<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message History Report</td>
<td>409</td>
</tr>
<tr>
<td>Message Summary Report</td>
<td>411</td>
</tr>
<tr>
<td>Sandstorm Activity Summary</td>
<td>411</td>
</tr>
<tr>
<td>Time of Click Summary</td>
<td>412</td>
</tr>
<tr>
<td>At risk users</td>
<td>412</td>
</tr>
<tr>
<td>People</td>
<td>413</td>
</tr>
<tr>
<td>Mailboxes</td>
<td>422</td>
</tr>
<tr>
<td>Quarantined Messages</td>
<td>424</td>
</tr>
<tr>
<td>Policies</td>
<td>425</td>
</tr>
<tr>
<td>Settings</td>
<td>437</td>
</tr>
<tr>
<td>Integrate Sophos Email with external services</td>
<td>458</td>
</tr>
<tr>
<td>Web Gateway</td>
<td>480</td>
</tr>
<tr>
<td>Dashboard</td>
<td>480</td>
</tr>
<tr>
<td>Logs</td>
<td>481</td>
</tr>
<tr>
<td>Reports</td>
<td>481</td>
</tr>
<tr>
<td>People</td>
<td>481</td>
</tr>
<tr>
<td>Computers</td>
<td>491</td>
</tr>
<tr>
<td>Policies</td>
<td>499</td>
</tr>
<tr>
<td>Settings</td>
<td>505</td>
</tr>
<tr>
<td>Protect Devices</td>
<td>524</td>
</tr>
<tr>
<td>Firewall Management</td>
<td>526</td>
</tr>
<tr>
<td>Dashboard</td>
<td>526</td>
</tr>
<tr>
<td>Firewalls</td>
<td>527</td>
</tr>
<tr>
<td>Phish Threat</td>
<td>529</td>
</tr>
<tr>
<td>Dashboard</td>
<td>529</td>
</tr>
<tr>
<td>Logs &amp; Reports</td>
<td>530</td>
</tr>
<tr>
<td>People</td>
<td>531</td>
</tr>
<tr>
<td>Campaigns</td>
<td>541</td>
</tr>
<tr>
<td>Settings</td>
<td>545</td>
</tr>
<tr>
<td>Explore Products</td>
<td>549</td>
</tr>
<tr>
<td>Account and Licensing</td>
<td>550</td>
</tr>
<tr>
<td>Account Details</td>
<td>550</td>
</tr>
<tr>
<td>Licensing</td>
<td>554</td>
</tr>
<tr>
<td>Early Access Programs</td>
<td>556</td>
</tr>
<tr>
<td>Supported Web Browsers</td>
<td>558</td>
</tr>
<tr>
<td>Get additional help</td>
<td>559</td>
</tr>
<tr>
<td>Legal notices</td>
<td>560</td>
</tr>
</tbody>
</table>

(2019/04/26)
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.

Note
We're changing license activation. The choices in the last step below might not be available yet.

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 might 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. See How the "Change" option works (page 2).

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 x 6 months) to the time on the new licenses (50 x 12 months). The total is 900 months.
- Distribute the time over all 100 licenses. The licenses now run for 9 months from the date when the key was applied (and their expiry dates are 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.

If you have more than one product licensed then you will see 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.

Alerts

Alerts shows the number of High, Medium and Info alerts. Info alerts are for information only and don't require you to take action.

Click a number to see those alerts or click View All Alerts to see all alerts.

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.

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** (page 42).

### Endpoint and server web control

**Endpoint and server 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 stats

**Web Gateway Stats** 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.

## 3.2 Alerts

**Some features might not be available for all customers yet.**

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

**Note**

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.

For advice on what to do, see **How to deal with threats** (page 11).

**Note**

If you have Intercept X Advanced with EDR you can investigate, block and clean up threats from Threat Cases, see **Threat Cases** (page 17).
Group alerts

You can group together all alerts for a particular 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 particular priority, click the figures for **High alerts**, **Medium alerts** or **Low alerts** at the top of the page.

To view alerts for a particular 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 fold-out arrow next to an alert to open its details.

In **Action**, click an action button (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. See **Allowed applications** (page 97).

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 Ransomware**: 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](#) (page 559). This action becomes available when you might need help, for example when malware cleanup fails.

- **Cleanup PUA(s)**: 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, see Alerts for Threat Protection (page 6).

- **Authorize PUA(s):** 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 a particular 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. See Configure email alerts (page 91).

**Related concepts**

- Alerts for Threat Protection (page 6)
- Alerts for Installation, Updating and Compliance (page 9)
- Events Report (page 26)
- Configure email alerts (page 91)
- Get additional help (page 559)

### 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. For information on these, see knowledge base article 127331.

**High**

- **Real-time protection disabled**
  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 (page 4).

- 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(s) 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 in 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 my computer option in Sophos Endpoint Security and Control 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.

3.2.2 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.
For more information, see Knowledgebase Article 132029.

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.

3.2.3 Wireless Alerts

View access point generated wireless alerts.

High

- **Access Point has bad health**
  The load on the access point is too high. This is caused by too many connected clients. Check you have enough access points to cover the area.

Medium

- **Access Point is offline**
  The access point has no internet connection, or has no power, or has experienced a software error. If a software error occurs, a restart may help.
- **Access Point is not broadcasting any network**
  There is currently no configuration on the access point. Configure the access point under Wireless > Access Points.
- **Access Point command done**
  The restart is done.

There are some alerts where restarting the access point may solve the problem:

- **Access Point configuration failed**
- **Access Point(s) failed to update to the new firmware**

Call Sophos Support. They will need remote access to investigate the issue (Wireless > Settings > Remote Login to Access Points for Sophos Support).

Low

- **Access Point will be updated with new firmware**
  Wireless is off for approximately 5 minutes.
- **All Access Points will be updated with new firmware**
  Wireless is off for approximately 5 minutes.
• Access Point has been successfully updated with new firmware
• All Access Points have been successfully updated

3.2.4 How to deal with threats

For advice on dealing with threats, see:
• Deal with ransomware (page 11).
• Deal with exploits (page 12).
• Deal with web browser attacks (page 13).
• Deal with malware detected by deep learning (page 13).
• Deal with application lockdown events (page 14).
• Deal with false positives (page 14).

For advice on malware, see the sections on malware alerts listed in 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 (page 14).

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.
  For help with sample submission, see our knowledge base article.
• 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 (page 4).
• 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.

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 (page 14).

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 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.

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 Allow an application that’s been detected (page 98).

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.

For details, see these topics:

• Stop detecting an application (page 14)
• Stop detecting an exploit (page 15)
• Stop detecting ransomware (page 16)

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.
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.

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.

If you have an Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server 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.

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 (page 19).

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. See Device isolation (page 171).

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.
   If you have Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server, you'll see more advanced analysis, see Latest threat intelligence (page 20). You can also do further detection and cleanup, as shown in the steps that follow.

7. Click Search to search for more examples of the file on your network.
   If the Threat Search Results page shows any more examples of the file, you can click Isolate this 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 Threat Cases list, select the case and click Close.
About the threat cases list

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

You can filter the cases by 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:

- **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.
- **User**: The user that caused the infection. Click the user name to view the user's details.
- **Device**: The device that caused the infection. Click the device name to see its details.

You can click any column to sort the cases.

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 Threat Cases page. Click its name to see a summary, details of the artifacts (processes, files, keys) affected, and a diagram showing how the threat developed.

For an overview of what to do, see How to investigate and clean up threats (page 18).

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 with EDR for Server. See *Isolate this device* (page 20).

**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.

**Isolate this device**

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

In **Suggested next steps**, you can 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, see *Scanning exclusions* (page 172).

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

For more information, see *Admin Isolated Devices* (page 101).

Note
You don't see **Isolate this device** if the device has already isolated itself automatically. See *Device isolation* (page 171).

**Latest threat intelligence**

When you click on an affected item, you will see a details pane. If someone has already submitted the file to Sophos, you'll 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 prevalence.
If you have Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server, you'll see more information in tabbed sections, as follows.

**Process details**
This tab shows an assessment of the item's reputation and tells you if you need to investigate.

**Report summary**
This shows the file's reputation and prevalence. It also summarizes the results of our machine learning analysis, which indicate how suspicious the file is.

**Machine learning analysis**
This shows full results of our machine learning analysis. For more information, see Machine learning analysis results (page 22).

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

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

You can also do searches from the Threat Searches page or from the Threat Searches pane in the Dashboard. For more information, see Threat Searches (page 23).

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

If a 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.

For more information, see Blocked items (page 211).

**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.
- **Time logged**: The time and date a process was accessed.
- **Reputation**
- **Interactions**
Create forensic snapshot

You can create a "forensic snapshot" of data from the affected device.
This gets data from a Sophos log of the device's activity and saves it on that device. You can then do your own analysis.
You'll need a converter (which we provide) to read the data.

To create a snapshot:
1. Go to a threat case's **Analyze** tab.
2. Click **Create forensic snapshot** (in the upper right of the list of artifacts).
3. Follow the steps in this knowledge base article.

**Related concepts**
- **Blocked items** (page 211)
- **Threat Searches** (page 23)
- **Admin Isolated Devices** (page 101)

**Machine learning analysis results**

You can submit files to Sophos for an in-depth machine learning analysis.

To submit files, you go to **Threat Cases**, open the relevant threat case, select the file, and click **Latest Threat Intelligence**.

The latest intelligence is shown in a set of tabs.

The tabs include **Machine learning analysis**. This shows the following results.

**Attributes**

We compare your file’s attributes to millions of known good and known bad files. The results can help you work out whether your file is more likely to be good or bad.

**Code similarity**

We pass your file through machine learning engines that determine whether it matches known good files or known bad. We’ll show the closest matches.

The more bad files it matches and the more closely it matches them, the more suspicious your file is.

The list shown here only includes the closest matches. Other matches count toward the result and may affect the rating for your file.

**File/path**

We compare your file’s path to known good and known bad files. If your file’s path more closely matches the path of known bad files, it’s 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, File breakdown

The File properties tab lists key properties of the file.

The File breakdown tab list details of certificates, PE file sections and PE imports.

3.3.2 Threat Searches

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

You can 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.

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. See Threat Search Results (page 24).
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 Cases (page 17)

Threat Search Results

Threat searches are only available if you have Intercept X Advanced with EDR or Intercept X Advanced with EDR for Server.

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

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, see Blocked items (page 211).

You can remove devices from isolation after you have investigated and taken action, see Admin Isolated Devices (page 101).

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 (page 25).

To find out how reports work and how you can customize, save and schedule them, see Reports (page 41).

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 (page 26).

- **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 (page 37).

Data Loss Prevention Events Log. All events triggered by data loss prevention rules for computers or servers, see Data Loss Prevention Events Log (page 38).

Message History. The email messages processed by Email Security for your protected mailboxes, see Message History Report (page 39).

Gateway Activity Logs. All the network activity logs associated with your Web Gateway protection, see Gateway Activity (page 40).

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 (page 27).

For advice on what to do about threats, see How to deal with threats (page 11).

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-AJWL"), 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.

Date range: Use the From and To fields to select the time period for 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 Report: 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
- **When**: 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
- **Device**: Device that caused the event

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.

**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. For more information, see **Alerts** (page 4).

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 <strong>Alerts</strong> page, and a “Running malware cleaned up” event will be added to the <strong>Events</strong> 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>
</tbody>
</table>
| Running malware not cleaned up           | High     | Yes              | 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:  
  • Running malware requires manual cleanup.  
  • Computer scan required to complete running malware cleanup.  
  • Reboot required to complete running malware cleanup.  
  • Running malware not cleaned up. |
<p>| Running malware cleaned up               | Low      | No               |                                                                                                                                             |
| Malicious activity detected              | High     | Yes              | Malicious network traffic, possibly headed to a command-and-control server involved in a botnet or other malware attack, has been detected. |
| Running malware alert locally cleared    | Low      | No               | A running malware alert has been cleared from the alerts list on an endpoint computer.                                                      |
| Ransomware detected                      | High     | No               | An unauthorised program attempted to encrypt a protected application.                                                                     |
| Ransomware attack resolved               | Low      | No               |                                                                                                                                             |
| Remotely-run ransomware detected         | Medium   | Yes              | An unauthorized program attempted to remotely encrypt a protected application.                                                               |</p>
<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remotely-run ransomware attack resolved</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Ransomware attacking a remote machine detected</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>

**Application control**

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled application blocked</td>
<td>Medium</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Controlled 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. You can find more information about these in knowledge base article 127331.
<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>Malware not cleaned up</td>
<td>High</td>
<td>Yes</td>
<td>The following events may be displayed for this event type: • Manual cleanup required. • Computer scan required to complete cleanup. • Reboot required to complete cleanup. • 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 the threat. It may be because the threat has hidden components that haven't been detected.</td>
</tr>
<tr>
<td>Threat removed</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Malware alert locally cleared</td>
<td>Low</td>
<td>No</td>
<td>A malware alert has been cleared from the alerts list on an endpoint 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>
<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) alert 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>
</tbody>
</table>

Copyright © Sophos Limited
### Real-time protection

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time protection</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>disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time protection</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>re-enabled</td>
<td></td>
<td></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>

### Updating

<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

<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</td>
<td>Low</td>
<td>No</td>
<td>registered</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>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>
<tr>
<td>Failed to protect computer or server</td>
<td>High</td>
<td>Yes</td>
<td>A computer has started installation of the agent software but has not become protected for one hour.</td>
</tr>
<tr>
<td>Error reported</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Scan completion</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New logins added</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New users added automatically</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Peripherals**

| Event type                     | Severity  | Action required? | |
|--------------------------------|-----------|-----------------| |
| Peripheral detected            | Medium    | Yes             | |
| Peripheral allowed             | Low       | No              | |
| Peripheral restricted to read-only | Low     | No              | |
| Peripheral blocked             | Low       | No              | |

**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.
### Duplicate device detection

<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 <strong>Alerts</strong> page if a duplicate device is detected. Duplicated devices are re-registered with a new ID.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>

For more information, see [Knowledgebase Article 132029](#).

### ADSync

<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 <strong>Alerts</strong> 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. For more information, see [Knowledgebase Article 121319](#).

<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>
</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>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong> 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>Encryption failed</td>
<td>Medium</td>
<td>See Note</td>
<td>A volume could not be encrypted.</td>
</tr>
<tr>
<td>Encryption info</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>Device not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Device Encryption status changed from ... to ...</td>
<td>Low</td>
<td>See Note</td>
<td>The Device Encryption status changed from one status to another status. See Computers (page 55).</td>
</tr>
<tr>
<td>Device Encryption is suspended</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key received</td>
<td>Low</td>
<td>See Note</td>
<td>Sophos Central received a recovery key from an endpoint computer.</td>
</tr>
<tr>
<td>Recovery key revoked</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 file 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 file 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.

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 the activity or change was carried out.

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

**Date range**: Use the **From** and **To** fields to select the time period for which you want to view events. You can view events that occurred in the past 90 days or less.

**Rule Name**: You can filter the events by rule name.

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

**Update Report**: 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**: Name of the destination that caused the event

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**

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

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

• **Search**: You can search emails by subject, sender or recipient.

• Use the **From** and **To** fields to select the time period for which you want to view the email processing history. You can view email that has been processed in the past 30 days or less. By default the report displays the emails that have been processed during the current day.

• **Direction**: Select **Inbound** or **Outbound** from the drop-down menu to view emails that have been received or sent.

• Select **Status** from the drop-down menu to filter emails by status.

• **Update**: Click this to refresh the report if you have changed the date range, entered a search term or filtered the emails.

**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.
  — **Deleted**: The email was deleted due to its content or block list configuration.

  **Note**
  When you select **Deleted**, you can select a **Reason** for deletion from the drop-down menu. Choose from, **Customer block list**, **Header Anomaly**, **Spam**, **User block list**, **Virus**, **Malicious URL**, **Advanced threat** and **All**.

  — **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.

**Note**
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, see Email Security Policy (page 428).

- **Date**: Date and time the email was processed.
- **Sender**: The sender of the email.
- **Recipients**: The recipient(s) of the email.
- **Subject**: The subject line of the email.

**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.

  Click **Block IP** if you want to add the IP to the Inbound Allow/Block list then click **Block** to confirm your choice.

  **Note**
  Any sender using this IP address is blocked.

  Click **Cancel** to cancel the action. See Inbound Allow/Block (page 108).

  Click on the **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. For more information, see https://tools.ietf.org/html/rfc3463.

- **Raw Header**: shows the email header details.
- **Attachments**: shows the name and size of attachments.

**Gateway Activity**
The **Gateway Activity Logs** 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.
• **Print**: Send a copy of the report to the printer.
• **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.**

**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 Details.**
   - This shows you the password (and previous passwords).

### Gateway Reports

The **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

This option is only available if your license includes Sophos Email.
The **Message Summary** report details the email messages processed by Email Security for your protected mailboxes.

Use the **From** and **To** fields to select the time period for which you want to view processed messages. 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 Security.
- **Legitimate:** Messages that have been allowed.
- **Spam:** Messages classified as spam.
- **DLP policy violations:** Messages that violated Data Loss Prevention policies.
- **Virus:** Messages classified as containing viruses.
- **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 failure:** Messages that failed authentication by DMARC, SPF or DKIM.

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

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

---

**Sandstorm Activity Summary**

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

The **Sandstorm activity summary** report details the email messages processed by Email Security for your protected mailboxes.

Use the **From** and **To** fields to select the time period for which you want to view processed messages. 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 and are classified as follows:

- **Scanned:** All messages checked by Sandstorm.
- **Legitimate:** All messages that are not classed as spam or do not contain advanced threats.
- **Advanced threat:** All messages that have been classified as containing advanced threats.

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** selected and all message types.

---

**Time of Click Summary**

This option is only available with an Email Advanced license.

The **Time of Click Summary** report details the email messages processed by Time of Click URL Protection for your protected mailboxes.
Use the From and To fields to select the time period for which you want to view processed messages. 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 option is only available with an Email Advanced license.

The **At risk users** report details all the users that have triggered Time Of Click protection in the last 30 days by clicking malicious links.

Use the From and To fields to select the time period for which you want to view details of at risk users. You can view details for the last 60 days or less. Details for the last 30 days are shown by default.

Click **Create phish threat campaign** to open the phish threat campaign wizard. The at risk users for the date range you have selected are automatically included in the campaign. You can also add and remove users manually.

You can see the following information in the report:

- **User**: The email address of the at risk user.
- **Risky sites clicked**: The total number of malicious links the user has clicked on.
- **Blocked sites**: A list of the clicked links that were blocked by Time of Click protection, and the number of times they were clicked on in total.
- **Warned sites**: A list of the clicked links that generated a warning from Time of Click protection, and the number of times they were clicked on in total.

### 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 sections below tell you about the users list and how to manage users.
About the users list

The current users are listed with their details:

- Security status. An icon shows whether the user has security alerts on any of their devices:
  - Green check mark if there are low-priority alerts or no alerts.
  - Amber warning sign if there are medium-priority alerts.
  - Red warning sign if there are critical alerts.
  
  Click on 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, see Administration Roles (page 76).
  
  This column is only visible if you are an administrator.

Click on 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 on the user's name. For more information, see User Summary (page 48).

Add a user manually

This also gives you the option to let the user protect their own devices.

You can add an individual user and protect them as follows.

1. On the Users page, click Add and select Add User.

2. In the Add User dialog, enter the following settings:
   
   First and Last Name. Enter the name of the user. Do not include a domain name.

   Role. Select an administration role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

   A user who is assigned an administration role will receive an email telling them how to set up their administration account.

   **Important**
   
   You can only see the Role option and assign administrator roles if you are a SuperAdmin.

   **Note**
   
   Anyone with a User role only has access to the Self Service Portal.

   **Email Address.** Enter the email address of the user.
Add Groups (optional). Select one of the available user groups and use the picker arrows to move it to the assigned groups.

**Tip**
You can start typing a name in the search box to filter the displayed 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.

3. Click **Save** or **Save & 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 by protecting their devices

You can add users automatically as follows.

Download an installer and run it yourself on a device (or devices). This adds the user of each device automatically. For installers, see the **Protect Devices** page.

### Import users from a CSV file

**This option may not be available for all customers yet.**

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 do this:

1. On the **Users** page, click **Add** and select **Import users from CSV**.
2. Click **Browse** and select your CSV file.

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

3. The CSV file can include groups a user is assigned to. To create groups not available yet, select **Create new groups**.
4. To send a registration email for the Sophos Central Self Service portal to each imported user, select **Activate new users**.
5. 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.
On the Users page, click the Set up Active Directory Sync link in the upper right of the page. Then see Set up synchronization with Active Directory (page 73).

Protect existing users
To email users you have already added to the list or imported:
1. On the Users page, select the user or users you want to protect. Click Email Setup Link in the upper right of the page.
2. In the Email Setup Link dialog, you are prompted to select the types of protection the user needs (if your license includes more than one).

   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.

Modify users
To modify a user's account:
On the Users page, click the user's name to open and edit their user details. For more information, see User Summary (page 48).

Delete users
To delete a user or users:
On the Users page, select the checkbox next to each user you want to delete. Click the Delete button in the upper right of the page.
Important

You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them, see Administration Roles (page 76).

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

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

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 will be added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they will be added as a user again the next time that Sophos Central synchronizes with Active Directory.

Export to CSV

To export a list of users:

Click on Export to CSV.

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

For example you can export a list of administrators by applying the Admins Only filter before clicking Export to CSV.

Related concepts

Active Directory Sync (page 72)

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.
Security status

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

✅ Green check mark if there are low-priority alerts or no alerts.

⚠️ Orange warning sign if there are medium-priority alerts.

❗️ Red warning sign if there are high-priority alerts.

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 adminstration 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 and Last name**: Enter the name of the user. Do not include a domain name.
   **Role**: Select a role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

   **Important**
   You can only see the Role option and assign administrator roles if you are a SuperAdmin.

   **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 (optional): 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.

Important
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.

For information on how policies work, see About Policies (page 425).

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 group(s) 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.

**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 knowledge base article 128136. Click the Details link beside the event and then allow the application, see **Allowed applications** (page 97).

**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.

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.

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 on the group’s name. For more information, see User Group Details (page 54).

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.
   Members: 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 (page 54).

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.
• 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 computers and computer groups.

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. For more information, see See 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 from Sophos Central. It also deletes 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.

**Note**
You can't uninstall Sophos Device Encryption on its own. Uninstall all products and then use custom installation to reinstall the products you want.
Export to CSV

To export a list of computers:

Click on 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 Devices 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. For more information, see Encryption Recovery Key Search (page 89).

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 on the other tabs on this page.

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

- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
- Red warning sign if there are high-priority alerts.

If there are alerts, you can click Show Status to see details.

Actions you can take

The actions links and buttons are in the left-hand pane.

- Isolate
  
  This isolates the computer from the network. See Isolate or remove from isolation (page 58).

- 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.

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 in 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.

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 (page 171).

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.

Endpoint 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.
• Agent Update Status: Shows whether the computer is up to date.
• Assigned Products: Shows the Sophos products are 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). **Change group** lets you add it to a group, move it to a different group, or remove it from its current group.

### Device Encryption summary

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.

**Note**

- 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 logon credentials. For more information, see [Retrieve recovery key](#) or [Retrieve recovery key (Macs)](#).

### 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 unless they have 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 **View Details** to manage the tamper protection password for the computer.

Update Cache and Message Relay status

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 status

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.

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:

- **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 [knowledge base article 128136](#).

Click the Details link beside the event and then allow the application, see **Allowed applications** (page 97).
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.

Computer Status
The Status tab in a computer's details page lets you see the computer's security status and details of any alerts. It also lets you take action against alerts.

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. See Alerts (page 4).
Activity

This shows whether the device is active or not and gives details of past activity.

**Computer Security Status**

**Note**
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).

**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.

**Computer Groups**

On the **Groups** tab of the **Computers** page, 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**

1. Click **Add Computer Group** in the upper right of the page.
2. Choose if you want to create a new group and click **Next**.
3. In the **Add Computer Group** dialog:
   - Enter a **Group name**.
   - Enter a **Group description**.
   - Select available computers and add them to the **Assigned Computers** list.
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.

4. Click Save.

Edit a group
To edit a group, click the group's name to open and edit the group details.

Move a group
You can move groups.
1. Select the group.
2. Click Move.
3. Click Save.

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.

Note
You can also delete a group at the group's details page. Click the group's name to open the details.

Computer Group Summary
This feature may not be available for all customers yet.
The Summary tab in a computer group’s details lets you:
• Add or remove computers.
• Delete the group.

Add or remove computers
To add or remove computers:
1. Click Edit in the left-hand pane.
2. In the Edit Computer Group dialog, use the picker arrows to add computers to the Assigned Computers list or remove them.
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.

3. Click **Save**.

**Delete the group**

To delete the group, click **Delete** in the left-hand pane.

Deleting a group will not delete its computers.

**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.

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.

### 3.6.2 Servers

On the **Servers** page, you can manage your servers and server groups.

**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 Address. Hover over the icon to see details of all IPv4 and IPv6 addresses.
- Operating System.

**Tip**

“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 particular health status, use the filters above the list.

**Tip**
The Sophos Security VMs filter displays instances of Sophos Security VM on a hypervisor.

Add a server

To add a server (i.e. 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.

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.
For more information, see Server Summary (page 65).

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.

Server Summary
The Summary tab in a server's details page lets you see server details and manage the server.

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 on 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.

- **Delete Server**: Deletes the server from Sophos Central. It also deletes the alerts associated with the server.

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

- **Update Now**: Updates the Sophos agent software on the 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 in 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.

Recent events

This lists recent events on the computer.

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

Summary

The summary shows these details:

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

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

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

- **Installed component versions**: Click this to see a full list of the Sophos components and their version numbers. This is only available for Windows servers.

- **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.

• **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.

• **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.

• **Tamper Protection**: This shows whether Tamper Protection (page 83) is enabled on the server or not. Click View Details 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 Status**

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.

---

**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 knowledge base article 128136.
Click the Details link beside the event and then allow the application, see Allowed applications (page 97).

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.

Server Status

The Status tab in a server’s details page lets you see the server’s security status and details of any alerts. It also lets you take action against alerts.
Activity
This shows whether the server is active or not and gives details of past activity.

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. See Alerts (page 4).

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. See Server Threat Protection Policy (page 321).

Note
Some automatic exclusions shown in the list might not work on servers running Windows Server 2003.

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 icons beside a policy name indicate the security settings (such as threat protection) included in the policy.

A gray icon indicates that this part of the policy does not apply to the computer. This happens if a higher-priority policy with settings for the same feature is applied to the server.

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

*Note*

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

**Server Groups**

On the **Groups** tab of the **Servers** 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. For more information, see Server Group Summary (page 71).

**Add a group**

1. Click **Add Server Group** in the upper right of the page.
2. In the **Add Server Group** dialog:
   - Enter a **Group name**.
   - Enter a **Group description**.
   - Select available servers and add them to the **Assigned Servers** list.

*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.

3. Click **Save**.
Edit a group

To edit a group, click the group's name to open and edit the group details. For more information, see Server Group Summary (page 71).

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.

Note

You can also delete a group at the group's details page. Click the group's name to open the details.

Server Group Summary

The Summary tab in a server group's details lets you:

• Add or remove servers.
• Delete the group.

Add or remove servers

To add or remove servers:

1. Click Edit in the left-hand pane.
2. In the Edit Server Group dialog, use the picker arrows to add servers to the Assigned Servers list or remove them.
   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.
3. Click Save.

Delete the group

To delete the group:

1. Click Delete in the left-hand pane.
2. In the Confirm Group Deletion pop-up, click Yes.
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.

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 groups from Active Directory to Sophos Central.

In Setting, 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.
- You can also configure settings for Azure Active Directory Synchronization.

Note
If you are using Office 365 you must use this option.

For instructions on setting up the utility, see **Set up synchronization with Active Directory** (page 73). For full details of how it works, see **About Active Directory synchronization** (page 73). Once you have set up synchronization you can review its status and other settings, see **Active Directory Sync Status** (page 72).

For instructions on configuring Azure Active Directory synchronization, see **Set up synchronization with Azure Active Directory** (page 75). Once you have set up synchronization you can review its status and other settings, see **Azure AD Sync Status** (page 75).

**Active Directory Sync Status**

In Settings, on the **Active Directory Sync Status** page, once you set up Active Directory synchronization, you can view:

**Status**

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Active Directory.
- The time of the last synchronization with Active Directory.
You can view Active Directory synchronization alerts on the Alerts page. You can view synchronization events on the Logs & Reports > Events page.

Sync Status

This shows the synchronization settings in Active Directory.

About Active Directory synchronization

Active Directory synchronization allows administrators to implement a service that maps users and 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 or groups.
- It supports automated, one-way synchronization from the Active Directory to Sophos Central. It does not support two-way synchronization between Sophos Central and Active Directory.
- For users imported from Active Directory:
  - You cannot modify their name, email, or Exchange login, or add or change or remove associated groups or logins managed by Active Directory.
  - You can add, change or remove groups or logins that are not managed by Active Directory.
- For groups imported from Active Directory:
  - You cannot modify their name.
  - You can add, change or remove groups or logins that are not managed by Active Directory.
- 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. Any information added or updated from the Active Directory cannot be edited in the console.
- 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 AD forest. We strongly recommend to synchronize different AD 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 deploying with Active Directory.

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.

To set up synchronization with Active Directory:

1. In Settings, on the Active Directory Sync page, click the link to download the Sophos Central AD Synchronization Utility installer, and then run it.
2. In the setup wizard, enter the information required.
   
   Follow the instructions in the Sophos Central AD Sync Utility Setup Wizard.
3. On the last page of the setup wizard, 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.

The Sophos Central AD Sync Utility Setup Wizard starts.

4. On the Sophos Credentials page, enter your Sophos Central account credentials.

5. 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, 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.

6. 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.

<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 &quot;base distinguished names&quot;). 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</td>
</tr>
</tbody>
</table>

   The above query will limit user discovery to users belonging to “testGroup”. Note that unless a group query filter is also specified, 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
Important
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.

7. 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.

8. 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 Sophos Central.
To stop the synchronization in progress, click Stop.

Set up synchronization with Azure Active Directory
Azure AD sync is only available if you have a Sophos Email license.
To configure Azure Active Directory synchronization:

1. In Settings, on the Active Directory Sync page, click the link to configure the settings for Azure AD Sync.
2. Set up your Azure Applications, if required.

Tip
Click the link to the instructions if you need help with this.

You can skip this step if you have already set up an Azure application.

3. Configure the Azure Sync Settings:
   a) Enter the Client ID.
   b) Set the Tenant Domain.
   c) Enter the Application Key and set its 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.
4. Click Test Connection to validate the Azure Sync connection.
5. Click Save.

Synchronization starts. This process may take some time.

Azure AD Sync Status
In Settings, on the Active Directory Sync Status page, once you configure Azure AD synchronization, you can view:
• The status of Azure AD synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
• The number of users and groups imported from Azure AD.
• The time of the last synchronization with Azure AD.

Note
Auto synchronization happens every 6 hours. You cannot change this interval.

• The configuration settings for Azure AD synchronization.
  You can amend these by clicking Edit, see Set up synchronization with Azure Active Directory (page 75).

Click Sync to run the synchronization process.
You can validate the Azure Sync connection by clicking Test Connection.
You can view Azure AD synchronization alerts on the Alerts page. You can view synchronization events on the Logs & Reports > Events page.

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.

Important
You can only see this option if you are a SuperAdmin 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.

Important
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. These roles cannot be edited or deleted.

Important
Your assigned administrator role affects what you can do.

Note
Anyone with a User role only has access to the Self Service Portal.

The available administration roles are:
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</table>
| **Super Admin** | Have access to everything in Sophos Central. In addition they can:  
• Manage roles and role assignments | There are no limitations. | None. |
|                 | Super Admin | There must be at least one administrator with a SuperAdmin role. |                           |                           |
| **Admin**       | Have access to everything in Sophos Central. | Manage roles and role assignments. | No Role Management options are displayed. |
| **Help Desk**   | Have read-only access for all settings in Sophos Central. In addition they can:  
• 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. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Resolve alerts on the individual device. | No Role Management options are displayed. In addition:  
• All other options apart from those related to receiving and clearing alerts are read-only.  
• Some options, such as Edit buttons, are not displayed. |
| **Read-only**   | Have read-only access for all settings in Sophos Central. In addition they can:  
• Look at sensitive logs or reports.  
• Receive alerts. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers. | No Role Management options are displayed. In addition:  
• All options are read-only.  
• Some options, such as Edit buttons, are not displayed. |
### Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details, see User Summary (page 48).

