Sophos Central Admin help
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Sophos Central</td>
<td>1</td>
</tr>
<tr>
<td>Activate Your License</td>
<td>2</td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td>3</td>
</tr>
<tr>
<td>Dashboard</td>
<td>3</td>
</tr>
<tr>
<td>Alerts</td>
<td>4</td>
</tr>
<tr>
<td>Root Cause Analysis</td>
<td>9</td>
</tr>
<tr>
<td>Logs &amp; Reports</td>
<td>11</td>
</tr>
<tr>
<td>People</td>
<td>24</td>
</tr>
<tr>
<td>Computers</td>
<td>33</td>
</tr>
<tr>
<td>Computer Groups</td>
<td>40</td>
</tr>
<tr>
<td>Policies</td>
<td>42</td>
</tr>
<tr>
<td>Settings</td>
<td>59</td>
</tr>
<tr>
<td>Protect Devices</td>
<td>80</td>
</tr>
<tr>
<td>Device Encryption</td>
<td>82</td>
</tr>
<tr>
<td>Dashboard</td>
<td>82</td>
</tr>
<tr>
<td>Alerts</td>
<td>82</td>
</tr>
<tr>
<td>Logs &amp; Reports</td>
<td>84</td>
</tr>
<tr>
<td>People</td>
<td>97</td>
</tr>
<tr>
<td>Computers</td>
<td>105</td>
</tr>
<tr>
<td>Computer Groups</td>
<td>113</td>
</tr>
<tr>
<td>Policies</td>
<td>115</td>
</tr>
<tr>
<td>Settings</td>
<td>119</td>
</tr>
<tr>
<td>Protect Devices</td>
<td>127</td>
</tr>
<tr>
<td>Server Protection</td>
<td>128</td>
</tr>
<tr>
<td>Dashboard</td>
<td>128</td>
</tr>
<tr>
<td>Alerts</td>
<td>129</td>
</tr>
<tr>
<td>Logs &amp; Reports</td>
<td>134</td>
</tr>
<tr>
<td>Servers</td>
<td>147</td>
</tr>
<tr>
<td>Server Groups</td>
<td>152</td>
</tr>
<tr>
<td>Policies</td>
<td>154</td>
</tr>
<tr>
<td>Settings</td>
<td>174</td>
</tr>
<tr>
<td>Protect Devices</td>
<td>192</td>
</tr>
<tr>
<td>Wireless</td>
<td>195</td>
</tr>
<tr>
<td>Wireless Dashboard</td>
<td>195</td>
</tr>
<tr>
<td>Wireless Alerts</td>
<td>195</td>
</tr>
<tr>
<td>Clients</td>
<td>197</td>
</tr>
<tr>
<td>Traffic Usage</td>
<td>197</td>
</tr>
<tr>
<td>Access Points</td>
<td>197</td>
</tr>
<tr>
<td>SSIDs</td>
<td>200</td>
</tr>
<tr>
<td>Sites</td>
<td>211</td>
</tr>
<tr>
<td>Settings</td>
<td>212</td>
</tr>
<tr>
<td>Protect Devices</td>
<td>212</td>
</tr>
<tr>
<td>Email Gateway</td>
<td>214</td>
</tr>
<tr>
<td>Dashboard</td>
<td>214</td>
</tr>
<tr>
<td>Message History Report</td>
<td>214</td>
</tr>
<tr>
<td>Messages Report</td>
<td>215</td>
</tr>
<tr>
<td>People</td>
<td>215</td>
</tr>
<tr>
<td>Mailboxes</td>
<td>224</td>
</tr>
<tr>
<td>Quarantined Messages</td>
<td>226</td>
</tr>
<tr>
<td>Policies</td>
<td>226</td>
</tr>
<tr>
<td>Settings</td>
<td>232</td>
</tr>
<tr>
<td>Web Gateway</td>
<td>245</td>
</tr>
<tr>
<td>Dashboard</td>
<td>245</td>
</tr>
</tbody>
</table>
1 About Sophos Central

This Help file provides information about Sophos Central Admin and explains procedures step by step.

You can help us to improve the Help. To make comments or suggestion, click Help (upper right of the user interface) and select Give Feedback.

For news about the latest improvements in Sophos Central, see What’s New. To access What’s New at any time, select Help > What’s New?.

2 Activate Your License

When you buy a new or upgraded license, you need to activate it. You do this in Sophos Central Admin (unless a Sophos Partner handles license activation for you).

**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:
1. Ensure you have the License Activation 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. In the **Apply Activation Code** field, enter your Key and click **Apply**.
3 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.

3.1 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.

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.

Messages

Messages shows the number of email messages processed by Email Security for your protected mailboxes for the last 30 days. It also shows the number of spam and malware messages detected.

Click See Report to open the Messages report and review the details of the processed messages, see Messages Report (page 301).

Web Stats

Web Stats 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.
3.2 Alerts

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

Alerts that are resolved automatically by Sophos Central are not displayed. For example, if malware is detected and then cleaned up automatically, no alert is displayed. If you want to view all events on your devices, go to the Logs & Reports > Events page.

Alerts

For each alert, the list shows the event that caused the alert, when it occurred, and which user and device are affected.

The list also shows the severity of alerts:

⚠️ Orange warning sign for medium-priority alerts.

🔴 Red warning sign for high-priority alerts.

For information about the different types of alerts, see the other Help pages in this section.

