices. See the Protect Devices page.

Related concepts
Create or Edit a Policy (page 542)
You can create or edit a policy as follows.

Web Gateway policy: filtering

For a Web Gateway policy, you can configure allow and block rules, and trusted domains and IP addresses.

To change the filtering settings, in the Web Gateway policy, click Settings to show the Filtering options.

Category Filtering

Use this to control which websites your users are allowed to visit. You can set options for security categories or productivity categories.

For more information on how Sophos filters websites, see Sophos Web Security and Control Test Site.

Security Categories

Use this section to configure access to websites that are known to be high-risk. You can choose these options:
• **Block risky downloads**: This will block all high-risk websites.
• **Block All**: This blocks all traffic categorized as security.
• **Custom**: Lets you choose which categories you want to **Allow**, **Audit**, **Warn** or **Block**.

To see the effect of an option on various categories of websites and downloads, click **View Details**.

### Productivity Categories

You can choose these options. To see the effect of an option on various categories of websites, click **View Details**.

• **Keep It Clean**: Prevents users from accessing adult and other potentially inappropriate or controversial websites.
• **Audit Potential Risks**: Allows administrators to flag events where users visited adult, controversial or data sharing websites that could be a potential risk. The user is not shown any type of warning.
• **Conserve Bandwidth**: Blocks inappropriate browsing and site categories likely to consume high bandwidth.
• **Business Only**: Only allows site categories that are generally business-related.
• **Block Data Sharing**: Blocks any website associated with data sharing activities. This helps prevent data loss.
• **Custom**: Lets you choose which category groups or individual categories of sites you want to **Allow**, **Audit**, **Warn** or **Block**.

### Web Filtering

Use this to control access to websites that you have "tagged", that is, put into your own categories, in **Settings > Website Management**.

1. Select **Web Filtering**.
2. Click **Add New** (on the right).
3. Select your **Website Tag** and set the **Action** to one of the following options.

   • **Allow** allows access to the website.
   • **Audit** allows access to the website, but associates an Audit action with the website so that you can filter and report on these events.
   • **Warn** displays a warning to the user, but allows them to proceed to the website if they decide they want to.
   • **Block** denies access to the website and shows the user a block page (which you can customize).

**Note**

In **Website Management**, you can change the category a website is in, but Web Gateway does not currently support such changes.

### Data Filters

Use this to specify keywords and regular expressions that should be identified and used for filtering web pages.

To set up a filtering rule:
1. Select **Data Filters**.
2. Click **Add New** (on the right).

   The **Add Data Filter** dialog is displayed.
3. Enter a **Name** for the rule.
4. Choose whether to **Allow**, **Audit**, **Warn** or **Block** the content once a rule is matched.
5. Choose whether the filter applies to **Download**, **Upload** or **Both**.
6. Select the **Type**:
   - **Manual**. If you select this, enter a Keyword and a Count (number of occurrences).
   - **Template**. If you select this, choose a template from the drop-down list.

   The rule is applied when all the conditions of the filter are met.

**Note**

Data filters apply to all content including web pages, files (\*pdf, \*doc, \*xls, and so on), and more. Data filters do not apply to HTTPS content if SSL decryption has also been enabled.

**Web Safe Mode**

Use this to help restrict access to inappropriate images or videos.

- **Enable Google SafeSearch**. This helps to block inappropriate or explicit images from Google search results.
- **Enable YouTube restricted mode**. This hides videos that may contain inappropriate content (as flagged by users and other criteria).

**SSL Scanning**

Use this to configure whether web pages should be decrypted to identify potential malware or content that should be filtered. You can select SSL scanning for:

- **Risky websites**.
- **Search engines and social media**.
- **Let me specify**. This lets you set options for each category of website.

For each category, you can specify whether to scan all sites in the category, or select **Let me specify** again to select which subcategories to scan.

**Note**

This is an automated process so no additional certificates need to be deployed. All SSL decryption is performed with a Sophos CA.

**Trusted Destination IPs & Domains**

Use this to specify IP addresses and domains for which traffic will not be routed through the Web Gateway. Instead that traffic will go directly to the internet.
Note
A port does not have to be specified. If you do not specify one, it is assumed that this rule will be applied on ALL ports.

Trusted Source IPs

Use this to specify source IP addresses and subnets where traffic will not be routed through the Web Gateway.

When the Web Gateway agent is on the specified IP address or subnet, Web Gateway will not run. This setting is often used for known safe networks where network security is already in place.

Related concepts
Create or Edit a Policy (page 542)
You can create or edit a policy as follows.

Related information
Sophos Web Security and Control Test Site

Web Gateway policy: protection

For a Web Gateway policy, you can configure protection settings such as advanced antivirus scanning options, network logging levels, and URL parameter stripping.

To change the protection settings, in the Web Gateway policy, click Settings and then Protection.

Logging & Privacy

Use this to configure how network events should be logged.

You can choose which types of events are logged and whether the user associated with an event is identified.

Enable Parameter Stripping

Use this to configure whether sensitive URL parameters (parameters showing sensitive data) should be stripped from URLs when they are stored for logging.

This setting is important when combined with SSL scanning, as often URL parameters contain information like usernames, passwords, accounts IDs and more.

Example: https://www.mysite.com/account?
user=ben.allen&password=login1234&account=22486371&cvo_crid=25298130

Related concepts
Create or Edit a Policy (page 542)
You can create or edit a policy as follows.

**Web Gateway policy: notifications**

For a Web Gateway policy, you can configure custom web pages to notify of blocks or warnings.

To change the notifications settings, in the Web Gateway policy, click **Settings** and then **Notifications**.

**Custom Block & Warn Pages**

Use this to customize the page that is shown to the user when a web page is blocked or when the user is warned about a risky site.

You can specify the text that is shown to the user and include your own logo.

**Note**
The logo must be self-hosted.

**Related concepts**

Create or Edit a Policy (page 542)

You can create or edit a policy as follows.

**9.7 Settings**

The Settings pages are used to specify security settings that apply to all your users and devices.

The pages displayed depend on the features included in your license. Some of these pages may also be displayed under Global Settings in Overview.

**Note**
If you want to apply settings only to certain users, servers, or devices, use the Policies pages instead.

**9.7.1 Active Directory Sync**

You can import users and user groups from Active Directory to Sophos Central.

In Settings, on the Active Directory Sync page, you can select the Active Directory service you want to use.

- There is a download link for the Sophos Central Active Directory synchronization utility.
- In Endpoint Protection and Email Gateway you can use Azure Active Directory synchronization instead.

**Note**
If you are using Office 365 you must use Azure Active Directory synchronization.
For instructions on setting up the utility, see the Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

**Related concepts**

*Active Directory Sync Status* (page 548)

On the **Active Directory Sync** page, you can check the sync status and download the installer.

*About Active Directory synchronization* (page 548)

Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

**Related tasks**

*Set up synchronization with Active Directory* (page 549)

Follow these instructions to set up synchronization with Active Directory.

**Active Directory Sync Status**

On the **Active Directory Sync** page, you can check the sync status and download the installer.

You need to set up Active Directory synchronization before you can see these options.

You can download the latest installer for setting up synchronization with Active Directory.

**Sync status**

This shows your synchronization status and the synchronization settings in Active Directory.

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The time of the last synchronization with Active Directory.
- The number of users and groups imported from Active Directory.

You can view Active Directory synchronization alerts on the **Overview > Alerts** page. You can view synchronization events on the **Overview > Logs & Reports > Events** page.

*About Active Directory synchronization*

Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

To synchronize with Active Directory, you need to download and install the Sophos Central Active Directory Sync utility. The utility works as follows.

It synchronizes active users and user groups.

It can run automatically on a regular basis, as set up by the Sophos Central administrator.

It doesn’t duplicate existing users or groups when they are matched to an existing Sophos Central user or group. For example, an email address from Active Directory may be added to an existing user in Sophos Central.

It supports only the Active Directory service.

It can synchronize multiple Active Directory forests. To do this, you need to install the utility on multiple machines and configure each utility to synchronize a different Active Directory forest. We strongly recommend to synchronize different Active Directory forests at different times of day, so that the synchronizations do not overlap.

It doesn’t help you to deploy the Sophos agent software to your users’ devices. Use other methods of deployment with Active Directory.
Set up synchronization with Active Directory

Follow these instructions to set up synchronization with Active Directory.

Before you can set up synchronization, you need .NET Framework 4 on the computer where you will run the Sophos Central AD Sync Utility.

**Warning**

Before you proceed, make sure all your active directory users are set up correctly with an email address. Users without an email address aren't protected and email going to an email address not tied to a user isn't delivered.

You need to use API credentials to synchronize with Active Directory.

To set up synchronization with Active Directory:

1. Set up your API credentials for AD sync. To do this, click **Settings > API credentials**.
2. Add a new credential. Enter the following information:
   - **Credential name**
   - **Description**
3. Copy the **Client ID** and **Client Secret**.
4. Click **Settings > Active Directory Sync**, and click the link to download the Sophos Central AD Synchronization Utility installer. Then run it.

   Alternatively, go to the **Start** menu and click **Sophos > Central > AD Sync**. If you are running Windows 8 or later, in the Apps list, find the app **AD Sync** listed under **Sophos**.

   The **Sophos Central AD Sync Utility Setup** assistant starts.
5. In the setup wizard, enter the information required.

   Follow the instructions in the **Sophos Central AD Sync Utility Setup** assistant.
6. On the last page of the setup assistant, select **Launch Sophos Central AD Sync Utility** and click **Finish**.
7. In the Active Directory Synchronization Setup utility, on the **Sophos Credentials** page, enter your **Client ID** and **Client Secret** instead of your Sophos Central account credentials.
8. On the **AD Configuration** page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the **Use LDAP over an SSL connection (recommended)** checkbox selected. If your LDAP environment doesn't support SSL, clear the **Use LDAP over an SSL connection (recommended)** checkbox and change the port number. The port number is usually 636 for SSL connections and 389 for insecure connections.
9. If you don’t want to synchronize the entire forest, on the **AD Filters** page, you can specify which domains to include in the synchronization. You can also specify additional search options (search bases and LDAP query filters) for each domain. Distinct options can be specified for users and user groups.

   **Note**

   AD Sync will only create groups that have members which include discovered users or devices, regardless of group filter settings.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search bases</td>
<td>You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format: OU=Finance,DC=myCompany,DC=com</td>
</tr>
<tr>
<td>LDAP query filters</td>
<td>To filter users, for example, by group membership, you can define a user query filter in this format: memberOf=CN=testGroup, DC=myCompany, DC=com. The above query limits user discovery to users belonging to “testGroup”. Note that if you don't specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter: CN=testGroup</td>
</tr>
</tbody>
</table>

**Note**
If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

10. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.

    **Note**
    A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

    If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select **Never. Only sync when manually initiated**.

11. Click **Finished**.

12. To synchronize immediately, in the AD Sync Utility, click **Preview and Sync**. Review the changes that will be made during the synchronization. If you are happy with the changes, click **Approve Changes and Continue**.

    The Active Directory users and groups are imported from the Active Directory to Sophos Central.

    To stop the synchronization in progress, click **Stop**.
9.7.2 Role Management

You can use pre-defined administration roles to divide up security tasks according to the administrators' responsibility level.

In **Settings**, the **Role Management** page shows a list of administration roles and the number of users assigned to each role.

You can only see this option if you are a Super Admin administrator.

Click on a role name to see a detailed description of the role and the names of the people that have that role assigned to them. You can manage the people assigned to a specific role in that role's page.

**Restriction**

An administrator role affects what a user can do.

Administration Roles

Predefined roles cannot be edited or deleted.

Your assigned administrator role affects what you can do.

A Super Admin can add custom roles. These roles are based on the predefined roles but you can restrict the access for a custom role to a specific product.

**Restriction**

You can add custom roles only if you are signed up to the Sophos Early Access Program.

Super Admin

Administrators with this role have access to everything in Sophos Central.

They can manage roles and role assignments. In addition, they can create, edit, assign, and delete custom roles.

There must be at least one administrator with the Super Admin role.

Admin

Administrators with this role have access to everything in Sophos Central.

They can't manage roles and role assignments.

Help Desk

Administrators with this role have read-only access for all settings in Sophos Central. They can also:

- Look at sensitive logs or reports.
- Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.
Sophos Central Admin

- Update the Sophos agent software on a computer.
- Scan computers.
- Modify co-branding.

They can't see role management options. Also they can't see some options, such as Edit buttons.

Read-only

Administrators with this role have read-only access for all settings in Sophos Central. They can also:
- Look at sensitive logs or reports.
- Receive alerts.

They can't see role management options. Also they can't see some options, such as Edit buttons.

User

Administrators with this role have no administration capabilities. They have access only to the Self Service Portal.

Related concepts
Administration Roles for Intercept X with EDR (page 553)
Administrators can do more if they have Intercept X with EDR.

User Summary (page 522)

Related tasks
Create an Enterprise Admin (page 629)
Remove administrators (page 557)

You can remove administrators. Removing an administration role from a user does not delete the user.

Administration role details
If you click a role on the Role Management page, its details are shown on a separate page.

The sections on that page include the following.

Permissions

This is the access level for a role. The options are Full, Help Desk, or Read-only.

Global Settings

These are the specialized capabilities for a role. The settings are:

- **Access sensitive logs & reports**: This option means that an administrator can view sensitive logs and reports; for example the Audit Logs.
- **Access policy management**: This option means that an administrator can change policy settings.
- **Access policy assignment**: This option means that an administrator can assign policies to users and devices.
Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details.

Administration Roles for Intercept X with EDR

Administrators can do more if they have Intercept X with EDR.

Super Admin and Admin

Administrators with these roles can also:
• View the intelligence report.
• Request the intelligence report
• Add items to the “Clean and Block” list.
• Remove items from the “Clean and Block” list.
• View blocked items.
• Request an on-demand threat case.
• View on-demand threat cases.
• Isolate and un-isolate devices.
• Request a forensic snapshot.
• Request a threat search.
• View a saved threat search.

Help Desk

Administrators with this role can also:
• View the intelligence report.
• Request the intelligence report.
• View blocked items.
• Request an on-demand threat case.
• View on-demand threat cases.
• Request a forensic snapshot.
• Request a threat search.
• View a saved threat search.

Read-only

Administrators with this role can also:
• View the intelligence report.
Add administrators

You assign administration roles to users using the Available Users list.

Existing administration roles, if any, are indicated next to the user's name.

A user can only have one assigned role.

For example if you add a Read-only administrator to the list of Help Desk administrators their assigned role will change to Help Desk administrator. They will no longer be a Read-only administrator.

To add an administrator:

1. In Settings, on the Role Management page, select the administrator role that you want to assign.
2. On the role details page, next to Role Members, click Edit.

   Note
   You can only see this option if you are a Super Admin.

3. In Edit Role Members, select a user in the Available Users list and use the picker arrows to add them to the Assigned Users list for the role. Select Save.

   Tip
   Enter a name or part of a name in the search box to filter the list of available users.

Add a custom role

You can add custom roles if you are a Super Admin.

Custom roles are based on the predefined roles. You can restrict the access for a custom role to a specific product. You can also create a role that allows an administrator to have full access to one product and read-only access to a second product.

Restriction
If a role doesn't have access to both Endpoint Protection and Server Protection (in some cases Encryption as well), the shared settings are read-only.

The shared settings are:

- Tamper protection
- Allowed applications
- Website management
- Proxy configuration
To create a custom role:

1. In **Settings**, on the **Role Management** page, select **Add role**.
2. Give the custom role a name and a description.
3. Select the **Base role** you want to use as the basis for the custom role.
   For example, if you choose **Help Desk** as the **Base role**, administrators with the custom role have **Help Desk** permissions.
4. Choose the product and access type you want the role to have.
   For example, you create a custom role called Endpoint Help Desk. This custom role uses **Read-only** as its **Base role** and **Endpoint Protection** as its selected product with an access type of **Help Desk**.
   This custom role allows any administrators assigned to this role to access **Endpoint Protection** with **Help Desk** permissions.
   a) Choose more than one product, if required.
      You can choose different access types for different products.
      For example, you can create a custom role that has **Help Desk** access permissions for **Endpoint Protection** and **Read-only** access for **Mobile**. You can set the permissions for all other products to **None**. This means that the custom role only has access to **Endpoint Protection** with **Help Desk** permissions and **Mobile** with **Read-only** permissions.
5. Choose the additional access and management options for the custom role.
   - **Enable access to logs & reports**.
   - **Enable policy management (add, edit, and delete)**.
   - **Enable policy assignment to users, device, etc..** (turn policies on and off; and add users, user groups, devices and device groups to existing policies).
   For example, this allows a Super Admin to add these permissions to a Read-only or Help Desk role. You can also use these options to reduce the permissions for an Admin role. For example, you could prevent the custom role from managing policies.