#### To 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.

1. Click Edit. This opens the Edit Role Members window.

   **Note**
   You can only see this option if you are a Super Admin administrator.

2. Select a user in the Available Users list and use the picker arrows to add them to the Assigned Users for the role.

   **Tip**
   Enter a name or part of a name in the search box to filter the list of available users.

**To delete 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.

1. Click Edit. This opens the Edit Role Members window.

   **Note**
   You can only see this option if you are a Super Admin administrator.

2. Remove assigned administrators from the role by selecting 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.

**Administration Roles for Intercept X with EDR**

For general information on Administration Roles, see Administration Roles (page 76).
The available administration roles for Intercept X with EDR are:
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can’t...</th>
</tr>
</thead>
</table>
| **Super Admin**  | • 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. | There are no limitations. |
|              |                                       |                                       |
| **Admin**     | • 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. | There are no limitations. |
|              |                                       |                                       |
| **Help Desk** | • View the intelligence report.  
• Request the intelligence report  
• View blocked items.  
• Request an on-demand threat case.  
• View on-demand threat cases.  
• Isolate and un-isolate devices.  
• Add items to the “Clean and Block” list.  
• Remove items from the “Clean and Block” list. |
Role | Administrators with this role can... | Administrators with this role can't...
--- | --- | ---
**Read-only** | • View the intelligence report. | • Request the intelligence report.  
• View blocked items. | • Add items to the “Clean and Block” list.  
• View on-demand threat cases. | • Remove items from the “Clean and Block” list.  
• View a saved threat search. | • Request an on-demand threat case.  
 |  | • Isolate and un-isolate devices.  
 |  | • Request a forensic snapshot.  
 |  | • Request a threat search.  

### 3.7.3 Federated sign-in

You must be a Super Admin to turn on federated sign-in for your administrators and users.

You can allow your administrators and users to sign in to Sophos Central and the SSP using their Microsoft sign-in credentials.

**Note**

When you turn on federated sign-in administrators and users can still sign in using their Sophos Central credentials.

**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.

**Note**

Sophos Central is not supported on mobile devices.

An Azure AD admin must give permission for Sophos Central to use federated sign in before you can turn it on. Once an admin gives consent, it means your Azure AD tenant trusts Sophos Central and administrators can sign in with their Microsoft credentials. See [https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience](https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience) for more information.

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 turn on federated sign-in:

1. Click **Federated sign-in** in **Settings**.
2. Click **Sign in with Sophos Central Admin or Microsoft credentials**.
3.7.4 Synchronized Security

Note
Synchronized Security is only available if you have a Sophos Endpoint license and a Sophos Email license.

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.

You can turn the Synchronized Security feature on and off from Global Settings > General > Synchronized Security.

• The originating mailbox is identified.
• The owner of the mailbox is identified, along with any devices assigned to the owner of the mailbox.
• The mailbox is blocked from sending emails for 1 hour. After 1 hour, the mailbox is unblocked automatically.

Important
The amount of time the mailbox is blocked for is doubled every time the spam threshold is reached. 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 mailbox should be unblocked, please contact Sophos Support.

• Sophos Anti-Virus runs an on-demand scan on the devices linked to the mailbox.
• An alert is sent to the administrator saying that the sender has been blocked.
• 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 Exploit Mitigation Exclusions

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

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.

In Settings, the Exploit Mitigation Exclusions page displays a list of applications excluded from protection against security exploits.

Note
These applications are excluded from exploit protection for all your users and their devices. You can only exclude applications that have been detected as a threat.
Important
Think carefully before you add exclusions because it reduces your protection.

To exclude an application:
1. Click Add Exclusion (on the right of the page). The Add Exploit Mitigation Exclusion dialog is displayed.
2. In the Application drop-down list, select the application you want to exclude. The names displayed here are the same as those shown in the Events Report.
3. Click Add or Add Another. The exclusion is added to the Excluded Applications list.
4. Click Save (on the right of the page) to save your changes to the list.

To delete an exclusion later, click on the ✗ to the right of the exclusion you wish to remove.

3.7.6 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 unless they have 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 select the Tamper Protection tab. 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.

For details, see Recover tamper protection passwords (page 42).
3.7.7 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 knowledgebase 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.

3.7.8 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.

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. Go to [https://www.sophos.com/en-us/threat-center/reassessment-request.aspx](https://www.sophos.com/en-us/threat-center/reassessment-request.aspx). 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 Control sites tagged in Website Management (page 185)

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 on the right of the entry.

To delete an entry, select the checkbox to the left of the entry and click **Delete**.

### 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 **System > System Services > Security Heartbeat**).

**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 **Deregister** 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 Global Exclusions

You can exclude files, websites and applications from scanning for threats, as described below.

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. See **Computer isolation (Windows)**.

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 on this page.
- To exclude certain applications from checking, use **Exploit Mitigation Exclusions** (page 82).

You set exclusions in **Settings**, on the **Global Exclusions** page.

**Note**
These exclusions will apply to all your users (and their devices) and servers. If you want them to apply only to certain users or servers, use the policy exclusions in the policies instead.

**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 from events.

**Important**
Think carefully before you add global exclusions because doing so may reduce your protection.

1. On the **Global Exclusions** page, 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, detected exploit or device isolation).
3. Specify the item or items you want to exclude. The following rules apply:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **File or folder (Windows)** | 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.** Examples:  
  - **Folder:** `C:\programdata\adobe\photoshop\` *(add a slash for a folder).*  
  - **Entire drive:** `D:`  
  - **File:** `C:\program files\program\*.vmg`  
  For more details, see [Windows Scanning Exclusions: Wildcards and Variables](#) (page 175). |
| **File or folder (Mac and Linux)** | You can exclude a folder or file. You can use the wildcards ? and *. Examples:  
  - `/Volumes/excluded` (Mac)  
  - `/mnt/hgfs/excluded` (Linux)  
  For more details, see [macOS Scanning Exclusions](#) (page 177) |
| **File or folder (Virtual Server)** | 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.  
  For more details, see [Virtual Server Scanning Exclusions: Wildcards](#) (page 330). |
| **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. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Website** | Websites can be specified as 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** | 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 and 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. |
| **Device isolation (Windows)** | 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 IP 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**.  
  - In **Local Port**, enter the port number.  
Example 2: |
### Option
### Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You want to be able to go to an isolated device and download cleanup tools from a server.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Outbound</strong>.</td>
</tr>
<tr>
<td></td>
<td>• In <strong>Remote IP address</strong>, enter the address of the server.</td>
</tr>
</tbody>
</table>

4. 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.

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**.

### 3.7.11 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 Manage Update Caches and Message Relays (page 95).

### 3.7.12 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 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 the Retrieve Recovery Key button.
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 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 the **Retrieve Recovery Key** button.

4. Enter at least five characters of the recovery key identifier.

5. Click the **Show key** button 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.

### 3.7.13 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 **Global Settings > HTTPS updating**.
2. Enable **HTTPS updating**.

### 3.7.14 Configure email alerts

You can manage how admins receive 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.
- 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 at 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.

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.
Set up a custom rule as follows:
1. Click Create new rule.
2. In Role, choose an administrator role that this rule will apply to. Click Next.
3. In Administrators and 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.
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.

### 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**.

**Note**

The **Hourly** and **Daily** options aren't a digest of all alerts generated in the specified time. Admins will get an email for each alert.

### 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.

### 3.7.15 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.

This means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos/Google Authenticator or email authentication to sign in.

This page tells you how to do the following:

- Set up multi-factor authentication.
• Sign in with multi-factor authentication for the first time.
• Sign in with email authentication (if you don't have Sophos/Google Authenticator).
• Reset an admin's sign-in details, for example if they lose their phone.

Set up multi-factor authentication

1. Go to Settings > Multi-factor authentication.
2. Choose how you want admins to sign in:
   • No MFA needed. This is the default.
   • All admins need MFA.
   • Select admins who will need MFA. This lets you select individual admins.
3. If you chose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). In the picker, move admins to the Assigned list and click Save.

When admins next try to sign in, they'll be prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

Here’s what to do the first time you sign in with MFA:
1. At the sign-in screen, enter your user ID (email address) and password.
2. A Set Up Your Login Information dialog explains that signing in needs additional authentication.
3. In the next dialog:
   • Enter the security code that has been sent to you in an email.
   • Create a 4-digit PIN. This enables you to use email as an authentication method.
4. In the next dialog, choose authentication type.
5. In Verify Your Device, scan the QR code and enter the security code that Sophos/Google Authenticator displays.

   Sophos Central opens.

The next time you sign in, you only need to enter a code from Sophos/Google Authenticator when prompted.

Sign in with email authentication

If you don't have access to Sophos/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/Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can let them set up their sign-in again.
1. Go to the Users page.
2. Find the user and click on their name to open their details.
3. 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.

3.7.16 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. Just set up your caches before installation.

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 (page 215).

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 particular 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 (page 215).

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 particular cache or relay.

Assign computers to a cache/relay

You can manually assign computers to use a particular cache or relay.

1. In Settings, go to the Manage Update Caches and Message Relays page.
2. Click on the link displaying the number of computers using the Update Cache or Message Relay.
3. Click on 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 on 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. Go to the **System Settings > 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**.

**3.7.17 Allowed applications**

At 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.
**Important**
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 knowledge base article 128136.

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).

3.7.18 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.
To control updates, go to Settings > Controlled Updates.
You have these options.

- Pause Updates Now (page 99)
- Pause Updates on a Set Date (page 99)
- Control Updates Manually (page 100)

Note
Computers still get automatic security updates to protect them against the latest threats.

Tip
You can go back to automatic updating at any time.

Pause Updates Now

You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.
On the Settings > Controlled Updates page, click on 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 resume product updates on all computers.
Automatic updates will stop for 90 days. Your computers will still get security updates.
1. On the Settings Controlled Updates page, click on Pause Updates on a Set Date.
2. On the Pause Updates on a Set Date page, select a Start date and a Resume Date. Click Apply.
On the Resume date, the computers will start updating automatically and get any updates that are available.

**Tip**
If you want to resume updating earlier, click **Resume Automatic Updating**.

### Control Updates Manually

You can control product updates manually. 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 on **Control Updates Manually**.

**Important**
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** 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.

**Test the new version**
In the Action column, next to Test Computers, click **Update test computers to newest version**.

**Roll out the new 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**.

**Why can I see a 'Previous' version now?**
If Sophos releases another product update when you already have test computers on **Newest** 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.

**3.7.19 Admin Isolated Devices**
At 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** (page 171).

You can isolate affected devices while you investigate a threat case, see **Threat Cases** (page 17). You can also search for other affected devices and isolate those from your threat search results, see **Threat Searches** (page 23).

You can allow isolated devices to communicate with other devices in limited circumstances, see **Global Exclusions** (page 86).
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**.

### 3.7.20 Amazon Web Services Accounts

In Settings, on the **Amazon Web Services 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 an AWS Account** dialog:
   a) Enter a **Friendly Account Name**. This will be used to refer to the account in Sophos Central.
   b) Enter **IAM user credential** (Access Key and Secret Key) for the AWS account that you want to connect.
   c) Select **Add**.

   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, please see these articles:
   - Creating an IAM User for Sophos Central
   - Troubleshooting Sophos Central connections to AWS

When you have added the AWS account:

- **AWS instances are listed on the AWS Instances page.** 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.**
3.7.21 Connect to Microsoft Azure

In Settings, on the Connect to Microsoft Azure 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 state 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 knowledge base article 127185.

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.

3.7.22 Data Loss Prevention Rules

You use Data Loss Prevention (DLP) rules to specify conditions for data loss prevention to detect, actions to be taken if the rules are matched, and any files to be excluded 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 List(s) in the rule to the specified destination.
  You use Content Control Lists to match file content. For more information about Content Control Lists (CCLs), see Content Control Lists (page 106).
- **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 Data Loss Prevention 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, see Create a Data Loss Prevention Rule (page 104), and search existing rules.

You can also filter rules by Type (choose from File or Content) and Source (choose from Custom or SophosLabs).

Click on the name of a rule to edit it.

Click to view details of a rule.

Click to clone a rule.

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.

Click to export custom rules. This creates an xml file containing the rule definition.

Click to delete a rule. 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.

Create a Data Loss Prevention Rule

There are two stages to creating a DLP rule; creation and configuration.

Creating a DLP rule

This 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 on 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**.

---

**Configuring a DLP rule**

This sets up the conditions for monitored files, file types or destinations and the exclusions for the rule.

The conditions you set depend on whether you are creating a **File** or **Content** rule.

1. To set up conditions for a content rule:
   a) Click on **File contains** and select the Content Control Lists you want to use.
      
      You can search the list of CCLs. You can filter the CCLs by **Tags**, **Source** (choose from **SophosLabs** or **Custom**) and **Region**. You can also create a new CCL, see Create Custom Content Control List (page 106).

      **Tip**
      Once the CCL has been matched for the set number of times it will trigger the rule.

   b) For each CCL: click on the matches and set the required number of matches.

2. To set up conditions for a file rule: Specify the file names or file types for the rule.

3. 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).

4. Set the exclusion details for the rule.

5. Click **Finish** to create the rule.
3.7.23 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 to 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. For more information on rules, see Data Loss Prevention Rules (page 103).

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 Content Control Lists in your rules, or create your own CCLs, see Create Custom Content Control List (page 106).

You can filter the CCLs by:

• Region
• Source (choose from SophosLabs or Custom)
• Type

You also can search the list of CCLs.

Click ☐ to view details of a CCL.

For each custom CCL you can also:

• Click on the name of a CCL to edit it.
• Click ☐ to export a CCL. This creates an XML file containing the definition for the CCL.
• Click ☐ to clone a CCL. 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.
• Click ✗ to delete a CCL. Click Delete item to confirm deletion.

You can also import Content Control Lists:

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

To create a custom Content Control List:

1. Click on Add Custom Content Control List.
2. Give the CCL a Name and a Description.
3. Click in 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 the text you want to match in Terms and click Add Term.
• All of these terms: Enter the Terms and click Add Term.
• Exactly this phrase: Enter the phrase you want to match in Phrase.
• Advanced Setup: Use this option to set up an Advanced Expression, as described below.

5. Click Save to create the CCL.

Set up an Advanced Expression

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 Content Control List is matched.

2. Enter a Perl 5 regular expression in Expression.
   For a description of Perl 5 regular expressions, refer to Perl documentation or visit http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html.

3. Set the Score for the CCL. This 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.

   Click to delete an expression.

   Click to edit an expression. Once you have finished your edit, click 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>
3.7.24 Inbound Allow/Block

The **Inbound Allow/Block** list is part of Email Security and this option is only available if you have a Sophos Email license.

Email Security provides protection against spam, spoofing, viruses and malware. Set up Email Security, if you have not already done so, see [Email Security Policy](#) (page 428).

- Allow/Block lists help you to control spam. You create a list of email domains and addresses that you trust or don't trust. This list is global and applies to all protected mailboxes.
- 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. See [Message History Report](#) (page 39) and [Quarantined Messages](#) (page 424).
- You can block or allow an entire domain or specific email addresses. The domain or email address is added to the list and shown as either allowed or blocked.
- This setting only applies to inbound messages.
- 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).

In Settings, on the **Email Security > Inbound Allow/Block** page you can:

- Add an allowed domain or address
- Add a blocked domain or address
- Remove a domain or address

### Add an allowed domain or address

To add an allowed domain or address:

1. Click on **Add** at the right side of the page above the **Inbound Allow/Block** list.
2. Select **Add Allow** from the drop-down list.
3. Enter a single domain name or email address in the **Email Address or Domain** text field.
   - Example: `example.com` or `jane.smith@example.com`.
4. Choose whether you want to **Override duplicates**.

   **Note**
   
   If you add the same address or domain to both the allow and block lists, **Override duplicates** uses the most recent option you chose.

5. Click **OK**.

   The allowed email address or domain is added to the **Inbound Allow/Block** list.

### Add a blocked domain or address

To add a blocked domain or address:
1. Click on Add at the right side of the page above the Inbound Allow/Block list.
2. Select Add Block from the drop-down list.
3. Enter a single domain name or email address in the Email Address or Domain text field. Example: example.com or jane.smith@example.com.
4. Choose whether you want to Override duplicates.

   Note
   If you add the same address or domain to both the allow and block lists, Override duplicates uses the most recent option you chose.

5. Click OK.
   The blocked email address or domain is added to the Inbound Allow/Block list.

Remove a domain or address

   To remove a domain or address:
   1. Select the entry you want to delete from the allow/block list.
   2. Click Delete at the right side of the page above the Inbound Allow/Block list.
   3. Click Yes to confirm deletion.

3.7.25 Manage settings for Sophos Central Self Service

   This option is only available if you have an Sophos Email license.
   Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Set up Email Security (page 111).
   In Settings, click Self Service Settings, 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.

3.7.26 Manage Domains

   Email Security is only available if you have a Sophos Email license.
   Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Email Security Policy (page 428).
   You configure and manage protected email domains on the Email Security > Settings > Domain Settings/Status page, using the options described below.
Add a domain

To add a domain:

1. Click **Add Domain** (on the right of the page).

   **Tip**
   
   Instructions on how to set up your domain for common providers are available. Example: Office 365.
   
   To view the instructions:
   
   a) Expand **Information to configure External Dependencies**.
   
   b) Click **Instructions for Common Providers**.
   
   c) Click **Inbound Settings** and click the link for your chosen provider.
   
   d) Use the information to help you configure your email domain.
   
   Click **Outbound Settings** to view your outbound relay host.

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**.

   **Note**
   
   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 **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 a FQDN (fully qualified domain name) in the **IP/FQDN** text field. Example: 111.111.111.111 or mymail@example.com.

b) If you selected **MX** enter a FQDN in the **FQDN** 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, see **Email Security Policy** (page 428).

    **Important**

    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:

1. Click on the ✗ to the right of the domain you wish to remove.

**Edit a domain**

To edit a domain:

1. Click on the domain name in the list, change the settings and click **Save**.

**Set up Email Security**

Email Security provides protection against spam, spoofing, viruses and advanced threats.

Email Security is only available if you have a Sophos Email license.

To use Email Security:

1. Ensure that the users and email addresses you want to protect have been added to Sophos Central. See the instructions in **Add email addresses** or **Add users and email addresses** below.

   **Tip**
   
   You can add an email address for a user or import a list of email addresses without using Active Directory Synchronization or Office 365, see **Mailboxes** (page 422).

2. Add your protected email domains, see **Settings** (page 437).

3. Configure spam protection in the email security policy, see **Email Security Policy** (page 428).
4. Set up global controls on spam using allow and block lists for senders, see Inbound Allow/Block (page 108).

Note
Users without an email address will not be protected. Email going to an email address not tied to a user will not be delivered.

Add email addresses

If you have existing users but no email addresses then you need to add the email information. You can do this by updating your Active Directory synchronization and then adding your email domains. To do this:

1. In Settings, on the Email Security > Settings page, click the link to configure email connection settings.
2. Click the link in the Email Security Setup dialog to download the latest version of the AD sync tool and re-sync your users. See Set up synchronization with Active Directory (page 73).
3. You can then add your email domains by clicking Continue.

Add users and email addresses

If you are a new customer with no users or mailboxes set up you need to add users and mailboxes. To do this:

1. In Settings, on the Email Security > Settings page, click the link to configure email connection settings.
   The Email Security Setup dialog is displayed.
2. To add users and mailboxes (as a new customer) you can either use the AD sync tool or you can import mailboxes. Click the appropriate link.
   • Download our Ad Sync tool and synchronize your users and their email addresses.
   • Use Mailbox Import to import your users and their email addresses.

   Note
   If you are using Office 365 you must use this option.

3. To import mailboxes:
   a) In the Mailbox Import dialog click a link to download a template CSV file. You can choose from a blank template or one with example data.
   b) Create your import mailbox data in the correct format and save it. You can now import the mailboxes.
   c) Click Browse, select your CSV file and click Open.
   d) Click Import.

   Note
   The maximum file size is 1 MB.
The file is imported and the number of successfully imported mailboxes is shown together with any failures. Mailboxes that have not been imported are indicated by the line number in the .CSV file and a reason, for example duplicate entry. You can download a list of mailboxes that failed to import by clicking the link. You can also view the details of failed imports by clicking "View failed lines". These options are not shown if there are no failures.

Note
If you use active directory synchronization, this overrides any changes you make by importing a CSV file. You should only make changes using a CSV file if you don't use active directory synchronization.

4. Click Continue.
5. Add your email domains, see Settings (page 437).

3.7.27 Email Encryption

This feature is only available with an Email Advanced license.

The encryption type Sophos Email uses is push based email encryption using AES 265.

To turn encryption on or off, go to Email Gateway > 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 https://wiki.openssl.org/index.php/FIPS_mode_and_TLS.

General Settings

**Attention**
- 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.

• 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.

Important
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 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.
- Wildcards are not supported.

3.7.28 Time of Click Block/Warn Pages

Time of Click URL Protection is only available with an Email Advanced license.

To manage Time of Click URL Protection settings for suspicious sites, go to Email Gateway > Settings > Time of Click Block/Warn Pages.

Turn on Custom Block and 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.

3.8 Protect Devices

At 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.

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:

- Endpoint Protection (page 116)
- Encryption (page 117)
- Server Protection (page 117)
- Server Protection on Microsoft Azure (page 117)
- Virtual Environment Protection (page 118)
- Web Gateway (page 118)
- Firewall Protection (page 119)

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.
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 Endpoint Protection > 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:
  
  — Intercept X (protection from ransomware and exploits).
  — Endpoint Protection (protection from malware).
  — 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 user names 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, e.g., 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 Sophos Knowledgebase Article 119265.
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 the Sophos Central Device Encryption administrator guide.

Download and run installer

Go to Device Encryption > Protect Devices.

Download an 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:
  
  — Intercept X (protection from ransomware and exploits).
  
  — Endpoint Protection (protection from malware).
  
  — 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.

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.

Download the installer for your server operating system and run it on a server you want to protect.

When you protect a server:

- The server is added to the Servers list in Sophos Central.

- Default policies are applied to the server.

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 Server Protection > 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.

Follow the steps in the article to deploy the new VM.

### 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 **Server Protection > 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.

**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 Web Gateway > 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 user name.
• 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 Web Gateway > Protect Devices.
Click on 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 Sophos knowledge base article 133040.
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.

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.

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.

Endpoint and server web control

Endpoint and server 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 Alerts

Some features might not be available for all customers yet.

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

Note

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.
For advice on what to do, see How to deal with threats (page 11).

Note
If you have Intercept X Advanced with EDR you can investigate, block and clean up threats from Threat Cases, see Threat Cases (page 17).

Group alerts
You can group together all alerts for a particular 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 particular priority, click the figures for High alerts, Medium alerts or Low alerts at the top of the page.
To view alerts for a particular 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 fold-out arrow next to an alert to open its details.
In Action, click an action button (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. See Allowed applications (page 97).

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 Ransomware**: 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 (page 559). This action becomes available when you might need help, for example when malware cleanup fails.
- **Cleanup PUA(s)**: 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, see Alerts for Threat Protection (page 6).
- **Authorize PUA(s)**: 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 a particular 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. See Configure email alerts (page 91).

### Related concepts

- Alerts for Threat Protection (page 6)
- Alerts for Installation, Updating and Compliance (page 9)
- Events Report (page 26)
- Configure email alerts (page 91)
- Get additional help (page 559)

### 4.2.1 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.

For more information, see Knowledgebase Article 132029.

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.

4.2.2 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. For information on these, see knowledge base article 127331.

High

**Real-time protection disabled**

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 (page 4).

- 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(s) 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 in 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 my computer option in Sophos Endpoint Security and Control 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.

### 4.2.3 How to deal with threats

For advice on dealing with threats, see:

- Deal with ransomware (page 11).
- Deal with exploits (page 12).
- Deal with web browser attacks (page 13).
- Deal with malware detected by deep learning (page 13).
- Deal with application lockdown events (page 14).
- Deal with false positives (page 14).

For advice on malware, see the sections on malware alerts listed in 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 (page 14).

**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.
  For help with sample submission, see our knowledge base article.
- 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 (page 4).
- 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.

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 (page 14).

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 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.

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 Allow an application that's been detected (page 98).

**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.

For details, see these topics:
• Stop detecting an application (page 14)
• Stop detecting an exploit (page 15)
• Stop detecting ransomware (page 16)

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.

### 4.3 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** (page 25).

To find out how reports work and how you can customize, save and schedule them, see **Reports** (page 41).

#### 4.3.1 Logs

The following logs are available for Endpoint Protection:

- **Events**. All events on your devices, see **Events Report** (page 26).
  - **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** (page 37).

- **Data Loss Prevention Events Log**. All events triggered by data loss prevention rules for computers or servers, see **Data Loss Prevention Events Log** (page 38).

To find out how reports work and how you can customize, save and schedule them, see **Reports** (page 41).

**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** (page 27).

For advice on what to do about threats, see **How to deal with threats** (page 11).

**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-AJWL"), 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.

**Date range:** Use the **From** and **To** fields to select the time period for 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 Report:** 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
- **When:** 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
- **Device:** Device that caused the event

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.

### 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. For more information, see **Alerts** (page 4).

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 &quot;Running malware cleaned up&quot; event will be added to the Events list.</td>
</tr>
</tbody>
</table>
| Running malware not cleaned up | High     | Yes             | 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:  
  - Running malware requires manual cleanup.  
  - Computer scan required to complete running malware cleanup.  
  - Reboot required to complete running malware cleanup.  
  - Running malware not cleaned up. |
<p>| Running malware cleaned up | Low      | No              |                                                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 alert 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 unauthorised 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 detected</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>
## Application control

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

## Malware

If you have deep learning enabled, you may see malware detections shown as ML/PE-A. You can find more information about these in knowledge base article 127331.

<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>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>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>Recurring infection</td>
<td>High</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>Threat removed</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Malware alert locally cleared</td>
<td>Low</td>
<td>No</td>
<td>A malware alert has been cleared from the alerts list on an endpoint 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>
<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) alert 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>

Updating

<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>
</tbody>
</table>
### Sophos Central Admin

**Event type** | **Severity** | **Action required?**
--- | --- | ---
Reboot recommended | Low | No
Reboot required | Medium | Yes

### Protection

<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>
<tr>
<td>Failed to protect computer or server</td>
<td>High</td>
<td>Yes</td>
<td>A computer has started installation of the agent software but has not become protected for one hour.</td>
</tr>
<tr>
<td>Error reported</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Scan completion</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New logins added</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New users added automatically</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Peripherals

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

For more information, see Knowledgebase Article 132029.

**ADSync**

<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. For more information, see Knowledgebase Article 121319.
### Sophos Central Admin

<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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>
</tbody>
</table>

Copyright © Sophos Limited 141
<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Encryption failed</td>
<td>Medium</td>
<td>See Note</td>
<td>A volume could not be encrypted.</td>
</tr>
<tr>
<td>Encryption info</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>Device not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Device Encryption status changed from ... to ...</td>
<td>Low</td>
<td>See Note</td>
<td>The Device Encryption status changed from one status to another status. See Computers (page 55).</td>
</tr>
<tr>
<td>Device Encryption is suspended</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key received</td>
<td>Low</td>
<td>See Note</td>
<td>Sophos Central received a recovery key from an endpoint computer.</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>Recovery key revoked</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 file 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 file 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.

**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 the activity or change was carried out.

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

**Date range**: Use the **From** and **To** fields to select the time period for which you want to view events. You can view events that occurred in the past 90 days or less.

**Rule Name**: You can filter the events by rule name.

**File type**: You can filter the events by file type.
**Update Report:** 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:** Name of the destination that caused the event

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.

**4.3.2 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**.

**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 Details**.
   This shows you the password (and previous passwords).

### 4.4 People

On the **People** page, you can manage your users and user groups.
4.4.1 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 sections below tell you about the users list and how to manage users.

About the users list

The current users are listed with their details:

- Security status. An icon shows whether the user has security alerts on any of their devices:
  - Green check mark if there are low-priority alerts or no alerts.
  - Amber warning sign if there are medium-priority alerts.
  - Red warning sign if there are critical alerts.

  Click on 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, see Administration Roles (page 76).
  
  This column is only visible if you are an administrator.

Click on 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 on the user’s name. For more information, see User Summary (page 48).

Add a user manually

This also gives you the option to let the user protect their own devices.

You can add an individual user and protect them as follows.

1. On the Users page, click Add and select Add User.
2. In the Add User dialog, enter the following settings:
   - First and Last Name. Enter the name of the user. Do not include a domain name.
   - Role. Select an administration role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

A user who is assigned an administration role will receive an email telling them how to set up their administration account.
Important
You can only see the Role option and assign administrator roles if you are a SuperAdmin.

Note
Anyone with a User role only has access to the Self Service Portal.

Email Address. Enter the email address of the user.

Add to Groups (optional). Select one of the available user groups and use the picker arrows to move it to the assigned groups.

Tip
You can start typing a name in the search box to filter the displayed 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.

3. Click Save or Save & 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 by protecting their devices

You can add users automatically as follows.

Download an installer and run it yourself on a device (or devices). This adds the user of each device automatically. For installers, see the Protect Devices page.

Import users from a CSV file

This option may not be available for all customers yet.

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 do this:

1. On the Users page, click Add and select Import users from CSV.
2. Click Browse and select your CSV file.

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

3. The CSV file can include groups a user is assigned to. To create groups not available yet, select Create new groups.
4. To send a registration email for the Sophos Central Self Service portal to each imported user, select **Activate new users**.

5. 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.

On the Users page, click the **Set up Active Directory Sync** link in the upper right of the page. Then see Set up synchronization with Active Directory (page 73).

### Protect existing users

To email users you have already added to the list or imported:

1. On the Users page, select the user or users you want to protect. Click **Email Setup Link** in the upper right of the page.

2. In the Email Setup Link dialog, you are prompted to select the types of protection the user needs (if your license includes more than one).

   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.

### Modify users

To modify a user's account:

On the Users page, click the user's name to open and edit their user details. For more information, see User Summary (page 48).

### Delete users

To delete a user or users:
On the **Users** page, select the checkbox next to each user you want to delete. Click the **Delete** button in the upper right of the page.

**Important**
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them, see **Administration Roles** (page 76).

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

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

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 will be added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they will be added as a user again the next time that Sophos Central synchronizes with Active Directory.

**Export to CSV**

To export a list of users:

Click on **Export to CSV**.

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

For example you can export a list of administrators by applying the **Admins Only** filter before clicking **Export to CSV**.

**Related concepts**
Active Directory Sync (page 72)

**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**.
Security status

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

- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
- Red warning sign if there are high-priority alerts.

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 and Last name**: Enter the name of the user. Do not include a domain name.
   - **Role**: Select a role for the user. Choose from: **SuperAdmin**, **Admin**, **Help Desk**, **Read-only** or **User**. For help on the administration roles, see *Administration Roles* (page 76).

   **Important**
   
   You can only see the **Role** option and assign administrator roles if you are a **SuperAdmin**.

   **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 (optional): 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.

Important
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.

For information on how policies work, see About Policies (page 425).

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 group(s) 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.

**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 knowledge base article 128136.

Click the Details link beside the event and then allow the application, see *Allowed applications* (page 97).

*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.

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.

4.4.2 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 on the group’s name. For more information, see User Group Details (page 54).

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.
   Members: 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 (page 54).

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.
• 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.

4.5 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).
- Device Encryption. This shows the encryption status. For more information, see See 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 from Sophos Central. It also deletes 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.

**Note**
You can’t uninstall Sophos Device Encryption on its own. Uninstall all products and then use custom installation to reinstall the products you want.

### Export to CSV

To export a list of computers:

Click on **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 **Devices** 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. For more information, see Encryption Recovery Key Search (page 89).

### 4.5.1 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 on the other tabs on this page.

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

- ![Green check mark](image) Green check mark if there are low-priority alerts or no alerts.
- ![Orange warning sign](image) Orange warning sign if there are medium-priority alerts.
- ![Red warning sign](image) Red warning sign if there are high-priority alerts.