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

Actions on alerts

There is a checkbox next to each alert. When you select one or more checkboxes, you can apply certain actions on alerts. The action buttons are displayed in the upper right of the page.

The following actions may be available, 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 Contact Sophos Support (page 368). 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 285).
3.2.1 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.

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.

Related concepts
Events Report (page 289)
Email Alerts (page 287)
Contact Sophos Support (page 368)
3.2.2 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.

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 283).

- 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.

3.2.3 Email Alerts

Sophos Central automatically sends email alerts to administrators when events occur (for example, “Potentially Unwanted Application detected”).

Sophos Central does as follows:

• Sends alerts for Medium or High severity events that require action. For details of events in these categories, see Alerts (page 283).
• Sends alerts to all administrators. To see details of administrators, go to System Settings > Role Management.
• Does not send alerts if an alert for the same type of event has been sent within the previous 24 hours.

You cannot change the email alert settings.
3.3 Root Cause Analysis

Root Cause Analysis allows you to investigate the chain of events surrounding a malware infection and pinpoint areas where you can improve your security.

When a Windows computer running Sophos Endpoint detects a malware infection that needs investigation, it creates a Root Cause Analysis case and sends it to Sophos Central.

The Root Cause Analysis page lists all the Root Cause Analysis cases. Cases are listed for 90 days.

Click on a number to view All the cases, or only the New cases, In-Progress cases and Closed cases.

Search: If you want to view cases for a certain user, computer, or threat name (for example, "Troj/Agent-AJWL"), enter the name of the user, computer, or threat in the search box. The list shows only results related to your search term.

For each case the list shows:

• Priority: An initial priority is set when the case is created. You can change it when you view the case.
• Summary: This is the name of the detected threat. Click on the name to view the details of the case.
• Status: This is the status of the case. It is set to New, by default. You can set the status when you view the case.
• Time Created: Time and date when the case was created.
• User: The name of the user that caused the infection. You can click on the name to view the user’s details
• Device: Computer that caused the infection. You can click on a computer name to see more details about that computer.

You can order the list by Priority, Status or Time Created by clicking on the arrow at the top of those columns.

3.3.1 Root Cause Analysis Details

Use the Root Cause Analysis Details page to investigate a case. For each case you can see an overview, details of the artifacts affected and visual representation of how the threat developed. Once your investigation is complete you can close the case.

• Priority:[current priority]: This shows the current priority of the case. Set the priority: choose from High, Medium or Low.
• Status:[current status]: This shows the current status of the case. All cases are given a New status, by default. Set the status: choose from In Progress or Closed.

Note
Once you have set the status to In Progress you cannot reset it to New.

Overview

The Overview tab shows you a summary of the threat. You can view and update a record of the investigation.
• **Threat Summary**: This an outline of the threat detected.
  — **What**: Threat detected.
  — **Where**: Name of the computer and its user.
  — **When**: Infection time and date. Detection time and date.
  — **How**: Source of the infection, if known.
• **Next Steps**: This contains suggestions for what to do next in your investigation. At the moment the information is static. You can:
  — Click the link to see if your business files have been affected by the threat.
  — Click the link to see the progress of the threat infection.
• **Activity Record**: This is a record of investigation. It shows the creation date, when the status changed and the progress of the investigation. You can add comments by typing in the text box and clicking **Add Comment**.

**Artifacts**

This is a list of all the affected artifacts, for example business files, processes, registry keys, or IP addresses.

You can view only the affected business files, other files, registry keys and network connections by clicking on the appropriate number.

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**: The name of the artifact.
  — Click on the name to see more information. The details for the artifact are shown in a flyout on the right of the list.
  — You can add your own comments by typing in the text box and clicking **Add Comment**. The comment is added to the **Activity Record** for the case.
  — Click > to close the flyout.
• **Type**: The type of artifact, such as a business file or a registry key.
• **Time logged**: The time and date a process was accessed.

**Visualize**

This shows the chain of events surrounding the threat infection. It also shows the root cause and where the infection was detected (beacon). The effects of the infection are shown as a series of bubbles and arrows. The bubbles represent the affected artifacts and the arrows show the path of the infection and how the infection occurred.

Different artifact types are shown as different colors and a letter. The key along the top of the map shows which type of artifact is represented by each color. You can:
• Use the switches in the key to turn on or off the display of the different artifact types.
• Use the **Show labels** switch to display the names of all artefacts.
• Hover over an artifact to display its name.

To view the effects of the infection:
• Select an artifact by clicking on a bubble.
This displays its role in the infection process. The details for the selected artifact are shown in a flyout on the right of the infection map.

### 3.4 Logs & Reports

The **Logs & Reports** pages provide detailed reports on the security features in Sophos Central. Some of these reports may be available in **Logs & Reports** under **Overview** if you have more than one product.

#### 3.4.1 Logs

The following logs are available for Endpoint Protection:

- **Events.** All events on your devices, see **Events Report** (page 289).
- **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 300).
- **Data Loss Prevention Events Log.** All events triggered by data loss prevention rules for computers or servers, see **Data Loss Prevention Events Log** (page 301).

#### Events Report

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

For information about the different types of event, see **Event types** (page 290).

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

**Note**

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).

You can find the following features and information on the **Events** page:

**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.

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

- **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 283).

After you have taken an action or ignored the alert, it is no longer displayed on the Alerts page, but the event remains in the Events list.