   **Note**
   These additional options only apply to the selected products for the custom role.

   The additional options are the same for all products and access types for the custom role.
6. Select **Save**.
   You can now assign this role to administrators.

**Related concepts**
Administration Roles (page 551)

**Related tasks**
Delete custom role (page 556)
You can delete custom roles if you are a Super Admin.

You can change the assigned roles for administrators if you are a Super Admin.

**Change roles**

You can change the assigned roles for administrators if you are a Super Admin.
You can change roles for multiple administrators at the same time.

**Restriction**

You can't change roles for administrators who are currently signed in.

To change roles:

1. In **Settings**, on the **Role Management** page, select the administrator role that you want to assign to other administrators. For example, select a read-only administrator role if you want to assign that role to other administrators.
2. On the role details page, next to **Role Members**, click **Edit**.

   **Note**
   
   You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, add users from the **Available Users** list or remove users from the **Assigned Users** list. Select **Save**.

   **Tip**
   
   Enter a name or part of a name in the search box to filter the list of available users.

**Delete custom role**

You can delete custom roles if you are a Super Admin.

You can only delete custom roles. You can't delete roles that have administrators assigned to them.
You must change their role first.

1. In **Settings**, on the **Role Management** page, select the role you want to remove and select **Delete**.
   
   To select a role, click anywhere in the row apart from the name.
2. Select **Delete** to confirm role deletion.

**Related concepts**

*Administration Roles* (page 551)

**Related tasks**

*Add a custom role* (page 554)
You can add custom roles if you are a Super Admin.

*Change roles* (page 556)
You can change the assigned roles for administrators if you are a Super Admin.

*Remove administrators* (page 557)
You can remove administrators. Removing an administration role from a user does not delete the user.

**Remove administrators**

You can remove administrators. Removing an administration role from a user does not delete the user.

**Note**

You cannot delete a user who has an assigned administration role. You must remove the role from the user before deleting the user.

To delete administrators:

1. In **Settings**, on the **Role Management** page, select the administrator role from which you want to remove users.
2. On the role details page, next to **Role Members**, click **Edit**.

**Note**

You can only see this option if you are a Super Admin.

3. In **Edit Role Members**, select a user in the **Assigned Users** list and use the picker arrows to remove them.

**Tip**

Enter a name or part of a name in the search box to filter the list of assigned users.

### 9.7.3 Tamper Protection

You can enable or disable tamper protection for all your servers and users’ computers.

To do this, in **Settings**, open the **Tamper Protection** page.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer. They need the necessary password:

- Change settings for on-access scanning, suspicious behavior detection (HIPS), web protection, or Sophos Live Protection.
- Disable tamper protection.
- Uninstall the Sophos agent software.

**Manage tamper protection for a specific device**

You can change the tamper protection settings for a specific device or server.

Open the device’s details page and look under **Tamper Protection**. There you can do as follows:

- View the password.
- Generate a new password.
- Temporarily disable tamper protection for that device.
Recover tamper protection passwords

You can recover the tamper protection passwords of devices that you’ve recently deleted.
You might need to do this so that you can uninstall Sophos software that is still on those devices.

9.7.4 API Token Management

You can generate and manage the API token used for secure access to the Security Information and Event Management (SIEM) Integration API. This enables you to pull new event and alert data from Sophos Central. For further information, click the knowledge base article link provided on the page.

To add a token:
1. In Settings, open the API Token Management page.
2. Click Add Token.
3. Give the token a name and click Save.
   This generates the API token. The token is valid for a year.
Click Renew to extend the validity of the token.
Click Delete to remove the token.

9.7.5 API credentials

You can manage and add credentials for Sophos Central Admin.

Note
The first time you click API credentials you must read and accept the terms and conditions of use.

To add credentials, do the following:
1. Click Add Credential and give the credential details.
   This generates the credential, together with a Client ID and a Client Secret.
2. Copy the Client ID and Client Secret.

   Note
   You can only see the Client Secret once.

To delete an API credential, select it in API credentials and click Delete.

9.7.6 Website Management

This page is not available if you do not have a Web Control or Web Gateway license.
Note
If an option is locked, global settings have been applied by your partner or Enterprise administrator.

You can extend the website filtering provided by Sophos Central. For more information on how Sophos filters websites see Sophos Web Security and Control Test Site.

In Settings, on the Website Management page, you can use a website list to:

- Control websites not in one of the Sophos categories.
- Tag websites to put them in groups, which are like custom categories. You can then use policies to control these websites for certain users.
- Override the Sophos category for a site. This changes that site’s category for all your users.

Note
If you think Sophos has put a website in the wrong category, you can ask us to change it. To do this, see Open a Support Case. We suggest you try this instead of overriding the category.

To add a site to the website list:

1. Click Add in the upper right of the page.
   The Add Website Customization dialog is displayed.
2. Enter sites.
   Entries in the website list can be single URLs, full domains, TLDs, IP addresses, CIDR ranges, or even top level domains.

   Note
   Managing websites using IP addresses only controls browser-based access. It does not block other applications or interact with rules for a local firewall.

3. Select Enable Category Override if you want to associate a specific category with the sites you have entered. Then select a Category.
4. Select Enable Tags to associate a tag with the sites you have entered. Then type a tag name.
   Tags can be used when creating web control policies for endpoint computers or servers. See the Log web control events section in Web Control Policy.
5. Enter text in the Comments text box.
   It can be helpful to include information about tags you have created and categories you have overridden for troubleshooting policy issues in the future.
6. Click Save.
   Your entry will be added to the website list.

You can also edit entries in the list or delete them.

To edit an entry, click the edit icon . The icon is on the right of the entry.
To delete an entry, select the checkbox to the left of the entry and click Delete.

Related information
Open a Support Case
9.7.7 Global Exclusions

You can exclude files, websites, and applications from scanning for threats.

Introduction

You use exclusions to tune the detection behavior of Sophos Central.

Related reference

**Website exclusions** (page 563)
You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

**Process exclusions (Windows)** (page 563)
You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

**Device isolation exclusions (Windows)** (page 563)
You can allow isolated devices to have limited communications with other devices.

Related information

Sophos Threat Center

Exclusions

Global exclusions apply to all your users (and their devices) and servers.

If you want exclusions to apply only to certain users or servers, use policy exclusions instead.

You can set up the following types of exclusion:

- Exclude files or folders from scanning.
  
  If you exclude files from scanning, we'll still check the excluded items for exploits.

- Exclude from checking any process that runs from an application.

- Exclude websites from checking.

- Exclude applications from protection against security exploits.

- Exclude applications that are normally detected as spyware and previously detected exploits from scanning and detection.

- Exclude previously detected malicious behavior exploits. This is only available if you are signed up to the Early Access Program.

You can also use exclusions to allow isolated devices to communicate with other devices under restrictions. This feature is available if you have Intercept X Advanced with EDR.

**Warning**

Think carefully before you add global exclusions because doing so may reduce your protection.
Can’t edit the exclusions?

If an option is locked global settings have been applied by your partner or Enterprise administrator. You can still stop detecting applications, exploits and ransomware from events.

Exploit exclusions

If you exclude files from scanning, we'll still check the excluded items for exploits. If you want exclusions from exploit checking, do as follows:

• To stop checking for an exploit that has been detected, use a Detected Exploits exclusion.
• To exclude certain applications from checking, use Exploit Mitigation Exclusions.
• To stop checking for a malicious behavior exploit that has been detected, use a Behavioral Protection exclusion.

Set up exclusions

You can exclude files, websites and applications from scanning for threats.

To set exclusions:
1. Go to Global Exclusions.
2. Click Add Exclusion.
   The Add Exclusion dialog is displayed.
3. In the Exclusion Type drop-down list select what you want to exclude.
4. Specify the item or items you want to exclude.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File or folder (Windows)</td>
<td>You can exclude a drive, folder or file by full path. You can use the wildcard * for file name or extension but ** is not valid.</td>
</tr>
<tr>
<td>File or folder (Mac/Linux)</td>
<td>You can exclude a folder or file. You can use the wildcards ? and *.</td>
</tr>
<tr>
<td>File or folder (Sophos Security VM)</td>
<td>On Windows guest VMs protected by a Sophos security VM, you can exclude a drive, folder or file by full path. You can use the wildcards * and ? but only for file names.</td>
</tr>
<tr>
<td>Process (Windows)</td>
<td>You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process). If possible, enter the full path from the application.</td>
</tr>
<tr>
<td>Website (Windows/Mac)</td>
<td>You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Potentially Unwanted Application (Windows/Mac)</strong></td>
<td>You can exclude applications that are normally detected as spyware. Specify the exclusion using the same name under which it was detected by the system. Find more information about PUAs in the Sophos Threat Center.</td>
</tr>
<tr>
<td><strong>Detected Exploits (Windows/Mac)</strong></td>
<td>You can exclude any exploit that has already been detected. We’ll no longer detect it for the affected application and no longer block the application.</td>
</tr>
<tr>
<td><strong>Device isolation (Windows)</strong></td>
<td>You can allow isolated devices to have limited communications with other devices. Choose whether isolated devices will use outbound or inbound communications, or both. You can then restrict communications.</td>
</tr>
<tr>
<td><strong>Malicious Network Traffic Prevention (IPS) (Windows)</strong></td>
<td>You can exclude specific network traffic from inspection. Choose whether to exclude outbound or inbound traffic. Then specify the address or ports the traffic uses.</td>
</tr>
<tr>
<td><strong>Exploit Mitigation (Windows)</strong></td>
<td>You can exclude applications from protection against security exploits. For example, you might want to exclude an application that is incorrectly detected as a threat until the problem has been resolved.</td>
</tr>
<tr>
<td><strong>AMSI Protection (Windows)</strong></td>
<td>You can exclude a drive, folder or file by full path. Code in this location is not scanned. You can use the wildcard * for file name or extension.</td>
</tr>
<tr>
<td><strong>Behavioral Protection (Windows)</strong></td>
<td>You can exclude applications from protection against behavioral exploits. For example, you might want to exclude an application that has been incorrectly detected as behaving maliciously. You can't edit these exclusions after you create them. This option is only available if you are signed up to the Early Access Program.</td>
</tr>
</tbody>
</table>

5. For File or folder exclusions, in the **Active for** drop-down list, specify if the exclusion should be valid for real-time scanning, for scheduled scanning, or for both.

6. Click **Add** or **Add Another**. The exclusion is added to the scanning exclusions list.

To edit an exclusion later, click its name in the exclusions list, enter new settings and click **Update**.
**Device isolation exclusions (Windows)**

You can allow isolated devices to have limited communications with other devices. You can choose whether isolated devices will use outbound or inbound communications, or both.

Use the following settings to restrict communications:

- **Local Port**: Any device can use this port on isolated devices.
- **Remote Port**: Isolated devices can use this port on any device.
- **Remote Address**: Isolated devices can only communicate with the device with this IP.

**Example 1**

You want remote desktop access to an isolated device so that you can troubleshoot.

- In **Direction**, select **Inbound Connection**.
- In **Local Port**, enter the port number.

**Example 2**

You want to be able to go to an isolated device and download cleanup tools from a server.

- In **Direction**, select **Outbound Connection**.
- In **Remote Address**, enter the address of the server.

**Website exclusions**

You can specify websites for exclusion using IP address, IP address range (in CIDR notation), or domain.

Examples:

- IP address: 192.168.0.1
- IP address range: 192.168.0.0/24
- The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range.

Thus /24 equals the netmask:

```
11111111.11111111.11111111.00000000
```

In our example, the range includes all IP addresses starting with 192.168.0.

- **Domain**: google.com

**Process exclusions (Windows)**

You can exclude any process running from an application. This also excludes files that the process uses (but only when they are accessed by that process).

If possible, enter the full path from the application, not just the process name shown in Task Manager.

Example:
%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe

Note
To see all processes or other items that you need to exclude for an application, see the application vendor's documentation.

Note
You can use wildcards and variables.

9.7.8 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

Set the bandwidth used

In Settings, on the Bandwidth Usage page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.

This helps to ensure that updating does not cause computers to run slowly.

You can specify a custom bandwidth or unlimited bandwidth.

Note
This setting is for Windows computers only.

Note
This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos. To save bandwidth in this case, see Manage Update Caches and Message Relays.

Related concepts
Manage Update Caches and Message Relays (page 567)

9.7.9 Multi-factor authentication

If you're a Super Admin, you can make some or all of the Sophos Central admins sign in with multi-factor authentication.

Introduction

Using multi-factor authentication means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos or Google Authenticator, SMS or email authentication to sign in.

Multi-factor authentication is turned on by default for newly created Sophos Central accounts.
This page tells you how to do the following:

- Set up multi-factor authentication.
- Sign in with multi-factor authentication for the first time.
- Add another method for multi-factor authentication.
- Sign in with email authentication if you don’t have Sophos or Google Authenticator.
- Reset an admin’s sign-in details, for example if they lose their phone.
- Turn off multi-factor authentication for an admin.

Set up multi-factor authentication

If you're a Super Admin, you can choose how your administrators sign in.

To set up multi-factor authentication, do as follows:

1. Go to Settings > Multi-factor Authentication (MFA).
2. Choose how you want admins to sign in:
   - No MFA needed.
   - All admins need MFA. This is the default for new accounts.
   - Select admins who will need MFA. This lets you select individual admins.
3. If you choose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). Move admins to the Assigned Users list and click Add.
4. Click Save.

When admins next sign in, they are prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

The first time you sign in with MFA, do as follows:

1. At the sign-in screen, enter your user ID (email address) and password.
   A Set Up Your Login Information dialog explains that signing in needs additional authentication.
2. In the next dialog:
   a) Enter the security code that has been sent to you in an email.
   b) Create a 4-digit PIN. This enables you to use email as an authentication method.
3. In the next dialog, choose authentication type.
4. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
   You also need to enter a security code to verify a device if you have chosen SMS as your authentication type.

Sophos Central Admin opens.

The next time you sign in, you only need to enter a code from Sophos or Google Authenticator when prompted.
Add another authentication option for multi-factor authentication

You can set up multiple authentication options for a Sophos Central Admin account. You can authenticate with SMS and Sophos or Google Authenticator. You must have an authentication option already set up.

To set up another authentication option, do as follows:

1. Sign in to Sophos Central Admin.
2. Click your account name and click Manage Login Settings.
3. Click Create New Method.
4. Choose another authentication method.
5. Click Next.
6. In Verify Your Device, scan the QR code and enter the security code that Sophos or Google Authenticator displays.
7. To confirm that the new method has been added, click your account name and click Manage Login Settings. An additional authentication method has been added.

Sign in with email authentication

If you don't have access to Sophos or Google Authenticator, you can sign in with email authentication instead.

1. At the sign-in screen, enter the user ID (email address) and password.
2. In Verify Your Login, click Choose Another Method.
3. In Pick Your Challenge, click the email option. An email is sent to you.
4. Open the email and find the security code.
5. In Verify Your Login, enter the security code and your 4-digit PIN.

You’ll be asked for the security code and PIN each time you sign in from now on, until you switch back to using Sophos or Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can allow them to set up their sign-in again.

1. On the People page, under Users, find the user and click their name to open their details.
2. In the user details, on the left of the screen, you’ll see their MFA status and settings. Click Reset and confirm that you want to do a reset.

The next time the admin tries to sign in, they’ll need to go through the setup steps again.

Turn off multi-factor authentication

If you’re a Super Admin, you can turn off multi-factor authentication for an administrator.

To turn off multi-factor authentication, do as follows:

1. Go to Settings > Multi-factor Authentication (MFA).
2. Click Select admins who will need MFA.
3. Click Add admins.
4. Move the administrator from the **Assigned Users** list and to the **Available Users** list.
5. Click **Add**.
6. Click **Save**.

### 9.7.10 Manage Update Caches and Message Relays

This saves you bandwidth, as updates are downloaded only once, by the server.

You can also enable computers to communicate with Sophos Central through a message relay on a server on your network.

A message relay server must also have an update cache set up on it.

This help page tells you how caches and relays work and how you set them up.

**Tip**

Computers can get the latest Sophos agent from a cache the first time you run the Sophos installer on them. You need to set up your caches before installation. If you have endpoints that can't connect to Sophos directly, you also need to set up your update caches as message relays.

**Note**

If you use the **Reject network connections** feature (for customers with Sophos XG Firewall), it could prevent a cache server from delivering updates. To avoid this, see **Reject network connections**.

#### How caches and relays work

When you set up a cache (and optionally relay) on a server, Sophos Central does as follows:

- Installs Sophos caching software (and relay software).
- Fetches updates from Sophos and puts them in a cache.
- Automatically configures computers in your network to update from a cache (and use a relay).
  - You can also assign computers to use a specific cache or relay.

Using caches doesn't affect how often or when computers are updated.

#### Computers that can use caches and relays

You can install caches and relays on Windows Server 2008 or later (2008 R2 for relays).