If there are alerts, you can click **Show Status** to see details.

Actions you can take

The actions links and buttons are in the left-hand pane.

**Isolate**
This isolates the computer from the network. See Isolate or remove from isolation (page 58).

**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.

**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 in 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.

**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 (page 171).

### 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.

### Endpoint 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.
- **Agent Update Status**: Shows whether the computer is up to date.
- **Assigned Products**: Shows the Sophos products are 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). **Change group** lets you add it to a group, move it to a different group, or remove it from its current group.

### Device Encryption summary

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.

**Note**
- 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 logon credentials. For more information, see Retrieve recovery key (page 57) or Retrieve recovery key (Macs) (page 90).

**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 unless they have 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 **View Details** to manage the tamper protection password for the computer.

**Update Cache and Message Relay status**
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 status

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.

4.5.2 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:

- **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 knowledge base article 128136.

Click the Details link beside the event and then allow the application, see Allowed applications (page 97).

**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.

### 4.5.3 Computer Status

The **Status** tab in a computer's details page lets you see the computer's security status and details of any alerts. It also lets you take action against alerts.

**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. See **Alerts** (page 4).

**Activity**

This shows whether the device is active or not and gives details of past activity.

**Computer Security Status**

**Note**

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).

### 4.5.4 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.

## 4.6 Computer Groups

On the **Groups** tab of the **Computers** page, 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

1. Click **Add Computer Group** in the upper right of the page.
2. Choose if you want to create a new group and click **Next**.
3. In the **Add Computer Group** dialog:
   - Enter a **Group name**.
   - Enter a **Group description**.
   - Select available computers and add them to the **Assigned Computers** list.

   **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.

4. Click **Save**.

### Edit a group

To edit a group, click the group's name to open and edit the group details.

### Move a group

You can move groups.
1. Select the group.
2. Click **Move**.
3. Click **Save**.

### 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.

**Note**

You can also delete a group at the group's details page. Click the group's name to open the details.

### 4.6.1 Computer Group Summary

**This feature may not be available for all customers yet.**

The **Summary** tab in a computer group's details lets you:

- Add or remove computers.
- Delete the group.

### Add or remove computers

To add or remove computers:

1. Click **Edit** in the left-hand pane.
2. In the **Edit Computer Group** dialog, use the picker arrows to add computers to the **Assigned Computers** list or remove them.
   
   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.
3. Click **Save**.

### Delete the group

To delete the group, click **Delete** in the left-hand pane.

Deleting a group will not delete its computers.

### 4.6.2 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.

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.

4.7 Policies

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).

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.

4.7.1 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 particular 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.

4.7.2 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. 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.

4.7.3 Threat Protection Policy

Attention
This help page describes policy settings for workstation users. Different policy settings apply for servers.

Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.

To set it up:
• Create a Threat Protection policy. See Create or Edit a Policy (page 168).
• 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
Sophos Labs 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.

Important
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, and denies access unless 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. For more information, see Knowledgebase Article 121319. You can specify:
  - The **Action to take:** 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:** 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
Automatic cleanup doesn't apply to PE (Portable Executable) files, like applications, libraries and system files. 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. See Threat Cases (page 17).
- **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. See Threat Searches (page 23).

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**: 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.
- **Detect network traffic 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).
- **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.

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.

  **Note**
  Scanning archives 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 System Settings > Global Exclusions page.

To create a policy scanning exclusion:

1. Click **Add Exclusion** (on the right of the page).

   The Add Policy 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. The following rules apply:
<table>
<thead>
<tr>
<th>Feature</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. Examples:</td>
</tr>
<tr>
<td></td>
<td>• Folder: <code>C:\programdata\adobe\photoshop</code> \ (add a slash for a folder).</td>
</tr>
<tr>
<td></td>
<td>• Entire drive: <code>D:</code></td>
</tr>
<tr>
<td></td>
<td>• File: <code>C:\program files\program\*.vmg</code></td>
</tr>
<tr>
<td></td>
<td>For more details, see <em>Windows Scanning Exclusions: Wildcards and Variables</em> (page 175).</td>
</tr>
<tr>
<td>File or folder (Mac and Linux)</td>
<td>You can exclude a folder or file. You can use the wildcards ? and *. Examples:</td>
</tr>
<tr>
<td></td>
<td>• <code>/Volumes/excluded</code> (Mac)</td>
</tr>
<tr>
<td></td>
<td>• <code>/mnt/hgfs/excluded</code> (Linux)</td>
</tr>
<tr>
<td></td>
<td>For more details, see <em>macOS Scanning Exclusions</em> (page 177).</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, not the process name shown in Task Manager. For example: <code>%PROGRAMFILES%\Microsoft Office\Office 14\Outlook.exe</code>.</td>
</tr>
<tr>
<td>Website</td>
<td>Websites can be specified as an IP address, IP address range (in CIDR notation), or domain. Examples:</td>
</tr>
<tr>
<td></td>
<td>• IP address: 192.168.0.1</td>
</tr>
<tr>
<td></td>
<td>• IP address range: 192.168.0.0/24</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Domain: google.com</td>
</tr>
<tr>
<td>Potentially Unwanted Application</td>
<td>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 <em>Sophos Threat Center</em>.</td>
</tr>
<tr>
<td>Detected Exploits (Windows and 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>
</tbody>
</table>
Device isolation (Windows)

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 IP 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**.
- 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**.
- In **Remote IP 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

**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.
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.

**Important**
Think carefully before you add scanning exclusions because doing so may reduce your protection.

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>
</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 |
<p>| \ (Backslash) | Either \ or /                                |                                                                          |
| / (Forward slash) | Either / or \                               |                                                                          |
| ? (Question mark) | One single character, unless at the end of a string where it can match zero characters. |                                                                          |</p>
<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
</table>
| . (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." |

**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><strong>\foo</strong></td>
<td>Exclude any file named foo (in any location).</td>
</tr>
<tr>
<td>foo\bar</td>
<td><strong>\foo\bar</strong></td>
<td>Exclude any file named bar in a folder named foo (in any location).</td>
</tr>
<tr>
<td>*.txt</td>
<td><strong>*.txt</strong></td>
<td>Exclude all files named *.txt (in any location).</td>
</tr>
<tr>
<td>C:</td>
<td>C:</td>
<td>Exclude drive C: from scanning (including the drive's master boot record).</td>
</tr>
<tr>
<td>C:\</td>
<td>C:\</td>
<td>Exclude all files on drive C: from scanning (but scan the drive's master boot record).</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>
<th>Windows Server 2008 and later</th>
<th>Windows Server 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>%allusersprofile%</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
macOS Scanning Exclusions

This help page describes policy settings for macOS workstations.

When you add or edit an exclusion, you can type any POSIX path, whether it is a volume, folder, or file.

**Important**
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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Windows 7 and later</th>
<th>Windows 7 and later</th>
<th>Windows XP</th>
<th>Windows XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>appdata%</td>
<td>%appdata%</td>
<td>%appdata%</td>
<td>%appdata%</td>
<td>%appdata%</td>
</tr>
<tr>
<td></td>
<td>C:\Users*\AppData\Roaming</td>
<td>C:\Documents and Settings*\Application Data</td>
<td>C:\Documents and Settings*\Application Data</td>
<td>C:\Documents and Settings*\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>commonprogramfiles%</td>
<td>%commonprogramfiles%</td>
<td>%commonprogramfiles%</td>
<td>%commonprogramfiles%</td>
<td>%commonprogramfiles%</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Common Files</td>
<td>C:\Program Files\Common Files</td>
<td>C:\Program Files\Common Files</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>commonprogramfiles(x86)%</td>
<td>%commonprogramfiles(x86)%</td>
<td>%commonprogramfiles(x86)%</td>
<td>%commonprogramfiles(x86)%</td>
<td>%commonprogramfiles(x86)%</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files (x86)\Common Files</td>
<td>C:\Program Files (x86)\Common Files</td>
<td>C:\Program Files (x86)\Common Files</td>
<td>C:\Program Files (x86)\Common Files</td>
</tr>
<tr>
<td>localappdata%</td>
<td>%localappdata%</td>
<td>%localappdata%</td>
<td>%localappdata%</td>
<td>%localappdata%</td>
</tr>
<tr>
<td></td>
<td>C:\Users*\AppData\Local</td>
<td>C:\Documents and Settings*\Local Settings\Application Data</td>
<td>C:\Documents and Settings*\Local Settings\Application Data</td>
<td>C:\Documents and Settings*\Local Settings\Application Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>programdata%</td>
<td>%programdata%</td>
<td>%programdata%</td>
<td>%programdata%</td>
<td>%programdata%</td>
</tr>
<tr>
<td></td>
<td>C:\ProgramData</td>
<td>C:\ProgramData</td>
<td>C:\ProgramData</td>
<td>C:\ProgramData</td>
</tr>
<tr>
<td>programfiles%</td>
<td>%programfiles%</td>
<td>%programfiles%</td>
<td>%programfiles%</td>
<td>%programfiles%</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files</td>
<td>C:\Program Files</td>
<td>C:\Program Files</td>
<td>C:\Program Files</td>
</tr>
<tr>
<td>programfiles(x86)%</td>
<td>%programfiles(x86)%</td>
<td>%programfiles(x86)%</td>
<td>%programfiles(x86)%</td>
<td>%programfiles(x86)%</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files (x86)</td>
<td>C:\Program Files (x86)</td>
<td>C:\Program Files (x86)</td>
<td>C:\Program Files (x86)</td>
</tr>
<tr>
<td>systemdrive%</td>
<td>%systemdrive%</td>
<td>%systemdrive%</td>
<td>%systemdrive%</td>
<td>%systemdrive%</td>
</tr>
<tr>
<td></td>
<td>C:\</td>
<td>C:\</td>
<td>C:\</td>
<td>C:\</td>
</tr>
<tr>
<td>systemroot%</td>
<td>%systemroot%</td>
<td>%systemroot%</td>
<td>%systemroot%</td>
<td>%systemroot%</td>
</tr>
<tr>
<td></td>
<td>C:\Windows</td>
<td>C:\Windows</td>
<td>C:\Windows</td>
<td>C:\Windows</td>
</tr>
<tr>
<td>temp% or %tmp%</td>
<td>%temp% or %tmp%</td>
<td>%temp% or %tmp%</td>
<td>%temp% or %tmp%</td>
<td>%temp% or %tmp%</td>
</tr>
<tr>
<td></td>
<td>C:\Users*\AppData\Local \Temp</td>
<td>C:\Documents and Settings*\Local Settings\Temp</td>
<td>C:\Documents and Settings*\Local Settings\Temp</td>
<td>C:\Documents and Settings*\Local Settings\Temp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Does not work for real-time scanning.</td>
<td>Does not work for real-time scanning.</td>
</tr>
<tr>
<td>userprofile%</td>
<td>%userprofile%</td>
<td>%userprofile%</td>
<td>%userprofile%</td>
<td>%userprofile%</td>
</tr>
<tr>
<td></td>
<td>C:\Users*</td>
<td>C:\Documents and Settings*</td>
<td>C:\Documents and Settings*</td>
<td>C:\Documents and Settings*</td>
</tr>
<tr>
<td>windir%</td>
<td>%windir%</td>
<td>%windir%</td>
<td>%windir%</td>
<td>%windir%</td>
</tr>
<tr>
<td></td>
<td>C:\Windows</td>
<td>C:\Windows</td>
<td>C:\Windows</td>
<td>C:\Windows</td>
</tr>
</tbody>
</table>
### Table 1: 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 <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>&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>

### Table 2: 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>
<tr>
<td>myapplication</td>
<td>The file myapplication anywhere locally or on the network</td>
</tr>
<tr>
<td><em>.</em>.mov</td>
<td>All files whose filename extension is .mov anywhere locally or on the network</td>
</tr>
<tr>
<td>/myfolder/*.mov</td>
<td>All files whose filename extension is .mov in a specific location</td>
</tr>
</tbody>
</table>
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>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>

For details of other threat protection options, see Threat Protection Policy (page 169).

4.7.4 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.

To set it up:

• Create an Peripheral Control policy. See Create or Edit a Policy (page 168).
• 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'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.

**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.

**4.7.5 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* (page 168).
- Open the policy's **Settings** tab and configure it 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 Plugin**.
   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 Application Control settings.

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 **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.

    **Important**
    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 applications**.

    **Remember**
    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.

4.7.6 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 (page 103). 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 (page 425).

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 an Data Loss Prevention policy. See Create or Edit a Policy (page 168).
- Open the policy's Settings tab and configure it as described below. Make sure the policy 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.
   - To create a custom policy, click Create Custom Policy and click Add New Rule. Choose whether you want to use existing rule or create a new rule, see Create a Data Loss Prevention Rule (page 104). Select the rules you want to add and click Save Selection.

2. Click on the fields in the Messages area to add your own message to the standard confirmation and block notifications. Each message can have a maximum of 100 characters.

   Note
   You can switch 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 Save.
4.7.7 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 (page 168).
• 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 web sites.
• 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 Custom. Choosing Custom allows you to configure individual categories within these groups.

  **Note**
  For more control over how policy affects web sites you can use the System Settings > Website Management page.

---

**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.

---

**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.
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.

4.7.8 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 a **Updating** policy. See **Create or Edit a Policy** (page 168).
- 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.

Remember that if computers aren't on, they won't get the update until they are next on at the scheduled update time.

4.7.9 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.

**Important**
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 (page 168).
- 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 and 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**

**4.8 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 be displayed under **Global Settings** in **Overview**, if you have more than one product.

**Note**
If you want to apply settings only to certain users, servers or devices, use the Policies pages instead.

**4.8.1 Active Directory Sync**

You can import users and groups from Active Directory to Sophos Central.
In Setting, 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.
- You can also configure settings for Azure Active Directory Synchronization.

**Note**

If you are using Office 365 you must use this option.

For instructions on setting up the utility, see Set up synchronization with Active Directory (page 73). For full details of how it works, see About Active Directory synchronization (page 73). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 72).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 75). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 75).

### Active Directory Sync Status

In Settings, on the **Active Directory Sync Status** page, once you set up Active Directory synchronization, you can view:

**Status**

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Active Directory.
- The time of the last synchronization with Active Directory.

You can view Active Directory synchronization alerts on the **Alerts** page. You can view synchronization events on the **Logs & Reports > Events** page.

**Sync Status**

This shows the synchronization settings in Active Directory.

**About Active Directory synchronization**

Active Directory synchronization allows administrators to implement a service that maps users and 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 or groups.
- It supports automated, one-way synchronization from the Active Directory to Sophos Central. It does not support two-way synchronization between Sophos Central and Active Directory.
- For users imported from Active Directory:
  - You cannot modify their name, email, or Exchange login, or add or change or remove associated groups or logins managed by Active Directory.
  - You can add, change or remove groups or logins that are not managed by Active Directory.
• For groups imported from Active Directory:
  — You cannot modify their name.
  — You can add, change or remove groups or logins that are not managed by Active Directory.
• 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. Any information added or updated from the Active Directory cannot be edited in the console.
• 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 AD forest. We strongly recommend to synchronize different AD 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 deploying with Active Directory.

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.

To set up synchronization with Active Directory:

1. In Settings, on the Active Directory Sync page, click the link to download the Sophos Central AD Synchronization Utility installer, and then run it.
2. In the setup wizard, enter the information required.
   Follow the instructions in the Sophos Central AD Sync Utility Setup Wizard.
3. On the last page of the setup wizard, 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.
   The Sophos Central AD Sync Utility Setup Wizard starts.
4. On the Sophos Credentials page, enter your Sophos Central account credentials.
5. 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, 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.
6. 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.
### 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:

```
OU=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 will limit user discovery to users belonging to "testGroup". Note that unless a group query filter is also specified, 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
```

**Important**
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.

7. 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**.

8. 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 Sophos Central.

   To stop the synchronization in progress, click **Stop**.

### Azure AD Sync Status
In Settings, on the **Active Directory Sync Status** page, once you configure Azure AD synchronization, you can view:
- The status of Azure AD synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Azure AD.
- The time of the last synchronization with Azure AD.

**Note**
Auto synchronization happens every 6 hours. You cannot change this interval.

- The configuration settings for Azure AD synchronization.
  You can amend these by clicking **Edit**, see [Set up synchronization with Azure Active Directory](#) (page 75).

Click **Sync** to run the synchronization process.

You can validate the Azure Sync connection by clicking **Test Connection**.

You can view Azure AD synchronization alerts on the **Alerts** page. You can view synchronization events on the **Logs & Reports > Events** page.

**Set up synchronization with Azure Active Directory**

Azure AD sync is only available if you have a Sophos Email license.

To configure Azure Active Directory synchronization:

1. In Settings, on the **Active Directory Sync** page, click the link to configure the settings for Azure AD Sync.
2. Set up your Azure Applications, if required.

   **Tip**
   Click the link to the instructions if you need help with this.

You can skip this step if you have already set up an Azure application.

3. Configure the Azure Sync Settings:
   a) Enter the **Client ID**.
   b) Set the **Tenant Domain**.
   c) Enter the **Application Key** and set its 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.
4. Click **Test Connection** to validate the Azure Sync connection.
5. Click **Save**.
   Synchronization starts. This process may take some time.

**4.8.2 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.
Important
You can only see this option if you are a **SuperAdmin** 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.

Important
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. These roles cannot be edited or deleted.

**Important**
Your assigned administrator role affects what you can do.

**Note**
Anyone with a **User** role only has access to the Self Service Portal.

The available administration roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</table>
| **Super Admin**  
There must be at least one administrator with a SuperAdmin role.  
In addition they can:  
• Manage roles and role assignments | Have access to everything in Sophos Central. | There are no limitations. | None. |
| **Admin**  
Have access to everything in Sophos Central.  
Manage roles and role assignments. | | No Role Management options are displayed. | |
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>Have read-only access for all settings in Sophos Central. In addition they can:</td>
<td>Manage roles and role assignments. In addition they can't:</td>
<td>No Role Management options are displayed. In addition:</td>
</tr>
<tr>
<td></td>
<td>• Look at sensitive logs or reports.</td>
<td>• Assign policies.</td>
<td>• All other options apart from those related to receiving and clearing alerts are read-only.</td>
</tr>
<tr>
<td></td>
<td>• Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.</td>
<td>• Change settings.</td>
<td>• Some options, such as Edit buttons, are not displayed.</td>
</tr>
<tr>
<td></td>
<td>• Update the Sophos agent software on a computer.</td>
<td>• Resolve alerts on the individual device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scan computers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read-only</td>
<td>Have read-only access for all settings in Sophos Central. In addition they can:</td>
<td>Manage roles and role assignments. In addition they can't:</td>
<td>No Role Management options are displayed. In addition:</td>
</tr>
<tr>
<td></td>
<td>• Look at sensitive logs or reports.</td>
<td>• Assign policies.</td>
<td>• All other options are read-only.</td>
</tr>
<tr>
<td></td>
<td>• Receive alerts.</td>
<td>• Change settings.</td>
<td>• Some options, such as Edit buttons, are not displayed.</td>
</tr>
<tr>
<td>User</td>
<td>Have no administration capabilities.</td>
<td>Manage roles and role assignments. In addition they can't:</td>
<td>Has access only to the Self Service Portal.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assign policies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Clear alerts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Update the Sophos agent software on a computer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Scan computers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Look at sensitive logs or reports.</td>
<td></td>
</tr>
</tbody>
</table>

If you have Intercept X with EDR, please see Administration Roles for Intercept X with EDR (page 79).

Permissions

This is the access level for a role. The options are Full, Help Desk or Read-only.
Additional 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 assignment to users/devices**: This option means that an administrator can assign policies to users and devices.
- **Notifications**: This option means that an administrator can receive and clear alerts.

**Note**

*Read-only* administrators can only receive alerts.

Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details, see *User Summary* (page 48).

**To 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.

**Note**

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.

1. Click *Edit*. This opens the *Edit Role Members* window.

**Note**

You can only see this option if you are a *Super Admin* administrator.

2. Select a user in the *Available Users* list and use the picker arrows to add them to the *Assigned Users* for the role.

**Tip**

Enter a name or part of a name in the search box to filter the list of available users.

**To delete 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.
1. Click **Edit**. This opens the **Edit Role Members** window.

   **Note**
   You can only see this option if you are a **Super Admin** administrator.

2. Remove assigned administrators from the role by selecting 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.

### Administration Roles for Intercept X with EDR

For general information on Administration Roles, see Administration Roles (page 76).

The available administration roles for Intercept X with EDR are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can't...</th>
</tr>
</thead>
</table>
| **Super Admin**
  There must be at least one administrator with a SuperAdmin role. | • 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. | There are no limitations. |
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can't...</th>
<th>There are no limitations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>• 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Help Desk</td>
<td>• 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.</td>
<td>• Add items to the “Clean and Block” list. • Remove items from the “Clean and Block” list. • Isolate and un-isolate devices.</td>
<td></td>
</tr>
<tr>
<td>Read-only</td>
<td>• View the intelligence report. • View blocked items. • View on-demand threat cases. • View a saved threat search. • Request the intelligence report. • Add items to the “Clean and Block” list. • Remove items from the “Clean and Block” list. • Request an on-demand threat case. • Isolate and un-isolate devices. • Request a forensic snapshot. • Request a threat search.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.8.3 Federated sign-in

You must be a Super Admin to turn on federated sign-in for your administrators and users.

You can allow your administrators and users to sign in to Sophos Central and the SSP using their Microsoft sign-in credentials.
Note
When you turn on federated sign-in administrators and users can still sign in using their Sophos Central credentials.

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.

Note
Sophos Central is not supported on mobile devices.

An Azure AD admin must give permission for Sophos Central to use federated sign in before you can turn it on. Once an admin gives consent, it means your Azure AD tenant trusts Sophos Central and administrators can sign in with their Microsoft credentials. See https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience for more information.

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 turn on federated sign-in:
1. Click Federated sign-in in Settings.
2. Click Sign in with Sophos Central Admin or Microsoft credentials.

4.8.4 Exploit Mitigation Exclusions

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

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.

In Settings, the Exploit Mitigation Exclusions page displays a list of applications excluded from protection against security exploits.

Note
These applications are excluded from exploit protection for all your users and their devices. You can only exclude applications that have been detected as a threat.

Important
Think carefully before you add exclusions because it reduces your protection.

To exclude an application:
1. Click Add Exclusion (on the right of the page).
   The Add Exploit Mitigation Exclusion dialog is displayed.
2. In the Application drop-down list, select the application you want to exclude.
   The names displayed here are the same as those shown in the Events Report.
3. Click Add or Add Another. The exclusion is added to the Excluded Applications list.
4. Click **Save** (on the right of the page) to save your changes to the list.

To delete an exclusion later, click on the ✗ to the right of the exclusion you wish to remove.

### 4.8.5 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 unless they have 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 select the **Tamper Protection** tab. 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.

For details, see **Recover tamper protection passwords** (page 42).

### 4.8.6 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 knowledgebase 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.
4.8.7 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.

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. Go to https://www.sophos.com/en-us/threat-center/reassessment-request.aspx. 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 Control sites tagged in Website Management (page 185)
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.
4.8.8 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 System > System Services > Security Heartbeat).

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 Deregister 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.
4.8.9 Global Exclusions

You can exclude files, websites and applications from scanning for threats, as described below.

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. See Computer isolation (Windows).

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 on this page.
- To exclude certain applications from checking, use Exploit Mitigation Exclusions (page 82).

You set exclusions in Settings, on the Global Exclusions page.

Note
These exclusions will apply to all your users (and their devices) and servers. If you want them to apply only to certain users or servers, use the policy exclusions in the policies instead.

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 from events.

Important
Think carefully before you add global exclusions because doing so may reduce your protection.

1. On the Global Exclusions page, 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, detected exploit or device isolation).

3. Specify the item or items you want to exclude. The following rules apply:

<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. Examples:</td>
</tr>
<tr>
<td></td>
<td>• Folder:C:\programdata\adobe \photoshop\ (add a slash for a folder).</td>
</tr>
<tr>
<td></td>
<td>• Entire drive: D:</td>
</tr>
<tr>
<td></td>
<td>• File:C:\program files\program *.vmg</td>
</tr>
<tr>
<td></td>
<td>For more details, see Windows Scanning Exclusions: Wildcards and Variables (page 175).</td>
</tr>
</tbody>
</table>

| File or folder (Mac and Linux) | You can exclude a folder or file. You can use the wildcards ? and *. Examples: |

Copyright © Sophos Limited 201
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>/Volumes/excluded (Mac)</td>
<td>• /Volumes/excluded (Mac)</td>
</tr>
<tr>
<td>/mnt/hgfs/excluded (Linux)</td>
<td>• /mnt/hgfs/excluded (Linux)</td>
</tr>
<tr>
<td></td>
<td>For more details, see macOS Scanning Exclusions (page 177)</td>
</tr>
<tr>
<td>File or folder (Virtual Server)</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></td>
<td>For more details, see Virtual Server Scanning Exclusions: Wildcards (page 330).</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, not just the process name shown in Task Manager. Example:</td>
</tr>
<tr>
<td></td>
<td>• %PROGRAMFILES%\Microsoft Office \Office 14\Outlook.exe</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>To see all processes or other items that you need to exclude for an application, see the application vendor's documentation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>You can use wildcards and variables.</td>
</tr>
<tr>
<td>Website</td>
<td>Websites can be specified as IP address, IP address range (in CIDR notation), or domain.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>• IP address: 192.168.0.1</td>
</tr>
<tr>
<td></td>
<td>• IP address range: 192.168.0.0/24</td>
</tr>
<tr>
<td></td>
<td>• The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range.</td>
</tr>
<tr>
<td></td>
<td>Thus /24 equals the netmask: 11111111.11111111.11111111.00000000</td>
</tr>
<tr>
<td></td>
<td>In our example, the range includes all IP addresses starting with 192.168.0.</td>
</tr>
<tr>
<td></td>
<td>• Domain: google.com</td>
</tr>
<tr>
<td>Potentially Unwanted Application</td>
<td>Here, you can exclude applications that are normally detected as spyware. Specify the</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Detection of Exclusion</td>
<td>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>Detected Exploits (Windows and 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. Restrict those communications with one or more of these settings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Local Port</strong>: Any device can use this port on isolated devices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote Port</strong>: Isolated devices can use this port on any device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote IP address</strong>: Isolated devices can only communicate with the device with this IP.</td>
</tr>
<tr>
<td></td>
<td>Example 1:</td>
</tr>
<tr>
<td></td>
<td>You want remote desktop access to an isolated device so that you can troubleshoot.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Inbound</strong>.</td>
</tr>
<tr>
<td></td>
<td>• In <strong>Local Port</strong>, enter the port number.</td>
</tr>
<tr>
<td></td>
<td>Example 2:</td>
</tr>
<tr>
<td></td>
<td>You want to be able to go to an isolated device and download cleanup tools from a server.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Outbound</strong>.</td>
</tr>
<tr>
<td></td>
<td>• In <strong>Remote IP address</strong>, enter the address of the server.</td>
</tr>
</tbody>
</table>

4. 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.

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**.

4.8.10 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 Manage Update Caches and Message Relays (page 95).

### 4.8.11 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 **Global Settings > HTTPS updating**.
2. Enable **HTTPS updating**.

### 4.8.12 Configure email alerts

You can manage how admins receive 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.
- 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 at 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.

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.

Set up a custom rule as follows:

1. Click Create new rule.
2. In Role, choose an administrator role that this rule will apply to. Click Next.
3. In Administrators and 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.

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.
Sophos Central Admin

- 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.

Note
The Hourly and Daily options aren't a digest of all alerts generated in the specified time. Admins will get an email for each alert.

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.

4.8.13 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.
This means that admins must use another form of authentication, as well as their username and password.
Admins can use Sophos/Google Authenticator or email authentication to sign in.
This page tells you how to do the following:
- Set up multi-factor authentication.
- Sign in with multi-factor authentication for the first time.
- Sign in with email authentication (if you don't have Sophos/Google Authenticator).
- Reset an admin's sign-in details, for example if they lose their phone.

Set up multi-factor authentication

1. Go to Settings > Multi-factor authentication.
2. Choose how you want admins to sign in:
   - No MFA needed. This is the default.
   - All admins need MFA.
   - Select admins who will need MFA. This lets you select individual admins.
3. If you chose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). In the picker, move admins to the Assigned list and click Save.

When admins next try to sign in, they'll be prompted to set up a new method of authentication.
Sign in with multi-factor authentication for the first time

Here’s what to do the first time you sign in with MFA:
1. At the sign-in screen, enter your user ID (email address) and password.
2. A Set Up Your Login Information dialog explains that signing in needs additional authentication.
3. In the next dialog:
   • Enter the security code that has been sent to you in an email.
   • Create a 4-digit PIN. This enables you to use email as an authentication method.
4. In the next dialog, choose authentication type.
5. In Verify Your Device, scan the QR code and enter the security code that Sophos/Google Authenticator displays.

Sophos Central opens.
The next time you sign in, you only need to enter a code from Sophos/Google Authenticator when prompted.

Sign in with email authentication

If you don't have access to Sophos/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/Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can let them set up their sign-in again.
1. Go to the Users page.
2. Find the user and click on their name to open their details.
3. 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.
4.8.14 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. Just set up your caches before installation.

**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** (page 215).

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 particular 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** (page 215).

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.
4. Click **Set Up Cache/Relay**.

Sophos Central automatically configures computers in your network to use a cache or relay. You can also manually assign computers to use a particular cache or relay.

### Assign computers to a cache/relay

You can manually assign computers to use a particular cache or relay.
1. In Settings, go to the **Manage Update Caches and Message Relays** page.
2. Click on the link displaying the number of computers using the Update Cache or Message Relay.
3. Click on **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 on 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.
Sophos Central Admin

- 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. Go to the System Settings > 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.

4.8.15 Allowed applications

At 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.

Important
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 knowledge base article 128136.

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).

**4.8.16 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

Admin Isolated Devices (page 101)

4.8.17 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.

To control updates, go to **Settings > Controlled Updates**.

You have these options.

- **Pause Updates Now** (page 99)
- **Pause Updates on a Set Date** (page 99)
- **Control Updates Manually** (page 100)
Note
Computers still get automatic security updates to protect them against the latest threats.

Tip
You can go back to automatic updating at any time.

Pause Updates Now
You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

On the Settings > Controlled Updates page, click on 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 resume product updates on all computers.
Automatic updates will stop for 90 days. Your computers will still get security updates.

1. On the Settings > Controlled Updates page, click on Pause Updates on a Set Date.
2. On the Pause Updates on a Set Date page, select a Start date and a Resume Date. Click Apply.
On the Resume date, the computers will start updating automatically and get any updates that are available.

Tip
If you want to resume updating earlier, click Resume Automatic Updating.

Control Updates Manually
You can control product updates manually.
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 on Control Updates Manually.
Important
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** 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.

**Test the new version**
In the **Action** column, next to **Test Computers**, click **Update test computers to newest version**.

**Roll out the new 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**.

Why can I see a 'Previous' version now?
If Sophos releases another product update when you already have test computers on **Newest** 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.

4.8.18 Reject network connections

You can configure computers to reject connections from other computers on the network that may be unsafe.

This setting only applies to computers connected to an XG firewall.

When you turn on the setting, it rejects connections to or from computers with red health or with a missing Security Heartbeat.

Note
You might have servers that are critical for your organization, for example message relays. In this case, set up exclusions to ensure that computers always accept connections from them even if their health is red.

1. Go to Settings > Reject network connections.
2. Turn on Allow computers to reject connections from other computers with red health.
3. Set up Exclusions if you need to.

Exclusions

You can exclude certain servers to ensure that computers always accept connections from them.

1. On the Reject network connections page, go to Exclusions.
2. Select the server or servers and move them to the Excluded list.

4.8.19 Amazon Web Services Accounts

In Settings, on the Amazon Web Services 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 an AWS Account** dialog:
   a) Enter a **Friendly Account Name**. This will be used to refer to the account in Sophos Central.
   b) Enter **IAM user credential** (Access Key and Secret Key) for the AWS account that you want to connect.
   c) Select **Add**.

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, please see these articles:
   - Creating an IAM User for Sophos Central
   - Troubleshooting Sophos Central connections to AWS

When you have added the AWS account:

• AWS instances are listed on the **AWS Instances** page. 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.