Runtime detections

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running malware detected</td>
<td>Medium</td>
<td>No</td>
<td>A program that was running on a computer and exhibited malicious or suspicious behavior has been detected. Sophos Central will attempt to remove the threat. If it succeeds, no alerts will be displayed on the Alerts page, and a “Running malware cleaned up” event will be added to the Events list.</td>
</tr>
<tr>
<td>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 unauthorised 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

<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.                                                                                                                                                                                                                                               |
| Malware cleaned up          | Low      | No               |                                                                                                                                                                                                                                                                                                                                          |
| Recurring infection         | High     | Yes              | 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.                                                                                                                                                           |
| Threat removed              | Low      | No               | A malware alert has been cleared from the alerts list on an endpoint computer.                                                                                                                                                                                                                                                             |
| Malware alert locally cleared | Low      | No               |                                                                                                                                                                                                                                                                                                                                          |
### 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>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>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>
<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>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>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>

**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.

<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>
</tbody>
</table>

**Note**
This occurs only if you change your reputation checking settings to “Log only”.

Firewall

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

Copyright © 2017 Sophos Limited
### Event type

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing heartbeat</td>
<td>High</td>
<td>Yes</td>
<td>A computer is no longer sending security heartbeat signals to the Sophos Firewall but is still sending network traffic. The computer may be compromised. The Sophos Firewall may have restricted the computer’s network access (depending on the policy your company set).</td>
</tr>
<tr>
<td>Restored heartbeat</td>
<td>Low</td>
<td>No</td>
<td>A computer has resumed sending security heartbeat signals to the Sophos 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>
</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>Disk not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>The client 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.</td>
</tr>
<tr>
<td>The Device Encryption status changed from Encrypted to Unmanaged</td>
<td>Low</td>
<td>See Note</td>
<td>Encryption on this computer is no longer managed by Sophos Central. This can happen because a policy is disabled or removed, or because encryption is disabled in the policy. Recovery is still possible at the computer’s details page if recovery keys are available.</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>A recovery key for an encrypted volume cannot be found in the Sophos Central database.</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 “allow file transfer on acceptance by user” 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 “allow file transfer” action was taken</td>
<td>A file containing controlled information was transferred.</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 in the last 365 days.

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 logged on.
- **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 Admin 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 Admin 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, the last 90 days or the last 365 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.
   - **CSV of past 365 days** or **PDF of past 365 days**: Exports activities from the past 365 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.

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.

**3.4.2 Reports**

The reports that you can see depend on your license.
If you're new to reports, read this page to find out how reports work. You can customise the information displayed in the report pages by using filters and limiting the time range for the displayed data.

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

**How do I 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.

**How do I 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.

**How do I 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.

### 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 details including:
- 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 address.
- Role. This shows what administration role, if any, the user has, see Administration Roles (page 333).

This column is only visible if you are an administrator.

To see full details for a user, click on the user’s name. For more information, see User Summary (page 307).

To display different types of user, click the drop-down arrow on the filter above the list.

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 333).

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. 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 330).

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 307).

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 333).

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.
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 333).

   **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.
   
   **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.

**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 226).

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.
For each 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 (such as blocked websites or policy non-compliance) detected on the user’s devices.

You can customize the list by selecting the start and finish dates.

The list shows:

- A description of the event.
- The time and date when the event occurred.
- An icon that indicates the importance of the event.
- The device associated with the event.

To see the events arranged by type, as well as a graph showing events day by day, click **View Events Report**.

### Key to the icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="checkmark.png" alt="Green Check" /></td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td><img src="warning.png" alt="Yellow Exclamation" /></td>
<td>Warning.</td>
</tr>
<tr>
<td><img src="exclamation.png" alt="Red Exclamation" /></td>
<td>Action required.</td>
</tr>
<tr>
<td><img src="info.png" alt="Information" /></td>
<td>For information only.</td>
</tr>
</tbody>
</table>

## 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 312).

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 312).

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 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.
- Delete computers.
- Install or uninstall software.
- Recover PIN/Password for encrypted computers (if you are using Sophos Device Encryption).

View computer details

The computers are listed with details of the operating system, the last user, the last time they were used, and the security and compliance status of the device.

The security status is indicated by an icon, as follows:

- 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.

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

To display different types of computer, click the drop-down arrow on the filter above the list.

You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

Delete computers

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

This deletes the computer from the Sophos Central Admin console. It does not uninstall the Sophos agent software, but the computer will not get updates any more.

**Note**  
If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

### 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.

### Retrieve recovery key (Windows computers)

If users are unable to log in to their encrypted computer, you can get a recovery password which used to unlock the computer. There is a recovery key (password) 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 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, you need to find the recovery key identifier for the computer 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.
3. In Sophos Central, go to Computers and click the Retrieve Recovery Key button.
4. Enter the recovery identifier provided by the user and display the recovery key.

**Note**
If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

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.

**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 computer can be unlocked. 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, they can use a recovery key to regain access to their data.

To get the recovery key, you need to find the recovery key identifier for the computer 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 the recovery identifier provided by the user and display the recovery key.

**Note**
If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

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.

**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. They can use it to access the computer and create a new password. Once they have created a new password they can access their computer again.

**Note**
You can recover access to encrypted non-startup volumes on Mac, see [Sophos Central Device Encryption administrator guide](#).

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.