The following computers can use caches or relays:

- Windows 7 and later (including servers), Macs and Linux computers can use a cache.
- Windows 7 and later (including servers) and Linux computers can use a relay.

#### Set up a cache/relay

You can set up a cache and a relay at the same time, or a cache only. You can also set up a relay on a server that already has a cache.
Before you set up a cache or a relay, ensure that:

- The server is running Windows Server 2008 or later.
- The server has at least 5GB free disk space.
- Port 8190 and 8191 are available and accessible to computers that will update from the cache and use the relays.

The installers will open ports 8190 and 8191 in Windows Firewall. When Update Cache or Message Relay are uninstalled, the ports are closed again.

If you use the Reject network connections feature (for customers with Sophos XG Firewall), you might need to add the server to the exclusions. See Reject network connections.

To set up a cache or a relay:

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. In the filter above the table, click the drop-down arrow and select Cache Capable Servers to see which servers are suitable for a cache and a relay. If you have already set up a cache on some servers, to hide them from view, select Servers without Update Cache. If you want to set up a relay on a server with a cache, select Servers with Update Cache.
3. Select the server or servers where you want to set up a cache or relay.

Sophos Central automatically configures computers in your network to use a cache or relay. You can also manually assign computers to use a specific cache or relay.

Assign computers to a cache/relay

You can manually assign computers to use a specific cache or relay.

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. For the server on which the cache or relay is installed, click the link displaying the number of computers using the Update Cache or Message Relay, in the Updated from cache column or the Using Relay column, respectively.
3. Click Manual assignment.
4. Select the computers.
5. Click Save.

See which computers use caches and relays

On the Manage Update Caches and Message Relays page you can view which servers have update caches and message relays. You can see how many computers are using them as caches or relays and the activity of the update caches.

Click a server to see the details of the computers using its update cache or message relay.
Remove a cache/relay

Note
If you want to remove a cache that has computers manually assigned to it you must reassign them first.

When you remove a cache, Sophos Central does as follows:

- Uninstalls caching software, removes the cache of downloaded updates, and closes port 8191 in Windows Firewall.
- Also uninstalls the message relay software (if installed) and closes port 8190 in Windows Firewall.
- Reconfigures computers that update from this server to update from another update cache, if you have one.
- Reconfigures computers that use the relay to use another message relay, if you have one.

If you remove all your caches, computers will update directly from Sophos.

If you remove all of your message relays, computers will communicate directly with Sophos Central.

To remove a cache/relay:

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. In the filter above the table, click the drop-down arrow and select Servers with Update Cache to see which servers have a cache set up. You can also select Servers with Message Relay to see which servers have a message relay set up.
3. Select the server or servers you want to remove a cache/relay from.
4. Click Remove Cache/Relay.

Related concepts
Reject network connections (page 136)
You can configure devices to reject connections from other devices on the network that may be unsafe.

9.8 Protect Devices

On this page, you download Sophos installers and use them to protect your devices.

The installers you can see may depend on the license or licenses you have.

Before you start, check which operating systems you can protect with Sophos Central.

Related information
check which operating systems you can protect with Sophos Central

9.8.1 Web Gateway

You install Sophos Web Gateway on workstations or mobile devices to provide advanced web security.

It can block malicious, risky, or inappropriate websites, and provide scanning for secure sites (SSL), keyword filtering, trusted networks, and comprehensive reporting.
Install Web Gateway on workstations

Go to Protect Devices.

Download the installer for your operating system and run it on workstations you want to protect.

Note
You can install Web Gateway alongside the Endpoint Protection agent or on its own.

When you protect a workstation:
• The installer checks if there is already an Endpoint Protection agent on the computer. If not, it asks you for a username.
• If the user is new, they are added to the Users list.
• If the computer is not already in the Computers list, it is added.
• If you have a Web Gateway policy enabled for the user or computer, it starts protecting the computer.

Install Web Gateway on mobile devices

Go to Protect Devices.

Click the operating system you want. You'll see instructions for sending a configuration profile to a mobile device and applying a policy.
10 Firewall Management

Firewall management lets you monitor and configure Sophos XG Firewalls that can connect to Sophos Central.

10.1 Dashboard

The Firewall Management dashboard lets you see firewall activity at a glance.

Go to Firewall Management > Dashboard.

Note
If you haven’t added any firewalls to Sophos Central yet, this page invites you to start a free trial of Sophos XG Firewall.

You can see details of the following:

- Alerts
- Firewalls
- Advanced threat protection
- Intrusion prevention
- Web activity

Alerts

The Alerts section shows you statistics for alerts in Sophos Central. This shows all alerts, not just firewall alerts.

To see full details of all alerts, click View All Alerts.

To see a filtered list of alerts, click on the figure for the alert priority (High, Medium or Info).

At the main alerts list, you can investigate and take action against alerts.

Firewalls

The Firewalls section shows the current status of firewalls. You can see here if firewalls need attention for any of these reasons:

- Not connected
- Not managed
- License expiring
- Health issues

To see the full list of firewalls and resolve issues, click Show All Firewalls.
Advanced Threat Protection

This shows you statistics for threats detected by firewalls in the previous two hours.

Advanced threat protection (ATP) analyzes incoming and outgoing network traffic (for example, DNS requests, HTTP requests, and IP packets) for threats. Using ATP, you can quickly detect compromised clients in your network and raise an alert or drop the traffic from those clients.

ATP also uses cloud-based sandboxing, which analyzes suspicious content, so that you can decide whether files are safe to allow.

If an attack starts, ATP can prevent devices from connecting to command-and-control servers outside your network.

Intrusion Attacks

This shows statistics for intrusion prevention.

Intrusion prevention looks for anomalies in network traffic in order to detect and prevent denial of service (DoS) and other spoofing attacks.

In Sophos XG Firewall you can specify the action to take when anomalies are found.

Web activity

The graph shows web activity measured at five-minute intervals for the previous two hours.

10.2 Firewalls

You can view and configure any Sophos XG Firewall that can connect to Sophos Central.

Go to Firewall management > Firewalls.

You can manage firewalls individually or as a group. Firewalls that are managed individually are placed in a group called Ungrouped.

The information displayed for each firewall includes the following:

- **Alerts**: Alerts in the last 24 hours.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄 100%</td>
<td>CPU usage alert: to see a graph of CPU usage in the last two hours, click the icon.</td>
</tr>
<tr>
<td>⚠️ 1</td>
<td>Management and reporting alert: for more information, click the icon.</td>
</tr>
</tbody>
</table>

- **Sync & Management**
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronized</td>
<td>The firewall is online and sending regular heartbeats. The firewall’s configuration matches the group policy.</td>
</tr>
<tr>
<td>Connected</td>
<td>If the firewall is ungrouped, this status indicates that the firewall is online and sending regular heartbeats.</td>
</tr>
<tr>
<td></td>
<td>If the firewall is in a group and this status remains unchanged for more than about a minute, this indicates that the firewall is online and sending regular heartbeats but it is not starting to synchronize with the group policy. This may be because the synchronization tasks have not been created or the tasks have been created but the firewall is not pulling them. In this case, inspect the tasks queue to find out which transactions are pending.</td>
</tr>
<tr>
<td>Error needs attention</td>
<td>The firewall’s configuration does not match the group policy. The admin needs to inspect the tasks queue to find out which policy cannot be applied.</td>
</tr>
<tr>
<td>Synchronizing</td>
<td>The firewall has just been added to the group. Sophos Central is applying the group policy to the firewall.</td>
</tr>
<tr>
<td>Last seen x hours ago</td>
<td>The firewall is offline.</td>
</tr>
<tr>
<td>(for Sophos XG Firewall 18 or later) or Disconnectsed</td>
<td>The firewall is offline.</td>
</tr>
<tr>
<td>Approval Pending</td>
<td>The firewall has been registered with Sophos Central by a local admin from the firewall’s web admin console. It is waiting for approval by a Sophos Central admin. When approved, the firewall is ready for group and individual device management.</td>
</tr>
<tr>
<td>Management Disabled</td>
<td>The firewall is registered with Sophos Central. However, Sophos Central management has not been turned on from the firewall’s web admin console.</td>
</tr>
</tbody>
</table>

If you click a status, more information is displayed:

<table>
<thead>
<tr>
<th>Additional information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing since x hours</td>
<td>The firewall sends a heartbeat message every minute. If five heartbeat messages are missed, Sophos Central considers the firewall to be offline.</td>
</tr>
</tbody>
</table>
### Failed to apply a policy x days ago
A policy could not be applied to the firewall. The tasks queue may have more details about the reason for the failure.

### Firewall is suspended.
The firewall has been offline or out of sync with the group policy for more than 30 days. This means that Sophos Central cannot discover its current status. To resolve this issue, remove the firewall from the group and re-add it.

### Central Reporting is Disabled
Firewall reporting can be turned on from the firewall’s web admin console.

### Synchronized Security

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>The number of apps discovered by the firewall</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Reporting is turned off</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Reporting is turned on</td>
</tr>
</tbody>
</table>

### Version
The firewall OS version.

Click a firewall to open the firewall’s web admin console. This lets you configure the firewall.

**Note**
You must be an Admin or Super Admin in Sophos Central to open the web admin console. This gives you the same permissions as the firewall’s local "admin" account. It also lets you change the password for an "admin" account, which is necessary when you deploy firewalls via Zero Touch.

**Note**
For information on using Zero Touch configuration, see Add a firewall with Zero Touch.

### Add firewalls
You add firewalls so that you can monitor them in Sophos Central and also manage them from the web admin console.

The steps depend on whether you want to add a new firewall or add a firewall that has already been deployed.

To add a new firewall:
1. Click **Add Firewall** and select the option to add a new firewall.
2. Register your serial number.
   You're guided through registration and deployment.
To add a firewall that is already deployed:

1. Log in to your firewall.
2. On the Central Synchronization page, turn on Manage from Sophos Central.
3. In Sophos Central, on the Firewalls page, expand the Ungrouped group, find the firewall, and click Accept services.

Watch a video of these steps here: XG Firewall Management from Sophos Central.
If you have problems accessing the video, you can also find it in our XG Firewall How-To Library.

Create group

If your firewalls are on firmware version 18.0 or later, you can add them to a group and configure them all simultaneously using a group policy.

Note
You must be an Admin or Super Admin in Sophos Central to create a group.

1. Click Create New Group.
2. Enter a name for the group.
3. Assign firewalls to the group.
   You don’t have to assign firewalls when you create a group. You can create an empty group, edit its policy, and then assign firewalls to it. The group policy is applied to the firewalls as they are assigned, even if they are assigned after the group policy has been edited. From then on, the firewall configuration is in sync with the group policy.
4. Click Save.

Edit group policy

You can edit the policy that will apply to all firewalls in a group.
1. Click the ellipsis button (…) on the right of the group for which you want to edit the policy.
2. Select Manage Policy to open the group policy editor.
   In the main menu, under Manage Firewalls > Firewalls, the name of the group is displayed.
3. Change the policy as required, in any of the sections in the main menu. For an explanation, see the Sophos XG Firewall help.
   If your policy refers to firewall zones or interfaces, you may need to create dynamic zones or interfaces. See Dynamic objects.
You can view the tasks queue to see the status of the application of the policy to the firewalls.

CAUTION
When you add firewall or NAT rules, the Top and Bottom settings apply only to the ordering of rules within Sophos Central, not rules that may have been created locally on the firewall. Furthermore, all rules pushed from Sophos Central are inserted at the top of the rules list on the firewall. To avoid unexpected firewall behavior, when a firewall is managed from Sophos Central, we recommend that all rules are created and pushed from Sophos Central.
Create subgroup

You can create a subgroup within a group. This enables you to edit the group policy differently for each subgroup. For example, if you have a group called “Acme Corporation” that contains subgroups called “Boston”, “London”, and “Hyderabad”, the policy created for Acme Corporation is automatically applied to all firewalls in all the subgroups. However, if you edit the policy for Boston, your changes are applied only to firewalls in the Boston subgroup, not firewalls in the London and Hyderabad subgroups.

1. Click the ellipsis button (…) on the right of the group in which you want to create a subgroup.
2. Select **Add a Subgroup**.
3. Enter a name for the subgroup.
4. Assign firewalls to the subgroup.
   You don’t have to assign firewalls when you create a subgroup. You can create an empty subgroup, edit its policy, and then assign firewalls to it. The subgroup policy is applied to the firewalls as they are assigned, even if they are assigned after the subgroup policy has been edited. From then on, the firewall configuration is in sync with the subgroup policy.
5. Click **Save**.

Inheritance of objects and settings by subgroup policies

“Objects” are those pages in the group policy editor that typically have **Add** and **Delete** buttons. Examples are firewall rules, NAT rules, FQDN hosts, and IP hosts. Objects you create for a parent group policy cannot be modified by a subgroup policy. For example, if you create a custom **FQDN Host** object for the Acme Corporation policy, the Boston, London, and Hyderabad policies inherit a read-only copy of the object, which appears dimmed in the Boston, London, and Hyderabad policies. However, a subgroup policy can use an object created by its parent group policy to create its own rules. A subgroup policy is also free to create its own objects. Such objects are visible only to that subgroup policy and the policies of its subgroups.

If you try to remove an object from a parent group policy, it is automatically removed from subgroup policies if it is not used by any of the them. However, if it is used, removal is prevented, and you are informed of the subgroup and rule where the object is used.

“Settings” are those pages in the group policy editor that typically have an **Apply** button. You cannot delete a setting, only configure it and turn it on or off. Examples of settings are **Advanced Threat** settings. Settings can only be configured in the topmost parent group policy. They cannot be configured in any of the subgroup policies. When a setting is applied to the topmost parent group policy, it is applied automatically to all the subgroup policies.

Upgrade firmware for firewalls

You can upgrade firmware for Sophos XG Firewall. If an upgrade is available, you see a **Firmware upgrade** button next to all firewalls eligible for it.

1. Click **Firmware upgrade** to see full details of the available upgrades.
2. If more than one version is available, select the version you want. Then click **Upgrade Firmware** to start the upgrade.

Repeat for each firewall you want to upgrade.
10.2.1 Add a firewall with Zero Touch

You can deploy Sophos XG Firewall using Zero Touch configuration.

Zero Touch lets you specify all the firewall settings in a configuration file. You then send that file to another administrator (for example, in a branch office) who can use it to deploy the firewall, without entering any more settings.

Zero Touch configuration is available for hardware appliances that will be managed from Sophos Central.

Here are the key steps:

1. In Sophos Central Admin, go to Firewall management > Firewalls.
2. Click Add Firewall and select the option to add a new firewall.
3. The installer guides you through these steps:
   a) Enter the serial number of the appliance.
   b) Register the firewall.
   c) Accept the license agreement.
   d) Configure the firewall (LAN settings and setting up a protected network).
4. Download the Zero Touch file or send it to the administrator who will use it.
   If you need to configure any internet settings, you can do so before you download or send the file.

At the site where the firewall needs to be deployed, the local administrator must do as follows:

5. Copy the Zero Touch configuration file onto a USB stick.
6. Put the USB stick into the appliance and start the firewall.
   The firewall detects the Zero Touch configuration file and accepts the internet settings (if any).

In Sophos Central Admin, you must do as follows:

7. When you are prompted, “accept” the new firewall.
   Once the firewall is accepted, the remaining settings get applied.
   When the firewall is accessed, a message prompts Super Admin administrators to set a password for the firewall.

Note
If this admin password isn't set, admins may have trouble accessing the firewall if it loses its connection or is disconnected from Sophos Central Admin in future.
10.2.2 Turn on firewall reporting

You can view the report dashboard and the reports page for a Sophos XG Firewall if you register it with Sophos Central and turn on firewall reporting.

To turn on firewall reporting, do the following:

1. In the web admin console of the Sophos XG Firewall for which you want to turn on firewall reporting, on the Central synchronization page, ensure that the firewall has been registered with Sophos Central. If not, click Register and enter your Sophos Central account credentials.
2. If Sophos Central services is turned off, turn it on. If it is already turned on, click Configure.
3. In the Firewall Management and Reporting from Sophos Central dialog box, select Use Sophos Central reporting and click Apply.
4. In Sophos Central, go to Firewall Management > Firewalls and click Accept services next to the firewall that has just been registered.

Within five minutes, the firewall sends data to Sophos Central. Sophos Central then inserts the data into its database, which can take between five and thirty minutes. Then Sophos Central displays the data in the reports. The firewall sends data at least every five minutes.

Related concepts
Firewall report dashboard (page 578)
The firewall report dashboard shows key information about the hardware, security threats and the performance against policy for the Sophos XG Firewall that you select on the Firewall Management – Firewalls page.

Firewall reports (page 580)
The firewall reports page shows various reports about the security threats and hardware for the Sophos XG Firewall that you select on the Firewall Management – Firewalls page.