### 4.8.20 Data Loss Prevention Rules

You use Data Loss Prevention (DLP) rules to specify conditions for data loss prevention to detect, actions to be taken if the rules are matched, and any files to be excluded 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 List(s) in the rule to the specified destination.

  You use Content Control Lists to match file content. For more information about Content Control Lists (CCLs), see **Content Control Lists** (page 106).

• **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 Data Loss Prevention 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, see Create a Data Loss Prevention Rule (page 104), and search existing rules.

You can also filter rules by Type (choose from File or Content) and Source (choose from Custom or SophosLabs).

Click on the name of a rule to edit it.

Click to view details of a rule.

Click to clone a rule.

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.

Click to export custom rules. This creates an xml file containing the rule definition.

Click to delete a rule. 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.

Create a Data Loss Prevention Rule

There are two stages to creating a DLP rule; creation and configuration.

Creating a DLP rule

This 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 on 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**.

### Configuring a DLP rule

This sets up the conditions for monitored files, file types or destinations and the exclusions for the rule.

The conditions you set depend on whether you are creating a **File** or **Content** rule.

1. To set up conditions for a content rule:
   a) Click on **File contains** and select the Content Control Lists you want to use.
      
      You can search the list of CCLs. You can filter the CCLs by **Tags**, **Source** (choose from **SophosLabs** or **Custom**) and **Region**. You can also create a new CCL, see Create Custom Content Control List (page 106).
   b) For each CCL: click on the matches and set the required number of matches.

   **Tip**
   Once the CCL has been matched for the set number of times it will trigger the rule.

2. To set up conditions for a file rule: Specify the file names or file types for the rule.

3. 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).

4. Set the exclusion details for the rule.

5. Click **Finish** to create the rule.

### 4.8.21 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 to 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. For more information on rules, see Data Loss Prevention Rules (page 103).
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 Content Control Lists in your rules, or create your own CCLs, see Create Custom Content Control List (page 106).

You can filter the CCLs by:

- **Region**
- **Source** (choose from SophosLabs or Custom)
- **Type**

You also can search the list of CCLs.

Click 🔄 to view details of a CCL.

For each custom CCL you can also:

- Click on the name of a CCL to edit it.
- Click 🔄 to export a CCL. This creates an XML file containing the definition for the CCL.
- Click 🔄 to clone a CCL. 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.
- Click ✗ to delete a CCL. Click **Delete item** to confirm deletion.

You can also import Content Control Lists:

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

To create a custom Content Control List:

1. Click on **Add Custom Content Control List**.
2. Give the CCL a **Name** and a **Description**.
3. Click in **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 the text you want to match in **Terms** and click **Add Term**.
   - **All of these terms**: Enter the **Terms** and click **Add Term**.
   - **Exactly this phrase**: Enter the phrase you want to match in **Phrase**.
   - **Advanced Setup**: Use this option to set up an **Advanced Expression**, as described below.
5. Click **Save** to create the CCL.
Set up an Advanced Expression

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 Content Control List is matched.

2. Enter a Perl 5 regular expression in Expression.
   For a description of Perl 5 regular expressions, refer to Perl documentation or visit [http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html](http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html).

3. Set the Score for the CCL. This 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.
   Click \( \times \) to delete an expression.
   Click \( \checkmark \) to edit an expression. Once you have finished your edit, click 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>

4.9 Protect Devices

At 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.

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:

- **Endpoint Protection** (page 116)
- **Encryption** (page 117)
- **Server Protection** (page 117)
- **Server Protection on Microsoft Azure** (page 117)
- **Virtual Environment Protection** (page 118)
- **Web Gateway** (page 118)
- **Firewall Protection** (page 119)

### 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.

#### 4.9.1 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 **Endpoint Protection > 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:
  
  - **Intercept X** (protection from ransomware and exploits).
  - **Endpoint Protection** (protection from malware).
  - **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 user names 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, e.g., 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 [Sophos Knowledgebase Article 119265](#).
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 Alerts

Some features might not be available for all customers yet.

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

Note

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.

For advice on what to do, see How to deal with threats (page 11).

Note
If you have Intercept X Advanced with EDR you can investigate, block and clean up threats from Threat Cases, see Threat Cases (page 17).

Group alerts
You can group together all alerts for a particular 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 particular priority, click the figures for High alerts, Medium alerts or Low alerts at the top of the page.

To view alerts for a particular 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 fold-out arrow next to an alert to open its details.
In Action, click an action button (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. See Allowed applications (page 97).

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 Ransomware**: 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 (page 559). This action becomes available when you might need help, for example when malware cleanup fails.
- **Cleanup PUA(s)**: 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, see Alerts for Threat Protection (page 6).

- **Authorize PUA(s)**: 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 a particular 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. See Configure email alerts (page 91).

---

### Related concepts

- Alerts for Threat Protection (page 6)
- Alerts for Installation, Updating and Compliance (page 9)
- Events Report (page 26)
- Configure email alerts (page 91)
- Get additional help (page 559)

---

### 5.2.1 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.

## 5.3 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** (page 25).

To find out how reports work and how you can customize, save and schedule them, see **Reports** (page 41).

### 5.3.1 Logs

The following logs are available for Encryption:

• **Events**. All events on your devices, see **Events Report** (page 26).

• **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** (page 37).

**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** (page 27).

For advice on what to do about threats, see **How to deal with threats** (page 11).

**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-AJWL"), 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.

Date range: Use the From and To fields to select the time period for 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 Report: 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
- When: 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
- Device: Device that caused the event

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.

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. For more information, see Alerts (page 4).

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 &quot;Running malware cleaned up&quot; 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 alert 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 unauthorised 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 detected</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>
### Application control

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlled application blocked</td>
<td>Medium</td>
<td>No</td>
<td>A controlled application has been detected and then allowed.</td>
</tr>
<tr>
<td>Controlled 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. You can find more information about these in [knowledge base article 127331](#).

<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>
</tbody>
</table>
| Malware not cleaned up      | High     | Yes              | The following events may be displayed for this event type:  
  - Manual cleanup required.  
  - Computer scan required to complete cleanup.  
  - Reboot required to complete cleanup.  
  - Malware not cleaned up. |
<p>| Malware cleaned up          | Low      | No               |                                                                                                                                              |</p>
<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurring infection</td>
<td>High</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>Threat removed</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Malware alert locally cleared</td>
<td>Low</td>
<td>No</td>
<td>A malware alert has been cleared from the alerts list on an endpoint 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>
<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) alert 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 <strong>Alerts</strong> 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 <strong>Alerts</strong> 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>

### Updating

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

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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

<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>
<tr>
<td>Failed to protect computer or server</td>
<td>High</td>
<td>Yes</td>
<td>A computer has started installation of the agent software but has not become protected for one hour.</td>
</tr>
<tr>
<td>Error reported</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Scan completion</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New logins added</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New users added automatically</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

#### Peripherals

<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>

For more information, see Knowledgebase Article 132029.

ADSync

<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. For more information, see Knowledgebase Article 121319.
### User deleted low reputation download

<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>
</tbody>
</table>

### User trusted low reputation download

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

### Low reputation download automatically trusted

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
</tbody>
</table>

Note: This occurs only if you change your reputation checking settings to "Log only".

---

### 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>
</tbody>
</table>
### Restored heartbeat reported

- **Event type**: Restored heartbeat reported
- **Severity**: Low
- **Action required?**: No
- **Description**: A computer has resumed sending security heartbeat signals to a Sophos XG Firewall.

---

**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>Encryption failed</td>
<td>Medium</td>
<td>See Note</td>
<td>A volume could not be encrypted.</td>
</tr>
<tr>
<td>Encryption info</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>Device not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Device Encryption status changed from ... to ...</td>
<td>Low</td>
<td>See Note</td>
<td>The Device Encryption status changed from one status to another status. See Computers (page 55).</td>
</tr>
<tr>
<td>Device Encryption is suspended</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key received</td>
<td>Low</td>
<td>See Note</td>
<td>Sophos Central received a recovery key from an endpoint computer.</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 file 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 file 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.

### 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 the activity or change was carried out.

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

**5.3.2 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**.

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

### 5.4 People

On the **People** page, you can manage your users and user groups.
5.4.1 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 sections below tell you about the users list and how to manage users.

About the users list

The current users are listed with their details:

- Security status. An icon shows whether the user has security alerts on any of their devices:
  - Green check mark if there are low-priority alerts or no alerts.
  - Amber warning sign if there are medium-priority alerts.
  - Red warning sign if there are critical alerts.
  
  Click on 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, see Administration Roles (page 76).

  This column is only visible if you are an administrator.

Click on 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 on the user’s name. For more information, see User Summary (page 48).

Add a user manually

This also gives you the option to let the user protect their own devices.

You can add an individual user and protect them as follows.

1. On the Users page, click Add and select Add User.

2. In the Add User dialog, enter the following settings:

   **First and Last Name.** Enter the name of the user. Do not include a domain name.

   **Role.** Select an administration role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

   A user who is assigned an administration role will receive an email telling them how to set up their administration account.
**Important**
You can only see the **Role** option and assign administrator roles if you are a **SuperAdmin**.

**Note**
Anyone with a **User** role only has access to the Self Service Portal.

**Email Address**. Enter the email address of the user.

**Add to Groups** (optional). Select one of the available user groups and use the picker arrows to move it to the assigned groups.

**Tip**
You can start typing a name in the search box to filter the displayed 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.

3. Click **Save** or **Save & 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 by protecting their devices**

You can add users automatically as follows.

Download an installer and run it yourself on a device (or devices). This adds the user of each device automatically. For installers, see the **Protect Devices** page.

**Import users from a CSV file**

**This option may not be available for all customers yet.**

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 do this:

1. On the **Users** page, click **Add** and select **Import users from CSV**.
2. Click **Browse** and select your CSV file.

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

3. The CSV file can include groups a user is assigned to. To create groups not available yet, select **Create new groups**.
4. To send a registration email for the Sophos Central Self Service portal to each imported user, select **Activate new users**.

5. 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.

On the **Users** page, click the **Set up Active Directory Sync** link in the upper right of the page. Then see Set up synchronization with Active Directory (page 73).

---

**Protect existing users**

To email users you have already added to the list or imported:

1. On the **Users** page, select the user or users you want to protect. Click **Email Setup Link** in the upper right of the page.

2. In the **Email Setup Link** dialog, you are prompted to select the types of protection the user needs (if your license includes more than one).

   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.

---

**Modify users**

To modify a user's account:

On the **Users** page, click the user's name to open and edit their user details. For more information, see **User Summary** (page 48).

---

**Delete users**

To delete a user or users:
On the **Users** page, select the checkbox next to each user you want to delete. Click the **Delete** button in the upper right of the page.

**Important**
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them, see Administration Roles (page 76).

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

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

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 will be added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they will be added as a user again the next time that Sophos Central synchronizes with Active Directory.

**Export to CSV**

To export a list of users:
Click on **Export to CSV**.

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

For example you can export a list of administrators by applying the **Admins Only** filter before clicking **Export to CSV**.

**Related concepts**
Active Directory Sync (page 72)

**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**.
Security status

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

- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
- Red warning sign if there are high-priority alerts.

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 and Last name: Enter the name of the user. Do not include a domain name.
   - Role: Select a role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

   Important
   You can only see the Role option and assign administrator roles if you are a SuperAdmin.

   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** (optional): 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.

**Important**
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.

For information on how policies work, see About Policies (page 425).

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 group(s) 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.

**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 knowledge base article 128136.

Click the Details link beside the event and then allow the application, see Allowed applications (page 97).

**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.

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.

5.4.2 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 on the group's name. For more information, see User Group Details (page 54).

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.
   - Members: 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 (page 54).

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.
• 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.

5.5 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).
- Device Encryption. This shows the encryption status. For more information, see See 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 from Sophos Central. It also deletes 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.

**Note**
You can't uninstall Sophos Device Encryption on its own. Uninstall all products and then use custom installation to reinstall the products you want.

Export to CSV

To export a list of computers:

Click on **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 **Devices** 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. For more information, see **Encryption Recovery Key Search** (page 89).

**5.5.1 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 on the other tabs on this page.

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

- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
- Red warning sign if there are high-priority alerts.

If there are alerts, you can click Show Status to see details.

Actions you can take

The actions links and buttons are in the left-hand pane.

Isolate
This isolates the computer from the network. See Isolate or remove from isolation (page 58).

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.

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 in 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.

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** (page 171).

**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.

**Endpoint 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.
- **Agent Update Status**: Shows whether the computer is up to date.
- **Assigned Products**: Shows the Sophos products are 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). **Change group** lets you add it to a group, move it to a different group, or remove it from its current group.

**Device Encryption summary**

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.

Note
- 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 logon credentials. For more information, see Retrieve recovery key (page 57) or Retrieve recovery key (Macs) (page 90).

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 unless they have 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 View Details to manage the tamper protection password for the computer.

Update Cache and Message Relay status
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 status

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.

5.5.2 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:

- **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 [knowledge base article 128136](#).

Click the Details link beside the event and then allow the application, see [Allowed applications](#) (page 97).

**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.

5.5.3 Computer Status

The Status tab in a computer’s details page lets you see the computer’s security status and details of any alerts. It also lets you take action against alerts.

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. See Alerts (page 4).

Activity

This shows whether the device is active or not and gives details of past activity.

Computer Security Status

Note
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).

5.5.4 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.

5.6 Computer Groups

On the Groups tab of the Computers page, 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

1. Click Add Computer Group in the upper right of the page.
2. Choose if you want to create a new group and click Next.
3. In the Add Computer Group dialog:
   - Enter a Group name.
   - Enter a Group description.
   - Select available computers and add them to the Assigned Computers list.

   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.

4. Click Save.

Edit a group

To edit a group, click the group’s name to open and edit the group details.

Move a group

You can move groups.
1. Select the group.
2. Click Move.
3. Click Save.

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.

Note
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

This feature may not be available for all customers yet.
The Summary tab in a computer group’s details lets you:
• Add or remove computers.
• Delete the group.

Add or remove computers

To add or remove computers:
1. Click Edit in the left-hand pane.
2. In the Edit Computer Group dialog, use the picker arrows to add computers to the Assigned Computers list or remove them.
   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.
3. Click Save.

Delete the group

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.
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.

5.7 Policies

A policy is a set of options (for example, settings for malware protection) that Sophos Central applies to protected devices or servers.

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.

Important
Your assigned administrator role affects what you can do, see Administration Roles (page 76).

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 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 particular 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.
   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.

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 (page 168).**
• **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 will be encrypted as soon as one of the users the policy is applied to logs in.

**Note**
A Windows endpoint will stay encrypted even if a different user who is not included in the policy logs in.
**Attention**
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.
This option 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 forces a change of the BitLocker password or PIN after the specified time. An event is logged when users change their 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.

**Encrypt used space only**
This option allows you to encrypt only the used space instead of 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)**

**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. When they send it back, they can protect the file 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.

### 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 be displayed under **Global Settings** in **Overview**, if you have more than one product.

**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 groups from Active Directory to Sophos Central.

In Setting, 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.
- You can also configure settings for Azure Active Directory Synchronization.

**Note**

If you are using Office 365 you must use this option.

For instructions on setting up the utility, see **Set up synchronization with Active Directory** (page 73). For full details of how it works, see **About Active Directory synchronization** (page 73). Once you have set up synchronization you can review its status and other settings, see **Active Directory Sync Status** (page 72).

For instructions on configuring Azure Active Directory synchronization, see **Set up synchronization with Azure Active Directory** (page 75). Once you have set up synchronization you can review its status and other settings, see **Azure AD Sync Status** (page 75).

**Active Directory Sync**

You can import users and groups from Active Directory to Sophos Central.

In Setting, 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.
• You can also configure settings for Azure Active Directory Synchronization.

**Note**
If you are using Office 365 you must use this option.

For instructions on setting up the utility, see **Set up synchronization with Active Directory** (page 73). For full details of how it works, see **About Active Directory synchronization** (page 73). Once you have set up synchronization you can review its status and other settings, see **Active Directory Sync Status** (page 72).

For instructions on configuring Azure Active Directory synchronization, see **Set up synchronization with Azure Active Directory** (page 75). Once you have set up synchronization you can review its status and other settings, see **Azure AD Sync Status** (page 75).

**About Active Directory synchronization**

Active Directory synchronization allows administrators to implement a service that maps users and 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 or groups.
• It supports automated, one-way synchronization from the Active Directory to Sophos Central. It does not support two-way synchronization between Sophos Central and Active Directory.
• For users imported from Active Directory:
  — You cannot modify their name, email, or Exchange login, or add or change or remove associated groups or logins managed by Active Directory.
  — You can add, change or remove groups or logins that are not managed by Active Directory.
• For groups imported from Active Directory:
  — You cannot modify their name.
  — You can add, change or remove groups or logins that are not managed by Active Directory.
• 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. Any information added or updated from the Active Directory cannot be edited in the console.
• 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 AD forest. We strongly recommend to synchronize different AD 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 deploying with Active Directory.

**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.

To set up synchronization with Active Directory:
1. In Settings, on the **Active Directory Sync** page, click the link to download the Sophos Central AD Synchronization Utility installer, and then run it.

2. In the setup wizard, enter the information required.

   Follow the instructions in the Sophos Central AD Sync Utility Setup Wizard.

3. On the last page of the setup wizard, 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**.

   The Sophos Central AD Sync Utility Setup Wizard starts.

4. On the **Sophos Credentials** page, enter your Sophos Central account credentials.

5. 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, 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.

6. 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.

<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:  
OU=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 will limit user discovery to users belonging to “testGroup”. Note that unless a group query filter is also specified, 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: |
## Azure AD Sync Status

In Settings, on the **Active Directory Sync Status** page, once you configure Azure AD synchronization, you can view:

- The status of Azure AD synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Azure AD.
- The time of the last synchronization with Azure AD.

**Note**
Auto synchronization happens every 6 hours. You cannot change this interval.

- The configuration settings for Azure AD synchronization.
  
  You can amend these by clicking **Edit**, see [Set up synchronization with Azure Active Directory](#) (page 75).

Click **Sync** to run the synchronization process.

You can validate the Azure Sync connection by clicking **Test Connection**.

You can view Azure AD synchronization alerts on the **Alerts** page. You can view synchronization events on the **Logs & Reports > Events** page.

**Set up synchronization with Azure Active Directory**

Azure AD sync is only available if you have a Sophos Email license.
To configure Azure Active Directory synchronization:

1. In Settings, on the **Active Directory Sync** page, click the link to configure the settings for Azure AD Sync.

2. Set up your Azure Applications, if required.

   **Tip**
   Click the link to the instructions if you need help with this.

   You can skip this step if you have already set up an Azure application.

3. Configure the Azure Sync Settings:
   a) Enter the **Client ID**.
   b) Set the **Tenant Domain**.
   c) Enter the **Application Key** and set its 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.

4. Click **Test Connection** to validate the Azure Sync connection.

5. Click **Save**.

   Synchronization starts. This process may take some time.

### 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.

**Important**
You can only see this option if you are a **SuperAdmin** 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.

**Important**
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. These roles cannot be edited or deleted.

**Important**
Your assigned administrator role affects what you can do.
Note
Anyone with a **User** role only has access to the Self Service Portal.

The available administration roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</table>
| **Super Admin**  
There must be at least one administrator with a SuperAdmin role. | Have access to everything in Sophos Central.  
In addition they can:  
• Manage roles and role assignments | There are no limitations. | None. |
| **Admin** | Have access to everything in Sophos Central. | Manage roles and role assignments. | No Role Management options are displayed. |
| **Help Desk** | Have read-only access for all settings in Sophos Central. In addition they can:  
• 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. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Resolve alerts on the individual device. | No Role Management options are displayed.  
In addition:  
• All other options apart from those related to receiving and clearing alerts are read-only.  
• Some options, such as Edit buttons, are not displayed. |
| **Read-only** | Have read-only access for all settings in Sophos Central. In addition they can:  
• Look at sensitive logs or reports.  
• Receive alerts. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers. | No Role Management options are displayed.  
In addition:  
• All options are read-only.  
• Some options, such as Edit buttons, are not displayed. |
### Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details, see User Summary (page 48).

**To 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.
Note
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.

1. Click **Edit**. This opens the **Edit Role Members** window.

   **Note**
   You can only see this option if you are a **Super Admin** administrator.

2. Select a user in the **Available Users** list and use the picker arrows to add them to the **Assigned Users** for the role.

   **Tip**
   Enter a name or part of a name in the search box to filter the list of available users.

**To delete 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.

1. Click **Edit**. This opens the **Edit Role Members** window.

   **Note**
   You can only see this option if you are a **Super Admin** administrator.

2. Remove assigned administrators from the role by selecting 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.

**Administration Roles for Intercept X with EDR**

For general information on Administration Roles, see **Administration Roles** (page 76).
The available administration roles for Intercept X with EDR are:
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can't...</th>
</tr>
</thead>
</table>
| **Super Admin** | • 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.  | There are no limitations.                                      |
| **Admin**   | • 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.  | There are no limitations.                                      |
| **Help Desk** | • View the intelligence report.  
• Request the intelligence report.  
• View blocked items.  
• Request an on-demand threat case.  
• View on-demand threat cases.  
• Isolate and un-isolate devices.  | • Add items to the “Clean and Block” list.  
• Remove items from the “Clean and Block” list.  |

There must be at least one administrator with a SuperAdmin role.
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can’t...</th>
</tr>
</thead>
</table>
| **Read-only** | • View the intelligence report.  
• View blocked items.  
• View on-demand threat cases.  
• View a saved threat search. | • Request the intelligence report.  
• Add items to the “Clean and Block” list.  
• Remove items from the “Clean and Block” list.  
• Request an on-demand threat case.  
• Isolate and un-isolate devices.  
• Request a forensic snapshot.  
• Request a threat search. |

### 5.8.3 Federated sign-in

You must be a Super Admin to turn on federated sign-in for your administrators and users.

You can allow your administrators and users to sign in to Sophos Central and the SSP using their Microsoft sign-in credentials.

**Note**

When you turn on federated sign-in administrators and users can still sign in using their Sophos Central credentials.

**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.

**Note**

Sophos Central is not supported on mobile devices.

An Azure AD admin must give permission for Sophos Central to use federated sign in before you can turn it on. Once an admin gives consent, it means your Azure AD tenant trusts Sophos Central and administrators can sign in with their Microsoft credentials. See [https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience](https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience) for more information.

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 turn on federated sign-in:

1. Click **Federated sign-in** in **Settings**.
2. Click **Sign in with Sophos Central Admin or Microsoft credentials**.

### 5.8.4 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 Global Settings > HTTPS updating.
2. Enable HTTPS updating.

5.8.5 Configure email alerts

You can manage how admins receive 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.
- 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 at 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.

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.

Set up a custom rule as follows:
1. Click Create new rule.
2. In **Role**, choose an administrator role that this rule will apply to. Click **Next**.

3. In **Administrators and 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.

**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**.

**Note**

The **Hourly** and **Daily** options aren’t a digest of all alerts generated in the specified time. Admins will get an email for each alert.

**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.
5.8.6 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.

This means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos/Google Authenticator or email authentication to sign in.

This page tells you how to do the following:
• Set up multi-factor authentication.
• Sign in with multi-factor authentication for the first time.
• Sign in with email authentication (if you don't have Sophos/Google Authenticator).
• Reset an admin's sign-in details, for example if they lose their phone.

Set up multi-factor authentication

1. Go to Settings > Multi-factor authentication.
2. Choose how you want admins to sign in:
   • No MFA needed. This is the default.
   • All admins need MFA.
   • Select admins who will need MFA. This lets you select individual admins.
3. If you chose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). In the picker, move admins to the Assigned list and click Save.

When admins next try to sign in, they'll be prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

Here's what to do the first time you sign in with MFA:
1. At the sign-in screen, enter your user ID (email address) and password.
2. A Set Up Your Login Information dialog explains that signing in needs additional authentication.
3. In the next dialog:
   • Enter the security code that has been sent to you in an email.
   • Create a 4-digit PIN. This enables you to use email as an authentication method.
4. In the next dialog, choose authentication type.
5. In Verify Your Device, scan the QR code and enter the security code that Sophos/Google Authenticator displays.

Sophos Central opens.

The next time you sign in, you only need to enter a code from Sophos/Google Authenticator when prompted.
Sign in with email authentication

If you don't have access to Sophos/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/Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can let them set up their sign-in again.

1. Go to the Users page.
2. Find the user and click on their name to open their details.
3. 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.

5.8.7 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 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 the **Retrieve Recovery Key** button.
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 **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 the **Retrieve Recovery Key** button.
4. Enter at least five characters of the recovery key identifier.
5. Click the **Show key** button 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

At 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.

For more details on the installer for encryption, see this topic:
• Encryption (page 117)

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.

For more details, including what each product does and how Sophos Central registers users and applies policies, read the other topics in this section.

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 the Sophos Central Device Encryption administrator guide.
Download and run installer

Go to **Device Encryption > Protect Devices**.

Download an 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:
  
  — Intercept X (protection from ransomware and exploits).
  
  — Endpoint Protection (protection from malware).
  
  — 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.
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.

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.

Endpoint and server web control

Endpoint and server 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 Alerts

Some features might not be available for all customers yet.
The Alerts page lists all the alerts that require your action.
Alerts that are resolved automatically are not shown. To view all events, go to Logs & Reports > Events.

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.

For advice on what to do, see How to deal with threats (page 11).

If you have Intercept X Advanced with EDR you can investigate, block and clean up threats from Threat Cases, see Threat Cases (page 17).

Group alerts

You can group together all alerts for a particular 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 particular priority, click the figures for High alerts, Medium alerts or Low alerts at the top of the page.

To view alerts for a particular 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 fold-out arrow next to an alert to open its details. In Action, click an action button (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. See **Allowed applications** (page 97).

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 Ransomware**: 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** (page 559). This action becomes available when you might need help, for example when malware cleanup fails.

- **Cleanup PUA(s)**: 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, see **Alerts for Threat Protection** (page 6).

- **Authorize PUA(s)**: 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 a particular 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. See **Configure email alerts** (page 91).

**Related concepts**

- Alerts for Threat Protection (page 6)
- Alerts for Installation, Updating and Compliance (page 9)
- Events Report (page 26)
- Configure email alerts (page 91)
- Get additional help (page 559)
6.2.1 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.

For more information, see Knowledgebase Article 132029.

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.

6.2.2 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. For information on these, see knowledge base article 127331.

High

Real-time protection disabled
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 (page 4).

- 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(s) 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 in 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 my computer option in Sophos Endpoint Security and Control 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.

6.2.3 How to deal with threats
For advice on dealing with threats, see:
• Deal with ransomware (page 11).

For advice on malware, see the sections on malware alerts listed in 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 (page 14).

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.
  
  For help with sample submission, see our knowledge base article.
• 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 (page 4).
• 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.

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 (page 14).

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 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.

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 Allow an application that's been detected (page 98).

**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:
Sophos Central Admin

• 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.

For details, see these topics:
• Stop detecting an application (page 14)
• Stop detecting an exploit (page 15)
• Stop detecting ransomware (page 16)

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.

### 6.3 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** (page 25).

To find out how reports work and how you can customize, save and schedule them, see **Reports** (page 41).

#### 6.3.1 Logs

The following logs are available for Server Protection:

- **Events**. All events on your devices, see **Events Report** (page 26).
- **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** (page 37).
- **Data Loss Prevention Events Log**. All events triggered by data loss prevention rules for computers or servers, see **Data Loss Prevention Events Log** (page 38).

**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** (page 27).

For advice on what to do about threats, see **How to deal with threats** (page 11).
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-AJWL”), 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.

**Date range**: Use the From and To fields to select the time period for 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 Report**: 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
- **When**: 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
- **Device**: Device that caused the event

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.

**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. For more information, see Alerts (page 4).

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 &quot;Running malware cleaned up&quot; event will be added to the Events list.</td>
</tr>
</tbody>
</table>
| Running malware not cleaned up | High     | Yes              | 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:  
- Running malware requires manual cleanup.  
- Computer scan required to complete running malware cleanup.  
- Reboot required to complete running malware cleanup.  
- Running malware not cleaned up. |
<p>| Running malware cleaned up  | Low      | No               |                                                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 alert 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 unauthorised 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 detected</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>
### Application control

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

### Malware

If you have deep learning enabled, you may see malware detections shown as ML/PE-A. You can find more information about these in knowledge base article 127331.

<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>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>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>Recurring infection</td>
<td>High</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>Threat removed</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Malware alert locally cleared</td>
<td>Low</td>
<td>No</td>
<td>A malware alert has been cleared from the alerts list on an endpoint computer.</td>
</tr>
<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>
<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) alert 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>

## Updating

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

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot recommended</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>Reboot required</td>
<td>Medium</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Protection

<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>
<tr>
<td>Failed to protect computer or server</td>
<td>High</td>
<td>Yes</td>
<td>A computer has started installation of the agent software but has not become protected for one hour.</td>
</tr>
<tr>
<td>Error reported</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Scan completion</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New logins added</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>New users added automatically</td>
<td>Low</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Peripherals

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

For more information, see Knowledgebase Article 132029.

ADSync

<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. For more information, see Knowledgebase Article 121319.
### Event type

<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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>
</tbody>
</table>
### Event types and descriptions

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Encryption failed</td>
<td>Medium</td>
<td>See Note</td>
<td>A volume could not be encrypted.</td>
</tr>
<tr>
<td>Encryption info</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>Device not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Device Encryption status changed from ... to ...</td>
<td>Low</td>
<td>See Note</td>
<td>The Device Encryption status changed from one status to another status. See Computers (page 55).</td>
</tr>
<tr>
<td>Device Encryption is suspended</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>See Alerts for Device Encryption (page 225).</td>
</tr>
<tr>
<td>Recovery key received</td>
<td>Low</td>
<td>See Note</td>
<td>Sophos Central received a recovery key from an endpoint computer.</td>
</tr>
</tbody>
</table>
**Event type** | **Severity** | **Action required?** | **Description**
--- | --- | --- | ---
Recovery key revoked | Low | See Note | A recovery key has been viewed in Sophos Central, so it has been revoked and will be replaced.

**Data Loss Prevention**

<table>
<thead>
<tr>
<th>Event type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An &quot;allow file 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 file 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.

**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 the activity or change was carried out.

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

**Date range**: Use the **From** and **To** fields to select the time period for which you want to view events. You can view events that occurred in the past 90 days or less.

**Rule Name**: You can filter the events by rule name.

**File type**: You can filter the events by file type.
**Update Report**: 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**: Name of the destination that caused the event

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.

### 6.3.2 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.
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**.

**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 Details**.
   This shows you the password (and previous passwords).

**6.4 Servers**

On the **Servers** page, you can manage your servers and server groups.

**6.4.1 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 Address. Hover over the icon to see details of all IPv4 and IPv6 addresses.
- Operating System.

**Tip**
"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 particular health status, use the filters above the list.

**Tip**
The Sophos Security VMs filter displays instances of Sophos Security VM on a hypervisor.

Add a server

To add a server (i.e. 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.

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.

For more information, see Server Summary (page 65).
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.

Server Summary

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

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 on 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.

- **Delete Server**: Deletes the server from Sophos Central. It also deletes the alerts associated with the server.

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

- **Update Now**: Updates the Sophos agent software on the 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 in 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.

**Recent events**

This lists recent events on the computer.

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

**Summary**

The summary shows these details:

• **Last Sophos Central Activity**: The last time the server communicated with Sophos Central.
• **Last Agent Update**: The last time the Sophos agent was updated.
• **Agent Version**: The version number of the Sophos agent.
• **Installed component versions**: Click this to see a full list of the Sophos components and their version numbers. This is only available for Windows servers.
• **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.
• **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.
• **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.
• **Tamper Protection**: This shows whether Tamper Protection (page 83) is enabled on the server or not. Click **View Details** 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 Status

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.

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 [knowledge base article 128136](#).

Click the Details link beside the event and then allow the application, see [Allowed applications](#) (page 97).

*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.

Server Status

The **Status** tab in a server's details page lets you see the server’s security status and details of any alerts. It also lets you take action against alerts.

Activity

This shows whether the server is active or not and gives details of past activity.

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. See Alerts (page 4).

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. See Server Threat Protection Policy (page 321).