### 3.6.1 Computer Summary

The **Summary** tab in a computer’s details page lets you see the following:
- Security status of the computer.
- Recent events on the computer.
- Endpoint Agent summary. This agent provides threat protection and more.
- Device Encryption summary. This is not displayed if the encryption policy has been disabled.
- Web Gateway summary (if you have Sophos Web Gateway). This agent provides advanced protection against risky or inappropriate web browsing.
- Tamper protection settings.
- Update cache status. This is not displayed if a cache has not been set up.

### Security status

In the left-hand pane, you can see details of the security status.

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

**Status**
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.

Delete

The Delete option deletes the computer from the Sophos Central Admin console. This does not uninstall the Sophos agent software, but the computer will not get updates any more.

Tip

If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

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:

- Endpoint Agent (for threat protection and more).
- Web Gateway Agent (advanced web protection).

Endpoint Agent Summary

The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.

The summary shows the last activity on the endpoint. It also shows whether the endpoint agent is up to date.

If you need to take action, buttons are displayed:

- Update: Updates the Sophos agent software on the computer.
- Scan Now: Scans the computer 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 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.

Device Encryption summary

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers.

This summary shows the encryption status and type of authentication used (or “Protector” in BitLocker terms) for each volume.

Retrieve recovery key

You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their PIN or passphrase or lose the USB drive they use to log on.

1. Click Retrieve next to the volume. This displays the recovery key ID and latest recovery key.
2. 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.

3. Give the recovery key to the user.

The computer can be unlocked. 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.

**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 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.

This shows that a cache has been set up for the computer. It shows which server is being used.

**3.6.2 Computer Events**

The **Events** tab in a computer’s details page displays events (such as blocked websites or policy non-compliance) detected on the computer.

You can customize the list by selecting the start and finish dates.

The list shows:
• A description of the event.
• The time and date when the event occurred.
• An icon that indicates the importance of the event. See the Key to the icons.
• An icon that indicates which Sophos agent reported the event. See the Key to the icons.

To see the events arranged by type, as well as a graph showing events day by day, click View Events Report.

**Key to the icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>🔴</td>
<td>Warning.</td>
</tr>
<tr>
<td>🔴</td>
<td>Action required.</td>
</tr>
<tr>
<td>🔄</td>
<td>For information only.</td>
</tr>
<tr>
<td>🔄</td>
<td>Endpoint Agent event.</td>
</tr>
<tr>
<td>🔄</td>
<td>Gateway Agent event.</td>
</tr>
</tbody>
</table>

### 3.6.3 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 283).

#### Activity

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

**Computer Security Status**
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).

### 3.6.4 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.

### 3.7 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.
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.

3.7.1 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.

   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.

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.

---

### 3.7.2 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.

---

### 3.8 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**.

---

### 3.8.1 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.

3.8.2 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.

3.8.3 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 228).
• 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.

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.
Sophos Central Admin

- 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.

Live Protection

You can select:

- **Use Live Protection to check the latest threat information from SophosLabs online.** This checks suspicious files against the latest information in the SophosLabs database.

  **Note**
  This option uses Live Protection during real-time scanning. If you also want to use it during scheduled scans, select **Use Live Protection during scheduled scans.**

- **Automatically submit malware samples to SophosLabs.** This sends a sample of detected malware to Sophos for analysis.
- **Use Live Protection during scheduled scans.** This checks files against the latest threat information online during any scheduled scans you have set up.
- **Collect reputation data during on-demand scans.** When a scheduled scan runs, or you use “Scan Now”, Live Protection will collect data about the software on users’ computers and send it to Sophos. The data helps us decide which software is most widely used and so likely to be trustworthy.

  **Note**
  We use this “reputation data” in our Download Reputation security feature.

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 download a low-reputation file. They can then trust or delete the file. This is the default setting.
  
  — The **Reputation level.** If you select **Strict**, medium-reputation as well as low-reputation files will be detected. The default setting is **Recommended**.

**Remediation**

If you select **Remediation**, Sophos Central will attempt to clean up detected malware automatically.

**Note**

If cleanup is successful, the malware detected alert is deleted from the **Alerts** list. The malware detection and the cleanup are shown in the **Events** list.

If you enable Root Cause Analysis you can investigate the chain of events surrounding a malware infection and pinpoint areas where you can improve your security, see **Root Cause Analysis** (page 9).

**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 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, such as Java applications. You can select which application types you wish to protect.

• **Protect against application hijacking.** 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

**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. You can also exclude applications from detected exploits.

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 Scanning Exclusions** page.

To create a policy scanning exclusion:

1. Click **Add Exclusion** (on the right of the page).
   
   The **Add Scanning Exclusion** dialog is displayed.

2. In the **Exclusion Type** drop-down list, select a type of item to exclude (file or folder, website, or potentially unwanted application).

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

   **File or folder (Windows).** You can exclude a drive, folder or file by full path. For file title or extension the wildcard * may be used, though **.* is not valid. Examples:

   - Folder: `C:\programdata\adobe\photoshop\` ([add a slash for a folder]).
   - Entire drive: `D:`
   - File: `C:\program files\program\*.vmg`

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

   - `/Volumes/excluded` (Mac)
   - `/mnt/hgfs/excluded` (Linux)

   **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)** Here you can exclude any exploit that’s been detected. Sophos Central will no longer detect it for the affected application. Sophos Central will also no longer block the affected application. Select the detected exploit you want to exclude from the list.

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**

**Attention**
This help page describes policy settings for workstations.

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. If you upgrade to Windows 7 you can use all of them.
## Wildcards

You can use the wildcards shown in this table.