10.2.3 Firewall report dashboard

The firewall report dashboard shows key information about the hardware, security threats and the performance against policy for the Sophos XG Firewall that you select on the Firewall Management – Firewalls page.

To view the report dashboard:

1. Go to Firewall management > Firewalls.
2. Select the ellipsis button (…) on the right of the firewall for which you want to view the dashboard.
3. Select View device reports.

The Firewall reporting - Report dashboard page is shown.

The dashboard is split into the following areas:

- Network
- Security
- Policy

Each area shows a snapshot of information at the time the dashboard page was displayed.

For all areas, in each circle, the color of the value indicates the severity:

- Red: Critical
• Yellow: Warning
• Gray: OK

If you click one of the circles, more detailed information about that attribute is shown in the lower part of the area, for the last 24 hours.

In the lower part of each area, there is a View Report link. If this is enabled, you can click it to view the related report on the firewall reports page.

Network

The Network area shows the following information:

• **CPU** shows the percentage CPU usage. Severity:
  — Red: more than 90%
  — Yellow: 80–90%
  — Gray: less than 80%
• **Memory** shows the percentage memory usage. Severity:
  — Red: more than 90%
  — Yellow: 80–90%
  — Gray: less than 80%
• **VPN** shows the number of VPN tunnels that are in a connected state in the firewall.
• **RED** shows the number of Sophos Remote Ethernet Devices that are connected to the firewall.
• **Interfaces** shows the number of ports that the firewall has.

Security

The Security area shows the following information:

• **ATP** shows the number of threats that have been detected by Sophos Advanced Threat Protection, which is included in the firewall. Severity:
  — Red: more than 0
  — Gray: 0
• **Intrusion attacks** shows the number of intrusion attacks that have been detected by the firewall. Severity:
  — Red: At least one attack has a firewall severity level of 4
  — Yellow: At least one attack has a firewall severity level of 3
  — Gray: All attacks have a firewall severity level from 0 to 2
• **Sandstorm cleaned** shows the number of malicious files that were scanned and how many were cleaned. Severity:
  — Red: A malicious file has been detected
  — Gray: No malicious file has been detected
Policy

The Policy area shows the following information:

- **Allowed app categories** shows the number of application categories that are allowed by the firewall.
- **Apps new/mapped** shows the number of newly-detected applications that are unknown to the firewall and the number of detected applications that have been sorted into a category.
- **Risky apps seen** shows the number of applications that were detected that are categorized with a Sophos XG Firewall risk level of 4 (high) or 5 (very high). Severity:
  - Red: At least one application is categorized as risk level 5
  - Yellow: At least one application is categorized as risk level 4
  - Gray: All applications are categorized as risk level 3 or lower
- **New cloud apps** shows the number of new cloud applications that were detected by the firewall.
- **Blocked app categories** shows the number of website categories that were accessed and blocked by the firewall.
- **Objectionable category** shows the number of website categories that were accessed that are classified as objectionable. Severity:
  - Red: more than 0
  - Gray: 0

**Related concepts**

**Alerts** (page 4)
The Alerts page lists all the alerts that require your action.

**Firewall reports** (page 580)
The firewall reports page shows various reports about the security threats and hardware for the Sophos XG Firewall that you select on the Firewall Management – Firewalls page.

**Related tasks**

**Turn on firewall reporting** (page 578)
You can view the report dashboard and the reports page for a Sophos XG Firewall if you register it with Sophos Central and turn on firewall reporting.

**10.2.4 Firewall reports**

The firewall reports page shows various reports about the security threats and hardware for the Sophos XG Firewall that you select on the Firewall Management – Firewalls page.

To view the reports page:

1. Go to Firewall management > Firewalls.
2. Select the ellipsis button (...) on the right of the firewall for which you want to view the reports.
3. Select View device reports.
4. Go to Reports.

The Firewall reporting - Bandwidth usage page is shown.

The page includes the following tabs:
• **Report Generator**: This enables you to select a report template, specify filters, and generate a report.

• **Queue**: This lists reports that you have generated with a time frame longer than 30 days that couldn’t be generated immediately.

### Related concepts

**Firewall report dashboard** (page 578)
The firewall report dashboard shows key information about the hardware, security threats and the performance against policy for the Sophos XG Firewall that you select on the **Firewall Management – Firewalls** page.

### Related tasks

**Turn on firewall reporting** (page 578)
You can view the report dashboard and the reports page for a Sophos XG Firewall if you register it with Sophos Central and turn on firewall reporting.

### Firewall reporting – Report Generator

The firewall reporting **Report Generator** tab enables you to select a report template, specify filters, and generate a report.

The tab includes the following areas:

- Filters
- Chart
- Table

### Filters

The filters area enables you to select which report to generate and to filter that report on time period and other variables.

Under **Report templates**, you can select one of the following report templates:

- **Bandwidth usage** Amount of internet usage of specific applications
- **VPN usage** Amount of usage of specific VPN connections
- **Web usage** Visits to specific websites, including whether connections have been allowed or blocked
- **Firewall** Numbers of connections between specific IP addresses
- **ATP** Threats coming from specific IP addresses that have been detected by Advanced Threat Protection
- **IPS** Attempted attacks, including source and destination
- **Sandstorm events** Files and emails that contain suspicious attachments that have been sent to Sandstorm
- **Log viewer & search** Log entries that have been generated by the firewall in non-aggregated form
- **Antivirus** Malware or suspicious items that have been blocked
- **Threat geo activity** Threats of certain types, by source or destination country, that have been blocked
- **Threats & events blocked** All types of threat and event, by source or destination country, that have been blocked
The **Log viewer & search** report does not include a chart, only a table.

Under **Time frame**, you can specify the time period for which information is shown by selecting one of the options. If you select **Custom**, you can use the date selection boxes to select the dates and times between which information is shown.

**Restriction**

If you do not have a firewall reporting license, you cannot specify a time period that starts more than seven days ago.

Under **Filter Query**, you can enter values on which to filter the report:

1. In the text box, select or type the name of the column on which you want to filter.
   
   A further text box is shown in which you enter the value(s) on which you want to filter.

2. To change the operator that is used for comparison, click the equals sign next to the column name to show a drop-down list:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Rows shown</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Rows in which the column value matches the value on which you want to filter</td>
</tr>
<tr>
<td></td>
<td>The value is case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>To show all rows in which the domain matches a specific domain, enter the following:</td>
</tr>
<tr>
<td></td>
<td><strong>DOMAIN = <a href="http://www.bing.com">www.bing.com</a></strong></td>
</tr>
<tr>
<td></td>
<td>To show all rows in which the IP address matches a specific address, enter the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Source IP = 10.8.9.191</strong></td>
</tr>
<tr>
<td>!=</td>
<td>Rows in which the column value does not match the value on which you want to filter</td>
</tr>
<tr>
<td></td>
<td>The value is case-sensitive.</td>
</tr>
<tr>
<td>&lt;</td>
<td>Rows in which the column value is less than the value on which you want to filter (applies only to numeric values)</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Rows in which the column value is less than or equal to the value on which you want to filter (applies only to numeric values)</td>
</tr>
<tr>
<td>&gt;</td>
<td>Rows in which the column value is greater than the value on which you want to filter (applies only to numeric values)</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Rows in which the column value is greater than or equal to the value on which you want to filter (applies only to numeric values)</td>
</tr>
<tr>
<td>Operator</td>
<td>Rows shown</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>IN</strong></td>
<td>Rows in which the column value matches any value in a comma-separated list of values on which you want to filter. The values are case-sensitive. <strong>Example:</strong> To show all rows in which the destination IP address matches any value in a list of IP addresses, enter the following: <strong>Destination IP IN</strong> 13.107.21.200,204.79.197.200</td>
</tr>
<tr>
<td><strong>~</strong></td>
<td>Rows in which the column value matches a wildcard expression on which you want to filter – the wildcard is an asterisk: * The expression is not case-sensitive. <strong>Examples:</strong> To show all rows in which the URL contains a specific string, enter the following: <strong>URL ~ <em>amazon</em></strong> To show all rows in which the source IP address matches any address in a subnet, enter the following: <strong>Source IP ~ 13.225.78.</strong>*</td>
</tr>
<tr>
<td><strong>!~</strong></td>
<td>Rows in which the column value does not match a wildcard expression on which you want to filter – the wildcard is an asterisk: * The expression is not case-sensitive.</td>
</tr>
</tbody>
</table>

3. Repeat this process if you want to add more filters. A row is shown only if it meets the conditions of all the filters.

4. To remove a filter, click the delete button next to the filter: \(\times\)

Click **Generate** to show the selected report using the filters that you have specified.

If the time frame that you have selected is longer than 30 days, it may take some time to retrieve the data. If it takes more than a few seconds, you see a message:

- To continue waiting to see the report, click **OK**. The report is added to the queue. When it is ready, it is shown on the **Report Generator** tab automatically.

  If you later decide to stop waiting, you can click **Start Another Report**. This allows you to view another report while you’re waiting. However, when the first report is ready, you must go to the **Queue** tab to view it.

- To stop generating the report, click **Cancel**.
Chart

In the chart area, you can select one of the following chart types by clicking one of the buttons in the top right of the area:

- Bar
- Horizontal bar
- Pie
- Line
- Stack-area

To select which information is shown on each axis:

1. Click the screwdriver and spanner button in the top right of the area:

2. In the top box, click the arrow and select which information is shown on the x axis.
3. In the next box, click the arrow and select which information is shown on the y axis.
4. If a line or stack-area chart is shown, in the bottom box, click the arrow and select which information is shown on the z axis.

When you select a different chart type, it shows default information on each axis, even if you previously changed it.

If you hover the mouse pointer over the chart, the data values are shown next to the pointer.

Table

In the table area, when the table is first shown, it uses a default set of columns. You can select which columns to show by clicking the column selection button in the top right of the area:

The rows are aggregated to remove duplicate rows. For example, by default the Firewall report table shows the number of hits for a specific rule ID, source IP, destination IP, and country. This is represented by one row:

<table>
<thead>
<tr>
<th>FIREWALL RULE ID</th>
<th>SOURCE IP</th>
<th>DESTINATION IP</th>
<th>SOURCE COUNTRY</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1.1.1.1</td>
<td>255.255.255.255</td>
<td>Australia</td>
<td>3</td>
</tr>
</tbody>
</table>

However, if you add another column in which the data is different in each row, for example the user, one row is shown for each hit, with each row having the same rule ID, source IP, destination IP, and country:

<table>
<thead>
<tr>
<th>FIREWALL RULE ID</th>
<th>USER</th>
<th>SOURCE IP</th>
<th>DESTINATION IP</th>
<th>SOURCE COUNTRY</th>
<th>HITS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>John Smith</td>
<td>1.1.1.1</td>
<td>255.255.255.255Australia</td>
<td>Australia</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>Paul Jones</td>
<td>1.1.1.1</td>
<td>255.255.255.255Australia</td>
<td>Australia</td>
<td>1</td>
</tr>
<tr>
<td>FIREWALL RULE ID</td>
<td>USER</td>
<td>SOURCE IP</td>
<td>DESTINATION IP</td>
<td>SOURCE COUNTRY</td>
<td>HITS</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>--------------</td>
<td>----------------</td>
<td>---------------------</td>
<td>------</td>
</tr>
<tr>
<td>0</td>
<td>George Harris</td>
<td>1.1.1.1</td>
<td>255.255.255.255</td>
<td>Australia</td>
<td>1</td>
</tr>
</tbody>
</table>

In summary, the more columns that you add, the more granular the information that is shown.

If the date column is shown, duplicate rows are grouped on the date and time as follows:

<table>
<thead>
<tr>
<th>Time frame</th>
<th>Row grouping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than or equal to 1 hour</td>
<td>Rows in which the date and time are the same to the nearest minute</td>
</tr>
<tr>
<td>Greater than 1 hour but less than or equal to 48 hours</td>
<td>Rows in which the date and time are the same to the nearest hour</td>
</tr>
<tr>
<td>Greater than 48 hours</td>
<td>Rows in which the date and time are the same to the nearest day</td>
</tr>
</tbody>
</table>

Some columns include values that are hyperlinks. If you click one of these, a filter on that value is added to the Filter Query box in the filters area, which you can use to filter the report. For example, in the table above, if you click “Australia”, a filter is added: “Source Country = Australia”. You can repeat this for other values to make the filter more specific. For the Threats & events blocked report, such hyperlinks also link to one of the other reports.

For the Log viewer & search report, the buttons in the top right of the area enable you to switch between tabular view, which shows a limited number of columns, and raw view, which shows all columns.

**Threat geoactivity**

The Threat geoactivity report shows threats of certain types, listed by source or destination country, that have been blocked by a specific firewall.

The types of threat include those detected by the following firewall modules:

- ATP
- Antivirus
- IPS
- Sandstorm

The numbers relate to threats that have been blocked and have caused a warning alert.

**Filters**

Select the time period for which you want to view details. Threats from the last 24 hours are shown by default.

**Chart**

In the chart area, you can select one of the following chart types:

- World map that highlights the top 10 countries, by number of threats
• Globe that highlights the top 10 countries, by number of threats

If you hover the mouse pointer over one of the circles on the chart, the data values are shown next to the pointer.

If you change which threat type is shown on the y axis of the chart, the sizes of the circles vary depending on the number of threats of that type in that country. For example, if you select Antivirus, circles that represent a higher number of antivirus threats are bigger.

You can move the map or the globe in any direction by dragging it with the mouse.

Table

In the Source Country column, the Reserved country includes source or destination IPs that are private. Such IPs do not enable the actual source or destination country to be identified.

Threats & events blocked

The Threats & events blocked report shows all types of threat and event, listed by source or destination country, that have been blocked by a specific firewall.

The types of threat include those detected by the following firewall modules:

• ATP
• Antivirus
• IPS
• Sandstorm
• Firewall
• Web
• Web Application Firewall

The numbers relate to threats that have been blocked and have caused a warning alert.

Filters

Select the time period for which you want to view details. Threats and events from the last 24 hours are shown by default.

Chart

In the chart area, you can select one of the following chart types:

• Horizontal bar chart of the threats that have been blocked
• World map that highlights the top 10 countries, by number of threats
• Globe that highlights the top 10 countries, by number of threats

World map and globe

If you hover the mouse pointer over one of the circles on the chart, the data values are shown next to the pointer.

If you change which threat type is shown on the y axis of the chart, it changes the threat type that each circle represents. The size of each circle represents the number of threats of that type. For example, if you select the threat type Antivirus, each circle represents the number of antivirus
threats in a specific country, and circles that represent a higher number of antivirus threats are bigger.

You can move the map or the globe in any direction by dragging it with the mouse.

**Table**

In the **Source Country** column, the **Reserved** country includes source or destination IPs that are private. Such IPs do not enable the actual source or destination country to be identified.

This report summarizes information from several of the other firewall reports. If you click one of the values in one of the following table columns, the corresponding report is shown:

- Antivirus
- ATP
- Firewall
- IPS
- Sandstorm events
- Web

**Firewall reporting – Queue**

The firewall reporting **Queue** tab lists reports with a time frame longer than 30 days that couldn’t be generated immediately.

Each report in the list has a name that includes the report template and the time at which you generated it.

Some of the reports may be ready to view now. Others may not be ready yet.

To view a report, click its name. The report is shown on the **Report Generator** tab. You cannot make any changes to it.

Each report is deleted automatically 24 hours after you generated it. To delete a report sooner, click the trash can icon in the same row.

**10.2.5 Firewall reporting – licensing**

**Firewall reporting – licensing** shows how your firewall reporting licenses are allocated to each firewall.

**Restriction**
These options may not be available for all users.

To view **Firewall reporting – licensing**:

1. Click your account name (upper right of the user interface) and select **Licensing**.
2. In the **License Details** table, for firewall reporting licenses, click **Manage**.

Each license represents a specific amount of storage capacity in Sophos Central. This storage is used to store the data for generating reports. When the capacity has been reached, the oldest data is no longer stored. Data is deleted on a first-in, first-out basis. The amount of time for which data is available depends on the incoming volume of data and licensed capacity. A license also gives you access to advanced firewall reporting features.
Summary

The summary above the table shows the following:

- **Licenses used / available.** The number of firewall reporting licenses you are using as a proportion of the number you have. Each license allows you a specific amount of storage capacity. You can have one or more per firewall.

- **Firewall reporting expiration date.** The date on which the firewall reporting licenses expire.

Firewall table

The firewall table shows each firewall with the number of licenses allocated to it and its usage. The columns include the following:

- **Central Storage Used.** The amount of storage used as a proportion of the amount made available by the licenses.

- **Allocate Licenses.** The number of licenses that are allocated to the firewall. You can click the plus and minus buttons to adjust the number and, therefore, the total storage. The number of licenses that you can allocate depends on the firewall model. For example, you can allocate more licenses to a more advanced firewall. Click **Save** to save any changes that you make to the allocation of licenses for one or more firewalls. Similarly, click **Cancel** to cancel all changes that you have made to license allocation.