**Note**

Some automatic exclusions shown in the list might not work on servers running Windows Server 2003.

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 icons beside a policy name indicate the security settings (such as threat protection) included in the policy.

A gray icon indicates that this part of the policy does not apply to the computer. This happens if a higher-priority policy with settings for the same feature is applied to the server.

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

**Note**

Editing the policy affects all servers to which this policy is applied.
6.4.2 Azure VMs

On the Azure VMs tab in the Servers 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 (page 103).

The Azure VMs are listed with these details:

- **Virtual machine name**: Click the VM name to view details.
- **Sophos agent installed**: 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**

6.4.3 Server Groups

On the Groups tab of the Servers 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. For more information, see Server Group Summary (page 71).

Add a group

1. Click Add Server Group in the upper right of the page.
2. In the Add Server Group dialog:
   - Enter a Group name.
   - Enter a Group description.
   - Select available servers and add them to the Assigned Servers list.

   **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.

3. Click **Save**.

**Edit a group**

To edit a group, click the group’s name to open and edit the group details. For more information, see **Server Group Summary** (page 71).

**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.

**Note**
You can also delete a group at the group’s details page. Click the group’s name to open the details.

**Server Group Summary**

The **Summary** tab in a server group’s details lets you:
- Add or remove servers.
- Delete the group.

**Add or remove servers**

To add or remove servers:
1. Click **Edit** in the left-hand pane.
2. In the **Edit Server Group** dialog, use the picker arrows to add servers to the **Assigned Servers** list or remove them.
   
   **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.
3. Click **Save**.

**Delete the group**

To delete the group:
1. Click **Delete** in the left-hand pane.
2. In the **Confirm Group Deletion** pop-up, click **Yes**.
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.

6.5 Servers on AWS

The Servers on AWS pages let you see and manage your AWS instances and S3 storage buckets.

6.5.1 Servers on AWS map

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 particular continent, AWS instances, S3 storage or AWS account.
The map

Each location or region is indicated by a donut chart. Click the donut chart to see the regions within a continent in more detail. 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)

Click the globe icon (in the upper left) to return to a view of the entire globe at any time.

6.5.2 AWS Instances

On the AWS Instances tab in the Servers 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 (page 102).

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 page or the UTM web admin.
- **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.
- **Lifecycle state**: This shows which state of the AWS lifecycle the instance is in, see http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-lifecycle.html.
- **AWS account**
- **AWS region**
- **Auto scaling group**: Click on the group name to view the server group details.
- **VPC ID**
6.5.3 AWS S3 storage

On the S3 storage tab on the Servers 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 (page 102).

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:

- Name
- AWS region
- AWS account
- Default encryption.
- Versioning.
- Access control list (public access)
- Bucket policy
- CloudTrail logging

You can review the settings for a S3 storage bucket and stop the settings influencing its health status. To do this:

1. Click on a S3 storage bucket Name.
2. Optional: Click the Connect to AWS for more storage information link, if required.
3. Review the health info. For each option:
   a) Click Acknowledge to stop it influencing the health status for the S3 storage bucket.
      The health status updates as you review the options.
4. Click Save.
   The health status updates in the S3 storage tab.

6.6 Policies

A policy is a set of options (for example, settings for malware protection) that Sophos Central applies to protected servers.

Server policies define the security measures that will be used for your servers.
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.

### 6.6.1 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 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 particular 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.

6.6.2 Policies

A policy is a set of options (for example, settings for malware protection) that Sophos Central applies to protected servers.

Server policies define the security measures that will be used for your servers.
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.

### 6.6.3 Server Threat Protection Policy

**Attention**
The Intercept X Advanced with EDR for Server features are available if you are signed up to the Early Access Program.

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. See Create or Edit a Policy (page 168).
- 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.

**Important**
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.

**Note**
If you enable any of these features, servers assigned to this policy will use an Intercept X Advanced for Server license.
For details of all the options, see Server Protection: Intercept X Advanced (page 325).

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. See Knowledgebase Article 121461.

For details of all the options, see Server Protection: Default settings (page 326).

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. See Knowledgebase Article 121461.

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 System 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 (Virtual Server). 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. 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.** 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.** 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).** 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.

- **Device 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 with EDR for Server.
  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 IP 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.**
    - 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.**
    - In **Remote IP 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

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.

Server Protection: Intercept X Advanced

If you have an Intercept X Advanced for Server license, you'll see these options in your threat protection policy.

These options are available 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. 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.

- **Mitigate exploits in vulnerable applications**: This protects the applications most prone to exploitation by malware. You can select which application types to protect.

- Click Advanced: customize exploit mitigation to display 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.

- **Detect CPU malicious code**: 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

You can select these options:

- **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. See Threat Cases (page 17).

- **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. See Threat Searches (page 23).

  **Note**  
  This option is available if you are signed up to the Early Access Program for Intercept X Advanced with EDR for Server.

Server Protection: Default settings

The Server threat protection 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.

  **Important**  
  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**.

Real-time scanning (Local files and network shares)

Real-time scanning scans files as users attempt to access them, and denies access unless the file is clean.

You can select these options for scanning local files and network shares:

- **Local and remote files**. 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. 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. For more information, see Knowledgebase Article 121319. You can specify:
  - The **Action to take.** 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**

You can select this option:

- **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**
  Automatic cleanup doesn't apply to PE (Portable Executable) files, like applications, libraries and system files. PE files are quarantined and can be restored.

**Runtime protection**

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

- **Detect network traffic 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).
- **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.

**Real-time scanning (Options)**

You can select these additional 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
Knowledgeable Article 121461. You can manually exclude activity by other applications by using the **Scanning 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.

### 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.

**Important**

Think carefully before you add scanning exclusions because doing so may reduce your protection.

### 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>
</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:\foomore\bar              |                                                                         |
| \ (Backslash) | Either \ or /                                                          |                                                                         |
| / (Forward slash) | Either / or \                                                       |                                                                         |
| ? (Question mark) | One single character, unless at the end of a string where it can match zero characters. |                                                                         |
Token | Matches | Comments
--- | --- | ---
. (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." 

**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>C:</td>
<td>C:</td>
<td>Exclude drive C: from scanning (including the drive’s master boot record).</td>
</tr>
<tr>
<td>C:\</td>
<td>C:\</td>
<td>Exclude all files on drive C: from scanning (but scan the drive’s master boot record).</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 Windows Server 2008 and later</th>
<th>Windows XP Windows Server 2003</th>
</tr>
</thead>
<tbody>
<tr>
<td>%allusersprofile%</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users</td>
</tr>
</tbody>
</table>

Copyright © Sophos Limited
<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>%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>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>%commonprogramfiles(x86)%</td>
<td>C:\Program Files (x86)\Common Files</td>
<td>C:\Program Files (x86)\Common Files</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>C:\Program Files</td>
</tr>
<tr>
<td>%programfiles(x86)%</td>
<td>C:\Program Files (x86)</td>
<td>C:\Program Files (x86)</td>
</tr>
<tr>
<td>%systemdrive%</td>
<td>C:</td>
<td>C:</td>
</tr>
<tr>
<td>%systemroot%</td>
<td>C:\Windows</td>
<td>C:\Windows</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>C:\Windows</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.

**Important**
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>* (Star)</td>
<td>Zero or more of any character except \ or /</td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• c:\foo**\bar matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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:\foomore\bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td></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, unless at the end of a string where 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>
<tr>
<td></td>
<td></td>
<td>• * matches all files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• .* matches all files without an extension</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &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.
### Expression Table

<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>C:</td>
<td>C:</td>
<td>Exclude drive C: from scanning (including the drive's master boot record).</td>
</tr>
<tr>
<td>C:\</td>
<td>C:\</td>
<td>Exclude all files on drive C: from scanning (but scan the drive's master boot record).</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>

### 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>
<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>
Exclusions that do NOT work

The expressions shown in this table are not valid for Virtual Server exclusions.

<table>
<thead>
<tr>
<th>Exclusion</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>Cannot specify a file without a file extension.</td>
</tr>
<tr>
<td>\folder</td>
<td>Cannot specify a folder without the full path.</td>
</tr>
<tr>
<td>file*</td>
<td>Cannot use * within a filename.</td>
</tr>
<tr>
<td>file*.com</td>
<td>Cannot use * within a filename.</td>
</tr>
<tr>
<td>file*.*</td>
<td>Cannot use * within a filename.</td>
</tr>
<tr>
<td>C:?\</td>
<td>Cannot replace the folder name with a wildcard.</td>
</tr>
<tr>
<td>C:\folder*\</td>
<td>Cannot use * within a folder name.</td>
</tr>
</tbody>
</table>

6.6.4 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 (page 168).
• **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’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.

   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.

### 6.6.5 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** (page 168).
- Open the policy’s **Settings** tab and configure it 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 Plugin**.
   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 Application Control settings.

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 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.

   Important
   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 applications.

   Remember
   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.

6.6.6 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 (page 168).
• 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**.

### 6.6.7 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 **Server Lockdown** policy. See Create or Edit a Policy (page 168).
- 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/folder**

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**.

**6.6.8 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 (page 103). 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 (page 425).

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 an **Data Loss Prevention** policy. See Create or Edit a Policy (page 168).
• Open the policy’s **Settings** tab and configure it as described below. Make sure the policy 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 New Rule**.

   - To create a custom policy, click **Create Custom Policy** and click **Add New Rule**. Choose whether you want to use an existing rule or create a new rule, see [Create a Data Loss Prevention Rule](#) (page 104). Select the rules you want to add and click **Save Selection**.

2. Click on the fields in the **Messages** area to add your own message to the standard confirmation and block notifications. Each message can have a maximum of 100 characters.

   **Note**
   You can switch 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 **Save**.

### 6.6.9 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 a **Updating** policy. See [Create or Edit a Policy](#) (page 168).
- 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.

Remember that if computers aren’t on, they won’t get the update until they are next on at the scheduled update time.
6.6.10 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.

**Important**

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 (page 168).
- 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 and 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**

6.6.11 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:

1. Go to **Server Protection > Policies**.
2. Create a **File Integrity Monitoring** policy or edit the Base Policy. See Create or Edit a Policy (page 168).
3. Open the policy's **Settings** tab.

4. Select **Use File Integrity Monitoring**.

By default, we monitor critical Windows system files. For details, see [https://community.sophos.com/kb/en-us/132146](https://community.sophos.com/kb/en-us/132146). 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 by default but not the files in it.

To monitor the files, you must fill out **Monitor these file types**.

To stop monitoring the folder, deselect **Monitor changes to the folder as well as the files**.

**Note**

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](#) (page 343).

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 (page 343).

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.

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>
<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>

6.7 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 be displayed under Global Settings in Overview, if you have more than one product.

Note
If you want to apply settings only to certain users, servers or devices, use the Policies pages instead.

6.7.1 Active Directory Sync
You can import users and groups from Active Directory to Sophos Central.
In Setting, 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.
• You can also configure settings for Azure Active Directory Synchronization.

**Note**
If you are using Office 365 you must use this option.

For instructions on setting up the utility, see Set up synchronization with Active Directory (page 73).
For full details of how it works, see About Active Directory synchronization (page 73). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 72).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 75). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 75).

**Active Directory Sync Status**

In Settings, on the **Active Directory Sync Status** page, once you set up Active Directory synchronization, you can view:

**Status**

• The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
• The number of users and groups imported from Active Directory.
• The time of the last synchronization with Active Directory.

You can view Active Directory synchronization alerts on the **Alerts** page. You can view synchronization events on the **Logs & Reports > Events** page.

**Sync Status**

This shows the synchronization settings in Active Directory.

**About Active Directory synchronization**

Active Directory synchronization allows administrators to implement a service that maps users and 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 or groups.
• It supports automated, one-way synchronization from the Active Directory to Sophos Central. It does not support two-way synchronization between Sophos Central and Active Directory.
• For users imported from Active Directory:
  — You cannot modify their name, email, or Exchange login, or add or change or remove associated groups or logins managed by Active Directory.
  — You can add, change or remove groups or logins that are not managed by Active Directory.
• For groups imported from Active Directory:
  — You cannot modify their name.
  — You can add, change or remove groups or logins that are not managed by Active Directory.
• 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. Any information added or updated from the Active Directory cannot be edited in the console.
• 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 AD forest. We strongly recommend to synchronize different AD 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 deploying with Active Directory.

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.

To set up synchronization with Active Directory:

1. In Settings, on the **Active Directory Sync** page, click the link to download the Sophos Central AD Synchronization Utility installer, and then run it.
2. In the setup wizard, enter the information required.
   Follow the instructions in the Sophos Central AD Sync Utility Setup Wizard.
3. On the last page of the setup wizard, 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.

   The Sophos Central AD Sync Utility Setup Wizard starts.
4. On the **Sophos Credentials** page, enter your Sophos Central account credentials.
5. 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, 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.
6. 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.

<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,</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>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></td>
<td>LDAP query filters</td>
</tr>
<tr>
<td></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</td>
</tr>
<tr>
<td></td>
<td>The above query will limit user discovery to users belonging to “testGroup”. Note that unless a group query filter is also specified, 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>

**Important**

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.

7. 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**.

8. 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 Sophos Central.

To stop the synchronization in progress, click **Stop**.

**Azure AD Sync Status**

In Settings, on the **Active Directory Sync Status** page, once you configure Azure AD synchronization, you can view:

- The status of Azure AD synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Azure AD.
- The time of the last synchronization with Azure AD.

**Note**
Auto synchronization happens every 6 hours. You cannot change this interval.

- The configuration settings for Azure AD synchronization.
  You can amend these by clicking **Edit**, see Set up synchronization with Azure Active Directory (page 75).

Click **Sync** to run the synchronization process.
You can validate the Azure Sync connection by clicking **Test Connection**.
You can view Azure AD synchronization alerts on the **Alerts** page. You can view synchronization events on the **Logs & Reports > Events** page.

Set up sync with Azure Active Directory
Azure AD sync is only available if you have a Sophos Email license.

To configure Azure Active Directory synchronization:
1. In Settings, on the **Active Directory Sync** page, click the link to configure the settings for Azure AD Sync.
2. Set up your Azure Applications, if required.

**Tip**
Click the link to the instructions if you need help with this.

You can skip this step if you have already set up an Azure application.

3. Configure the Azure Sync Settings:
   a) Enter the **Client ID**.
   b) Set the **Tenant Domain**.
   c) Enter the **Application Key** and set its 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.
4. Click **Test Connection** to validate the Azure Sync connection.
5. Click **Save**.
   Synchronization starts. This process may take some time.

### 6.7.2 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.

**Important**
You can only see this option if you are a **SuperAdmin** 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.

**Important**
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. These roles cannot be edited or deleted.

**Important**
Your assigned administrator role affects what you can do.

**Note**
Anyone with a User role only has access to the Self Service Portal.

The available administration roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</table>
| **Super Admin**

There must be at least one administrator with a SuperAdmin role.

- Have access to everything in Sophos Central.
- In addition they can:
  - Manage roles and role assignments

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin</strong></td>
<td>Have access to everything in Sophos Central.</td>
<td>Manage roles and role assignments.</td>
<td>No Role Management options are displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Help Desk**       | Have read-only access for all settings in Sophos Central. In addition they can:
  - 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.
|                     | Manage roles and role assignments. In addition they can’t:
  - Assign policies.
  - Change settings.
  - Resolve alerts on the individual device. | No Role Management options are displayed. In addition:
  - All other options apart from those related to receiving and clearing alerts are read-only.
  - Some options, such as Edit buttons, are not displayed. |                             |
## Role

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</table>
| Read-only  | Have read-only access for all settings in Sophos Central. In addition they can:  
• Look at sensitive logs or reports.  
• Receive alerts. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers. | No Role Management options are displayed. In addition:  
• All options are read-only.  
• Some options, such as Edit buttons, are not displayed. |
| User       | Have no administration capabilities. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers.  
• Look at sensitive logs or reports. | Has access only to the Self Service Portal. |

If you have Intercept X with EDR, please see Administration Roles for Intercept X with EDR (page 79).

### Permissions

This is the access level for a role. The options are Full, Help Desk or Read-only.

### Additional 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 assignment to users/devices**: This option means that an administrator can assign policies to users and devices.

- **Notifications**: This option means that an administrator can receive and clear alerts.

**Note**

Read-only administrators can only receive alerts.
Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details, see User Summary (page 48).

To 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.

Note
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.

1. Click Edit. This opens the Edit Role Members window.

   Note
   You can only see this option if you are a Super Admin administrator.

2. Select a user in the Available Users list and use the picker arrows to add them to the Assigned Users for the role.

   Tip
   Enter a name or part of a name in the search box to filter the list of available users.

To delete 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.

1. Click Edit. This opens the Edit Role Members window.

   Note
   You can only see this option if you are a Super Admin administrator.

2. Remove assigned administrators from the role by selecting 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.
Administration Roles for Intercept X with EDR

For general information on Administration Roles, see Administration Roles (page 76).

The available administration roles for Intercept X with EDR are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can't...</th>
</tr>
</thead>
</table>
| **Super Admin** | • 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. | There are no limitations. |
| **Admin**     | • 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. | There are no limitations. |
## 6.7.3 Federated sign-in

You must be a Super Admin to turn on federated sign-in for your administrators and users.

You can allow your administrators and users to sign in to Sophos Central and the SSP using their Microsoft sign-in credentials.

**Note**
When you turn on federated sign-in administrators and users can still sign in using their Sophos Central credentials.

**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.

**Note**
Sophos Central is not supported on mobile devices.

An Azure AD admin must give permission for Sophos Central to use federated sign in before you can turn it on. Once an admin gives consent, it means your Azure AD tenant trusts Sophos Central and administrators can sign in with their Microsoft credentials. See [https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience](https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience) for more information.

---

### Role Permissions

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can’t...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Help Desk</strong></td>
<td>• View the intelligence report.</td>
<td>• Add items to the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>• Request the intelligence report.</td>
<td>• Remove items from the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>• View blocked items.</td>
<td>• Isolate and un-isolate devices.</td>
</tr>
<tr>
<td></td>
<td>• Request an on-demand threat case.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View on-demand threat cases.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request a forensic snapshot.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request a threat search.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View a saved threat search.</td>
<td></td>
</tr>
<tr>
<td><strong>Read-only</strong></td>
<td>• View the intelligence report.</td>
<td>• Request the intelligence report.</td>
</tr>
<tr>
<td></td>
<td>• View blocked items.</td>
<td>• Add items to the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>• View on-demand threat cases.</td>
<td>• Remove items from the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>• View a saved threat search.</td>
<td>• Request an on-demand threat case.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Isolate and un-isolate devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Request a forensic snapshot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Request a threat search.</td>
</tr>
</tbody>
</table>
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 turn on federated sign-in:
1. Click **Federated sign-in** in **Settings**.
2. Click **Sign in with Sophos Central Admin or Microsoft credentials**.

### 6.7.4 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 unless they have 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 select the **Tamper Protection** tab. 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.

For details, see **Recover tamper protection passwords** (page 42).

### 6.7.5 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 knowledgebase 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.

### 6.7.6 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.

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. Go to [https://www.sophos.com/en-us/threat-center/reassessment-request.aspx](https://www.sophos.com/en-us/threat-center/reassessment-request.aspx). 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 [Control sites tagged in Website Management](page 185)
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.

6.7.7 Global Exclusions

You can exclude files, websites and applications from scanning for threats, as described below.

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. See Computer isolation (Windows).

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 on this page.
- To exclude certain applications from checking, use Exploit Mitigation Exclusions (page 82).

You set exclusions in Settings, on the Global Exclusions page.

Note
These exclusions will apply to all your users (and their devices) and servers. If you want them to apply only to certain users or servers, use the policy exclusions in the policies instead.

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 from events.

Important
Think carefully before you add global exclusions because doing so may reduce your protection.

1. On the Global Exclusions page, 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, detected exploit or device isolation).
3. Specify the item or items you want to exclude. The following rules apply:

<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. Examples:</td>
</tr>
<tr>
<td></td>
<td>- Folder: C:\programdata\adobe \photoshop\ (add a slash for a folder).</td>
</tr>
<tr>
<td></td>
<td>- Entire drive: D:</td>
</tr>
<tr>
<td></td>
<td>- File: C:\program files\program *.vmg</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **File or folder (Mac and Linux)** | You can exclude a folder or file. You can use the wildcards ? and *. Examples:  
  • /Volumes/excluded (Mac)  
  • /mnt/hgfs/excluded (Linux)  
  For more details, see macOS Scanning Exclusions (page 177) |
| **File or folder (Virtual Server)** | 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.  
  For more details, see Virtual Server Scanning Exclusions: Wildcards (page 330). |
| **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** | Websites can be specified as 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:  
  11111111.11111111.11111111.11111111.00000000 |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In our example, the range includes all IP addresses starting with 192.168.0.</td>
</tr>
<tr>
<td></td>
<td>• Domain: google.com</td>
</tr>
<tr>
<td>Potentially Unwanted Application</td>
<td>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.</td>
</tr>
<tr>
<td>Detected Exploits (Windows and 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. Restrict those communications with one or more of these settings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Local Port</strong>: Any device can use this port on isolated devices.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote Port</strong>: Isolated devices can use this port on any device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote IP address</strong>: Isolated devices can only communicate with the device with this IP.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 1:</strong> You want remote desktop access to an isolated device so that you can troubleshoot.</td>
</tr>
<tr>
<td></td>
<td>• Select Inbound.</td>
</tr>
<tr>
<td></td>
<td>• In Local Port, enter the port number.</td>
</tr>
<tr>
<td></td>
<td><strong>Example 2:</strong> You want to be able to go to an isolated device and download cleanup tools from a server.</td>
</tr>
<tr>
<td></td>
<td>• Select Outbound.</td>
</tr>
<tr>
<td></td>
<td>• In Remote IP address, enter the address of the server.</td>
</tr>
</tbody>
</table>

4. 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.

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**.
6.7.8 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 Manage Update Caches and Message Relays (page 95).

6.7.9 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 Global Settings > HTTPS updating.
2. Enable HTTPS updating.

6.7.10 Configure email alerts

You can manage how admins receive 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.
- 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 at 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**.

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.

Set up a custom rule as follows:

1. Click **Create new rule**.

2. In **Role**, choose an administrator role that this rule will apply to. Click **Next**.

3. In **Administrators and 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.
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**.

**Note**
The **Hourly** and **Daily** options aren't a digest of all alerts generated in the specified time. Admins will get an email for each alert.

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.

**6.7.11 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. This means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos/Google Authenticator or email authentication to sign in.

This page tells you how to do the following:

- Set up multi-factor authentication.
- Sign in with multi-factor authentication for the first time.
- Sign in with email authentication (if you don't have Sophos/Google Authenticator).
- Reset an admin's sign-in details, for example if they lose their phone.

Set up multi-factor authentication

1. Go to **Settings > Multi-factor authentication**.
2. Choose how you want admins to sign in:
   - **No MFA needed**. This is the default.
• All admins need MFA.
• Select admins who will need MFA. This lets you select individual admins.

3. If you chose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). In the picker, move admins to the Assigned list and click Save.

When admins next try to sign in, they’ll be prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

Here’s what to do the first time you sign in with MFA:

1. At the sign-in screen, enter your user ID (email address) and password.
2. A Set Up Your Login Information dialog explains that signing in needs additional authentication.
3. In the next dialog:
   • Enter the security code that has been sent to you in an email.
   • Create a 4-digit PIN. This enables you to use email as an authentication method.
4. In the next dialog, choose authentication type.
5. In Verify Your Device, scan the QR code and enter the security code that Sophos/Google Authenticator displays.

Sophos Central opens.

The next time you sign in, you only need to enter a code from Sophos/Google Authenticator when prompted.

Sign in with email authentication

If you don’t have access to Sophos/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/Google Authenticator.

Reset an admin’s sign-in details

If an admin replaces or loses their phone, you can let them set up their sign-in again.

1. Go to the Users page.
2. Find the user and click on their name to open their details.
3. 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.

### 6.7.12 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. Just set up your caches before installation.

**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* (page 215).

#### 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 particular 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** (page 215).

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.
4. Click **Set Up Cache/Relay**.

Sophos Central automatically configures computers in your network to use a cache or relay. You can also manually assign computers to use a particular cache or relay.

**Assign computers to a cache/relay**

You can manually assign computers to use a particular cache or relay.

1. In Settings, go to the **Manage Update Caches and Message Relays** page.
2. Click on the link displaying the number of computers using the Update Cache or Message Relay.
3. Click on **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 on 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. Go to the System Settings > 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.

6.7.13 Allowed applications

At 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.

Important
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 knowledge base article 128136.
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).

**6.7.14 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.

To control updates, go to Settings > Controlled Updates.
You have these options.

- **Pause Updates Now** (page 99)
- **Pause Updates on a Set Date** (page 99)
- **Control Updates Manually** (page 100)

**Note**
Computers still get automatic security updates to protect them against the latest threats.

**Tip**
You can go back to automatic updating at any time.

### Pause Updates Now

You can stop product updates on all computers for 90 days. Your computers will still get automatic security updates.

On the **Settings > Controlled Updates** page, click on **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 resume product updates on all computers.
Automatic updates will stop for 90 days. Your computers will still get security updates.

1. On the **Settings > Controlled Updates** page, click on **Pause Updates on a Set Date**.
2. On the **Pause Updates on a Set Date** page, select a Start date and a Resume Date. Click **Apply**.

On the Resume date, the computers will start updating automatically and get any updates that are available.

**Tip**
If you want to resume updating earlier, click **Resume Automatic Updating**.

### Control Updates Manually

You can control product updates manually.
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 on Control Updates Manually.

**Important**
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** 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.

**Test the new version**

In the **Action** column, next to Test Computers, click **Update test computers to newest version**.

**Roll out the new 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**.

Why can I see a 'Previous' version now?

If Sophos releases another product update when you already have test computers on **Newest** 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.

### 6.7.15 Amazon Web Services Accounts

In Settings, on the **Amazon Web Services 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 an AWS Account** dialog:
   a) Enter a **Friendly Account Name**. This will be used to refer to the account in Sophos Central.
   b) Enter **IAM user credential** (Access Key and Secret Key) for the AWS account that you want to connect.
   c) Select **Add**.

   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, please see these articles:
   - Creating an IAM User for Sophos Central
   - Troubleshooting Sophos Central connections to AWS

When you have added the AWS account:
• AWS instances are listed on the **AWS Instances** page. 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.

### 6.7.16 Connect to Microsoft Azure

In **Settings**, on the **Connect to Microsoft Azure** 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 state** 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 [knowledge base article 127185](#).

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.

### 6.7.17 Data Loss Prevention Rules

You use Data Loss Prevention (DLP) rules to specify conditions for data loss prevention to detect, actions to be taken if the rules are matched, and any files to be excluded 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 List(s) in the rule to the specified destination.

You use Content Control Lists to match file content. For more information about Content Control Lists (CCLs), see Content Control Lists (page 106).

• **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.

| Manage Data Loss Prevention Rules |

This page lists the existing Data Loss Prevention 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, see Create a Data Loss Prevention Rule (page 104), and search existing rules.

You can also filter rules by **Type** (choose from **File** or **Content**) and **Source** (choose from **Custom** or **SophosLabs**).

Click on the name of a rule to edit it.

Click ![details](https://example.com) to view details of a rule.

Click ![clone](https://example.com) to clone a rule.

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.

Click ![export](https://example.com) to export custom rules. This creates an xml file containing the rule definition.

Click ![delete](https://example.com) to delete a rule. 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.

| Create a Data Loss Prevention Rule |

There are two stages to creating a DLP rule: creation and configuration.
Creating a DLP rule

This 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 on 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.

Configuring a DLP rule

This sets up the conditions for monitored files, file types or destinations and the exclusions for the rule.

The conditions you set depend on whether you are creating a File or Content rule.

1. To set up conditions for a content rule:
   a) Click on File contains and select the Content Control Lists you want to use.
      You can search the list of CCLs. You can filter the CCLs by Tags, Source (choose from SophosLabs or Custom) and Region. You can also create a new CCL, see Create Custom Content Control List (page 106).
   b) For each CCL: click on the matches and set the required number of matches.

Tip
Once the CCL has been matched for the set number of times it will trigger the rule.
2. To set up conditions for a file rule: Specify the file names or file types for the rule.

3. 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).

4. Set the exclusion details for the rule.

5. Click **Finish** to create the rule.

### 6.7.18 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 to 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. For more information on rules, see Data Loss Prevention Rules (page 103).

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 Content Control Lists in your rules, or create your own CCLs, see Create Custom Content Control List (page 106).

You can filter the CCLs by:

- **Region**
- **Source** (choose from **SophosLabs** or **Custom**)
- **Type**

You also can search the list of CCLs.

Click ![](image) to view details of a CCL.

For each custom CCL you can also:

- Click on the name of a CCL to edit it.

- Click ![](image) to export a CCL. This creates an XML file containing the definition for the CCL.

- Click ![](image) to clone a CCL. 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.

- Click ![](image) to delete a CCL. Click **Delete item** to confirm deletion.

You can also import Content Control Lists:

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

To create a custom Content Control List:
1. Click on **Add Custom Content Control List**.
2. Give the CCL a **Name** and a **Description**.
3. Click in **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 the text you want to match in **Terms** and click **Add Term**.
   - **All of these terms**: Enter the **Terms** and click **Add Term**.
   - **Exactly this phrase**: Enter the phrase you want to match in **Phrase**.
   - **Advanced Setup**: Use this option to set up an **Advanced Expression**, as described below.
5. Click **Save** to create the CCL.

### Set up an Advanced Expression

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 Content Control List is matched.
2. Enter a Perl 5 regular expression in **Expression**.
   - For a description of Perl 5 regular expressions, refer to Perl documentation or visit [http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html](http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html).
3. Set the **Score** for the CCL. This 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**.
   - Click **X** to delete an expression.
   - Click **✓** to edit an expression. Once you have finished your edit, click 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.
### 6.8 Protect Devices

At 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.

For more details on downloading and using each type of Server Protection installer, see these topics:

- [Server Protection](#) (page 117)
- [Server Protection on Microsoft Azure](#) (page 117)
- [Virtual Environment Protection](#) (page 118)

#### 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.

#### 6.8.1 Server Protection

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

Download the installer for your server operating system and run it on a server you want to protect.

When you protect a server:

- The server is added to the Servers list in Sophos Central.
- Default policies are applied to the server.

#### 6.8.2 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 [Server Protection > 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.

Follow the steps in the article to deploy the new VM.

### 6.8.3 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 **Server Protection > 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 clients.

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 circles in the legend to include or exclude information from a graph.

- Filled circle: Information is included
- Empty circle: Information is excluded

Get information on the following topics:

- 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 issues.</td>
</tr>
<tr>
<td>Critical</td>
<td>Access point is up but 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 is not configured.</td>
</tr>
</tbody>
</table>

- 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>
</tbody>
</table>
Untrusted | Network that doesn't belong to your account.
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.

- Security Heartbeat

<table>
<thead>
<tr>
<th>Client at risk</th>
<th>Active malware detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client may 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>Client is connected but the endpoint is not sending heartbeat</td>
</tr>
<tr>
<td>No Security Heartbeat™</td>
<td>Sophos Endpoint or Sophos Mobile Protection is not installed</td>
</tr>
</tbody>
</table>

Alerts

- **All**: Shows all alerts including high, medium, and info.
- **Warnings**: Shows access points that are offline or not broadcasting.
- **Info**: Shows updates or information.

Click **Details** for more information.

Clients

Number of clients connected. Click **Details** for more information.

Usage insight

Traffic generated by the wireless clients 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. This is caused by too many connected clients. Check you have enough access points to cover the area.

Medium

- **Access Point is offline**
  The access point has no internet connection, or has no power, or has experienced a software error. If a software error occurs, a restart may help.
- **Access Point is not broadcasting any network**
  There is currently no configuration on the access point. Configure the access point under Wireless > Access Points.
- **Access Point command done**
  The restart is done.

There are some alerts where restarting the access point may solve the problem:

- **Access Point configuration failed**
- **Access Point(s) failed to update to the new firmware**

Call Sophos Support. They will need remote access to investigate the issue ([Wireless > Settings > Remote Login to Access Points for Sophos Support](#)).