**Note**

Only * and ? can be used on Windows XP.

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
</table>
| * [Star] | Zero or more of any character except \ or / | For example:  
- `c:\foo\**\bar` matches:  
  - `c:\foo\bar`  
  - `c:\foo\more`  
  - `c:\foo\even`  
  - `c:\foo\bar`  
  - `**\bar` matches `c:\foo\bar`  
  - `c:\foo\**` matches `c:\foo`  
  - `c:\foo\bar` matches `c:\foo\more\bar`  
  - `c:\foo\*bar` matches `c:\foonore\bar` but NOT `c:\foo\more\bar` |
| ** [Star Star] | Zero or more characters including \ and /, when bracketed by \ or / characters or used at the start or end of an exclusion. Any other use of a ** is treated as a single * and matches zero or more characters excluding \ and /.| |
| \ [Backslash] | Either \ or / | |
| / [Forward slash] | Either / or \ | |
| ? [Question mark] | One single character, unless at the end of a string where it can match zero characters. | Note that:  
- `*.` matches all files  
- `*.` matches all files without an extension  
- `"foo."` matches "foo" and "foo." |
| . [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. | |

### 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>
</tbody>
</table>
### Expression | Interpreted as | Description
--- | --- | ---
*.txt | **\*.txt | Exclude all files named *.txt (in any location).
C: | C: | Exclude drive C: from scanning (including the drive’s master boot record).
C:\ | C:\ | Exclude all files on drive C: from scanning (but scan the drive’s master boot record).
C:\foo\ | C:\foo\ | All files and folders underneath C:\foo, including C:\foo itself.
C:\foo\*.txt | C:\foo\*.txt | All files or folders contained in C:\foo named *.txt

### 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 + later</th>
<th>Windows XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>%allusersprofile%</td>
<td>C:\ProgramData</td>
<td>C:\Documents and Settings\All Users</td>
</tr>
<tr>
<td>%appdata%</td>
<td>C:\Users*\AppData\Roaming</td>
<td>C:\Documents and Settings* Application Data</td>
</tr>
<tr>
<td>%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>
</tbody>
</table>

**Note**

Does not work for real-time scanning.
### Variable Table

<table>
<thead>
<tr>
<th>Variable</th>
<th>Windows 7 + later</th>
<th>Windows XP</th>
</tr>
</thead>
<tbody>
<tr>
<td>%localappdata%</td>
<td>C:\Users*\AppData\Local</td>
<td>C:\Documents and Settings *\Local Settings\Application Data</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>%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>

#### Note

Does not work for real-time scanning.

---

### 3.8.4 Peripheral Control Policy

Peripheral control lets you control access to peripherals and removable media. You can also exempt individual peripherals from that control.

To set it up:
- Create an **Peripheral Control** policy. See Create or Edit a Policy (page 228).
- 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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The totals include all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent policies for all devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>MTP/PTP</strong> category includes devices such as phones, tablets, cameras and media players that connect using the MTP or PTP protocols.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Bluetooth, Infrared, and Modem categories do not have the <strong>Read Only</strong> option.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Wireless Network Adaptor category has a <strong>Block Bridged</strong> option. This prevents bridging of two networks.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripherals are detected when you are in monitoring mode or if there is an access restriction for that type of peripheral.</td>
</tr>
</tbody>
</table>
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.

### 3.8.5 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.

To set it up:

- Create an **Application control** policy. See **Create or Edit a Policy** (page 228).
- 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**:
   - Select **Detect controlled applications during scheduled and on-demand scans**.
   - 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:
   - Find the applications you want to use and clear the checkbox next to them.
   - 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.

   - Click **Save to List**.

11. In **Detection Options**:
   - Select **Detect controlled applications when users access them**.
   - 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.

### 3.8.6 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 346). 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 226).

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 228).
- 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 an use existing rule or create a new rule, see Create a Data Loss Prevention Rule (page 347). 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.

3.8.7 Web Control Policy
You need to configure the Web Control options to protect users and computers. There are no default options.

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 228).
• 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

Select **Control sites tagged in Website Management** if you want to control access to websites that you have “tagged”, i.e. put into your own categories, at the **System Settings > Website Management** page.

1. Click **Add New**.
2. Select your **Website Tag** and the **Action** you want to apply to the websites with that tag.

### 3.8.8 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.
To set it up:

- Create a **Updating** policy. See [Create or Edit a Policy](page 228).
- 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 the next time they start.

### 3.9 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.

### 3.9.1 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 330). For full details of how it works, see [About Active Directory synchronization](page 330). Once you have set up synchronization you can review its status and other settings, see [Active Directory Sync Status](page 329).

For instructions on configuring Azure Active Directory synchronization, see [Set up synchronization with Azure Active Directory](page 332). Once you have set up synchronization you can review its status and other settings, see [Azure AD Sync Status](page 332).

### 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 the Sophos Central Admin console. It does not support two-way synchronization between the Sophos Central Admin console 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 the Sophos Central Admin console. 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 the Sophos Central Admin console.
    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 332).

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

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.

### 3.9.2 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 cannot...</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. |
| **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.  
• Update the Sophos agent software on a computer.  
• Scan computers. | Manage roles and role assignments. In addition they cannot:  
• Assign policies.  
• Change settings. | 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 cannot:  
• 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 cannot:  
• 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. |
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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read-only</strong> administrators can only receive alerts.</td>
</tr>
</tbody>
</table>

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 307).