- **Projected.** An estimate of how long your total storage will last. When you click the plus button to increase the number of licenses, an estimate of the additional time it will take to use up the total storage is shown in green. When you click the minus button to decrease the number of licenses, an estimate of how much less time is shown in red.

- **Oldest Avail. Data.** The date of the oldest data record for the firewall.

- **Tier.** Firewall reporting licensing is divided into two tiers:
  - **Central Firewall Reporting,** which is shown in the table as a dash. Reporting on your firewall is free. However, if you do not buy any reporting licenses for a firewall, you have only a small amount of storage, which varies according to the firewall model. You can store data for up to seven days. After this, the oldest data is no longer stored. Data is deleted on a first-in, first-out basis.
  - **Advanced.** If you do buy reporting licenses, you have more storage, which varies according to the firewall model. In addition, you can store data for up 365 days before it is deleted.

- **Actions.** Click the ellipsis button (…) to manage your storage and licenses. You can perform the following actions:
  - **Transfer reporting license.** If you have a firewall that has licenses allocated to it and you want to deactivate it, select this and choose which firewall you want to transfer the licenses to. The licenses are transferred and the two firewalls are shown in the table as a single cluster. To view each firewall and its data usage, click the arrow to the left of the cluster to expand it. You cannot transfer licenses from a cluster, only from an individual firewall.
  - **Reclaim reporting license.** If you have a firewall that has licenses allocated to it and you want to use these licenses for another firewall, select this. The licenses are returned to the central license pool and the firewall’s **Tier** status changes to a dash. If the firewall is in a cluster, you cannot select this option from the firewall itself. You can only select the option from the cluster.
  - **Delete log data.** If you have a firewall that you want to deactivate, select this to delete all the data that is stored for that firewall. If the firewall is in a cluster, you cannot select this option.
from the firewall itself. You can only select the option from the cluster and this deletes all the data that is stored for all firewalls in the cluster.

- **HA Status.** In the nested table that is displayed when you expand a firewall cluster, the **HA Status** column shows whether the cluster is a high-availability cluster.

As well as individual firewalls, the table may also show clusters of firewalls. These are indicated by an arrow to the left of them in the table. Click this to expand the cluster. There are two types of cluster:

- A high-availability cluster includes two firewalls that are configured to provide continuous protection. If one firewall has a problem, the other can take over.
- A cluster that includes one or more deactivated firewalls and an active firewall. If you want to deactivate a firewall, perhaps because it is faulty, you can transfer its licenses to a working firewall. The licenses are transferred and the two firewalls are shown in the table as a single cluster.

In each case, the licenses that you allocate to the cluster are shared between the firewalls in the cluster, and the data usage of each firewall is aggregated to a single figure for the cluster.

**Firewall reporting storage by firewall model**

The amount of storage that you can allocate depends on the firewall model.

Firewall reporting licensing is divided into two tiers:

- **Central Firewall Reporting.** Reporting on your firewall is free. However, if you do not buy any reporting licenses for a firewall, you have only a small amount of storage, which varies according to the firewall model. You can store data for up to seven days. After this, the oldest data is no longer stored. Data is deleted on a first-in, first-out basis.

- **Advanced.** If you do buy reporting licenses, you have more storage, which varies according to the firewall model. In addition, you can store data for up 365 days before it is deleted.

For each tier, the storage and storage period are shown in the tables below. In all cases, storage is limited by the max storage or max storage period, whichever is reached first.

**Table 4: Central Firewall Reporting tier storage**

<table>
<thead>
<tr>
<th>XG Firewall</th>
<th>XG Firewall virtual appliance</th>
<th>XG Firewall AWS cloud appliance</th>
<th>XG Firewall Azure cloud appliance</th>
<th>Max storage (GB)</th>
<th>Max storage period (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG/XG 86</td>
<td>SFV2C4</td>
<td>Medium</td>
<td>D2</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>SG/XG 86w</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG/XG 106</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG/XG 106w</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG/XG 115</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG/XG 115w</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG 115w-VCR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG/XG 125</td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>SG/XG 125w</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XG 125a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XG Firewall virtual appliance</td>
<td>Max storage (GB)</td>
<td>Max storage period (days)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------</td>
<td>--------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 135</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 135w</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 210</strong></td>
<td>13</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 230</strong></td>
<td>18</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 310</strong></td>
<td>26</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 330</strong></td>
<td>34</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 430</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 450</strong></td>
<td>90</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 550</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 650</strong></td>
<td>154</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 750</strong></td>
<td>SFVUNL</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SFV01V</strong></td>
<td>289</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Advanced tier storage

<table>
<thead>
<tr>
<th>XG Firewall virtual appliance</th>
<th>Min storage (GB)</th>
<th>Max storage (GB)</th>
<th>Unit of storage (GB)</th>
<th>Max storage period (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SG/XG 86</strong></td>
<td>D2</td>
<td>100</td>
<td>100</td>
<td>365</td>
</tr>
<tr>
<td><strong>SG/XG 86w</strong></td>
<td>Medium</td>
<td>Large</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 106</strong></td>
<td>SFV2C4</td>
<td>Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 106w</strong></td>
<td>SFV1C4</td>
<td>Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 115</strong></td>
<td>SFV1C4</td>
<td>Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SG/XG 115w- VCR</strong></td>
<td>SFV1C4</td>
<td>Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XG Firewall</td>
<td>XG Firewall virtual appliance</td>
<td>XG Firewall AWS cloud appliance</td>
<td>XG Firewall Azure cloud appliance</td>
<td>Min storage (GB)</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SG/XG 125</td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 125w</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XG 125a</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG/XG 135</td>
<td>SFV4C6</td>
<td>XLarge</td>
<td>A3</td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 135w</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG/XG 210</td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 230</td>
<td>SFV6C8</td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 310</td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 330</td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 430</td>
<td>SFV8C16</td>
<td>2XLarge</td>
<td>F8</td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 450</td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>SG/XG 550</td>
<td>SFV16C24</td>
<td>4XLarge</td>
<td>F16</td>
<td>200</td>
</tr>
<tr>
<td>SG/XG 650</td>
<td></td>
<td></td>
<td></td>
<td>200</td>
</tr>
<tr>
<td>SG/XG 750</td>
<td>SFVUNL SF01V</td>
<td>8XLarge</td>
<td></td>
<td>300</td>
</tr>
</tbody>
</table>

"Unit of storage" is the amount of storage that one license represents.
10.3 Tasks queue

The firewall management tasks queue enables you to see the status of the application of firewall group policies to the firewalls within a group.

Go to Firewall management > Tasks Queue.

A new task is created automatically when an admin updates a group policy. The information displayed for each task includes the following:

- **Task**: The task’s number.
- **Firewalls**: The number of firewalls to which the policy is applied.
- **Status**: The overall status of task completion, including the number of firewalls to which the policy has been applied successfully.
- **Entity** and **Sub-entity**: The part of the policy that was edited.
- **Time**: Initially, this shows the time at which the policy was created or updated (not necessarily the time when the policy started to be applied to the firewalls). Then, the time is updated as the policy is applied to all the firewalls. Eventually, it shows the time when the policy was applied to the last firewall.

To expand a task to reveal the firewalls to which the policy will be applied, click the down arrow on the right of the table.

To display completed or skipped tasks for firewalls or groups that have been deleted, select Show History.

10.4 Dynamic objects

Dynamic objects enable you to group zones or interfaces from different firewalls in a group into one logical zone or interface, so you can set up rules for that logical entity in a group policy.

Some configuration, such as that related to zones and interfaces, is very firewall-specific. As a Sophos Central admin, you don’t know which zones or interfaces exist on each firewall. So, any rule you create in a group policy may not work on all the firewalls in a group.

To solve this problem, you can create a dynamic zone or a dynamic interface. These enable you to specify, for each firewall, which zone or interface to use. Then you can use the dynamic zone or dynamic interface when you create a rule, knowing that the rule will work as desired on each firewall.

Dynamic zones

To create a dynamic zone, do as follows:

1. Go to Firewall management > Dynamic Objects.
2. Click Zones.
3. Click Add Dynamic Zone.
4. Enter the dynamic zone details.
   - **Zone Type**:
     - **LAN**: This is the default, which is used most often when creating dynamic objects. Depending on the device in use and network design, you can group from one to six physical...
ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.

**Note**
By default, the traffic to and from this zone is blocked, so it is the most secure zone. However, traffic between ports belonging to the same zone and traffic between LAN and Local zone services, for example Administration, Authentication and Network, will be allowed.

— DMZ: This zone is normally used for publicly accessible servers. Depending on the device in use and network design, you can group from one to five physical ports in this zone.

The choice of Zone Type determines which options are listed in the Zones available box (see below).

5. Enter the device zone mappings for all firewalls.

   - **Firewalls**: The firewall whose zone is to be mapped to the dynamic zone. The mapping for Default (Any firewall) is applied to any firewall you do not specify a mapping for, for example a firewall added later. However, the mapping must be a zone that exists on each firewall.

   - **Zones available**: The firewall zone to be mapped.

6. Click **Save**.

The dynamic zone is added to the dynamic objects table and can now be used in all other configurations where a zone can be configured, for example in Rules and policies. To see where a dynamic zone is used, click Usage References to show the group, policy, and part of the policy that use the dynamic zone.

To edit or delete a dynamic zone, click its name in the dynamic objects table.

**Dynamic interfaces**

To create a dynamic interface, do as follows:

1. Go to Firewall management > Dynamic Objects.
2. Click **Interfaces**.
3. Click **Add Dynamic Interface**.
4. Enter the dynamic interface details.

   - **IP Address Family**: The address family that corresponds to that used by the interfaces on the firewalls. The choice of IP Address Family determines which options are listed in the Interfaces available box (see below).

   - **Interface Type**: The choice of Interface Type determines which options are listed in the Interfaces available box (see below).

5. Enter the device interface mappings for all firewalls.

   - **Firewalls**: The firewall whose interface is to be mapped to the dynamic interface. The mapping for Default (Any firewall) is applied to any firewall you do not specify a mapping for, for example a firewall added later. However, the mapping must be an interface that exists on each firewall.

   - **Interfaces available**: The firewall interface to be mapped.

6. Click **Save**.
The dynamic interface is added to the dynamic objects table and can now be used in all other configurations where an interface can be configured, for example in Rules and policies. To see where a dynamic interface is used, click Usage References to show the group, policy, and part of the policy that use the dynamic interface.

To edit or delete a dynamic interface, click its name in the dynamic objects table.

10.5 Backup

You can back up and restore Sophos XG Firewall configurations from Sophos Central. We recommend that you set up scheduled backups and also do a backup before and after significant changes or before a firmware upgrade.

Schedule firewall backups

Schedule backups as follows. Make sure you set up a schedule that won’t overload your system.

1. Go to Firewall Management > Backup.
2. In Schedule Backup, select the Backup Frequency. The default is weekly.
3. Set the day of the week (or the date if you selected monthly backups) when the backup will happen.

   Note
   Backups happen at 0800 local time (the time zone of the region the account is in). You can’t change this.

4. In the Devices list, click Add New Item and add the firewall you want to back up.
5. Click Save.

Sophos Central keeps your five most recent backups but discards any earlier backups. If you want to keep a backup permanently (or until you delete it), see Store a backup permanently.

Back up a firewall now

To back up a firewall now:

1. Go to Firewall Management > Backup.
2. In Manage Backup, select the device you want to back up.
   If you don’t have any firewalls shown here, go to Schedule Backup and click Add New Item.
3. Click Generate Backup.

Store a backup permanently

To store a backup permanently:

1. Go to Firewall Management > Backup.
2. In Manage Backup, select the device for which you want to store a backup.
You can see a list of previous backups.

3. In the list, select a backup. Click the pin icon to make the backup the “stored backup”.
   
   You can only have one stored backup. If there is already a stored backup, it will be replaced.

   The backup will be kept until you replace it or delete it.

**Restore from a backup**

You can download a backup and use it to restore an earlier configuration.

1. Go to **Firewall Management > Backup**.
2. In **Manage Backup**, select the device where you want to restore the firewall configuration.
   
   You can see a list of previous backups.
3. In the list, select a backup. Click the download icon.
4. You’re prompted to set a password that will be used to re-encrypt the backup. Click **Download**.
5. Go to the firewall and use the download to restore the configuration. For details, see Sophos XG Firewall help (search for “Backup restore”).
11 Phish Threat

Sophos Phish Threat allows you to simulate phishing attacks and assess how your users respond to them. It also allows you to distribute anti-phishing training to your users.

To use Phish Threat:

1. Create a simulated phishing attack campaign or series.
2. Review your campaigns and their results.

Related concepts
Campaigns (page 610)
Here you can see your campaigns and start a new campaign or series.

Campaign overview (page 615)
This shows the details of a campaign and the activity associated with it.

11.1 Dashboard

The Phish Threat Dashboard is the start page of Sophos Phish Threat and lets you see the most important information at a glance. It consists of these areas.

Active Campaigns shows your campaigns that are currently running or upcoming. If you have more than two active campaigns, the two nearest to their completion date show on the Dashboard. You can view all of your campaigns from the Campaigns page.

Caught-to-open ratio shows the number of people in your organization who have been deceived by a simulated attack as a percentage of the number of people who have opened the phishing emails.

Report-to-open ratio shows the number of people in your organization who have reported the phishing emails as a percentage of the number of people who have opened them.

Caught users is a list of people in your organization who have been deceived by a simulated attack. The users who have been caught most frequently appear at the top of the list.

Threat reporters is a list of people in your organization who have reported phishing emails.

Awareness factors shows a breakdown of four critical metrics for understanding the effectiveness of a phishing awareness program.

• Users tested shows you what percentage of your user base has been subjected to a phishing simulation. You should aim to test everyone at least once a quarter.

• Last campaign helps you to see whether you are testing your users frequently enough.

• Users caught gives you an aggregate view of your users’ fail rate in attack simulations.

• Passed training shows the overall completion rate of users enrolled in awareness training.

Related concepts
Campaigns (page 610)
Here you can see your campaigns and start a new campaign or series.

11.2 Reports

The Reports pages provide detailed reports on Sophos Phish Threat features. The reports that you can see depend on your license. You can customize reports, save them and send them out as scheduled emails.

Note
A report may not support all the customization or viewing options.

Limit report data to a specific time range

In some reports, you can limit report data to a specific date range by entering a From and To date. In some reports, you can select a time period.

Filter reports

In some reports, you can filter the displayed information by clicking on the category tiles. For example in the Computers report you can show all the active computers by clicking on Active. You may also be able to filter by groups. You can also use Search to filter for specific information.

Print or export reports

You can print or export your reports.

- **Print**: Click this to open a printer-friendly view. Then press Ctrl+P to open the printer dialog.
- **Export to CSV**: Click this to export the current view as a comma separated file.
- **Export to PDF**: Click this to export the current view as a PDF file.

Save and email custom reports

You can create and save custom reports. A list of the saved reports is shown at the top of the Logs & Reports page. You can also choose to send custom reports by email and set up a schedule for them. You can save as many reports as you like, but you can only schedule up to 25.

1. Set up the report by selecting the appropriate filters.
2. Click **Save as Custom Report**.
   This opens the Save Report dialog.
3. Enter a Name for the report.
4. If you want to send the report by email, select one of these options:
• **Send a link to the report.**
• **Attach the report to the email.**

  We recommend that you send a link if the report includes personally identifiable information.

  You need to enter Sophos Central sign-in credentials to view reports from a link.

5. Select the **Frequency**. You can choose from monthly or weekly.
6. Select the format: **PDF** or **CSV**.
7. Click **Save**.

The email is received by the user who signs in and creates the report.

**Note**

Scheduled emails stop after six months. You can reschedule them if you want to.

### 11.2.1 User behavior

The **User Behavior** report shows a user’s involvement in phishing campaigns.

This includes the number of campaigns the user was enrolled in, the number of times they fell for the simulated attack in those campaigns, and related dates.

You can view a list of all users enrolled in phishing campaigns in the specified time period or a list filtered according to how users responded to campaigns, for example users who were caught by simulations.

**Creating campaigns from a report**

You can create a new campaign with all the users from your report pre-enrolled.

Click **Create campaign with these users** to start a new campaign.

### 11.2.2 User Training

The **User Training Report** report shows a user’s training enrollment and compliance status.

This includes the number of training courses the user was enrolled in, the number of those courses the user completed, and the date of their last training enrollment.

You can view a list of all users enrolled in training in the specified time period or a list of users who failed to complete training.

**Creating campaigns from a report**

You can create a new campaign with all the users from your report pre-enrolled.

Click **Create campaign with these users** to start a new campaign.
11.3 People

On the People page, you can manage your users and user groups.