Low

- **Access Point will be updated with new firmware**
  Wireless is off for approximately 5 minutes.
- **All Access Points will be updated with new firmware**
  Wireless is off for approximately 5 minutes.
- **Access Point has been successfully updated with new firmware**
- **All Access Points have been successfully updated**

7.3 Clients

View information about the connected clients.

The connected clients are listed with name, MAC address, IP address, vendor, access point, SSID, Security Heartbeat™, connection speed, and band.
You can also search for a particular client by using name, MAC address, IP address, or vendor details. You can filter clients by using Show all Security Heartbeat™ enabled clients, Online, Offline, and Online and Offline.

Security Heartbeat categorizes clients based on the following:

- **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 red (high risk) state, you need to refresh the browser twice to access the walled garden. You can also download or update Sophos Antivirus from here.

- **No Security Heartbeat™**: Indicates that Sophos Endpoint or Sophos Mobile Protection is not installed on the listed clients.

- **Client may 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 client is connected but the endpoint has not been sending heartbeat for 90 seconds.

**Client Details**

Click on a client to see the following 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 client'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 clients in categories such as search engines, social media, or advertisements. Click on a category to obtain more information in the category details list.

**Note**  
To show the traffic generated by users, in categories, you must switch on the Usage Insight option in Settings (page 406).

**7.5 Wireless Diagnostics**

Diagnose and view events, system logs, audit logs, and capture packets for troubleshooting. For all wireless related events, see Events (page 380).

For all activities monitored by Sophos Central, see Audit Logs (page 381).
To capture wireless packets generated from remote access points, see Packet Capture (page 382).

To capture syslog data generated from access points, see Syslog (page 384).

### 7.5.1 Events

View access point generated wireless events categorized under high, medium, or low.

You can filter events and generate reports. All wireless events are categorized as:

- **High**: Events with high severity are generated when the connected client 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 Wireless Alerts (page 10) page. After the action taken (or ignored), alerts are no longer displayed but events are retained in the event list. The events list provides the following:

- **Severity**: Severity of event.
- **When**: Time and date of events.
- **Event**: Type of event.

#### Table 3: Type of wireless events

<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 clients is high and needs to be reduced.</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 for Security Heartbeat.</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>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>
</tbody>
</table>
### Filter events

You can filter events by:

- **Access point name.**
- **Date:** Use **From** and **To** to filter information. You can view events that occurred in the past 90 days or less.

### Export events

- **Export:** 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.

### 7.5.2 Audit Logs

View all activities monitored by Sophos Central.

Lists all activities monitored by Sophos Central. By default, activities for the past seven days are displayed on the page with the following details:

- **Date:** Date and time of the activity or change.
- **Modified by:** Sophos Central account that made the change.
- **Item modified:** Added, changed, or deleted items.
- **Description:** Details about the activity or change.
- **IP address:** IP address from where the activity or change originated.

### Filter audit logs

You can filter audit logs by:

- **IP address or Sophos Central account.**
- **Date:** Use **From** and **To** to filter information. You can view information for the last 90 days.

**Note**

You can combine the search and date fields to filter information. If you don't use the search option, all activities within the selected date range will be displayed.
Export audit logs

- **Export**: Export the audit logs in a CSV (comma separated value) or PDF file. You can export the current view or logs for the past 90 days.

## 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**. For more information, see [Access Point Details](#) (page 390).

**Note**

The access point can't capture its own transmitted packets. It can only capture received (rx) packets.

### Table 4: 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>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>APX</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>
<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>
</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.
Note
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, wlan or tzsp && !(icmp) can be used 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.

For more information, see Frequently asked questions (page 385).

Configuration

Prerequisites:
• 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.
• In order 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.

Use the configured server IP address and port number to start capturing network packets.
• Status: You can capture packets only when the access point status is green.
  — Access point is online.
  — Access point is offline.
• 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.

Note
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: 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>Status</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Completed</td>
<td>Packet capture is complete.</td>
</tr>
<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>

### 7.5.4 Syslog

Capture syslog data from access points to debug client'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.

For more information, see [Frequently asked questions](#) (page 385).

### Configuration

**Prerequisites:**

- Install a syslog server on the PC or server. There are various syslog servers available for different operating systems.
- 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.

Use the configured server IP address and port number to capture syslog data. You can use Start to capture system generated logs for a particular access point.

- **Status:** Indicates whether the access point is offline or online. You can capture syslog data only when the access point status is green.

**Table 5: Access point status**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="#" alt="Green Icon" /></td>
<td>Access point is online.</td>
</tr>
<tr>
<td><img src="#" alt="Gray Icon" /></td>
<td>Access point is offline.</td>
</tr>
</tbody>
</table>

- 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>Status</th>
<th>Description</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>

### 7.5.5 Frequently asked questions

See the most frequently asked questions related to packet capture and syslog data capture.

#### Packet capture

<table>
<thead>
<tr>
<th>Questions</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Why don't I see packets in Wireshark?          | • Check if the server IP is configured properly.  
• Check if Wireshark is running on the right interface  
• Check if there is an incorrect filter in the Wireshark  
• Check if the access point is offline while running the packet capture  
• Check if firewall allows port 37008 if the server IP is in different subnet  |
| What happens when Wireshark isn't running on the server? | The access point will still send the packets to configured server. You must start Wireshark to see the packets. |
| Can I capture packets on multiple access points? | Yes, you can capture packets on multiple access points.                                                                                  |
| Can I capture packets without assigning SSIDs.  | 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 Autochannel. |
| Is Packet capture feature supported on all access point firmwares? | Packet capture is supported on v2.1.0-1 or later.                                                                                       |
| Why can’t I start Packet capture when access point status is Grey? | The access point is offline. You cannot capture packets when the access point is offline.                                              |

#### 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>
</tbody>
</table>
### Question

Why has my syslog server stopped receiving data?

### Solution

Check if the access point is up and running. Also, check the connectivity between the access point and the syslog server.

## 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.
- **Serial number**: Access point's serial number.
- **Access point state**: Access point's status such as online or offline.
- **Workload**: Connected client load on the access point. The workload details such as Tx/sec (transmit signal rate), Rx/sec (receive signal rate), CPU usage, and memory usage are displayed.
- **Radios**: Configured radio bands on the 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 the 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 be either a root or a mesh. You can view the mesh 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 in the Sophos Resource Center.

### Register an access point

You can register access points individually or in bulk.

To register an access point:

1. Click **Register**.
2. Enter the serial number and then click **Register**.
The access point is validated.

3. Click **Next**.

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 register multiple access points:

a) Click **Bulk Provisioning** and upload your CSV file.

The access points are validated.

b) Click **Next**.

4. Enter the hostname and click **Save Hostname**.

Registration can take a few minutes. The access point is displayed in the list once registered.

**LED behavior**

**Table 6: LED behavior with APX series**

<table>
<thead>
<tr>
<th>LED</th>
<th></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>
<tr>
<td>Green – solid</td>
<td>• Normal operation.</td>
</tr>
<tr>
<td></td>
<td>• After configuration has been pushed.</td>
</tr>
<tr>
<td>Red – solid</td>
<td>• Ethernet is unplugged.</td>
</tr>
<tr>
<td></td>
<td>• Cloud is not reachable.</td>
</tr>
<tr>
<td></td>
<td>• 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>

**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>Name</td>
<td>Standards</td>
<td>Band</td>
<td>Band for Mesh Networks</td>
<td>FCC regulatory domain (mainly US)</td>
<td>ETSI regulatory domain (mainly Europe)</td>
<td>Client capacity per radio</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------</td>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------</td>
<td>--------------------------</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>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 100</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 100C</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>APX 120</td>
<td>802.11a/b/g/n/ac wave2</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>
### Outdoor 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 100X</td>
<td>802.11a/b/g/n/ac</td>
<td>2.4/5 GHz dual-band/dual-radio</td>
<td>2.4 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.

**Note**
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 7: TX power reference**

<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>

**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.

**Note**
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.

**Note**
For clients 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 clients 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.
For advanced settings, see Advanced Settings (page 396)

Basic Settings

Configure basic settings for your SSID.

SSID
Enter a name. SSIDs are case-sensitive and must satisfy the following criteria:
• Between 1-32 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 recommend that you use this as it is a quick and strong cipher and is widely accepted.

Passphrase
Enter a passphrase between 8-63 ASCII printable characters to protect the SSID from unauthorized access.

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.
For more information on which access point types support the 5 GHz band, see Access points (page 386).

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. For more information, see Mesh Networks (page 393) and Create a Mesh Network (page 395)
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.

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.
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.

**Troubleshooting**

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:
- 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:
• 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.

There are not all access points in the mesh network:
• 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.

Related concepts
Access Point Details (page 390)
Configure, restart, or manage your access points.
Settings (page 392)
Configure, assign, and save your settings.

7.7.2 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 are able to 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.

Note
To use this feature, you need to have an Endpoint Advanced Protection license for your endpoints. For mobile protection, go to Setup > System setup > Network access control, and select Central 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.

**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.

**Important**
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 restriction. 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.

  For more information, see [Create a guest network](page 401).
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 Mangement 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 re-connect 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 client's capability between 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 dual-band devices 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. For more information, see Create a Hotspot (page 402).

**Attention**

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 and is visible to the user to accept the 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 are 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. For more information, see Create a voucher (page 403).

**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 to a specific website of your choice. For example, your company page.

---

**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 particular 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>
<tr>
<td>NAT Mode</td>
<td>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</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>communicate with each other, but can access the internet.</td>
</tr>
<tr>
<td>a) <strong>Primary DNS Server</strong>:</td>
<td>Specify the DNS server IP address to be used by clients when connected to the guest network.</td>
</tr>
<tr>
<td>b) <strong>Secondary DNS Server</strong>:</td>
<td>Specify the secondary DNS server IP address to be used by clients when connected to the guest network.</td>
</tr>
</tbody>
</table>

**Note**

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. Provide 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.

**Attention**

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 which can be turned into a hotspot.

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.
4. Select an authentication type to define how users can access the hotspot.

   **Note**
   It is not secure to use no authentication.

5. Select **Custom URL** if you want to redirect users to a specific URL after authentication.
6. 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:
- This is normal behavior.

Re-login required when roaming:
- This is normal behavior for security reasons.

LED on the access point is red:
- There is no connection to Sophos Central, try to reconnect.

**Note**
Passwords and vouchers will not expire.

**Related concepts**
- **SSIDs** (page 391)
  Configure and manage your Service Set Identifiers (SSIDs).
- **Settings** (page 392)
  Configure, assign, and save your settings.

**Create a voucher**
Create a voucher for the hotspot.
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:
   - **Name**: Enter a name.
   - **Access time**: Use the start and end date to set a time period for access. You can also make it always accessible.
   - **Timezone**: Set the timezone.
   - **Amount of vouchers**: Set the number of vouchers.
   - **Valid for**: Set the period the voucher is valid for.
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 SSIDs

The neighborhood SSIDs 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. Clients 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 based on the following:

<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.
Note
To show neighborhood SSIDs, you must enable Rogue Access Point Detection on the Wireless System Settings (page 406) page.

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.

1. Go to Sites and click Create.
2. Type the location.

Tip
Sophos Central uses Google maps. You must enter a real address.

3. Select access points you want to add to the site.

Note
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.

1. Go to Sites and click on a site.
2. Click on Create a floor.
3. Add a floorplan.

Note
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.
Note
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
Specify security settings for your access points.
The pages displayed depend on the features included in your license. Some of these pages may be displayed under Global Settings in Overview, if you have more than one product.

7.9.1 Wireless System Settings
Manage the firmware and wireless system settings.

Basic 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, see Events (page 380) and Audit Logs (page 381).
Diagnostics

**Forward access point logs**
Access point logs are forwarded to Sophos Support. We recommend that you turn on this option for debugging purposes.

**Remote Login to Access Points for Sophos Support**
Sophos Support will 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 listed in Usage Insight (page 379). 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 https://community.sophos.com/kb/en-us/123333.

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, see Sites (page 404).

Advanced roaming optimization

**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 advertises 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 Security is only available if you have a Sophos Email license.

Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Set up Email Security (page 111).

8.1 Email Gateway Dashboard

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

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

Inbound activity summary

**Inbound Activity Summary** shows information about the following message categories:

- **Legitimate**: Messages that are classified as clean, and therefore delivered.
- **Spam**: Messages classified as spam.
- **DLP policy violations**: Messages that violated Data Loss Prevention policies.
- **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 blacklist**: Messages detected due to a blacklisted sending IP.
- **Company blacklist**: Messages sent from an address that has already been added to the company blacklist (inbound allow/block).

Click **See Report** to open the **Message Summary** report and review the details of the processed messages, see Message Summary Report (page 42).

Outbound activity summary

**Outbound Activity Summary** 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 (page 42).
**Sandstorm activity summary**

**Note**
Sandstorm is only available with the 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** report and review the details of the processed messages, see **Sandstorm Activity Summary** (page 43).

**Note**
Sandstorm only checks messages from mailboxes where you’ve enabled it in the policy.

**Top at risk users**

**Top at risk users** shows the users that have clicked the most malicious links within the last 30 days.

Click **See Report** to open the **At risk users** report and review the details of the most at risk users, see **At risk users** (page 44).

Click **Create phish threat campaign for these users** to create a Phish Threat campaign which automatically includes the top at risk users.

**8.2 Message History Report**

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

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

- **Search**: You can search emails by subject, sender or recipient.
- Use the **From** and **To** fields to select the time period for which you want to view the email processing history. You can view email that has been processed in the past 30 days or less. By default the report displays the emails that have been processed during the current day.
- **Direction**: Select **Inbound** or **Outbound** from the drop-down menu to view emails that have been received or sent.
- Select **Status** from the drop-down menu to filter emails by status.
- **Update**: Click this to refresh the report if you have changed the date range, entered a search term or filtered the emails.

**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.
— **Deleted**: The email was deleted due to its content or block list configuration.

**Note**
When you select **Deleted**, you can select a **Reason** for deletion from the drop-down menu. Choose from, **Customer block list**, **Header Anomaly**, **Spam**, **User block list**, **Virus**, **Malicious URL**, **Advanced threat** and **All**.

— **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.

**Note**
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, see **Email Security Policy** (page 428).

- **Date**: Date and time the email was processed.
- **Sender**: The sender of the email.
- **Recipients**: The recipient(s) of the email.
- **Subject**: The subject line of the email.

**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.
  Click **Block IP** if you want to add the IP to the Inbound Allow/Block list then click **Block** to confirm your choice.

**Note**
Any sender using this IP address is blocked.
Click **Cancel** to cancel the action. See Inbound Allow/Block (page 108).

Click on the **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. For more information, see https://tools.ietf.org/html/rfc3463.

- **Raw Header**: shows the email header details.
- **Attachments**: shows the name and size of attachments.

### 8.3 Message Summary Report

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

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

Use the **From** and **To** fields to select the time period for which you want to view processed messages. 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 Security.
- **Legitimate**: Messages that have been allowed.
- **Spam**: Messages classified as spam.
- **DLP policy violations**: Messages that violated Data Loss Prevention policies.
- **Virus**: Messages classified as containing viruses.
- **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 failure**: Messages that failed authentication by DMARC, SPF or DKIM.

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

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

### 8.4 Sandstorm Activity Summary

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

The **Sandstorm activity summary** report details the email messages processed by Email Security for your protected mailboxes.

Use the **From** and **To** fields to select the time period for which you want to view processed messages. 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 and are classified as follows:

- **Scanned**: All messages checked by Sandstorm.
- **Legitimate**: All messages that are not classed as spam or do not contain advanced threats.
- **Advanced threat**: All messages that have been classified as containing advanced threats.

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** selected and all message types.

### 8.5 Time of Click Summary

This option is only available with an Email Advanced license.

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

Use the **From** and **To** fields to select the time period for which you want to view processed messages. 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 option is only available with an Email Advanced license.

The **At risk users** report details all the users that have triggered Time Of Click protection in the last 30 days by clicking malicious links.

Use the **From** and **To** fields to select the time period for which you want to view details of at risk users. You can view details for the last 60 days or less. Details for the last 30 days are shown by default.

Click **Create phish threat campaign** to open the phish threat campaign wizard. The at risk users for the date range you have selected are automatically included in the campaign. You can also add and remove users manually.

You can see the following information in the report:

- **User**: The email address of the at risk user.
- **Risky sites clicked**: The total number of malicious links the user has clicked on.
- **Blocked sites**: A list of the clicked links that were blocked by Time of Click protection, and the number of times they were clicked on in total.
• **Warned sites**: A list of the clicked links that generated a warning from Time of Click protection, and the number of times they were clicked on in total.

## 8.7 People

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

### 8.7.1 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 sections below tell you about the users list and how to manage users.

### About the users list

The current users are listed with their details:

- **Security status.** An icon shows whether the user has security alerts on any of their devices:
  - Green check mark if there are low-priority alerts or no alerts.
  - Amber warning sign if there are medium-priority alerts.
  - Red warning sign if there are critical alerts.

  Click on 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, see Administration Roles (page 76).

  This column is only visible if you are an administrator.

Click on 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 on the user's name. For more information, see User Summary (page 48).

### Add a user manually

This also gives you the option to let the user protect their own devices.

You can add an individual user and protect them as follows.

1. On the **Users** page, click **Add** and select **Add User**.
2. In the **Add User** dialog, enter the following settings:
First and Last Name. Enter the name of the user. Do not include a domain name.

Role. Select an administration role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

A user who is assigned an administration role will receive an email telling them how to set up their administration account.

Important
You can only see the Role option and assign administrator roles if you are a SuperAdmin.

Note
Anyone with a User role only has access to the Self Service Portal.

Email Address. Enter the email address of the user.

Add to Groups (optional). Select one of the available user groups and use the picker arrows to move it to the assigned groups.

Tip
You can start typing a name in the search box to filter the displayed 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.

3. Click Save or Save & 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 by protecting their devices

You can add users automatically as follows.

Download an installer and run it yourself on a device (or devices). This adds the user of each device automatically. For installers, see the Protect Devices page.

Import users from a CSV file

This option may not be available for all customers yet.

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 do this:

1. On the Users page, click Add and select Import users from CSV.
2. Click Browse and select your CSV file.
**Tip**
You can download template CSV files from the **Import Users from CSV** dialog.

3. The CSV file can include groups a user is assigned to. To create groups not available yet, select **Create new groups**.

4. To send a registration email for the Sophos Central Self Service portal to each imported user, select **Activate new users**.

5. 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.

On the **Users** page, click the **Set up Active Directory Sync** link in the upper right of the page. Then see Set up synchronization with Active Directory (page 73).

**Protect existing users**

To email users you have already added to the list or imported:

1. On the **Users** page, select the user or users you want to protect. Click **Email Setup Link** in the upper right of the page.

2. In the **Email Setup Link** dialog, you are prompted to select the types of protection the user needs (if your license includes more than one).
   
   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.

**Modify users**

To modify a user's account:
On the Users page, click the user's name to open and edit their user details. For more information, see User Summary (page 48).

Delete users

To delete a user or users:

On the Users page, select the checkbox next to each user you want to delete. Click the Delete button in the upper right of the page.

**Important**
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them, see Administration Roles (page 76).

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

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

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 will be added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they will be added as a user again the next time that Sophos Central synchronizes with Active Directory.

Export to CSV

To export a list of users:

Click on Export to CSV.

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

For example you can export a list of administrators by applying the Admins Only filter before clicking Export to CSV.

**Related concepts**
Active Directory Sync (page 72)

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.

Security status

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

- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
- Red warning sign if there are high-priority alerts.

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 and Last name**: Enter the name of the user. Do not include a domain name.
   - **Role**: Select a role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

   **Important**
   You can only see the Role option and assign administrator roles if you are a SuperAdmin.

   **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 (optional)**: 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.

**Important**
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.

For information on how policies work, see About Policies (page 425).

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 group(s) 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.

### 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 knowledge base article 128136.

Click the Details link beside the event and then allow the application, see **Allowed applications** (page 97).

**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.

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.

8.7.2 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 on the group’s name. For more information, see User Group Details (page 54).

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.
   Members: 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 (page 54).

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.
- 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.

**8.8 Mailboxes**

Email Security is only available if you have a Sophos Email license.
Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Set up Email Security (page 111).

On the Mailboxes page you can manage Email Security for users, distribution lists and public folders. All protected mailboxes are listed.

You can add a mailbox or import a list of email addresses without using Active Directory Synchronization or Office 365.

Active Directory Sync status is shown on the right of the page. You can 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 aliases, members and other associated information.

**Tip**
The mailbox type is indicated by its icon. Hovering over the mailbox icon displays its type.

### Add a mailbox

You can add individual mailboxes. To do this:

1. Click **Add** and select **Add Mailbox**.
2. Choose whether you want to add a mailbox for a user, distribution list or public folder.
3. Enter the details for the mailbox and click **Save and Add Another** or **Save**.

### Import Mailboxes & Aliases

You can import a list of mailboxes and aliases using a CSV file. This allows you to add email addresses and aliases without using Active Directory Synchronization or Office 365. To do this:

1. Click **Add** and select **Import Mailboxes & Aliases**.
2. Click **Browse** and select your CSV file.

**Tip**
Template CSV files are linked on the left of the **Import Mailboxes & Aliases** dialog.

3. Click **Add**.

You can edit the aliases for a mailbox, see Mailbox (page 423).

### 8.8.1 Mailbox

Each mailbox has a set of information associated with it such as name, type or policies. The information set depends on the type of mailbox.

The mailbox type, name and creation date is shown in the left-hand pane. There are three types:

- **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.

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

**Details**
You can view the policies and other associated information for a mailbox in the **Details** tab.

- **Policies**: This is a list of the policies used for the mailbox. Policies define the security measures that will be used for your users' email.

  **Note**
  Email Security is only available in the Base user policy.

- **Aliases**: This is a list of the email addresses that act as aliases for the main email address. You can add and remove aliases. Click **Edit** to make changes.

### 8.9 Quarantined Messages

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

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

It shows the messages received in the last 24 hours, by default. You can view the quarantined messages for the last 30 days.

You can also:

- Release messages from quarantine and send them to users. Select the message(s) and click **Release**.
- Delete quarantined messages. Select the message(s) and click **Delete**.

Click on a message subject to view the quarantined email message. This opens the **Message Details** dialog where you can view more details about the message, the raw header information, message contents and any attachments. You can release or delete a message in the **Message Details** dialog. Within **Message Details**, you can add an IP to your blocklist. See **Inbound Allow/Block** (page 108).

**Related concepts**
- **Set up Email Security** (page 111)
- **Data Loss Prevention** (page 435)
### 8.10 Policies

A policy is a set of options that Sophos Central applies to protected mailboxes.

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.

#### 8.10.1 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 particular 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.
8.10.2 Email Policies

You can now create multiple email security policies which can be applied to users, groups and domains.

Note
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.

You can create or edit a policy as follows.

Create a policy

1. Go to Email Gateway > Policies.
2. Click Add Policy (in the upper right).
3. On the Create New Email Policy page, use the tabs to:
   • Assign the policy to users, groups or domains.
     
     Note
     Domains refers to domains that you manage. If you select a domain, the policy will apply to all email addresses within the domain.
     
     • Enter settings for the policy. You can activate specific settings for different policies. For information on configuring settings, see Email Security Policy (page 428).
     • On the Policy Enforced tab you can enable or disable the policy. You can automatically disable the policy at a specific time.

Edit a policy

1. Go to the Email Gateway > Policies page.
   You will see a list of the policies you created and the base policy (default).
2. Find the policy you want to edit and click it.
3. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users, devices or domains.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.
8.10.3 Email Security Policy

Email Security is only available if you have a Sophos Email license.

Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Set up Email Security (page 111).

- Edit the Email Security policy. See Email Policies (page 427).
- Open the policy's Settings tab and configure it as described below. Make sure the policy is enabled.

If you're new to policies, see About Policies (page 425).

Note
The following settings only apply to inbound messages with the exception of Enhanced Email Malware 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.

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 and emails sent to you from a mailing list.
- **Suspected Spam**: These are messages that have been identified as suspicious.
- **Non-Spam**: These are messages that are confirmed to come from a trusted source and or contain no spam characteristics.

For each category choose an Action from:

- **Quarantine**: Message is quarantined.
- **Deliver**: Message is sent to the mail server for delivery.
- **Delete**: Message is deleted.
- **Tag subject line**: The message is tagged and delivered. The tag appears at the start of the subject line in the message. You can customise the tag, using up to 30 characters.

**Important**
You can only tag the subject line for Spam, Bulk and Suspected Spam messages.
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. 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 Central Admin then **Global Settings**. Under **Email Gateway**, go to **Self Service Settings** and turn the **Allow/Block List** option on.

**Note**
If a sender is already allowed, no **allow sender** or **block sender** links are displayed in the banner.

Emails from Sophos, for example, **Quarantine Summary** will not display banners.

**Important**
If your outbound gateway is not configured to route through Sophos, external recipients can view the banner and modify end-user allow and block lists.

We strongly recommend that you configure your outbound gateway to route through Sophos before turning **Smart banners** on. This means that we can strip the banner on replies and forwards outside the company. To configure your outbound gateway to route through Sophos, see **Manage Domains** (page 109).

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).

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. Switch on the sending of quarantine summary messages.
2. Select the **Time Zone, Days** and **Time** you want the messages sent.

**Tip**
All days are selected by default. Click on the day to deselect it.

3. One **Time** slot is shown by default, however you can add more by clicking on **Add another**. You can add three more. To delete a **Time** slot, click the delete icon next to the **Time** slot.
Note
The default Time slot can't be deleted.

4. Click Save.

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 to do this. Sender checks are performed in the order they appear on the UI. If an email fails the first sender check, the other checks will not be carried out.

Note
You can override the sender checks by adding domains and email addresses to the Allow list.

- **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: Message is sent to the mail server for delivery.

- **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 from addresses. This results in an SPF check rejecting the email.

- **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:
  
  Reject: Message is rejected. (This is the default value).
  
  Quarantine: Message is quarantined.
  
  Tag subject line: Email Security adds a tag to the message's subject line indicating that it is a spoofed message.
  
  Deliver: Message is sent to the mail server for delivery.

- 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**: Message is sent to the mail server for delivery.

For more information on Sender Checks, see **Sender Checks** (page 433).

### Enhanced Email Malware Scan

- **Enhanced content and file property scan**

**Note**
This setting applies to inbound and outbound messages.

This is an enhanced email content and file property scan and it is our highest level of protection against email malware. It is on by default.

**Important**
If malware is detected in a message, it is always discarded.

- **Manage emails that we can't scan**

**Note**
This setting applies to inbound messages only.

You can choose what happens to messages that are unscannable. There are three available actions:

- **Quarantine**
- **Delete**
- **Quarantine**

There are various reasons we may not be able to scan specific messages:

**Note**
The examples given are not totally comprehensive.
— 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.

Note
Email addresses and domains that you add to the Allow list and Sophos encrypted emails won't be scanned.

Email Advanced license features

These features are only available with an Email Advanced license.

When a new Email Advanced license customer is created, these features are turned on by default. They are also turned on when a new policy is created. (This applies to both existing and new Email Advanced licenses.)

- **Time of Click URL Protection**: 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 medium risk websites set to **Allow**, once the link has been checked and has been classified as not malicious, the link will take you to the original link destination.

  Note
  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.

Choose either **Block**, **Warn**, or **Allow** for each reputation category. You cannot **Allow** high risk websites.
You can also control whether URLs are rewritten in plain text messages, within securely signed messages and within attachments.

**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 **Rewrite URLs in plain text messages**.

**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 **Rewrite URLs within securely signed messages**.

**Important**
Please use caution if you choose to bypass URL re-writes, as URLs in these messages will not be protected.

For more information on SXL lookups, see knowledge base article: **Information on Sophos Extensible List**.

- **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. For further information, see **Sophos Sandstorm**

When Sandstorm is enabled, you can select your preferred sandbox location.

**Note**
Select **Let Sophos Decide** 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.

**Sender Checks**

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.

For more detailed information, see SPF: Sender Policy Framework.

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 its own hash that it compares it to the decrypted hash. If these do not match, the DKIM check will fail.

For more detailed information, see http://dkim.org/

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. Sophos Email's 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.

For more detailed information, see https://dmarc.org/

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 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 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.

8.10.4 Data Loss Prevention

This feature is only available with an Email Advanced license.

To add a new Data Loss Prevention rule, go to Email Gateway > Policies and click Add Policy. Select the Data Loss Prevention option and click Continue.

Add the Users, Groups and Domains you want the policy to apply to.

Under Settings, the rules are listed for inbound and outbound emails. You can turn the rules on and off. To view and edit rule settings, click on the rule name.

Only one action can be applied to each rule for example, Quarantine. When you create the policy, the action is set to the Sophos default. You can change this when you create or edit the rule.

Note
Rules are applied based on the action with the highest severity. Only the rule with the highest severity action will be applied to the email. For example, if one rule is set to delete emails containing specific keywords, and the email contains one of the keywords, it will be deleted and no other rules will take effect.

- Attachment file types: Specify the attachment types you want to filter. We recommend you use the default Sophos list. See Sophos default blocked file types (page 436). You can also use the custom list, and select the file type categories and file types within the categories you want to filter messages by. Choose the action you want to take when the attachment types are present in an email. The available actions are:
  - Quarantine: Quarantines emails containing any of the attachments on your list.
  - Encrypt: Encrypts emails containing any of the attachments on your list.
  - Strip attachments and deliver: Removes any attachments then delivers the email. You have the option to add a tag to the subject line. You can use the preset tag or add a custom tag.
  - Delete: Deletes emails containing any of the attachments on your list.
- Keywords: Specify the keywords you want to filter in the email subject, body or attachment name. You can add a maximum of 200 keywords. Keywords are case-insensitive. Choose the action you want to take when the keywords are present in an email. The available actions are:
Sophos Central Admin

— Quarantine: Quarantines emails containing any of the keywords on your list.
— Encrypt: Encrypts emails containing any of the keywords on your list.

Note
This option is only available when Encryption is turned on. It applies to outbound messages only.

— Strip attachments and deliver: Removes any attachments then delivers the email. You have the option to add a tag to the subject line. You can use the preset tag or add a custom tag.

Note
This action will only trigger if the keyword is located in the attachment name.

— Delete: Deletes emails containing any of the keywords on your list.

Sophos default blocked file types

The following file types will be blocked when you select Use Sophos list (recommended) in the Attachment file types rule:

• bat
• chm
• cmd
• com
• cpl
• crl
• exe
• hlp
• hta
• inf
• ins
• isp
• jse
• lnk
• mdb
• pcd
• pif
• reg
• scr
• sct
• shs
• APK
• ELF
• JS
• MACHO
• MS-DOS
• PIF
• VBE
• VBS
• WSF
• Microsoft Office document containing macros
• Obfuscated Script
• WebAssembly

8.11 Settings

The Settings pages are used to specify security settings that apply to your protected mailboxes. The pages displayed depend on the features included in your license. Some of these pages may be displayed under **Global Settings** in **Overview**, if you have more than one product.

**Note**
If you want to apply settings only to certain users, servers or devices, use the Policies pages instead.

8.11.1 Active Directory Sync

You can import users and groups from Active Directory to Sophos Central.

In Setting, 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.
• You can also configure settings for Azure Active Directory Synchronization.

**Note**
If you are using Office 365 you must use this option.

For instructions on setting up the utility, see **Set up synchronization with Active Directory** (page 73). For full details of how it works, see **About Active Directory synchronization** (page 73). Once you have set up synchronization you can review its status and other settings, see **Active Directory Sync Status** (page 72).

For instructions on configuring Azure Active Directory synchronization, see **Set up synchronization with Azure Active Directory** (page 75). Once you have set up synchronization you can review its status and other settings, see **Azure AD Sync Status** (page 75).
Active Directory Sync Status

In Settings, on the Active Directory Sync Status page, once you set up Active Directory synchronization, you can view:

Status

• The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
• The number of users and groups imported from Active Directory.
• The time of the last synchronization with Active Directory.

You can view Active Directory synchronization alerts on the Alerts page You can view synchronization events on the Logs & Reports > Events page.

Sync Status

This shows the synchronization settings in Active Directory.