**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.

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

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

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can only see this option if you are a <strong>Super Admin</strong> administrator.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a name or part of a name in the search box to filter the list of available users.</td>
</tr>
</tbody>
</table>

**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.

### 3.9.3 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.

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 **X** to the right of the exclusion you wish to remove.

### 3.9.4 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.

**Note**

You can change the settings for an individual device or server. Open its details page and select the **Tamper Protection** tab. There you can view the password, generate a new one, or temporarily disable tamper protection for that device.

### 3.9.5 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.

### 3.9.6 Website Management

This page is not available if you do not have a Web Control or Web Gateway license.

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 on the **Policies** page.

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**.

### 3.9.7 Registered Firewall Appliances

In Settings, on the **Registered Firewall Appliances** page, you can view Sophos Firewalls that have been registered with Sophos Central. You can also deregister (or "disconnect") them.

**Note**
You can only register a Sophos Firewall from the Firewall console (Go to **System > System Services > Security Heartbeat**).

**About registered Firewalls**

When a Sophos Firewall is registered with Sophos Central, your computers can send regular reports on their security status or "health" to the Firewall. These reports are known as "Security Heartbeats".

If more than one 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 Firewall can restrict its network access. The Firewall admin and the 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 Firewalls that are registered with Sophos Central:

• Name
• IP address
• Active. This indicates whether the Firewall has received Security Heartbeats within the previous hour.

To find a Firewall, start to enter the name in the **Search for a Firewall** field. As you type, the list is filtered to show only Firewalls that match.

Deregister Firewalls

You can deregister Firewalls from Sophos Central. For example, if you no longer use a Firewall, you could deregister it so that it is no longer shown here.

When you deregister a 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 the Firewall or Firewalls 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 the Firewalls.
   
   The selected Firewalls are removed from the list.

   If you deregister all the 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.

3.9.8 Global Scanning Exclusions

You can exclude files, websites and applications from scanning for threats. You can also exclude applications from detected exploits.

For example, you might exclude activity by some commonly-used applications to reduce the impact of scanning on performance.

You can do this in Settings, on the **Global Scanning 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 scanning exclusions in the policies instead.

1. On the **Global Scanning Exclusions** page, click **Add Exclusion** (on the right of the page).
   
   The **Add Scanning 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 detected exploit).

3. Specify the item or items you want to exclude. The following rules apply:
   
   • **File or folder (Windows)**. You can exclude a drive, folder or file by full path. For file title or extension the wildcard * may be used, though **.* is not valid. Examples:

   — Folder: `C:\programdata\adobe\photoshop\` (add a slash for a folder).
Sophos Central Admin

- Entire drive: D:
- File: C:\program files\program\*.vmg

For more details of exclusions for Windows servers, see Scanning exclusions (page 159).

- **File or folder (Mac/Linux).** You can exclude a folder or file. You can use the wildcards ? and *.
  Examples:
  - /Volumes/excluded (Mac)
  - /mnt/hgfs/excluded (Linux)

- **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 164).

- **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 11111111.11111111.11111111.00000000. 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’s been detected. Sophos Central will no longer detect it for the affected application. Sophos Central will also no longer block the affected application.

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.**
3.9.9 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

Set the bandwidth used

In Settings, on the Bandwidth Usage page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.

This helps to ensure that updating does not cause computers to run slowly.

You can specify a custom bandwidth or unlimited bandwidth.

Note

This setting is for Windows computers only.

Note

This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos Manage Update Cache (page 341).

3.9.10 Manage Update Cache

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.

When you set up a cache on a server, Sophos Central does as follows:

• Installs Sophos caching software.
• Fetches updates from Sophos and puts them in a cache.
• Automatically configures Windows computers in your network to update from a cache.

Using caches doesn’t affect how often or when computers are updated.

Note

Workstations and servers can both update from a cache.

Note

Windows Vista or XP workstations cannot update from a cache.

Set up a cache

Before you set up a cache, ensure that:

• The server has at least 5GB free disk space.
• Port 8191 is available and accessible to computers that will update from the cache.

**Note**
The Update Cache installer will open port 8191 in Windows Firewall. When Update Cache is uninstalled, the port will be closed again.

To set up a cache:
1. In Settings, go to the **Manage Update Cache** 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. If you have already set up a cache on some servers, to hide them from view, select **Servers without Update Cache**.
3. Select the server or servers where you want to set up a cache.
4. Click **Set Up Cache**.

**Remove a cache**

When you remove a cache:
- Sophos Central uninstalls caching software, removes the cache of downloaded updates, and closes port 8191 in Windows Firewall.
- Computers currently updating from this server are automatically reconfigured to update from another update cache, if you have one.

If you remove all your caches, computers will update directly from Sophos.

To remove a cache:
1. Go to the **System Settings > Manage Update Cache** 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.
3. Select the server or servers you want to remove a cache from.
4. Click **Remove Cache**.

**3.9.11 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 342)
- **Controlled Updates** (page 342)
- **Control Updates Manually** (page 343)
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 Updates.

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 Updates.

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 non-test computers 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.

**3.9.12 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.

When you add an AWS account on this page, Sophos Central will do as follows:

- Display AWS instance details.
- Remove terminated AWS instances automatically.
- Let you apply server policies to Auto Scaling Groups.

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.

3.9.13 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 348).

- **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 347), 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.

You can also export custom rules, click ➡️. This creates an xml file containing the rule definition.

Click ✗ to delete a rule and 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 349).