11.3.1 Users

On the Users tab of the People page, you can add or manage users, and get the users’ computers protected.

You can also enable the users to protect their own devices by emailing them a setup link.

The current users are listed with their details.

**Health Status.** An icon shows whether the user has security alerts on any of their devices.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>😶</td>
<td>Amber warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Red warning sign if there are critical alerts.</td>
</tr>
</tbody>
</table>

**Name** Click the user’s name to see details of devices and to see which has an alert.

**Email.**

**Exchange Login.**

**Last Active.** The last time a user reported to Sophos Central.

**Group Name.** This is shown if the user has been added to a user group.

**Role.** This shows what administration role, if any, the user has. This column is only visible if you are an administrator.

Click any column header to sort the users. By default, users are sorted according to the Last Active time.

To see full details for a user, click the user’s name.

You can add users manually or automatically by protecting their devices. You can also import users in bulk from a CSV file or from Active Directory. You can also protect existing users.

To modify users, click the user's name to open and edit their user details.

You can also delete users and export lists of users.

**Related concepts**

User Summary (page 600)

**Related tasks**

Add a user manually (page 605)
You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

**Add users automatically** (page 606)
You can add users automatically by protecting their devices.

**Import users from a CSV file** (page 606)
You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

**Import users from Active Directory** (page 607)
You can import users and groups from Active Directory.

**Protect existing users** (page 607)
You can protect users that you have already added to Sophos Central.

**Delete users** (page 607)
You can delete users from Sophos Central if you are a Super Admin.

**Export to CSV** (page 608)
You can export lists of users as CSV files.

### User Summary

The **Summary** tab in a user's details page shows a summary of the following:

- The user's security status, administration role, if any, and account details.
- Recent events on the user's devices.
- Mailboxes associated with the user.
- Devices associated with the user.
- Policies that apply to the user.
- Groups that the user belongs to.
- Logins.

You can find details of each below.

The security status and account details are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.

You can click on the other tabs for more on **Devices**, **Events**, and **Policies**.

### Health Status

In the left-hand pane, an icon shows you whether the user has security alerts on any of their devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️</td>
<td>Green check mark if there are low-priority alerts or no alerts.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Orange warning sign if there are medium-priority alerts.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Red warning sign if there are high-priority alerts.</td>
</tr>
</tbody>
</table>
You can see which devices have alerts in the **Devices** tab.

A padlock icon shows that the user has been imported from Active Directory.

A badge shows the user's assigned administration role. Click on the role name to view the settings for the role.

**Note**
Role information is only displayed for administration roles.

### Account details

In the left-hand pane, you can modify or delete the user's account.

**Note**
If a user has been imported from Active Directory, you cannot change the account details. However, you can add the user to a new Sophos Central group or add another login.

#### Modify the account

1. Click **Edit** and enter the following settings:

    **First & Last name**: Enter the name of the user. Do not include a domain name.

    **Role**: Select a role for the user. Choose from: Super Admin, Admin, Help Desk, Read-only, or User.

    **Restriction**
    You can only see the **Role** option and assign administrator roles if you are a Super Admin.

    **Note**
    You cannot amend your own administration role.

    **Note**
    Anyone with a **User** role only has access to the Self Service Portal.

    **Email Address**: Enter the email address of the user.

    **Exchange Login** (optional): Enter the Exchange account name of the user.

    **Note**
    In Sophos Mobile policies, you can use the placeholder `%USERNAME%` to refer to this setting.

    **Add to groups**: Select one of the available user groups and use the picker arrows to move it to the assigned groups.

    **Email Setup Link**: Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes more than one type of protection, select those the user needs.
Note
The user needs administrative privileges and internet access in order to protect their computer.

Note
Web Gateway provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.

2. Click **Save**.

Delete the account
To delete the account, click **Delete User** in the left-hand pane. Logins assigned to this user can afterward be assigned to another user.

**Restriction**
You cannot delete users who have an assigned administration role.

Multi-factor authentication
If the user is an admin, the left-hand pane shows whether multi-factor authentication (MFA) is enabled for them. If it is enabled, the admin must use another form of authentication, as well as their user name and password, to sign in.

If you're a Super Admin, you can edit the settings as follows:
Click **Reset** to let the admin set up their MFA sign-in details again.
Click **MFA Settings** to go to a page where you can enable or disable multi-factor authentication for the admin.

Recent Events
This lists recent events on the user's devices.
For a full list, click the **Events** tab.

Mailboxes
This lists all email addresses, including distribution lists and public folders, associated with the user. Primary indicates the user's primary email address. Owner indicates the user controls a distribution list or public folder.
For full details, click an email address.

Devices
This shows a summary of the devices associated with the user.
Click the device name to go to the device's details page for more information.
Click **Actions** to carry out any of the same actions that are available on the device's details page (for example, Scan Now and Update Now for a computer).

For full details of the user's devices, click the **Devices** tab.

### Policies

This shows a summary of the policies applied to the user.

The list shows the policy name, whether the policy is enabled or not, and icons that indicate the features included in the policy.

Click on a policy name to view and edit the user policy.

**Note**

Editing the policy affects all users to which this policy is applied.

For full details of all the policies applied to this user, click the **Policies** tab.

### Groups

This shows the groups the user belongs to.

Click on a group name to see details of the group.

Click **Edit** (on the right) to change the groups the user belongs to.

### Logins

This shows the user's logins.

Click **Edit** (on the right) to change the logins assigned to the user.

### User Devices

The **Devices** tab in a user's details page lets you see the devices associated with the user.

This tab also shows any servers where the user has logged on with Remote Desktop Services.

For each associated device you can see the device type and the operating system. You also have these options:

- **View Details**: This opens the full device details page.
- **Delete**: This removes the device from the list and stops Sophos Central managing it, but it does not uninstall the Sophos software.
- **Actions**: Actions you can take. These depend on the device type.

**Related information**

*How to investigate and resolve a potential False Positive or Incorrect Detection*
User Events

The **Events** tab in a user’s details page lets you see a list of events detected on the user’s devices. You can see details and, in some cases, take action to prevent unwanted detections.

The list includes:

- **Severity**: Hover over an icon to see what it means.
- **Type**: An icon shows which Sophos agent reported the event. Hover over it to see what it means.
- **Details**: This link (for certain events) lets you get further details and take action.

**View Events Report** shows events arranged by type and a graph of events day by day.

Stop detecting an application

If an application is reported as malware but you know it’s safe, you can allow it from the events list. For help with deciding whether an application is safe, see How to investigate and resolve a potential False Positive or Incorrect Detection.

Click the **Details** link beside the event and then allow the application.

**Note**

This currently applies only to malware events reported by Intercept X.

Stop detecting an exploit

If an exploit is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In **Event details**, look for **Don’t detect this again** and select an option:
   - **Exclude this Detection ID from checking**: prevents this detection on this app.
   - **Exclude this application from checking**: prevents any checks for exploits on this app.

   Try excluding the Detection ID first as that is more accurately targeted. If the same detection happens again, exclude the application next time.

3. Click **Exclude**.

We’ll add your exclusion to a list.

Detection ID exclusions go into the Global Exclusions. Application exclusions go into the Exploit Mitigation Exclusions.

Stop detecting ransomware

If ransomware is detected but you’re sure the detection is incorrect, you can stop it happening again. This will apply to all your users and computers.

1. On the **Events** tab, find the detection event and click **Details**.
2. In Event details, look for Don’t detect this again. Select Exclude this Detection ID from checking. This prevents this detection on this app.

3. Click Exclude. We’ll add your exclusion to the Global Exclusions list.

Related information
How to investigate and resolve a potential False Positive or Incorrect Detection

User Policies

The Policies tab in a user’s details page lets you see the policies that are enabled and applied to the user. Click a policy name to view and edit policy details. Editing the policy affects all users to which this policy is applied.

Add a user manually

You can add an individual user and protect them. This also gives you the option to let users protect their own devices.

To add a user:
1. Go to Users.
2. Click Add and select Add User.
3. In the Add User dialog, enter the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First and Last Name</td>
<td>Enter the name of the user. Do not include a domain name.</td>
</tr>
<tr>
<td>Role</td>
<td>Select an administration role for the user. A user who is assigned an administration role will receive an email telling them how to set up their administration account. Anyone with a User role only has access to the Self Service Portal.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter the email address of the user.</td>
</tr>
<tr>
<td>Add to groups (optional)</td>
<td>Select one of the available user groups and use the picker arrows to move it to the assigned groups. You can start typing a name in the search box to filter the displayed groups.</td>
</tr>
<tr>
<td>Email Setup Link</td>
<td>Select this if you want to send the user an email with links that enable them to protect their own devices. If your license includes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>more than one type of protection, select those the user needs.</td>
</tr>
<tr>
<td></td>
<td>The user needs administrative privileges and internet access in order to protect their computer.</td>
</tr>
<tr>
<td>Web Gateway</td>
<td>This provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.</td>
</tr>
</tbody>
</table>

4. Click **Save** or **Save and Add Another**. The new user is added to the user list.

When the user downloads and installs the software, their device is automatically associated with the user.

**Add users automatically**

You can add users automatically by protecting their devices.

To add users:
1. Download an installer from **Protect Devices**.
2. Run the installer on the devices.

This adds the user of each device automatically.

**Import users from a CSV file**

You can import a list of users using a CSV file. This allows you to add users in bulk without using Active Directory Synchronization.

To import users:
1. Go to **Users**.
2. Click **Add** and click **Import users from CSV**.
3. Click **Browse** and select your CSV file.

   **Tip**
   You can download template CSV files from the **Import users from CSV** dialog.

   The CSV file can include groups a user is assigned to.
4. To create new groups, click **Create new groups**.
5. To send a registration email for the Sophos Central Self Service portal to each imported user, click **Give users access to Sophos Central Self Service**.
6. Click **Add**.

**Note**

The CSV file can include the email address of each user's manager. If there's a manager who isn't already a user in Sophos Central, a user is created. So the number of users imported may exceed the number of rows in the file.
Note
If an email address in your CSV file matches an existing user in Sophos Central, the user is updated with the information in your import file.

Note
If an email address in your CSV file matches an existing user in Sophos Central that is managed through Active Directory Synchronization, the user is skipped during import and no changes are made to the user account.

Import users from Active Directory
You can import users and groups from Active Directory.

To do this:
1. Go to Users.
2. Click the Set up Active Directory Sync link in the upper right of the page.
3. Follow the set up synchronization process.

Related tasks
Set up synchronization with Active Directory (page 618)
Follow these instructions to set up synchronization with Active Directory.

Protect existing users
You can protect users that you have already added to Sophos Central.

To protect them you need to email them a setup link. To do this:
1. Go to Users.
2. Select the user or users you want to protect.
3. Click Email Setup Link in the upper right of the page.
4. In the Email Setup Link dialog, select the types of protection the user needs (if your license includes more than one).
   - **Web Gateway** provides more advanced web security for computers than Endpoint Protection. You can install it alongside Endpoint Protection or on its own.
   - Users need administrative privileges and internet access to use the setup link.

Delete users
You can delete users from Sophos Central if you are a Super Admin.

Restriction
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them.

Under some circumstances, the user may be recreated automatically in future:
- If the user logs in to an associated device that is still managed by Sophos Central, they are added as a user again.
If the user was added from Active Directory and is still in Active Directory, they are added as a user again the next time that Sophos Central synchronizes with Active Directory.

To delete users:
1. Go to **Users**.
2. Click the checkbox next to each user you want to delete.
3. Click **Delete**.

Deleting a user does not delete devices associated with that user or remove the Sophos software from these devices.

Logins assigned to a deleted user can afterwards be assigned to another user. You can edit logins by clicking the **Edit** link on a user's details page.

**Related concepts**

*User Summary* (page 600)

**Export to CSV**

You can export lists of users as CSV files.

You can export lists of different types of user.

For example you can export a list of administrators by applying the **Admins only** filter before you click **Export to CSV**.

To export users:
1. Go to **Users**.
2. Click **Export to CSV**.
   
   This creates a file called **users.csv**. Any currently active filters are applied to the list.

### 11.3.2 Groups

On the **Groups** tab of the **People** page, you can add or manage groups of users.

You can use groups to assign a policy to multiple users at once.

The sections below tell you about the groups list and how to add, modify or delete groups.

**About the groups list**

The current groups are listed and the number of users in each group is shown.

To see full details for a group, click the group's name.

**Add a group**

1. Click the **Add Group** button.
2. In the **Add Group** dialog, enter the following settings:
   
   **Group Name**: Enter the name of the new group.
   
   **Available Users**: Select users from the list of available users.
Tip
In the Search box you can start typing a name to filter down the displayed entries.

3. Click Save.

Modify a group
To modify a group, click the group's name to open and edit the group details. For more information, see User Group Details.

Delete a group
To delete a group, select it and click Delete in the upper right of the page.
Deleting a group will not delete its users.

Related concepts
User Group Details (page 609)

User Group Details
On a group's details page, you can:
• Add or remove members.
• Delete the group.

Add or remove members
To add or remove members:
1. Click Edit under the group name.
2. In the Edit Group dialog, use the picker arrows to add users to the Assigned Users list or remove them.
3. Click Save.

Delete the group
To delete the group:
1. Click Delete under the group name.
2. In the Confirm Group Deletion pop-up, click Yes.
Deleting a group will not delete its users.

User Group Policies
The Policies tab in a user group's details page lets you see the policies that are enabled and applied to the group.
Click a policy name to view and edit policy details.
Editing the policy affects all groups to which this policy is applied.

11.4 Campaigns

Here you can see your campaigns and start a new campaign or series.
The list of existing campaigns is grouped into active, upcoming and past campaigns and shows high-level information for each campaign. You can click on a campaign for more details.

You can create a New Campaign to test your users with an attack simulation or enroll them in mandatory training. New Series creates a series of campaigns.

Related concepts
Campaign overview (page 615)
This shows the details of a campaign and the activity associated with it.

Related tasks
Create a Phish Threat Campaign (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.
Create a campaign series (page 614)
Start a new campaign series to test your users with attack simulations or enroll them in mandatory training.

11.4.1 Create a Phish Threat Campaign

Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

You create campaigns with an assistant that uses templates. The templates can be customized to suit your organization and your users. To create a campaign:

1. Click New Campaign and give the campaign a name.
2. Select a campaign type.
3. Select the language for the email template and training modules.
4. Click Next.
5. On the Choose Attack page select attacks from the various styles and difficulty levels available. Click Next.
6. Select one or more training courses. Click Next
   Users who are tricked by the simulated attack are enrolled in these courses. Enrolling users in training after failing a test is optional.
7. In Customize you can tailor elements of the campaign for your organization and your users. Click Next.
   The elements you can customize differ depending on the type of attack and whether you are enrolling users on training courses after failing tests.

   Warning
   Customizations to the Reminder Email and the landing pages are set globally. They are used by all current and future campaigns in your account. There is no option to return them to their original format.

8. Choose which Users or user Groups to send the campaign to. Click Next
Click **Auto-enroll new users to this campaign** to enroll new users into this campaign as you add them to Sophos Central.

9. Review your selections from the previous steps.
10. Then schedule your campaign and set the **Sending Increment**.

**Note**

Any actions taken by users after the **End Date** are not factored into the campaign results.

11. Click **Done** to save the campaign.

**Related concepts**

Campaign overview (page 615)
This shows the details of a campaign and the activity associated with it.

Auto-enrollment (page 613)
You can automatically enroll new users into your campaigns and campaign series.

Template (page 611)
You can choose the type of campaign you want to use.

Customize (page 612)
Choose the attack template you want to use.

**Related tasks**

Create a campaign series (page 614)
Start a new campaign series to test your users with attack simulations or enroll them in mandatory training.

**Template**

You can choose the type of campaign you want to use.

Sophos Phish Threat includes templates for common attack types. These templates include emails, landing pages and training modules. You can customize these templates before sending your campaign out.

You can choose from the following template types:

- **Phishing**: This simulates a phishing attack against your users. It encourages your users to click a link in an email.

- **Credential Harvesting**: This simulates an attack designed to obtain login ids and passwords. It encourages your users to enter credentials into a fake website. No passwords are collected.

- **Attachment**: This simulates an attack designed to deploy malicious attachments on your system. It encourages your users to open an attachment in an email.

- **Training**: This allows you to send anti-phishing training to your users without a simulated attack.

You can also select the language used for the campaign.

When you select the attack type in **Choose Attack** you can choose from different difficulty levels.

**Related concepts**

Customize (page 612)
Choose the attack template you want to use.

**Related tasks**

Create a Phish Threat Campaign (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

**Customize**
Choose the attack template you want to use.

**Warning**
Customizations to the **Reminder Email** and the landing pages are set globally. They are used by all current and future campaigns in your account. There is no option to return them to their original format.