About Active Directory synchronization

Active Directory synchronization allows administrators to implement a service that maps users and 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 or groups.
• It supports automated, one-way synchronization from the Active Directory to Sophos Central. It does not support two-way synchronization between Sophos Central and Active Directory.
• For users imported from Active Directory:
  — You cannot modify their name, email, or Exchange login, or add or change or remove associated groups or logins managed by Active Directory.
  — You can add, change or remove groups or logins that are not managed by Active Directory.
• For groups imported from Active Directory:
  — You cannot modify their name.
  — You can add, change or remove groups or logins that are not managed by Active Directory.
• 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. Any information added or updated from the Active Directory cannot be edited in the console.
• 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 AD forest. We strongly recommend to synchronize different AD 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 deploying with Active Directory.

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.

To set up synchronization with Active Directory:
1. In Settings, on the Active Directory Sync page, click the link to download the Sophos Central AD Synchronization Utility installer, and then run it.
2. In the setup wizard, enter the information required.
   Follow the instructions in the Sophos Central AD Sync Utility Setup Wizard.
3. On the last page of the setup wizard, 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.
   The Sophos Central AD Sync Utility Setup Wizard starts.
4. On the Sophos Credentials page, enter your Sophos Central account credentials.
5. 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, 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.
6. 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.

<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</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>The above query will limit user discovery to users belonging to “testGroup”. Note that unless a group query filter is also specified, 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>

**Important**

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.

7. 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**.

8. 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 Sophos Central. To stop the synchronization in progress, click **Stop**.

**Azure AD Sync Status**

In Settings, on the **Active Directory Sync Status** page, once you configure Azure AD synchronization, you can view:

- The status of Azure AD synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Azure AD.
- The time of the last synchronization with Azure AD.

**Note**

Auto synchronization happens every 6 hours. You cannot change this interval.

- The configuration settings for Azure AD synchronization.

You can amend these by clicking **Edit**, see Set up synchronization with Azure Active Directory (page 75).
Click **Sync** to run the synchronization process.

You can validate the Azure Sync connection by clicking **Test Connection**.

You can view Azure AD synchronization alerts on the **Alerts** page. You can view synchronization events on the **Logs & Reports > Events** page.

**Set up synchronization with Azure Active Directory**

Azure AD sync is only available if you have a Sophos Email license.

To configure Azure Active Directory synchronization:

1. In Settings, on the **Active Directory Sync** page, click the link to configure the settings for Azure AD Sync.
2. Set up your Azure Applications, if required.

   **Tip**
   Click the link to the instructions if you need help with this.

   You can skip this step if you have already set up an Azure application.

3. Configure the Azure Sync Settings:
   a) Enter the **Client ID**.
   b) Set the **Tenant Domain**.
   c) Enter the **Application Key** and set its 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.

4. Click **Test Connection** to validate the Azure Sync connection.
5. Click **Save**.
   Synchronization starts. This process may take some time.

**8.11.2 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.

**Important**
You can only see this option if you are a **SuperAdmin** 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.

**Important**
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. These roles cannot be edited or deleted.

**Important**
Your assigned administrator role affects what you can do.

**Note**
Anyone with a **User** role only has access to the Self Service Portal.

The available administration roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can’t...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Super Admin</strong>&lt;br&gt;There must be at least one administrator with a SuperAdmin role.</td>
<td>Have access to everything in Sophos Central.&lt;br&gt;In addition they can:&lt;br&gt;• Manage roles and role assignments</td>
<td>There are no limitations.</td>
<td>None.</td>
</tr>
<tr>
<td><strong>Admin</strong></td>
<td>Have access to everything in Sophos Central.</td>
<td>Manage roles and role assignments.</td>
<td>No Role Management options are displayed.</td>
</tr>
<tr>
<td><strong>Help Desk</strong>&lt;br&gt;Have read-only access for all settings in Sophos Central. In addition they can:&lt;br&gt;• Look at sensitive logs or reports.&lt;br&gt;• Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.&lt;br&gt;• Update the Sophos agent software on a computer.&lt;br&gt;• Scan computers.</td>
<td>Manage roles and role assignments. In addition they can’t:&lt;br&gt;• Assign policies.&lt;br&gt;• Change settings.&lt;br&gt;• Resolve alerts on the individual device.</td>
<td>No Role Management options are displayed.&lt;br&gt;In addition:&lt;br&gt;• All other options apart from those related to receiving and clearing alerts are read-only.&lt;br&gt;• Some options, such as Edit buttons, are not displayed.</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>Administrators with this role...</td>
<td>Administrators with this role can't...</td>
<td>User Interface Restrictions</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------</td>
</tr>
</tbody>
</table>
| Read-only  | Have read-only access for all settings in Sophos Central. In addition they can:  
• Look at sensitive logs or reports.  
• Receive alerts. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers. | No Role Management options are displayed. In addition:  
• All options are read-only.  
• Some options, such as Edit buttons, are not displayed. |
| User       | Have no administration capabilities. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers.  
• Look at sensitive logs or reports. | Has access only to the Self Service Portal. |

If you have Intercept X with EDR, please see Administration Roles for Intercept X with EDR (page 79).

Permissions

This is the access level for a role. The options are Full, Help Desk or Read-only.

Additional 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 assignment to users/devices**: This option means that an administrator can assign policies to users and devices.

- **Notifications**: This option means that an administrator can receive and clear alerts.

Note

Read-only administrators can only receive alerts.
Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details, see User Summary (page 48).

**To 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.

**Note**

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.

1. Click **Edit**. This opens the **Edit Role Members** window.

   **Note**

   You can only see this option if you are a **Super Admin** administrator.

2. Select a user in the **Available Users** list and use the picker arrows to add them to the **Assigned Users** for the role.

   **Tip**

   Enter a name or part of a name in the search box to filter the list of available users.

**To delete 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.

1. Click **Edit**. This opens the **Edit Role Members** window.

   **Note**

   You can only see this option if you are a **Super Admin** administrator.

2. Remove assigned administrators from the role by selecting 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.
# Administration Roles for Intercept X with EDR

For general information on Administration Roles, see Administration Roles (page 76).

The available administration roles for Intercept X with EDR are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can't...</th>
</tr>
</thead>
</table>
| **Super Admin** | • 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. | There are no limitations. |
| **Admin**     | • 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. | There are no limitations. |
8.11.3 Federated sign-in

You must be a Super Admin to turn on federated sign-in for your administrators and users. You can allow your administrators and users to sign in to Sophos Central and the SSP using their Microsoft sign-in credentials.

**Note**
When you turn on federated sign-in administrators and users can still sign in using their Sophos Central credentials.

**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.

**Note**
Sophos Central is not supported on mobile devices.

An Azure AD admin must give permission for Sophos Central to use federated sign in before you can turn it on. Once an admin gives consent, it means your Azure AD tenant trusts Sophos Central and administrators can sign in with their Microsoft credentials. See [https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience](https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience) for more information.
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 turn on federated sign-in:
1. Click Federated sign-in in Settings.
2. Click Sign in with Sophos Central Admin or Microsoft credentials.

8.11.4 Synchronized Security

Note
Synchronized Security is only available if you have a Sophos Endpoint license and a Sophos Email license.

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.

You can turn the Synchronized Security feature on and off from Global Settings > General > Synchronized Security.

• The originating mailbox is identified.
• The owner of the mailbox is identified, along with any devices assigned to the owner of the mailbox.
• The mailbox is blocked from sending emails for 1 hour. After 1 hour, the mailbox is unblocked automatically.

Important
The amount of time the mailbox is blocked for is doubled every time the spam threshold is reached. 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 mailbox should be unblocked, please contact Sophos Support.

• Sophos Anti-Virus runs an on-demand scan on the devices linked to the mailbox.
• An alert is sent to the administrator saying that the sender has been blocked.
• 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.

8.11.5 Inbound Allow/Block

The Inbound Allow/Block list is part of Email Security and this option is only available if you have a Sophos Email license.

Email Security provides protection against spam, spoofing, viruses and malware. Set up Email Security, if you have not already done so, see Email Security Policy (page 428).

• Allow/Block lists help you to control spam. You create a list of email domains and addresses that you trust or don't trust. This list is global and applies to all protected mailboxes.
• 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. See Message History Report (page 39) and Quarantined Messages (page 424).

• You can block or allow an entire domain or specific email addresses. The domain or email address is added to the list and shown as either allowed or blocked.

• This setting only applies to inbound messages.

• 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).

In Settings, on the Email Security > Inbound Allow/Block page you can:

• Add an allowed domain or address

• Add a blocked domain or address

• Remove a domain or address

Add an allowed domain or address

To add an allowed domain or address:

1. Click on Add at the right side of the page above the Inbound Allow/Block list.
2. Select Add Allow from the drop-down list.
3. Enter a single domain name or email address in the Email Address or Domain text field. Example: example.com or jane.smith@example.com.
4. Choose whether you want to Override duplicates.

Note
If you add the same address or domain to both the allow and block lists, Override duplicates uses the most recent option you chose.

5. Click OK.

The allowed email address or domain is added to the Inbound Allow/Block list.

Add a blocked domain or address

To add a blocked domain or address:

1. Click on Add at the right side of the page above the Inbound Allow/Block list.
2. Select Add Block from the drop-down list.
3. Enter a single domain name or email address in the Email Address or Domain text field. Example: example.com or jane.smith@example.com.
4. Choose whether you want to Override duplicates.

Note
If you add the same address or domain to both the allow and block lists, Override duplicates uses the most recent option you chose.
5. Click OK.
   The blocked email address or domain is added to the Inbound Allow/Block list.

Remove a domain or address
To remove a domain or address:
1. Select the entry you want to delete from the allow/block list.
2. Click Delete at the right side of the page above the Inbound Allow/Block list.
3. Click Yes to confirm deletion.

8.11.6 Manage settings for Sophos Central Self Service
This option is only available if you have an Sophos Email license.
Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Set up Email Security (page 111).
In Settings, click Self Service Settings, 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.

8.11.7 Manage Domains
Email Security is only available if you have a Sophos Email license.
Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Email Security Policy (page 428).
You configure and manage protected email domains on the Email Security > Settings > Domain Settings/Status page, using the options described below.

Add a domain
To add a domain:
1. Click Add Domain (on the right of the page).
Tip
Instructions on how to set up your domain for common providers are available. Example: Office 365.

To view the instructions:

a) Expand Information to configure External Dependencies.
b) Click Instructions for Common Providers.
c) Click Inbound Settings and click the link for your chosen provider.
d) Use the information to help you configure your email domain.
   Click Outbound Settings to view your outbound relay host.

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.

   Note
   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 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 a 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 a FQDN in the FQDN 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.

1. Make a note of the appropriate settings so that you know where to allow SMTP traffic from.
2. 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, see [Email Security Policy](#) (page 428).

### Important

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:

1. Click on the **X** to the right of the domain you wish to remove.

#### Edit a domain

To edit a domain:

1. Click on the domain name in the list, change the settings and click **Save**.

### Set up Email Security

Email Security provides protection against spam, spoofing, viruses and advanced threats.

Email Security is only available if you have a Sophos Email license.

To use Email Security:

1. Ensure that the users and email addresses you want to protect have been added to Sophos Central. See the instructions in [Add email addresses](#) or [Add users and email addresses](#) below.

   **Tip**
   
   You can add an email address for a user or import a list of email addresses without using Active Directory Synchronization or Office 365, see [Mailboxes](#) (page 422).

2. Add your protected email domains, see [Settings](#) (page 437).
3. Configure spam protection in the email security policy, see [Email Security Policy](#) (page 428).
4. Set up global controls on spam using allow and block lists for senders, see [Inbound Allow/Block](#) (page 108).
Note
Users without an email address will not be protected. Email going to an email address not tied to a user will not be delivered.

Add email addresses

If you have existing users but no email addresses then you need to add the email information. You can do this by updating your Active Directory synchronization and then adding your email domains. To do this:
1. In Settings, on the Email Security > Settings page, click the link to configure email connection settings.
2. Click the link in the Email Security Setup dialog to download the latest version of the AD sync tool and re-sync your users. See Set up synchronization with Active Directory (page 73).
3. You can then add your email domains by clicking Continue.

Add users and email addresses

If you are a new customer with no users or mailboxes set up you need to add users and mailboxes. To do this:
1. In Settings, on the Email Security > Settings page, click the link to configure email connection settings.
   The Email Security Setup dialog is displayed.
2. To add users and mailboxes (as a new customer) you can either use the AD sync tool or you can import mailboxes. Click the appropriate link.
   - Download our Ad Sync tool and synchronize your users and their email addresses.
   - Use Mailbox Import to import your users and their email addresses.

   Note
   If you are using Office 365 you must use this option.
3. To import mailboxes:
   a) In the Mailbox Import dialog click a link to download a template CSV file. You can choose from a blank template or one with example data.
   b) Create your import mailbox data in the correct format and save it. You can now import the mailboxes.
   c) Click Browse, select your CSV file and click Open.
   d) Click Import.

   Note
   The maximum file size is 1 MB.

   The file is imported and the number of successfully imported mailboxes is shown together with any failures. Mailboxes that have not been imported are indicated by the line number in
the .CSV file and a reason, for example duplicate entry. You can download a list of mailboxes that failed to import by clicking the link. You can also view the details of failed imports by clicking "View failed lines". These options are not shown if there are no failures.

**Note**
If you use active directory synchronization, this overrides any changes you make by importing a CSV file. You should only make changes using a CSV file if you don't use active directory synchronization.

4. Click **Continue**.
5. Add your email domains, see **Settings** (page 437).

### 8.11.8 Email Encryption

This feature is only available with an Email Advanced license.

The encryption type Sophos Email uses is push based email encryption using AES 265.

To turn encryption on or off, go to **Email Gateway > 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+1PRF:+FIPS:kRSA+1PRF:+FIPS:+eNULL:+aNULL'. For more information, see https://wiki.openssl.org/index.php/FIPS_mode_and_TLS.

### General Settings

**Attention**
- 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.

• 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.

    Important
    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 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.
• Wildcards are not supported.
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 for Windows and Mac, Outlook Web Access, in Office 365 and Exchange environments.

Is my environment compatible with Sophos Outlook Add-in?

Sophos Outlook Add-in works for mail accounts in the following environments:

- Exchange Server 2013 or later (on-premise Exchange).
  
  **Important**
  Exchange Server 2013 API version 1.4 or older is not supported.

- Office 365 Business subscription (Exchange online).

  **Important**
  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).

Installing the Sophos Outlook Add-in

1. **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.

2. **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. See the following Microsoft documentation for installation steps, https://docs.microsoft.com/en-us/outlook/add-ins/sideload-outlook-add-ins-for-testing.

   - If you want to use **Office 365 Centralized Deployment**, check if centralized deployment of add-ins works for your environment.

     See the following Microsoft support documentation for more information, Determine if centralized deployment of add-ins works for your Office 365 organization.

     If you are ready to begin centralized deployment of Sophos Outlook Add-in, see the following instructions to get started, Manage deployment of Office 365 add-ins in the Office 365 Admin Center.

   - 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.
8.11.9 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.

This means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos/Google Authenticator or email authentication to sign in.

This page tells you how to do the following:
- Set up multi-factor authentication.
- Sign in with multi-factor authentication for the first time.
- Sign in with email authentication (if you don't have Sophos/Google Authenticator).
- Reset an admin's sign-in details, for example if they lose their phone.

Set up multi-factor authentication

1. Go to **Settings > Multi-factor authentication**.
2. Choose how you want admins to sign in:
   - **No MFA needed**. This is the default.
   - **All admins need MFA**.
   - **Select admins who will need MFA**. This lets you select individual admins.
3. If you chose **Select admins who will need MFA**, a user list is displayed. Click **Add admins** (on the right of the screen). In the picker, move admins to the **Assigned** list and click **Save**.

When admins next try to sign in, they'll be prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

Here's what to do the first time you sign in with MFA:

1. At the sign-in screen, enter your user ID (email address) and password.
2. **A Set Up Your Login Information** dialog explains that signing in needs additional authentication.
3. In the next dialog:
   - Enter the security code that has been sent to you in an email.
   - Create a 4-digit PIN. This enables you to use email as an authentication method.
4. In the next dialog, choose authentication type.
5. In **Verify Your Device**, scan the QR code and enter the security code that Sophos/Google Authenticator displays.

   Sophos Central opens.

The next time you sign in, you only need to enter a code from Sophos/Google Authenticator when prompted.
Sign in with email authentication

If you don't have access to Sophos/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/Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can let them set up their sign-in again.

1. Go to the Users page.
2. Find the user and click on their name to open their details.
3. 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.

**8.11.10 Time of Click Block/Warn Pages**

Time of Click URL Protection is only available with an Email Advanced license.

To manage Time of Click URL Protection settings for suspicious sites, go to Email Gateway > Settings > Time of Click Block/Warn Pages.

Turn on Custom Block and 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.

**8.11.11 Time of Click allow list**

Time of Click is only available with an Email Advanced license.

You can add domains to the allow list so that URLs from those domains are neither rewritten nor scanned by Time of Click protection.

Click Add, and enter the URL you want to allow e.g domain.com then click Save.
Note
Wildcards are supported, for example *.domain.com.

To delete a URL from the allow list, select the box next to the URL and click **Delete**.
You can select multiple URLs at once by clicking the boxes next to the URLs. To select all URLs, click the box next to **URL**.

8.12 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](#) (page 458) and [Set up outbound email handling with Microsoft Office 365](#) (page 464).
For Google, see [Set up Sophos Email for G Suite](#) (page 466) and [Set up outbound email handling with Google G Suite](#) (page 472).
For other services, see [How to configure Sophos Email for Exchange and all other clients](#) (page 473) and [Set up outbound email handling with Exchange and other clients](#) (page 478).

8.12.1 How to configure Sophos Email for Office 365

This section describes how to set up Sophos Email for Office 365. You need to:
1. **Add your domain and verify ownership**
2. **Add mailboxes to Sophos Email**
3. **Bypass Exchange Online Protection in Office 365**
4. **Restrict delivery to Sophos IP addresses**
5. **Configure a Secure connector between Office 365 and Sophos Email**
6. **Modify MX records to point to Sophos Email**
7. **Test and confirm mail flow**

*Add your domain and verify ownership*

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:
- Select **Domains**.
- Copy the value displayed for the expected MX record.
To add a domain in Sophos Central:

1. Sign in to Sophos Central Wireless.
2. Click Email Gateway > Settings.
3. Click Domain Settings / Status.
4. Click Add Domain.
5. Enter your email domain details, direction of traffic and delivery destination details.
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 @. If you are not sure how to do this, contact the organization that registered your domain name.
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.

Add mailboxes to Sophos Email

There are three ways to add users/mailboxes to Sophos Email:

1. Automatically via Active Directory Sync
2. Manually via the UI
3. Manually via .csv import

Add users/mailboxes via 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 unless a group query filter is also specified, 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

Important
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 on **Mailboxes** in the left hand navigation.
2. On the **Mailboxes** screen, click the **Add Mailbox** button in the upper right.
3. Select the **Add Mailbox** option.
4. Select a Mailbox Type. Types are User, Distribution List or Public Folder.
5. Enter a Name for the Mailbox, Distribution List or Public Folder.
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.

**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 and avoid having to access two email quarantines.

To bypass Exchange Online Protection:

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>
<tr>
<td>Audit this rule with severity level</td>
<td>Low</td>
</tr>
<tr>
<td>Choose a mode for this rule</td>
<td>Enforce</td>
</tr>
</tbody>
</table>

6. Click Save to add the rule.

**Restrict delivery to Sophos IP addresses**

**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.

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.

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>

**Important**
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**

To configure the secure connector between Office 365 and Sophos Email:
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 (See table in Restrict delivery to Sophos IP addresses (page 462)).
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

Important
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 do not have the ability to make these changes yourself, it will be necessary to 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>
</tbody>
</table>
### Region | MX Records
---|---
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 Central, click on **Reports & Logs**.
2. Scroll down to the bottom of the page.
3. Under Email Protection, 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. See [Get additional help](#) (page 559).

### 8.12.2 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. See Updating the SPF record for your domain (page 465)
2. Configure routing so that outbound mail is sent through Sophos Email. See Configuring outbound routing (page 465)

Updating the SPF record for your domain

Your organization should already have a SPF record for the domain(s) registered with Microsoft Office 365. When implementing Sophos Email with Microsoft Office 365, this record must be updated in the DNS zone for the relevant domain to include the following:

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

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.
6. Click Save.
7. Then click Configure External Dependencies.
8. Click Outbound Settings.
9. Copy the Outbound Relay Host address.
10. Log in to the Office 365 Admin Center.
11. Select the Admin > Exchange menu item. The Exchange Admin Center is displayed.
12. Select the Mail Flow > Connectors menu item and create a new Connector.
13. Complete the New Connector - Select Your Mail Flow Scenario dialog as follows:

<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>

14. Click the Next button.
15. Complete the **New Connector - New Connector dialog** as follows:

<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>

16. Click the **Next** button.
17. Select the **Only when email messages are sent to these domains** option.
18. Click the + icon to add the recipient domains that should use this connector.
19. Enter a value of * to route all outbound emails through Sophos.
20. Click the **OK** button.
21. Click the **Next** button.
22. Select the **Route Email Through These Smart Hosts** option.
23. Click the + icon to add the smart hosts.
24. To retrieve the text you need to insert into the smart host, sign in to Sophos Central.
25. 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 the **Save** button.
26. Click the **Next** button.
27. Select the following options:
   a) **Always use Transport Layer Security (TLS) to Secure the Connection (recommended)**
   b) **Any digital certificate, including self-signed certificates**
28. Click the **Next** button to verify your settings.
29. Click the **Next** button.
30. Add an email address of a recipient from a domain external to your organization.
31. Click the **Validate** button.
32. Once Office 365 has successfully validated your settings, click the **Save** button.
33. 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. See Get additional help (page 559).

**Note**

It may take up to 24 hours for the changes to propagate.

### 8.12.3 Set up Sophos Email for G Suite

This section describes how to set up Sophos Email for G Suite. You need to:

1. Add your domain and verify ownership
2. Configure multiple route MX records
3. Add mailboxes to Sophos Email
4. Restrict delivery to Sophos IP addresses
5. Create an inbound gateway in G Suite
6. Modify MX records to point to Sophos Email
7. Test and confirm mail flow

Add your domain and verify ownership

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, see G Suite MX record values
• 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. Sign in to Sophos Central.
2. Click Email Gateway > Settings.
3. Click Domain Settings / Status.
4. Click Add Domain.
5. Enter your email domain details.
6. 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.
7. Next, click Verify Domain Ownership.
8. Copy the TXT value presented in the Verify Domain Ownership dialog.
   This value is specific to your email domain.
9. 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 @.
10. 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.

Note
If you prefer, you can skip this step, and configure the delivery destination to point directly to ASPMX.L.GOOGLE.COM. See Add your domain and verify ownership (page 467). 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 Sophos Email

There are three ways to add users/mailboxes to Sophos Email:

1. Automatically via Active Directory Sync
2. Manually via the UI
3. Manually via .csv import

Note
Support for Azure Active Directory Sync is not yet available. Office 365 customers can import or manually create mailboxes in the UI until Azure AD Sync is available.

Add users/mailboxes via 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 unless a group query filter is also specified, 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:
      
      \[\text{CN=testGroup}\]

      **Important**
      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**.

---

**Restrict delivery to Sophos IP addresses**

**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.

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.

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>

**Important**
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.

Related information
Set up an inbound mail gateway

Modify MX records to point to Sophos Email

**Important**
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 do not have the ability to make these changes yourself, it will be necessary to 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>Region</td>
<td>MX Records</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------</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 Central, click on Reports & Logs.
2. Scroll down to the bottom of the page.
3. Under Email Protection, 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. See Get additional help (page 559).

8.12.4 Set up outbound 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. Navigate 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=spf1include:_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).

### 8.12.5 How to configure Sophos Email for Exchange and all other clients

This section describes how to set up Sophos Email for other email clients. You need to:

1. **Add your domain and verify ownership**
2. **Add mailboxes to Sophos Email**
3. **Restrict delivery to Sophos IP addresses**
4. **Modify MX records to point to Sophos Email**
5. **Test and confirm mail flow**
Add your domain and verify ownership

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. Sign in to Sophos Central.
2. Click Email Gateway > Settings.
3. Click Domain Settings / Status.
4. Click Add Domain.
5. Enter your email domain details, direction of traffic and delivery destination details.
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.

Add mailboxes to Sophos Email

There are three ways to add users/mailboxes to Sophos Email:
1. Automatically via Active Directory Sync
2. Manually via the UI
3. Manually via .csv import