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.

3.9.14 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 346).

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 349).

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 and 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.
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 X to delete an expression.
   Click ✔ to edit an expression. Once you have finished your edits, 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.
## 3.10 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.

### 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.

### 3.10.1 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.

- **Windows: Endpoint Advanced Installer.** Click this for an installer with all endpoint products your license covers.
- **Windows: Choose Products ...** Click this if you want to choose which products will be included in the installer. The choices are:
  - Endpoint Advanced (protection from malware).
  - Intercept X (protection from ransomware and exploits).
  - Device Encryption.
• **Download Mac OS X installer.** Click this for an installer for Macs.
• **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](#).
4 Device Encryption

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.

4.1 Dashboard

The Dashboard is the start page of Device Encryption 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.

4.2 Alerts

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

Alerts that are resolved automatically by Sophos Central are not displayed. For example, if malware is detected and then cleaned up automatically, no alert is displayed. If you want to view all events on your devices, go to the Logs & Reports > Events page.

Alerts

For each alert, the list shows the event that caused the alert, when it occurred, and which user and device are affected.

The list also shows the severity of alerts:

⚠ Orange warning sign for medium-priority alerts.

❗ Red warning sign for high-priority alerts.

For information about the different types of alerts, see the other Help pages in this section.
The alert event time is not updated if the same event occurs repeatedly.

Actions on alerts

There is a checkbox next to each alert. When you select one or more checkboxes, you can apply certain actions on alerts. The action buttons are displayed in the upper right of the page.

The following actions may be available, 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 Contact Sophos Support (page 368). 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 285).
- **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.

Related concepts

Events Report (page 289)
Email Alerts (page 287)
Contact Sophos Support (page 368)

4.2.1 Alerts for Device Encryption

There are the following types of alerts for Device Encryption:

Medium

- **Disk not encrypted**
  The client 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.
4.2.2 Email Alerts

Sophos Central automatically sends email alerts to administrators when events occur (for example, "Potentially Unwanted Application detected").

Sophos Central does as follows:

- Sends alerts for Medium or High severity events that require action. For details of events in these categories, see Alerts (page 283).
- Sends alerts to all administrators. To see details of administrators, go to System Settings > Role Management.
- Does not send alerts if an alert for the same type of event has been sent within the previous 24 hours.

You cannot change the email alert settings.

4.3 Logs & Reports

The Logs & Reports pages provide detailed reports on the security features in Sophos Central. Some of these reports may be available in Logs & Reports under Overview if you have more than one product.

4.3.1 Logs

The following logs are available for Encryption:

- **Events.** All events on your devices, see Events Report (page 289).
- **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 300).

Events Report

The Events Report page provides information about all events on your devices. For information about the different types of event, see Event types (page 290).

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

**Note**

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).

You can find the following features and information on the Events page:

**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.

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

**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:

- **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 283).

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               |                                                                                                                                            |
| 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.   |</p>
<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 unauthorised 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></td>
</tr>
</tbody>
</table>
### Controlled application allowed

<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>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

<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 “Malware cleaned up” 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>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>
</tbody>
</table>
### Malware alert locally cleared

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

A 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>
### 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 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>
<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>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

<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>

### 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>
</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>
<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>
</tbody>
</table>

**Note**

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

### Firewall

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

<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 the Sophos Firewall but is still sending network traffic. The computer may be compromised. The Sophos 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 the Sophos 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>
</tbody>
</table>
## Event Log

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>The client 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.</td>
</tr>
<tr>
<td>The Device Encryption status changed from Encrypted to Unmanaged</td>
<td>Low</td>
<td>See Note</td>
<td>Encryption on this computer is no longer managed by Sophos Central. This can happen because a policy is disabled or removed, or because encryption is disabled in the policy. Recovery is still possible at the computer’s details page if recovery keys are available.</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>A recovery key for an encrypted volume cannot be found in the Sophos Central database.</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>
</tbody>
</table>
A "block file transfer" action was taken
A transfer of a file containing controlled information was blocked.

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 in the last 365 days.

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 logged on.
- **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 Admin 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 Admin 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, the last 90 days or the last 365 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 dropdown 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.
   - **CSV of past 365 days** or **PDF of past 365 days**: Exports activities from the past 365 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.

### 4.3.2 Reports

The reports that you can see depend on your license.

If you’re new to reports, read this page to find out how reports work.

You can customise the information displayed in the report pages by using filters and limiting the time range for the displayed data.

**Note**

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

**How do I 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.

**How do I 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.

**How do I 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.
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 details including:

• 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 address.

• Role. This shows what administration role, if any, the user has, see Administration Roles (page 333).

  This column is only visible if you are an administrator.

To see full details for a user, click on the user’s name. For more information, see User Summary (page 307).

To display different types of user, click the drop-down arrow on the filter above the list.

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 333).

   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. Click Add.
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.

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.

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 330).

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 307).

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 333).

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.

**Related concepts**

*Active Directory Sync* (page 339)

**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 333).

   **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.

   **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.
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.

**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 226).

**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. For each 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 [such as blocked websites or policy non-compliance] detected on the user’s devices. You can customize the list by selecting the start and finish dates. The list shows:

- A description of the event.
- The time and date when the event occurred.
- An icon that indicates the importance of the event.
- The device associated with the event.

To see the events arranged by type, as well as a graph showing events day by day, click **View Events Report**.

**Key to the icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>⚠</td>
<td>Warning.</td>
</tr>
</tbody>
</table>
### 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 312).