You can change the emails and landing pages your campaign uses. The elements you can customize differ depending on the type of attack and whether you have chosen to use training for users who fail. You can customize any of the following:

- **Attack Email** (for all attack types).
- **Attack Landing** page where users are sent if they click on a link in an email.
- **Custom Attachment**.
- **global Reminder Email**.
- **global Caught Landing** page, where users are sent if they fail the test.
- **global Training Landing** page, where users are sent if you auto-enrolled users in training.

**Related tasks**
Create a Phish Threat Campaign (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

**Training**
Users who fall for a simulated attack are automatically enrolled in your selected training modules.
Select a training module from the **Choose Training** screen.
You can choose not to enroll users in training.
You can do a baseline assessment of your users by opting out of training auto-enrollment.

**Related tasks**
Create a Phish Threat Campaign (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

**Simulated Attack Series**
This allows you to test targeted users with phishing, attachment and credential harvesting campaigns.
Choose the type of attacks to send to your users.

- **Phishing**: This simulates a phishing attack against your users. It lures your users to click a link in an email.
- **Credential Harvesting**: This simulates an attack designed to obtain login ids and passwords. It lures your users to enter credentials into a fake website. No passwords are collected.
- **Attachment**: This simulates an attack designed to deploy malicious attachments on your system. It lures your users to open an attachment in an email.

You can select a combination of the attack types.
You can also select the difficulty of the simulations from easiest to hardest and whether you want to enroll users in training following the simulation. By default users are enrolled in training that matches the selected attacks.

**Related tasks**

Create a Phish Threat Campaign (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

**Training Series**

You can enroll your users in a training series.

Click a course to view a synopsis of the course. Click the **Choose this training** link to select a course. You can choose multiple courses.

**Related tasks**

Create a campaign series (page 614)
Start a new campaign series to test your users with attack simulations or enroll them in mandatory training.

**Enroll**

Choose the **Users** or **Groups** to send the campaign to.

**Related concepts**

Auto-enrollment (page 613)
You can automatically enroll new users into your campaigns and campaign series.

**Auto-enrollment**

You can automatically enroll new users into your campaigns and campaign series.

When you turn on auto-enrollment for a campaign or series any new users that are added to your Sophos Central account are enrolled.

For example you can automatically enroll your new hires in a mandatory security training campaign.

**How does auto-enrollment work?**

For a standalone phishing, credential harvesting, attachment, or training campaign, new users are enrolled in the campaign. The first campaign email is sent to these users 24 hours later. The campaign remains active until you end it manually.

For a security training series, new users are enrolled in each training campaign generated by the series. They always start with the first campaign in the series.

For a simulated attack series, new users are enrolled in the next campaign generated by the series.

**Related tasks**

Create a Phish Threat Campaign (page 610)
Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

Create a campaign series (page 614)
Start a new campaign series to test your users with attack simulations or enroll them in mandatory training.

**Review**

Here you can review your campaign and schedule it.

The **Start Date** is the date on which the first email is sent. The **End Date** is the date on which campaign data collection stops.

Any actions taken by users after the **End Date** are not factored into the campaign results.

If you are concerned about load on your network, you can choose to space out the campaign emails by sending a percentage of emails at set intervals.

**Related tasks**

Create a Phish Threat Campaign (page 610)

Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

### 11.4.2 Create a campaign series

Start a new campaign series to test your users with attack simulations or enroll them in mandatory training.

You can choose the type of campaign series you want to use. Sophos Phish Threat includes templates for common attack types.

To create a series:

1. Click **New Series** and give the campaign a name.
2. Choose what type of campaign series you want to set up.
   - **Simulated attack series**: This allows you to test targeted users with phishing, attachment and credential harvesting campaigns.
   - **Security training series**: This allows you to enroll your users in a security training series.
3. Choose the frequency of your campaign.
4. Choose the language of your email and training materials. Click **Next**.
5. Depending on the type of series that you chose, do one of the following:
   - **Set up an attack series**:
     a) Choose the type of attacks to send to your users. You can select a combination of the attack types.
     b) Choose the difficulty level of the simulation.
     c) Choose whether your users are enrolled in training after the simulation.
        By default users are enrolled in training that matches the selected attacks. Click **Next**.
   - **Set up a training series**:
     a) Click a training course to review a synopsis.
     b) Click **Choose this training** to select a training course. You can select multiple training courses. Click **Next**.
6. Choose which **Users** or user **Groups** to send the campaign series to.
   a) Click **Auto-enroll new users to this series** if you want to enroll new Sophos Central users in the series automatically.
b) Click **Next**.

7. Review the series options and click **Edit** to make any changes. Schedule the series:
   - For a simulated attack series, set when the series ends. You can choose an end date or allow a series to continue until you cancel it.
   - For a training series, set when the series starts.

   Any actions taken by users after the end date are not factored into the campaign results.

8. Click **Done**.

**Related concepts**

- **Training Series** (page 613)
  You can enroll your users in a training series.

- **Auto-enrollment** (page 613)
  You can automatically enroll new users into your campaigns and campaign series.

- **Campaign overview** (page 615)
  This shows the details of a campaign and the activity associated with it.

**Related tasks**

- **Create a Phish Threat Campaign** (page 610)
  Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

**11.4.3 Campaign overview**

This shows the details of a campaign and the activity associated with it.

The campaign summary shows the key high-level metrics for your campaign as well as the campaign start and end dates.

The **Campaign response timeline** plots user activity over the first few hours and days of your campaign, specifically showing emails sent, users caught, and users who reported during each hour of the campaign period. This is helpful for understanding how quickly a breach could occur in the event of a real phishing attack.

**Device breakdown** shows the types of device on which emails were opened and the types of device on which emails caught users.

**User Behavior** shows the responses of users to the emails.

**Email** shows the emails that are sent to users. Depending on the type of campaign, this includes the attack email, the training enrollment email, and the training reminder email.

**Training** shows which training course, if any, you selected for the campaign.

**11.4.4 Campaign results**

You can see a summary of each user's or group's activity.

For each user, time stamps are shown for the following events:

- **Email sent**: When the user was sent the campaign email.
- **Email opened**: When the user opened the email.
- **Reported Email**: When the user reported the email as a phishing email.
- **Clicked link**: When the user clicked the phishing link in the email.
• **Entered Credentials**: When the user entered credentials that were requested by the email in a **Credential Harvesting** campaign.

• **Started training**: When the user began the required training course.

• **Finished training**: When the user successfully passed the quiz at the end of the required training.

For each group, the numbers of users, instead of time stamps, are shown for each of the above events.

### 11.4.5 Migrate campaigns from Phish Threat version 1

If you are still using Phish Threat version 1, you can migrate your completed version 1 campaigns to version 2.

To be able to do this, you must be able to log in to Phish Threat version 1 from Sophos Central using single sign-on.

To migrate, do as follows:

1. In Phish Threat version 1, click **Campaigns > Migrate to V2**.
2. In **Campaign Migration Center**, click **Start Campaign Migration**.
3. Click **OK** to confirm.

   Phish Threat starts to migrate all your completed campaigns, and the **Migration Information** and the **Pending Campaign Migrations** table are updated.

When all your completed campaigns have been migrated, you can view all the campaign data in Phish Threat version 2, under **Campaigns**.

**Note**

Two months after you have successfully migrated all your completed campaigns, you cannot create new campaigns in Phish Threat version 1 and version 1 will no longer be available in Sophos Central.

If you stop the migration, campaign data that has already been migrated remains in version 2, ready for you to resume.

### Campaign Migration Center

In the **Campaign Migration Center**, you can start or stop a migration, and view details of migrations.

To migrate your campaigns, you must be able to log in to Phish Threat version 1 from Sophos Central using single sign-on.

**Start Campaign Migration**: Use this to start migrating your campaigns.

**Pending Campaign Migrations**: The table shows the completed campaigns that are awaiting migration.

**Completed Campaign Migrations**: The table shows the completed campaigns that have been migrated.

**Failed Campaign Migrations**: The table shows the completed campaigns that have not been migrated successfully. The technical reason for the failure is not displayed but it is logged and can be accessed by Sophos Support, if necessary.
11.5 Settings

The Settings pages are used to specify security settings that apply to all your users.

11.5.1 Active Directory Sync

You can import users and user groups from Active Directory to Sophos Central.

In Settings, on the **Active Directory Sync** page, you can select the Active Directory service you want to use.

- There is a download link for the Sophos Central Active Directory synchronization utility.
- In **Endpoint Protection** and **Email Gateway** you can use Azure Active Directory synchronization instead.

**Note**

If you are using Office 365 you must use Azure Active Directory synchronization.

For instructions on setting up the utility, see the Active Directory setup instructions. Once you have set up synchronization you can review its status and other settings.

**Related concepts**

- **Active Directory Sync Status** (page 617)
  On the **Active Directory Sync** page, you can check the sync status and download the installer.
- **About Active Directory synchronization** (page 618)
  Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

**Related tasks**

- **Set up synchronization with Active Directory** (page 618)
  Follow these instructions to set up synchronization with Active Directory.

**Active Directory Sync Status**

On the **Active Directory Sync** page, you can check the sync status and download the installer.

You need to set up Active Directory synchronization before you can see these options.

You can download the latest installer for setting up synchronization with Active Directory.

**Sync status**

This shows your synchronization status and the synchronization settings in Active Directory.

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The time of the last synchronization with Active Directory.
- The number of users and groups imported from Active Directory.
You can view Active Directory synchronization alerts on the Overview > Alerts page. You can view synchronization events on the Overview > Logs & Reports > Events page.

About Active Directory synchronization

Active Directory synchronization allows administrators to implement a service that maps users and user groups from the Active Directory to Sophos Central.

To synchronize with Active Directory, you need to download and install the Sophos Central Active Directory Sync utility. The utility works as follows.

It synchronizes active users and user groups.

It can run automatically on a regular basis, as set up by the Sophos Central administrator.

It doesn't duplicate existing users or groups when they are matched to an existing Sophos Central user or group. For example, an email address from Active Directory may be added to an existing user in Sophos Central.

It supports only the Active Directory service.

It can synchronize multiple Active Directory forests. To do this, you need to install the utility on multiple machines and configure each utility to synchronize a different Active Directory forest. We strongly recommend to synchronize different Active Directory forests at different times of day, so that the synchronizations do not overlap.

It doesn't help you to deploy the Sophos agent software to your users' devices. Use other methods of deployment with Active Directory.

Set up synchronization with Active Directory

Follow these instructions to set up synchronization with Active Directory.

Before you can set up synchronization, you need .NET Framework 4 on the computer where you will run the Sophos Central AD Sync Utility.

Warning

Before you proceed, make sure all your active directory users are set up correctly with an email address. Users without an email address aren't protected and email going to an email address not tied to a user isn't delivered.

You need to use API credentials to synchronize with Active Directory.

To set up synchronization with Active Directory:

1. Set up your API credentials for AD sync. To do this, click Settings > API credentials.
2. Add a new credential. Enter the following information:
   - Credential name
   - Description
3. Copy the Client ID and Client Secret.
4. Click Settings > Active Directory Sync, and click the link to download the Sophos Central AD Synchronization Utility installer. Then run it.
   Alternatively, go to the Start menu and click Sophos > Central > AD Sync. If you are running Windows 8 or later, in the Apps list, find the app AD Sync listed under Sophos.
   The Sophos Central AD Sync Utility Setup assistant starts.
5. In the setup wizard, enter the information required.
6. On the last page of the setup assistant, select Launch Sophos Central AD Sync Utility and click Finish.
7. In the Active Directory Synchronization Setup utility, on the Sophos Credentials page, enter your Client ID and Client Secret instead of your Sophos Central account credentials.

8. On the AD Configuration page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the Use LDAP over an SSL connection (recommended) checkbox selected. If your LDAP environment doesn’t support SSL, clear the Use LDAP over an SSL connection (recommended) checkbox and change the port number. The port number is usually 636 for SSL connections and 389 for insecure connections.

9. If you don’t want to synchronize the entire forest, on the AD Filters page, you can specify which domains to include in the synchronization. You can also specify additional search options (search bases and LDAP query filters) for each domain. Distinct options can be specified for users and user groups.

   **Note**
   AD Sync will only create groups that have members which include discovered users or devices, regardless of group filter settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search bases</td>
<td>You can specify search bases (also called “base distinguished names”). For example, if you want to filter by Organizational Units (OUs), you can specify a search base in this format: OU=Finance,DC=myCompany,DC=com</td>
</tr>
</tbody>
</table>
   | LDAP query filters   | To filter users, for example, by group membership, you can define a user query filter in this format: memberOf=CN=testGroup, DC=myCompany, DC=com
   |                      | The above query limits user discovery to users belonging to “testGroup”. Note that if you don't specify a group query filter, AD Sync will discover all groups to which these discovered users belong. If you wish group discovery to also be limited to “testGroup”, you could define the following group query filter: CN=testGroup |

   **Note**
   If you include base distinguished names in your search options or change your filter settings, some of the existing Sophos Central users and groups created during previous synchronizations may fall outside the search scope and may be deleted from Sophos Central.

10. On the Sync Schedule page, define the times at which the synchronization will be performed automatically.
Note
A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select Never. Only sync when manually initiated.

11. Click Finished.

12. To synchronize immediately, in the AD Sync Utility, click Preview and Sync. Review the changes that will be made during the synchronization. If you are happy with the changes, click Approve Changes and Continue.

The Active Directory users and groups are imported from the Active Directory to Sophos Central. To stop the synchronization in progress, click Stop.

Related tasks
Import users from Active Directory (page 607)
You can import users and groups from Active Directory.

11.5.2 Sophos Outlook add-in

Sophos Outlook add-in enables users to report suspected phishing and spam messages with one click right from within Outlook.

Sophos Outlook add-in is available for Outlook for Windows and Mac, Outlook Web Access, in Office 365 and Exchange environments.

Benefits of Sophos Outlook add-in

Sophos Outlook add-in simplifies the process your users have to follow to report suspicious mail. With one click, users can report a message to the proper destination in the proper format, eliminating the need to remember a specific email address or how to properly forward unwanted messages.

You and your team will get better visibility into the type and volume of suspicious email reaching your end users. This visibility allows you to better understand the threats facing your organization, both in real time, enabling you to respond quickly to potential security incidents, and from a strategic viewpoint, helping to fine tune your layered security strategy.

Using Sophos Outlook add-in to report suspicious email helps Sophos in its work to predict and prevent threats for our customers. The messages submitted to SophosLabs by your users allow us to continually improve our threat detection capabilities for all Sophos customers.

How do I install Sophos Outlook add-in?

Installing Sophos Outlook add-in involves three steps:

- Configuring Sophos Outlook add-in in Sophos Central.
- Downloading the XML manifest from Sophos Central.
- Deploying Sophos Outlook add-in to users.
**Configure Sophos Outlook add-in**

Before deploying Sophos Outlook add-in to users, you need to set up one or more mailboxes where reports of suspicious messages will be delivered.

To add a mailbox, click **Settings > Report Message Add-in for Outlook** and click **Add mailbox** to add a new mailbox.

To remove a mailbox, click the ‘x’ next to the mailbox in the list of mailboxes where reports of suspicious messages will be delivered.

**Download the XML manifest**

Once you have configured the mailboxes where reported messages will be delivered you need to download the XML manifest.

Click the **Download XML Manifest** link on **Settings > Report Message Add-in for Outlook**.

Save this file in a location where you will be able to access it during the deployment step.

**Deploy Sophos Outlook add-in**

Deploying the Sophos Outlook add-in involves several steps.

Sideloading is recommended for proof of concept and testing purposes only. Sideloading refers to the process of installing Sophos Outlook add-in on an individual end-user system, see the "Sideloading installation instructions".

You should check if Office 365 centralized deployment of add-ins will work in your environment.

If you are ready to begin centralized deployment of Sophos Outlook add-in, see the "Manage deployment" instructions to get started.

For customers in an on-premise environment without a connection to Office 365, use the Exchange Admin Center to install Sophos Outlook add-in for your organization.

**Related information**

- Sideloading installation instructions
- Determine if centralized deployment of add-ins works for your Office 365 organization
- Manage deployment of Office 365 add-ins in the Office 365 Admin Center
- Install or remove add-ins for Outlook for your organization
Reporting a message

Users with Sophos Outlook add-in installed have a Report Message button in their Outlook ribbon on the Home tab.

This button is present when they are reading a message in the reading pane or in a pop-out window. Users on Outlook Web Access or Office 365 web have a Report Message option in the message task pane.

To report a message the user clicks Report Message.

The user is then asked to confirm the submission.

Once the message is reported, the user sees a dialog thanking them for their awareness and informing them that the message has been submitted to their administrator and deleted from their mailbox.

What will my users see when they report a phishing simulation?

Sophos Outlook add-in works seamlessly with Sophos Phish Threat.