Note
Support for Azure Active Directory Sync is not yet available. Office 365 customers can import or manually create mailboxes in the UI until Azure AD Sync is available.
Add users/mailboxes via 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 unless a group query filter is also specified, 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
   ```
**Important**
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 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**

**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.
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.

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>

**Important**

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**

**Important**

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 do not have the ability to make these changes yourself, it will be necessary to 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>
</tbody>
</table>
### Region MX Records

<table>
<thead>
<tr>
<th>Region</th>
<th>MX Records</th>
</tr>
</thead>
<tbody>
<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 Central, click on **Reports & Logs**.
2. Scroll down to the bottom of the page.
3. Under Email Protection, 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. See Get additional help (page 559).

### 8.12.6 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.

1. To set up an SMTP connector, follow the instructions for your version of Exchange on Microsoft’s website:
2. When prompted select the **Route mail through smart hosts** option and click **+ Add**.
3. In the **Add smart host** dialog that appears, enter the corresponding smart host for your region.

To find the smarthost for your region:

- Log in to Sophos Central.
- Navigate to **Email Gateway > Settings > Domain Settings > Configure External Dependencies**.
- 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>
<tr>
<td>Ireland</td>
<td>relay-eu-west-1.prod.hydra.sophos.com</td>
</tr>
</tbody>
</table>

4. Disable 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. See **Get additional help** (page 559).

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=spf1include:_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=spf1include:_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. Log on to Sophos Central.
2. Navigate 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.
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.

Web Gateway stats

**Web Gateway Stats** 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 **Gateway Activity Logs** 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.
- **Print**: Send a copy of the report to the printer.
- **Export**: Export the data to XSLX, ODS, CSV or XML format.

9.3 Reports

The **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 sections below tell you about the users list and how to manage users.
About the users list

The current users are listed with their details:

- **Security status.** An icon shows whether the user has security alerts on any of their devices:
  - Green check mark if there are low-priority alerts or no alerts.
  - Amber warning sign if there are medium-priority alerts.
  - Red warning sign if there are critical alerts.

  Click on 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, see Administration Roles (page 76).
  
  This column is only visible if you are an administrator.

Click on 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 on the user's name. For more information, see User Summary (page 48).

Add a user manually

This also gives you the option to let the user protect their own devices.

You can add an individual user and protect them as follows.

1. On the **Users** page, click **Add** and select **Add User**.
2. In the **Add User** dialog, enter the following settings:

   **First and Last Name.** Enter the name of the user. Do not include a domain name.

   **Role.** Select an administration role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

   A user who is assigned an administration role will receive an email telling them how to set up their administration account.

   **Important**
   You can only see the **Role** option and assign administrator roles if you are a **SuperAdmin**.

   **Note**
   Anyone with a **User** role only has access to the Self Service Portal.

   **Email Address.** Enter the email address of the user.
Add to Groups (optional). Select one of the available user groups and use the picker arrows to move it to the assigned groups.

**Tip**
You can start typing a name in the search box to filter the displayed 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.

3. Click **Save** or **Save & 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 by protecting their devices

You can add users automatically as follows.

Download an installer and run it yourself on a device (or devices). This adds the user of each device automatically. For installers, see the **Protect Devices** page.

Import users from a CSV file

**This option may not be available for all customers yet.**

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 do this:

1. On the **Users** page, click **Add** and select **Import users from CSV**.
2. Click **Browse** and select your CSV file.

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

3. The CSV file can include groups a user is assigned to. To create groups not available yet, select **Create new groups**.
4. To send a registration email for the Sophos Central Self Service portal to each imported user, select **Activate new users**.
5. 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.

On the Users page, click the Set up Active Directory Sync link in the upper right of the page. Then see Set up synchronization with Active Directory (page 73).

Protect existing users

To email users you have already added to the list or imported:

1. On the Users page, select the user or users you want to protect. Click Email Setup Link in the upper right of the page.

2. In the Email Setup Link dialog, you are prompted to select the types of protection the user needs (if your license includes more than one).

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.

Modify users

To modify a user's account:

On the Users page, click the user’s name to open and edit their user details. For more information, see User Summary (page 48).

Delete users

To delete a user or users:

On the Users page, select the checkbox next to each user you want to delete. Click the Delete button in the upper right of the page.
Important
You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them, see Administration Roles (page 76).

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

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

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 will be added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they will be added as a user again the next time that Sophos Central synchronizes with Active Directory.

Export to CSV

To export a list of users:
Click on Export to CSV.

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

For example you can export a list of administrators by applying the Admins Only filter before clicking Export to CSV.

Related concepts
Active Directory Sync (page 72)

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.
Security status

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

✅ Green check mark if there are low-priority alerts or no alerts.

⚠️ Orange warning sign if there are medium-priority alerts.

❗️ Red warning sign if there are high-priority alerts.

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 and Last name**: Enter the name of the user. Do not include a domain name.

   **Role**: Select a role for the user. Choose from: **SuperAdmin**, **Admin**, **Help Desk**, **Read-only** or **User**. For help on the administration roles, see [Administration Roles](#) (page 76).

   **Important**
   You can only see the **Role** option and assign administrator roles if you are a **SuperAdmin**.

   **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 (optional): 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.

Important
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.
For information on how policies work, see About Policies (page 425).

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 group(s) 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.

**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 knowledge base article 128136. Click the Details link beside the event and then allow the application, see Allowed applications (page 97).

**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.

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.

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 on the group’s name. For more information, see **User Group Details** (page 54).

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.
   - **Members**: 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 (page 54).

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.
• 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).
- Device Encryption. This shows the encryption status. For more information, see See 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 from Sophos Central. It also deletes 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.

**Note**
You can't uninstall Sophos Device Encryption on its own. Uninstall all products and then use custom installation to reinstall the products you want.

**Export to CSV**
To export a list of computers:
Click on **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 **Devices** 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. For more information, see **Encryption Recovery Key Search** (page 89).

**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 on the other tabs on this page.

An icon shows you whether the computer has any security alerts:
- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
- Red warning sign if there are high-priority alerts.

If there are alerts, you can click Show Status to see details.

Actions you can take

The actions links and buttons are in the left-hand pane.

Isolate
This isolates the computer from the network. See Isolate or remove from isolation (page 58).

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.

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 in 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.

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** (page 171).

**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.

**Endpoint 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.
- **Agent Update Status**: Shows whether the computer is up to date.
- **Assigned Products**: Shows the Sophos products are 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). **Change group** lets you add it to a group, move it to a different group, or remove it from its current group.

**Device Encryption summary**

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.

Note
- 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 logon credentials. For more information, see Retrieve recovery key (page 57) or Retrieve recovery key (Macs) (page 90).

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 unless they have 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 View Details to manage the tamper protection password for the computer.

Update Cache and Message Relay status
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 status

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:

- **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 [knowledge base article 128136](#).

Click the Details link beside the event and then allow the application, see [Allowed applications](#) (page 97).

**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.

### 9.5.3 Computer Status

The **Status** tab in a computer's details page lets you see the computer's security status and details of any alerts. It also lets you take action against alerts.

**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. See **Alerts** (page 4).

**Activity**

This shows whether the device is active or not and gives details of past activity.

**Computer Security Status**

**Note**

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).

### 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 that Sophos Central applies to protected networks.

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.

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 particular 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.
3. You see a list of policy types.
4. 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:
• Create a Web Gateway policy. See Create or Edit a Policy (page 168).
• Open the policy’s Settings tab and configure it as described below. Make sure the policy is enabled.
• Install the Sophos Web Gateway agent on devices. See the Protect Devices page.

You can configure any of the following options.

Web Filtering by Categories

Use this to control which websites your users are allowed to visit. You can set options for security categories or productivity categories.

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.
Custom Web Filtering

Use this to control access to websites that you have "tagged", i.e. put into your own categories, at the System Settings > Website Management page.

1. Select Custom Web Filtering.
2. Click Add New (on the right).
3. Select your Website Tag and set the Action to Allow, Audit, Warn or Block

Note
On the Website Management page, you can change the category a website is in, but Web Gateway does not currently support such changes.

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).

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

SSL Scanning by Category

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.

### 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.

### Trusted Destination IPs and Domains

Use this to specify IPs 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 IPs and subnets where traffic will not be routed through the Web Gateway. When the Web Gateway agent is on the specified IP or subnet, Web Gateway will not run. This setting is often used for known safe networks where network security is already in place.

### 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. Click **Add New** (on the right).
   
   The **Add Data Filter** dialog is displayed.
2. Enter a **Name** for the rule.
3. Choose whether to **Allow**, **Audit**, **Warn** or **Block** the content once a rule is matched.
4. Choose whether the filter applies to **Download**, **Upload** or **Both**.
5. 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, etc) and more. Data filters do not apply to HTTPS content unless SSL decryption has also been enabled.

**What do Allow, Audit, Warn and Block do?**

The web filtering features offer you these options: Allow, Audit, Warn and Block.

• **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).

**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 be displayed under **Global Settings in Overview**, if you have more than one product.

**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 groups from Active Directory to Sophos Central.

In Setting, 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.

• You can also configure settings for Azure Active Directory Synchronization.

**Note**
If you are using Office 365 you must use this option.

For instructions on setting up the utility, see **Set up synchronization with Active Directory** (page 73). For full details of how it works, see **About Active Directory synchronization** (page 73). Once you have set up synchronization you can review its status and other settings, see **Active Directory Sync Status** (page 72).
For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 75). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 75).

**Active Directory Sync Status**

In Settings, on the Active Directory Sync Status page, once you set up Active Directory synchronization, you can view:

**Status**

- The status of Active Directory synchronization (whether the last synchronization was successful or whether any warnings or errors occurred).
- The number of users and groups imported from Active Directory.
- The time of the last synchronization with Active Directory.

You can view Active Directory synchronization alerts on the Alerts page You can view synchronization events on the Logs & Reports > Events page.

**Sync Status**

This shows the synchronization settings in Active Directory.

**About Active Directory synchronization**

Active Directory synchronization allows administrators to implement a service that maps users and 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 or groups.
- It supports automated, one-way synchronization from the Active Directory to Sophos Central. It does not support two-way synchronization between Sophos Central and Active Directory.
- For users imported from Active Directory:
  - You cannot modify their name, email, or Exchange login, or add or change or remove associated groups or logins managed by Active Directory.
  - You can add, change or remove groups or logins that are not managed by Active Directory.
- For groups imported from Active Directory:
  - You cannot modify their name.
  - You can add, change or remove groups or logins that are not managed by Active Directory.
- 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. Any information added or updated from the Active Directory cannot be edited in the console.
- 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 AD forest. We
strongly recommend to synchronize different AD 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 deploying with Active Directory.

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.

To set up synchronization with Active Directory:

1. In Settings, on the **Active Directory Sync** page, click the link to download the Sophos Central AD
Synchronization Utility installer, and then run it.

2. In the setup wizard, enter the information required.

3. On the last page of the setup wizard, 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**.

The Sophos Central AD Sync Utility Setup Wizard starts.

4. On the **Sophos Credentials** page, enter your Sophos Central account credentials.

5. 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, 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.

6. 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.

<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:</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>memberOf=CN=testGroup, DC=myCompany, DC=com</td>
<td>The above query will limit user discovery to users belonging to “testGroup”. Note that unless a group query filter is also specified, 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>

**Important**

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.

7. 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**.

8. 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 Sophos Central.

    To stop the synchronization in progress, click **Stop**.

### Azure AD Sync Status

In Settings, on the **Active Directory Sync Status** page, once you configure Azure AD synchronization, you can view:

- **The status of Azure AD synchronization** (whether the last synchronization was successful or whether any warnings or errors occurred).
- **The number of users and groups imported from Azure AD**.
- **The time of the last synchronization with Azure AD**.

    **Note**

    Auto synchronization happens every 6 hours. You cannot change this interval.

- **The configuration settings for Azure AD synchronization**.
You can amend these by clicking **Edit**, see Set up synchronization with Azure Active Directory (page 75).

Click **Sync** to run the synchronization process.

You can validate the Azure Sync connection by clicking **Test Connection**.

You can view Azure AD synchronization alerts on the **Alerts** page. You can view synchronization events on the **Logs & Reports > Events** page.

**Set up synchronization with Azure Active Directory**

Azure AD sync is only available if you have a Sophos Email license.

To configure Azure Active Directory synchronization:

1. In Settings, on the **Active Directory Sync** page, click the link to configure the settings for Azure AD Sync.
2. Set up your Azure Applications, if required.

   **Tip**
   
   Click the link to the instructions if you need help with this.

   You can skip this step if you have already set up an Azure application.

3. Configure the Azure Sync Settings:
   a) Enter the **Client ID**.
   b) Set the **Tenant Domain**.
   c) Enter the **Application Key** and set its 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.

4. Click **Test Connection** to validate the Azure Sync connection.
5. Click **Save**.

   Synchronization starts. This process may take some time.

### 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.

**Important**

You can only see this option if you are a **SuperAdmin** 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.

**Important**

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. These roles cannot be edited or deleted.

**Important**

Your assigned administrator role affects what you can do.

**Note**

Anyone with a **User** role only has access to the Self Service Portal.

The available administration roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Super Admin</strong></td>
<td>Have access to everything in Sophos Central.</td>
<td>There are no limitations.</td>
<td>None.</td>
</tr>
<tr>
<td></td>
<td>In addition they can:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manage roles and role assignments</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Admin</strong></td>
<td>Have access to everything in Sophos Central.</td>
<td>Manage roles and role assignments.</td>
<td>No Role Management options are displayed.</td>
</tr>
<tr>
<td></td>
<td>In addition they can:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Look at sensitive logs or reports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Update the Sophos agent software on a computer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scan computers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Help Desk</strong></td>
<td>Have read-only access for all settings in Sophos Central. In addition they can:</td>
<td>Manage roles and role assignments. In addition they can't:</td>
<td>No Role Management options are displayed.</td>
</tr>
<tr>
<td></td>
<td>• Look at sensitive logs or reports.</td>
<td>• Assign policies.</td>
<td>In addition:</td>
</tr>
<tr>
<td></td>
<td>• Receive and clear alerts. A Help Desk admin can only resolve alerts if they go to the Alerts page from the dashboard.</td>
<td>• Change settings.</td>
<td>• All other options apart from those related to receiving and clearing alerts are read-only.</td>
</tr>
<tr>
<td></td>
<td>• Update the Sophos agent software on a computer.</td>
<td>• Resolve alerts on the individual device.</td>
<td>• Some options, such as Edit buttons, are not displayed.</td>
</tr>
</tbody>
</table>
### Role

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role can't...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</table>
| Read-only     | Have read-only access for all settings in Sophos Central. In addition they can:  
• Look at sensitive logs or reports.  
• Receive alerts. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers. | No Role Management options are displayed. In addition:  
• All options are read-only.  
• Some options, such as Edit buttons, are not displayed. |
| User          | Have no administration capabilities. | Manage roles and role assignments. In addition they can't:  
• Assign policies.  
• Change settings.  
• Clear alerts.  
• Update the Sophos agent software on a computer.  
• Scan computers.  
• Look at sensitive logs or reports. | Has access only to the Self Service Portal. |

If you have Intercept X with EDR, please see Administration Roles for Intercept X with EDR (page 79).

### Permissions

This is the access level for a role. The options are **Full**, **Help Desk** or **Read-only**.

### Additional 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 assignment to users/devices**: This option means that an administrator can assign policies to users and devices.

- **Notifications**: This option means that an administrator can receive and clear alerts.

**Note**

**Read-only** administrators can only receive alerts.
Role Members

This is a list of the administrators that are assigned to the role. Click on a name to see their full details, see User Summary (page 48).

To 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.

Note
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.

1. Click Edit. This opens the Edit Role Members window.

   Note
   You can only see this option if you are a Super Admin administrator.

2. Select a user in the Available Users list and use the picker arrows to add them to the Assigned Users for the role.

   Tip
   Enter a name or part of a name in the search box to filter the list of available users.

To delete 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.

1. Click Edit. This opens the Edit Role Members window.

   Note
   You can only see this option if you are a Super Admin administrator.

2. Remove assigned administrators from the role by selecting 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.
Administration Roles for Intercept X with EDR

For general information on Administration Roles, see Administration Roles (page 76).

The available administration roles for Intercept X with EDR are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can’t...</th>
<th></th>
</tr>
</thead>
</table>
| **Super Admin** | • 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. | There are no limitations. |  |
| **Admin**  | • 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. | There are no limitations. |  |
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role can...</th>
<th>Administrators with this role can't...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Desk</td>
<td>- View the intelligence report.</td>
<td>- Add items to the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>- Request the intelligence report.</td>
<td>- Remove items from the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>- View blocked items.</td>
<td>- Isolate and un-isolate devices.</td>
</tr>
<tr>
<td></td>
<td>- Request an on-demand threat case.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- View on-demand threat cases.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Request a forensic snapshot.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Request a threat search.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- View a saved threat search.</td>
<td></td>
</tr>
<tr>
<td>Read-only</td>
<td>- View the intelligence report.</td>
<td>- Request the intelligence report.</td>
</tr>
<tr>
<td></td>
<td>- View blocked items.</td>
<td>- Add items to the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>- View on-demand threat cases.</td>
<td>- Remove items from the “Clean and Block” list.</td>
</tr>
<tr>
<td></td>
<td>- View a saved threat search.</td>
<td>- Isolate and un-isolate devices.</td>
</tr>
<tr>
<td></td>
<td>- Request a forensic snapshot.</td>
<td>- Request an on-demand threat case.</td>
</tr>
<tr>
<td></td>
<td>- Request a threat search.</td>
<td>- Request a threat search.</td>
</tr>
<tr>
<td></td>
<td>- Request a threat search.</td>
<td></td>
</tr>
</tbody>
</table>

### 9.7.3 Federated sign-in

You must be a Super Admin to turn on federated sign-in for your administrators and users.

You can allow your administrators and users to sign in to Sophos Central and the SSP using their Microsoft sign-in credentials.

**Note**

When you turn on federated sign-in administrators and users can still sign in using their Sophos Central credentials.

**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.

**Note**

Sophos Central is not supported on mobile devices.

An Azure AD admin must give permission for Sophos Central to use federated sign in before you can turn it on. Once an admin gives consent, it means your Azure AD tenant trusts Sophos Central and administrators can sign in with their Microsoft credentials. See https://docs.microsoft.com/en-us/azure/active-directory/develop/application-consent-experience for more information.
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 turn on federated sign-in:
1. Click **Federated sign-in** in **Settings**.
2. Click **Sign in with Sophos Central Admin or Microsoft credentials**.

### 9.7.4 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 unless they have 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 select the **Tamper Protection** tab. 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.

For details, see [Recover tamper protection passwords](#) (page 42).

### 9.7.5 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 knowledgebase 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.

### 9.7.6 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.

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. Go to [https://www.sophos.com/en-us/threat-center/reassessment-request.aspx](https://www.sophos.com/en-us/threat-center/reassessment-request.aspx). 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 [Control sites tagged in Website Management](#) (page 185)

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**.

9.7.7 Global Exclusions

You can exclude files, websites and applications from scanning for threats, as described below.

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. See **Computer isolation (Windows)**.

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 on this page.
- To exclude certain applications from checking, use **Exploit Mitigation Exclusions** (page 82).

You set exclusions in **Settings**, on the **Global Exclusions** page.

**Note**
These exclusions will apply to all your users (and their devices) and servers. If you want them to apply only to certain users or servers, use the policy exclusions in the policies instead.

**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 from events.

**Important**
Think carefully before you add global exclusions because doing so may reduce your protection.

1. On the **Global Exclusions** page, 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, detected exploit or device isolation).
3. Specify the item or items you want to exclude. The following rules apply:

<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. Examples:</td>
</tr>
<tr>
<td></td>
<td>• Folder: C:\programdata\adobe \photoshop\ (add a slash for a folder).</td>
</tr>
<tr>
<td></td>
<td>• Entire drive: D:</td>
</tr>
<tr>
<td></td>
<td>• File: C:\program files\program *.vmg</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>For more details, see [Windows Scanning Exclusions: Wildcards and Variables](page 175).</td>
</tr>
<tr>
<td>File or folder (Mac and Linux)</td>
<td>You can exclude a folder or file. You can use the wildcards ? and * . Examples:</td>
</tr>
<tr>
<td></td>
<td>• /Volumes/excluded (Mac)</td>
</tr>
<tr>
<td></td>
<td>• /mnt/hgfs/excluded (Linux)</td>
</tr>
<tr>
<td></td>
<td>For more details, see [macOS Scanning Exclusions](page 177).</td>
</tr>
<tr>
<td>File or folder (Virtual Server)</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></td>
<td>For more details, see [Virtual Server Scanning Exclusions: Wildcards](page 330).</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, not just the process name shown in Task Manager. Example:</td>
</tr>
<tr>
<td></td>
<td>• %PROGRAMFILES%\Microsoft Office \Office 14\Outlook.exe</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>To see all processes or other items that you need to exclude for an application, see the application vendor's documentation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>You can use wildcards and variables.</td>
</tr>
<tr>
<td>Website</td>
<td>Websites can be specified as IP address, IP address range (in CIDR notation), or domain. Examples:</td>
</tr>
<tr>
<td></td>
<td>• IP address: 192.168.0.1</td>
</tr>
<tr>
<td></td>
<td>• IP address range: 192.168.0.0/24</td>
</tr>
<tr>
<td></td>
<td>• The appendix /24 symbolizes the number of bits in the prefix common to all IP addresses of this range.</td>
</tr>
<tr>
<td></td>
<td>Thus /24 equals the netmask:</td>
</tr>
</tbody>
</table>
|                               | 11111111.11111111.11111111.00000000
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| In our example, the range includes all IP   | In our example, the range includes all IP addresses starting with 192.168.0.  
• Domain: google.com                          | addresses starting with 192.168.0.  
• Domain: google.com |
| Potentially Unwanted Application            | 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 and 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. |
| Device isolation (Windows)                  | 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 IP 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**.  
• 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**.  
• In **Remote IP address**, enter the address of the server. |

4. 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.  
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**.
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 Manage Update Caches and Message Relays (page 95).

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.

This means that admins must use another form of authentication, as well as their username and password.

Admins can use Sophos/Google Authenticator or email authentication to sign in.

This page tells you how to do the following:

• Set up multi-factor authentication.
• Sign in with multi-factor authentication for the first time.
• Sign in with email authentication (if you don't have Sophos/Google Authenticator).
• Reset an admin's sign-in details, for example if they lose their phone.

Set up multi-factor authentication

1. Go to Settings > Multi-factor authentication.
2. Choose how you want admins to sign in:
   • No MFA needed. This is the default.
   • All admins need MFA.
   • Select admins who will need MFA. This lets you select individual admins.
3. If you chose Select admins who will need MFA, a user list is displayed. Click Add admins (on the right of the screen). In the picker, move admins to the Assigned list and click Save.
When admins next try to sign in, they’ll be prompted to set up a new method of authentication.

Sign in with multi-factor authentication for the first time

Here’s what to do the first time you sign in with MFA:
1. At the sign-in screen, enter your user ID (email address) and password.
2. A Set Up Your Login Information dialog explains that signing in needs additional authentication.
3. In the next dialog:
   - Enter the security code that has been sent to you in an email.
   - Create a 4-digit PIN. This enables you to use email as an authentication method.
4. In the next dialog, choose authentication type.
5. In Verify Your Device, scan the QR code and enter the security code that Sophos/Google Authenticator displays.

Sophos Central opens.

The next time you sign in, you only need to enter a code from Sophos/Google Authenticator when prompted.

Sign in with email authentication

If you don't have access to Sophos/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/Google Authenticator.

Reset an admin's sign-in details

If an admin replaces or loses their phone, you can let them set up their sign-in again.
1. Go to the Users page.
2. Find the user and click on their name to open their details.
3. 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.
9.7.10 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. Just set up your caches before installation.

**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* (page 215).

**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 particular 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](#) (page 215).

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.
4. Click **Set Up Cache/Relay**.

Sophos Central automatically configures computers in your network to use a cache or relay. You can also manually assign computers to use a particular cache or relay.

### Assign computers to a cache/relay

You can manually assign computers to use a particular cache or relay.

1. In Settings, go to the **Manage Update Caches and Message Relays** page.
2. Click on the link displaying the number of computers using the Update Cache or Message Relay.
3. Click on **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 on 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. Go to the **System Settings > 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**.

### 9.8 Protect Devices

At 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.

#### 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 **Web Gateway > 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 user name.
• 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 Web Gateway > Protect Devices.

Click on 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 figures for alerts of a particular priority (High, Medium or Info).

At the main alerts list, you can investigate and take action against alerts. See Alerts (page 4).

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 see and access Sophos XG Firewalls that can connect to Sophos Central.

Go to Firewall management > Firewalls.

The list of firewalls shows:
- Name and IP address
- Workload: Hover over the workload status to see a graph of CPU usage in the previous two hours.
- OS version, model, serial no.
- Alerts in last 24 hours.
- Protection usage.

Click on a firewall to open the Firewall WebAdmin. This lets you configure the firewall.

Add firewalls

You add firewalls so that you can monitor them in Sophos Central and also manage them from your Firewall WebAdmin.

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**.
2. Register your serial number.
   You're guided through registration and deployment.

To add a firewall that is already deployed:
1. Login to your firewall.
2. On the **Central Synchronization** menu, turn on **Manage from Sophos Central**.
3. In Sophos Central, on the **Firewalls** page, click **Accept management**.

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.
11 Phish Threat

Sophos Phish Threat allows you to simulate phishing attacks and assess your users' response 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, see Campaigns (page 541).
2. Review your campaigns and their results, see Campaign Overview (page 544).

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

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, see Campaigns (page 541).

Click-to-open Rate

Click-to-open Rate (CTOR) is a measure of how good your users are at spotting phishing emails. CTOR helps you understand how users behave when they are face-to-face with a phishing attack. The dashboard shows your users' performance relative to the global average CTOR.

Awareness Factors

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.

Caught Users

Caught Users is a list of people in your organization who have fallen for a simulated attack. The users who have been caught most frequently appear at the top of the list.
11.2 Logs & Reports

The Logs & Reports pages provide detailed reports on Sophos Phish Threat features.

11.2.1 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.

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

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 filtered list of only users that were caught in 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.

User Training

The User Training 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.

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 sections below tell you about the users list and how to manage users.

About the users list

The current users are listed with their details:

- Security status. An icon shows whether the user has security alerts on any of their devices:
  - Green check mark if there are low-priority alerts or no alerts.
  - Amber warning sign if there are medium-priority alerts.
  - Red warning sign if there are critical alerts.

- Click on 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, see Administration Roles (page 76).
  - This column is only visible if you are an administrator.

Click on 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 on the user's name. For more information, see User Summary (page 48).

Add a user manually

This also gives you the option to let the user protect their own devices.

You can add an individual user and protect them as follows.

1. On the Users page, click Add and select Add User.

2. In the Add User dialog, enter the following settings:

   - First and Last Name. Enter the name of the user. Do not include a domain name.
   - Role. Select an administration role for the user. Choose from: SuperAdmin, Admin, Help Desk, Read-only or User. For help on the administration roles, see Administration Roles (page 76).

   A user who is assigned an administration role will receive an email telling them how to set up their administration account.
Important
You can only see the Role option and assign administrator roles if you are a SuperAdmin.

Note
Anyone with a User role only has access to the Self Service Portal.

Email Address. Enter the email address of the user.

Add to Groups (optional). Select one of the available user groups and use the picker arrows to move it to the assigned groups.

Tip
You can start typing a name in the search box to filter the displayed 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.

3. Click Save or Save & 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 by protecting their devices

You can add users automatically as follows.

Download an installer and run it yourself on a device (or devices). This adds the user of each device automatically. For installers, see the Protect Devices page.

Import users from a CSV file

This option may not be available for all customers yet.

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 do this:
1. On the Users page, click Add and select Import users from CSV.
2. Click Browse and select your CSV file.

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

3. The CSV file can include groups a user is assigned to. To create groups not available yet, select Create new groups.
4. To send a registration email for the Sophos Central Self Service portal to each imported user, select **Activate new users**.

5. 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.

On the **Users** page, click the **Set up Active Directory Sync** link in the upper right of the page. Then see Set up synchronization with Active Directory (page 73).

### Protect existing users

To email users you have already added to the list or imported:

1. On the **Users** page, select the user or users you want to protect. Click **Email Setup Link** in the upper right of the page.

2. In the **Email Setup Link** dialog, you are prompted to select the types of protection the user needs (if your license includes more than one).

   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.

### Modify users

To modify a user's account:

On the **Users** page, click the user's name to open and edit their user details. For more information, see **User Summary** (page 48).

### Delete users

To delete a user or users:
On the **Users** page, select the checkbox next to each user you want to delete. Click the **Delete** button in the upper right of the page.

**Important**

You cannot delete any users that are administrators. You must remove the administrator role from them before you can delete them, see *Administration Roles* (page 76).

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

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

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 will be added as a user again.
- If the user was added from Active Directory and is still in Active Directory, they will be added as a user again the next time that Sophos Central synchronizes with Active Directory.

**Export to CSV**

To export a list of users:

Click on **Export to CSV**.

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

For example you can export a list of administrators by applying the **Admins Only** filter before clicking **Export to CSV**.

**Related concepts**

*Active Directory Sync* (page 72)

**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**.
Security status

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

- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
- Red warning sign if there are high-priority alerts.

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 and Last name**: Enter the name of the user. Do not include a domain name.
   - **Role**: Select a role for the user. Choose from: **SuperAdmin**, **Admin**, **Help Desk**, **Read-only** or **User**. For help on the administration roles, see **Administration Roles** (page 76).

   **Important**
   
   You can only see the **Role** option and assign administrator roles if you are a **SuperAdmin**.

   **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** (optional): 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.

Important
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.

For information on how policies work, see About Policies (page 425).

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 group(s) 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.

### 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 knowledge base article 128136.

Click the Details link beside the event and then allow the application, see **Allowed applications** (page 97).

**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.

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.

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 on the group’s name. For more information, see User Group Details (page 54).

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.
   
   **Members**: 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 (page 54).

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.
• 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 active and past campaigns. You can also start new campaigns.
**Active Campaigns**: This is a list of campaigns that are still running with an overview of high-level results for each campaign.

**Past Campaigns**: Browse this list to see the history of campaigns run in your organization.

**New Campaign**: Start a new campaign to test your users with an attack simulation or enroll them in mandatory training, see Create a Phish Threat Campaign (page 543).

**Related concepts**
Campaign Overview (page 544)

### 11.4.1 Template

You can choose the type of campaign you want to use. Sophos Phish Threat includes templates for common attack types. These templates include email templates and training modules. You can then customize these templates before sending out your campaign, see Create a Phish Threat Campaign (page 543).

You can choose from:

- **Phishing**: This simulates a phishing attack against your users.
- **Credential Harvesting**: This simulates an attack designed to obtain login ids and passwords.
- **Attachment**: This simulates an attack designed to deploy malicious attachments on your system.
- **Training**: This allows you to send anti-phishing training to your users.

You can also select the language used in the email template and training modules.

### 11.4.2 Customize

Choose the attack template you want to use. You can filter the templates by difficulty (**Easy**, **Moderate**, and **Hard**).

**Note**
This option is not available for training campaigns.

**Related tasks**
Create a Phish Threat Campaign (page 543)

### 11.4.3 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.

**Remember**
You can do a baseline assessment of your users by opting out of training auto-enrollment.
Related tasks
Create a Phish Threat Campaign (page 543)

11.4.4 Enroll

Choose the Users or Groups to send the campaign to.

Related tasks
Create a Phish Threat Campaign (page 543)

11.4.5 Review

Here you can review your campaign and schedule it, see Create a Phish Threat Campaign (page 543).

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.

11.4.6 Create a Phish Threat Campaign

Start a new campaign to test your users with an attack simulation or enroll them in mandatory training.

1. Click New Campaign and give the campaign a name.
2. Select a campaign type. Choose from:
   - Phishing
   - Credential Harvesting
   - Attachment
   - Training
3. Select the language for the email template and training modules. Click Next.
4. Select the attack template. You can filter the templates by difficulty level (Easy, Moderate and Hard). Click Next.

   Note
   When you create a Training campaign you skip this step.

5. Select one or more training courses. You can choose not to enroll users in training. Click Next.

   Users who fall for the simulated attack are automatically enrolled in these courses.

   Tip
   You can opt out of auto-enrollment in training. This is a good way to assess your users.

6. Choose which Users or user Groups to send the campaign to. Click Next.
7. Review your selections from the previous steps and schedule your campaign. You can choose to space out the campaign emails by sending a percentage of emails at set intervals. Click **Save**.

Any actions taken by users after the **End Date** are not factored into the campaign results.

You can review your campaign, see Campaign Overview (page 544).

### 11.4.7 Campaign Overview

This shows the details of a campaign and the activity associated with it. You can also review detailed logs, see Campaign Logs (page 544) and campaign details for your users, see Campaign User Details (page 544).

#### Campaign summary

Shows the key high-level metrics for your campaign as well as the campaign start and end dates.

#### Click-to-open rate

The **Click-to-open rate** (CTOR) is a measure of how good your users are at spotting phishing emails. CTOR helps you understand how users behave when they are face-to-face with a phishing attack. Your dashboard shows your users’ performance relative to the global average CTOR.

#### Caught users timeline

The **Caught users timeline** plots user activity over the first 12 hours of your campaign, specifically showing emails sent and users caught 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.

#### Attack details

This shows which simulated attack was used in the campaign.

#### Training details

This shows which training course you selected for the campaign.

### Campaign Logs

The **Campaign Logs** page shows a detailed activity history for your campaign. Each event recorded for the campaign is listed in chronological order with the corresponding user and time stamp.

### Campaign User Details

For each user, you can see a summary of their activity, including time stamps for the following events:

- **Email sent**: When the user was sent the campaign email.
- **Email opened**: When the user opened the email.
• **Clicked link**: When the user clicked on the phishing link in the email.
• **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.

## 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 groups from Active Directory to Sophos Central.

In 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.
- You can also configure settings for Azure Active Directory Synchronization.

**Note**
If you are using Office 365 you must use this option.

For instructions on setting up the utility, see [Set up synchronization with Active Directory](#). For full details of how it works, see [About Active Directory synchronization](#). Once you have set up synchronization you can review its status and other settings, see [Active Directory Sync Status](#).

For instructions on configuring Azure Active Directory synchronization, see [Set up synchronization with Azure Active Directory](#). Once you have set up synchronization you can review its status and other settings, see [Azure AD Sync Status](#).

### 11.5.2 Sending domains and IPs

Here you can see the domains and IP addresses used for sending campaign email from Phish Threat.

**Note**
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 will be updated when we add new domains. See the Sophos Central [What’s New?](#) for news on new domains.

### 11.5.3 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 Sophos Labs 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, see Configure Sophos Outlook Add-in (page 546).
- Downloading the XML manifest from Sophos Central, see Download the XML manifest (page 546).
- Deploying Sophos Outlook Add-in to users, see Deploy Sophos Outlook Add-in (page 546).

Related concepts
Is my environment compatible with Sophos Outlook Add-in? (page 547)

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, 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

Sideloadng

This 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 following Microsoft documentation for installation steps, https://docs.microsoft.com/en-us/outlook/add-ins/sideload-outlook-add-ins-for-testing.

Office 365 Centralized Deployment

Check if centralized deployment of add-ins will work in your environment.

See the following Microsoft support documentation for more information, Determine if centralized deployment of add-ins works for your Office 365 organization.

If you are ready to begin centralized deployment of Sophos Outlook Add-in, see the following instructions to get started, Manage deployment of Office 365 add-ins in the Office 365 Admin Center.

Exchange Admin Center

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.

See the following Microsoft documentation, 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.
**Important**  
Exchange 2013 on-premises and Exchange 2016 on-premises are not supported.

- Office 365 Business subscription (Exchange online).

**Important**  
Non-Microsoft mail providers (such as Gmail or other POP/IMAP accounts) are not supported.

**Compatible mail clients**

- Outlook Web Access (Office 365 only).
12 Explore Products

On the Explore Products 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 Explore Products 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 Explore Products 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 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.

13.1 Account Details

The Account Details page lets you change your user name or password, manage your email subscriptions, view your account and partner details, and more.

To access this page, click your account name in the upper right of the user interface and select Account Details.

Company Info

Click your account name (upper right of the user interface), select Account Details, and click the Company Info tab.

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 Browse (on the right of the page), 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 setting 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, change the email address and password you use for logging into Sophos Central.

Click your account name (upper right of the user interface), select Account Details, and click the My Info tab.
Your administration role is shown at the top. Click on the role name for full details.

To change the login email address:
1. Make sure you have access to the email address you want to use for login (you'll need it during this process).
2. Enter a **New Email Address** and click **Save**.
   - A confirmation link is sent to the new email address.
3. Confirm the new address.

**Note**
You can now use the email address to log into Sophos Central. The old email address is no longer valid.

To change the password:
1. Enter your **Current Password**.
2. Create a **New Password**, confirm it, and click **Save**.
   - A notification email is sent to your configured email address.

**Note**
You can now log in with the new password. The old password is no longer valid.

### Partner Info

Click your account name (upper right of the user interface), select **Account Details**, and click the **Partner Info** tab.

This tab shows the contact information for your partner, if applicable.

### My Email Subscriptions

**Note**
This option is only available if you have a Web Gateway license.

You can manage your email subscriptions using the **My Email Subscriptions** tab in the **Account Details** page.

Click your account name (upper right of the user interface), select **Account Details**, and click the **My Email Subscriptions** tab.

To manage subscriptions:
1. Switch on your required email summaries, for example **Enable Web Gateway email summaries**.
2. Choose the frequency.
3. Click **Save**.

### 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 (upper right of the user interface), select **Account Details**, and click the **Account Preferences** tab.

**Important**
Once you have enabled this feature, it can only be disabled from Sophos Central Enterprise by an Enterprise Super Admin. See **Create an Enterprise Admin** (page 552).

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 the **Account Preferences** tab that Enterprise Management has been enabled and that you can see the Enterprise Admin's details.
2. Switch on Enterprise Admin access.

**Sophos Support**

You can select the types of Sophos Support you want to receive.

Click your account name (upper right of the user interface), select **Account Details**, and click the **Sophos Support** tab.

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.

**13.1.1 Create an Enterprise Admin**

Before you begin:

- You need to be a Super Admin administrator, see **Administration Roles** (page 76).
- 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.

In the Account Details page, in 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>
<tbody>
<tr>
<td>Use your Sophos Central login credentials.</td>
<td>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.</td>
</tr>
<tr>
<td>Create a new account.</td>
<td>To do this, enter new account information. You must use a unique email that is not already used in any other Sophos Central account.</td>
</tr>
</tbody>
</table>

4. Click Enable Enterprise Management and Save. The Account Preferences tab now shows that Enterprise Management has been enabled and the name of 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 log 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.
13.2 Licensing

You can activate and manage your Sophos licenses from the Sophos Central Admin console. Click your account name (upper right of the user interface), select Licensing.

License Management Type

Here you can see how your licenses are managed.

- **Enterprise Master Licenses.** Licenses are managed at enterprise level and shared between all the sub-estates managed by the enterprise. See Account Details (page 550).
- **Individual Sub-Estate Licences.** Licenses are managed at the sub-estate level. You can only use these licenses within the sub-estate.

**Note**
You can only activate and manage your licenses here if you are using Individual Sub-Estate Licenses.

Activate a license

You can activate a new or upgraded license here. Use the license key shown on the License Schedule that Sophos has emailed you. For details, see Activate Your License (page 2).

Buy a license

Click Buy Now to go to a page where you can sign up for license.

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.

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 "Trial" 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.
14 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.

Email Gateway currently has two new features available on EAP, Encryption and Data Loss Prevention.

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.

This section contains the help for current early access programs.

**Important**
There may be variations between product features and documentation, as the features are in development, therefore 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 Sophos early access program license agreement dialog, view the agreement and then click Accept.

   **Important**
   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 List**.
15 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 version 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.
16 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 Enable Remote Assistance. This enables 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 Remote Assistance, 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 Licensing & Administration, 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 Send.

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.
17 Legal notices

Copyright © 2019 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.