When a user reports a Phish Threat email, they will receive immediate feedback in Outlook thanking them for their awareness and reinforcing this positive behavior.

Is my environment compatible with Sophos Outlook add-in?

Sophos Outlook add-in works for mail accounts in the following environments.

- Exchange 2019 on-premises.
- Office 365 Business subscription (Exchange online).

Note

Exchange 2013 on-premises and Exchange 2016 on-premises are not supported. Non-Microsoft mail providers (such as Gmail or other POP/IMAP accounts) are also not supported.

Compatible mail clients

- Outlook Web Access (Office 365 only).

Note

Due to a recent bug in the official "office-js" Microsoft Office add-in library, Mac users will need to update their Outlook clients to build number 190514 or higher for the add-in to work. The Microsoft Office team has said this build is scheduled to be rolled out by the second week of June 2019. Before then, it is available by manually updating to the latest Microsoft Office Insider Fast build.
11.5.3 Sending domains and IPs

Here you can see the domains and IP addresses used for sending campaign email from Phish Threat. You must allow mail and web traffic to and from these IPs and domains on your email gateway, web proxy, firewall appliance, or anywhere else in your environment where mail and web filtering is done. This list updates when we add new domains.

Related information
Sophos Central What’s New?

11.5.4 Campaign Reminders

You can send out emails to administrators before a campaign launches. Choose the administrators you want to remind that a Phish Threat campaign will start in 7 days.

11.5.5 Training Reminder and Enrollment Emails

You can use a custom sending address for training reminder and enrollment emails. Sending these emails from a domain that your organization owns, instead of the default Sophos one, makes them more trustworthy.

To turn on using your custom email address, click Settings > Training Reminder and Enrollment Emails.

The sending domain used for simulated attack emails does not change. Your custom email address is used for sending the following types of email:

• Training reminder emails: used in all campaign types.
• Enrollment emails: only used in training campaigns.
• Caught emails: only used in attachment campaigns.

You must test the custom address to ensure it's valid. If you don't verify your custom email address, emails are sent using the Sophos address.

If there are problems with with your custom email address, emails are sent using the Sophos address.

You can also set a custom email address for emails sent out by the campaign test feature.
12 Cloud Optix

Sophos Cloud Optix is an AI-powered security and compliance platform for public cloud environments. You can start trials, manage licenses and access the Sophos Cloud Optix console from My Products.

Sophos Cloud Optix does the following:

- Provides a real-time inventory of your servers, storage and network elements in the cloud.
- Helps you manage resources, monitor security and meet compliance standards in one simple-to-use interface.

For more information, see the product information on the Sophos website or the Sophos Cloud Optix help pages.

Note
The Sophos Cloud Optix service is hosted in the US. Customers in other countries can purchase and use the US-hosted service. The service is not currently available from Cuba, Iran, North Korea, Russia, South Sudan, Sudan, Syria, Ukraine, and Venezuela.

Related information
Sophos Cloud Optix help
Sophos Cloud Optix product information
13 Free Trials

On the Free Trials page, you can learn about extra products you can add to Sophos Central. You can also:

- Start a product trial.
- Extend a product trial.
- Buy a product.

Start a trial

You can start a product trial without contacting Sophos or your Sophos partner.

**Note**

You can run multiple trials at the same time (unless the products have overlapping features). Your trials do not all have to start on the same date.

1. Under a product name, click **Start Trial**.
   A trial is started for you automatically.
2. On the page that is displayed, select and download the product.
   The trial license for this product is now shown on the Licensing page.
   The trial will expire after 30 days. The product will then be listed on the Free Trials page again.

Extend a trial

You can extend a trial or you can start another trial of the same product at a later date.

To extend a trial, contact your Sophos Partner (or the account team in Sophos, if applicable).

To start another trial of the product at a later date, go to the Free Trials page and start a trial as before.

**Note**

After a trial expires, you must wait 30 days before you can start another trial of the same product.

Buy a product

You can buy new products.

1. Under a product name, click **Buy Now**.
   You are taken to a Partner Info page where you can find a Sophos Partner.
2. Contact a Sophos Partner to license the product.
13.1 Trial license banners

If you have a trial license, Sophos Central shows various banners to remind you of when it expires. Which banner you see depends on how long ago the license started and how many trial licenses you have. A trial license lasts for 30 days. After this, you must either buy a full license or stop using the software or features.

**Your evaluation license for <product> will expire in 28 days.**

This is the first expiration banner that’s shown, at the start of the trial license, and shows you that the license is active.

**Your evaluation license for <product> will expire in 3 days. Contact your Sophos partner to buy a license.**

This warning is shown three days before your trial license expires. We recommend that you contact your partner to discuss purchase options.

**Your evaluation license for <product> has now expired. Contact your Sophos partner to buy a license.**

This warning is shown when the trial license has expired. It remains until you apply a license to Sophos Central for this product or feature or you stop using it.

The warning does not mean that updates or protection have been turned off.

**Related concepts**

Licensing (page 631)
You can activate and manage your Sophos licenses from Sophos Central Admin.
14 Account and Licensing

**Your account name.** Click here to see options to manage licenses, administrators and support settings, see your contact details or partner details, change to a different language, or log out.

If your account name is incorrect, please ask your Sophos partner to correct it, following the instructions in the Sophos Central Partner help.

### 14.1 Account Details

The **Account Details** page lets you change your password, manage your email subscriptions, view your account and partner details, and more.

To access this page, click your account name and select **Account Details**.

**Company Info**

Click your account name, select **Account Details**, and click **Company Info**.

This tab shows the contact information for your company.

Amend the information as required and click **Save**.

**Co-branding**

You can have your company logo or your partner’s logo displayed to your end users in the Sophos Central Self-Service Portal. This helps end users recognize that they’re going to an official web application for your company.

**Note**

You need to be a Super Admin or Admin user.

Click your account name, select **Account Details**, and click **Co-branding**.

Click **Browse**, select a file to upload, and click **Save**. Logo images must meet the requirements shown on the page.

**Use your partner’s logo**

To use your partner’s logo, check the option **Use settings from Sophos Central Partner**. A preview of the logo will be shown. Click **Save**.

**Change or remove the logo**

To add a new logo, or to go back to the Sophos logo, you must remove any current logo. Click **Remove** under the logo preview and click **Save**.

**My Info**

You can view your administration role details and the email address you use for signing into Sophos Central. You can change the sign-in password.
Click your account name, select **Account Details**, and click **My Info**.

Your administration role is shown at the top. Click the role name for full details.

To change the password:

1. Click **Change password**.
2. Enter your **Current password**.
3. Create a **New password**, confirm it, and click **Reset Password**.

   You are automatically signed in with the new password and returned to Sophos Central.

**Note**
The old password is no longer valid.

**Partner Info**

Click your account name, select **Account Details**, and click **Partner Info**.

This tab shows the contact information for your partner, if applicable.

**Account Preferences**

You can enable Enterprise Management for Sophos Central Enterprise.

Sophos Central Enterprise enables distributed security management. It gives administrators the ability to manage the security of an organization divided into multiple sub-estates. For example an organization that has several sites can manage the security for each site as a separate sub-estate.

Click your account name, select **Account Details**, and click **Account Preferences**.

**CAUTION**

Once you have turned on this feature, it can only be turned off from Sophos Central Enterprise by an Enterprise Super Admin.

When you enable Enterprise Management from a Sophos Central account any other accounts associated with your customer account are linked to your Sophos Central Enterprise account as sub-estates.

Sub-estates can't be managed in Sophos Central Enterprise until the sub-estate's Sophos Central administrator allows the Enterprise Admin to access the sub-estate's account. You must have the Super Admin role to do this. You cannot turn off Enterprise Admin access once you have opted in.

To allow access:

1. Check in **Account Preferences** that Enterprise Management has been enabled and that you can see the Enterprise Admin's details.
2. Switch on Enterprise Admin access.
My Email Subscriptions

Note
This option is only available if you have a Web Gateway license.

You can manage your email subscriptions using My Email Subscriptions on the Account Details page.

Click your account name, select Account Details, and click My Email Subscriptions.

To manage subscriptions:
1. Switch on your required email summaries, for example Enable Summary Email.
2. Choose the frequency.
3. Click Save.

Sophos Support

You can select the types of Sophos Support you want to receive.

Click your account name, select Account Details, and click Sophos Support.

The options are:

Remote Assistance. This enables Sophos support to access your Sophos Central session directly for 72 hours to help you. This option is disabled by default.

Note
You can also enable this option when you request support by clicking Help > Create Support Ticket at the top of the page.

Partner Assistance. This enables your designated partner to access your Sophos Central portal and to configure the Sophos Central service on your behalf. This option is disabled by default.

Note
If you do not enable partner assistance, your partner will only see high-level reporting information such as services purchased and current usage figures.

14.1.1 Create an Enterprise Admin

Before you begin:
• You need to be a Super Admin administrator.
• You must have an enterprise administrator to access Sophos Central Enterprise.
• You can use an existing Sophos Central Admin account. If you do, you won't be able to log in to Sophos Central Admin with that account.
• You can't turn on Enterprise Management from Sophos Central trial accounts.

After you enable Enterprise Management:
Enterprise Management can only be disabled from Sophos Central Enterprise by an Enterprise Super Admin. For more information, see the Account preferences section of Sophos Central Enterprise help.

Sophos Central Enterprise lets an administrator manage the security of an organization divided into multiple sub-estates. For example an organization that has several sites can manage the security for each site as a separate sub-estate.

On the Account Details page, on the Account Preferences tab, you can enable Enterprise Management and create an enterprise administrator.

The enterprise administrator manages the sub-estates using Sophos Central Enterprise. The enterprise administrator is a Super Admin administrator for each of the sub-estates.

When you enable Enterprise Management from a Sophos Central account any other accounts associated with your customer account are linked to your Sophos Central Enterprise account as sub-estates. You can also create new sub-estates in Sophos Central Enterprise.

If you create an Enterprise Admin from an existing Sophos Central Admin account the federated sign-in credentials and settings for that account are used for Sophos Central Enterprise account.

To enable Enterprise Management and create the Enterprise Admin:

1. Click your account name (upper right of the user interface), select Account Details, and click the Account Preferences tab.
2. Enable Enterprise Management and click Save. Click Continue.
3. Enter the account details to create the Enterprise Admin. Choose from:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use your Sophos Central login credentials. | To do this click, Use my Sophos Central login credentials to create the first Sophos Central Enterprise admin.  
If you do use your Sophos Central login credentials you won't be able to sign in to Sophos Central Admin with that account. |
| Create a new account.         | To do this, enter new account information. You must use a unique email that is not already used in any other Sophos Central account. |

4. Click Enable Enterprise Management and Save. 
   The Account Preferences tab now shows that Enterprise Management has been enabled and the name of the Enterprise Admin. The Enterprise Admin receives the password setup link in an email.

5. Click the link in the setup email and create the password for the Enterprise Admin account.
   You will now be able use these account details to access Sophos Central Enterprise.

6. To sign in to Sophos Central Enterprise, go to the Sophos Central Admin sign-in page and enter your Enterprise Admin credentials.
   This opens Sophos Central Enterprise.

**Related concepts**

Administration Roles (page 93)
Administration roles divide security administration by responsibility level. Sophos Central includes several predefined roles.

**Related information**

Sophos Central Enterprise Help
14.2 Licensing

You can activate and manage your Sophos licenses from Sophos Central Admin.
Click your account name (upper right of the user interface), select **Licensing**.

**View your licenses and usage**

A list shows your current license(s), with the following details for each license.

- **License**. The name of the license you purchased.
- **Type**. The type of license you have (for example, a **Full** license).
- **Usage**. The number of users or servers using this license.

**Note**
For end-user licenses, this number includes only users who have at least one device associated with them. It may also include protected devices that are not yet associated with a user.

**Note**
For end-user and server licenses, this number may include protected virtual machines (VMs). Hover over the icon to see a breakdown of users (or servers) and VMs.

- **Limit**. The maximum number of users or servers that can use this license. The limit depends on the subscription.
  
  If you are using Enterprise Master Licenses you can't see this option. Licenses are managed by your enterprise administrator.

- **Expires**. The date when the license expires.

- **License #**. License number.

For firewall reporting licenses, click **Manage** to allocate license units to individual firewalls.

A **Trial** license is generated automatically when you use unlicensed software or features. For example, if you are licensed only for Server Protection but you use Intercept X Advanced for Server features, you see both a paid Server Protection license and a trial Intercept X Advanced for Server license. Sophos may also generate trial licenses for temporary license extensions when a full license expires. A trial license lasts for 30 days. After this, you must either buy a full license or stop using the software or features.

**Apply License Key** or **Apply Activation Code**

You can activate a new or upgraded license here. Use the license key shown on the License Schedule that Sophos has emailed you.

**Contact Partner to Buy**

Click **Contact Partner to Buy** to show contact information for your Sophos partner.
Review end-user license agreement

Click this link to display the Sophos End-User License Agreement in a separate window. If you want to print it, press Ctrl+P.

Related concepts
Trial license banners (page 626)
If you have a trial license, Sophos Central shows various banners to remind you of when it expires.

Related tasks
Activate Your License (page 2)
When you buy a new license, you need to activate it.
15 Early Access Programs

Early access programs let you try out new product features before we release them to all customers.

You can take part in more than one program at the same time.

There are two types of early access program:

• **Open.** Anyone can take part.
• **Invitation only.** We invite you to take part in the program and send you the code you need for access.

**CAUTION**
As the product features are in development, they are subject to change.

Join programs

To join programs:

1. Click your account name (upper right of the user interface) and select **Early Access Programs**.
   
   On the **Early Access Programs** page, you'll see a list of the available programs.

   **Note**
   If you want to join an “invitation only” program, you must add the program to the list first. Under **Invitation only programs**, enter your invitation code.

2. Click the **Join** button next to a program.

3. A description of the program is displayed. Click **Continue**.

4. In the **End User License Agreement & Privacy Policy** dialog, view the agreement and then click **Accept**.

   **Note**
   If the program is for endpoint software, an **Add devices** button is displayed. You must continue to the next step.

5. Click the **Add devices** button.

6. On the **Manage devices** page, you see a list of the **Eligible devices** on which you can install the new feature. Use the picker to select the devices where you want to try the new feature. Click **Save**.

   **Note**
   You can add or remove devices at any time during the program. To do this, go to the **Early Access Programs** page again and click the **Manage** button beside the program.

   The software on the selected devices will be updated to include the new feature.
Leave programs

To leave a program, click the **Leave** button next to the program.

If you want to stop using a new feature, you can also simply remove your devices from a program as follows:

1. On the **Early Access Programs** page, click the **Manage** button next to the program.
2. On the **Manage devices** page, use the picker to remove all your devices from the **Assigned devices** list.
16 Supported Web Browsers

The following browsers are currently supported:

- Microsoft Internet Explorer 11 and Microsoft Edge.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (Mac only).

We recommend that you install or upgrade to a supported version in the above list and that you always run an up-to-date version. We aim to support the latest version and previous versions of Google Chrome, Mozilla Firefox, and Apple Safari. If an unsupported browser is detected you will be redirected to https://central.sophos.com/unsupported.

Note
Sophos Central is not supported on mobile devices.
17 Languages

Sophos Central supports the following languages.

- English
- German
- French
- Japanese
- Italian
- Traditional Chinese
- Spanish
- Brazilian Portuguese
- Korean

Sophos Endpoint Protection

Sophos Endpoint Protection supports the following languages on Windows.

- English
- German
- French
- Japanese
- Italian
- Simplified Chinese
- Traditional Chinese
- Spanish
- Brazilian Portuguese
- Polish
- Korean

Sophos Endpoint Protection supports the following languages on Mac.

- English
- German
- French
- Japanese
- Italian
- Spanish

Sophos Endpoint Protection supports the following languages on Linux (version 7 or 9).

- English
- Japanese
Intercept X

Intercept X supports the following languages on Windows.

- English
- German
- French
- Japanese
- Italian
- Simplified Chinese
- Traditional Chinese
- Spanish
- Brazilian Portuguese
- Polish
- Korean
18 Get additional help

To get help from Sophos Support:

1. Click Help in the top right of the user interface and select Create Support Ticket.
2. Fill in the form. Be as precise as possible so that Support can help you effectively.
3. Optionally, select the option to enable Support to directly access your Sophos Central session to be better able to help you.
4. Click Send.

Sophos will contact you within 24 hours.

Note
If you selected the option to enable Support to access your Sophos Central session, this function is enabled when you click Send. Remote assistance will automatically be disabled after 72 hours. To disable it sooner, click on your account name (upper right of the user interface), select Account Details, and click the Sophos Support tab.

Submit feedback

To submit feedback or a suggestion to Sophos Support:

1. Click Help in the top right of the user interface and select Give Feedback.
2. Fill in the form.
3. Click Submit.

Additional help

You can also find technical support as follows:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
19 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.