#### 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 312).
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.
- Delete computers.
- Install or uninstall software.
- Recover PIN/Password for encrypted computers (if you are using Sophos Device Encryption).
View computer details

The computers are listed with details of the operating system, the last user, the last time they were used, and the security and compliance status of the device.

The security status is indicated by an icon, as follows:

- 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.

To search for a computer, enter the name in the search field above the list.
To display different types of computer, click the drop-down arrow on the filter above the list.
You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

Delete computers

You can delete computers that you no longer need to manage from Sophos Central.
Select the computer or computers you want to delete and click Delete (in the upper right of the page).
This deletes the computer from the Sophos Central Admin console. It does not uninstall the Sophos agent software, but the computer will not get updates any more.

**Note**
If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

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.

Retrieve recovery key (Windows computers)

If users are unable to log in to their encrypted computer, you can get a recovery password which used to unlock the computer. There is a recovery key (password) 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 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, you need to find the recovery key identifier for the computer 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.
3. In Sophos Central, go to Computers and click the Retrieve Recovery Key button.
4. Enter the recovery identifier provided by the user and display the recovery key.

Note
If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

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.

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 computer can be unlocked. 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, they can use a recovery key to regain access to their data. To get the recovery key, you need to find the recovery key identifier for the computer 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 the recovery identifier provided by the user and display the recovery key.

   **Note**
   
   If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

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.

   **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. They can use it to access the computer and create a new password. Once they have created a new password they can access their computer again.

   **Note**
   
   You can recover access to encrypted non-startup volumes on Mac, see Sophos Central Device Encryption administrator guide.

On endpoints running macOS 10.12 or earlier, a new recovery key is created and stored in Sophos Central. A recovery key can only be used once. If you need to recover a computer again later, you need to retrieve a new recovery key.

On endpoints running macOS 10.13 and Apple File System (APFS), no new recovery key is created. The existing recovery key remains valid.
4.5.1 Computer Summary

The Summary tab in a computer’s details page lets you see the following:

- Security status of the computer.
- Recent events on the computer.
- Endpoint Agent summary. This agent provides threat protection and more.
- Device Encryption summary. This is not displayed if the encryption policy has been disabled.
- Web Gateway summary (if you have Sophos Web Gateway). This agent provides advanced protection against risky or inappropriate web browsing.
- Tamper protection settings.
- Update cache status. This is not displayed if a cache has not been set up.

Security status

In the left-hand pane, you can see details of the security status.

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

**Status**
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.

**Delete**
The **Delete** option deletes the computer from the Sophos Central Admin console. This does not uninstall the Sophos agent software, but the computer will not get updates any more.

**Tip**
If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

**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:

- Endpoint Agent (for threat protection and more).
Web Gateway Agent (advanced web protection).

**Endpoint Agent Summary**

The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.

The summary shows the last activity on the endpoint. It also shows whether the endpoint agent is up to date.

If you need to take action, buttons are displayed:

- **Update**: Updates the Sophos agent software on the computer.
- **Scan Now**: Scans the computer 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 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.

**Device Encryption summary**

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers.

This summary shows the encryption status and type of authentication used (or “Protector” in BitLocker terms) for each volume.

**Retrieve recovery key**

You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their PIN or passphrase or lose the USB drive they use to log on.

1. Click **Retrieve** next to the volume. This displays the recovery key ID and latest recovery key.
2. 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.

3. Give the recovery key to the user.

The computer can be unlocked. 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.

**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 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.

This shows that a cache has been set up for the computer. It shows which server is being used.

**4.5.2 Computer Events**

The **Events** tab in a computer’s details page displays events (such as blocked websites or policy non-compliance) detected on the computer.

You can customize the list by selecting the start and finish dates.

The list shows:

- A description of the event.
- The time and date when the event occurred.
- An icon that indicates the importance of the event. See the Key to the icons.
- An icon that indicates which Sophos agent reported the event. See the Key to the icons.

To see the events arranged by type, as well as a graph showing events day by day, click **View Events Report**.

**Key to the icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Warning.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Action required.</td>
</tr>
</tbody>
</table>
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 283).

### 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.
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.
   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.
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 (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 333).

### 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.
   
   You see a list of policy types.
3. Click on the policy type to open a list of policies.
4. Find the policy you want to edit and click it.
5. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users or devices.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.

### 4.7.3 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.

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 228).
- Open the policy’s **Settings** tab and configure it as described below. Make sure the policy is enabled.

#### Settings

**Enable encryption of endpoints**

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.

Advanced Windows Settings

Require startup authentication
This option is enabled by default.
This option enforces authentication via TPM+PIN, passphrase, or USB key. If this setting is disabled, TPM-only logon protection will be installed on supported computers. For more information on authentication methods, see the Sophos Central Device Encryption administrator guide.

Encrypt used space only
This option is disabled by default.
This option allows you to encrypt used space only instead of encrypting the whole drive. You can use it to make initial encryption (when the policy is first applied to a computer) much faster.

Warning
If you encrypt used space only, deleted data on the computer might not be encrypted, so you should only use this option for newly set up computers.

Note
This option has no effect on endpoints running Windows 7.

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 330). For full details of how it works, see About Active Directory synchronization (page 330). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 329).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 332). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 332).

### 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 330). For full details of how it works, see About Active Directory synchronization (page 330). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 329).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 332). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 332).

### 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 the Sophos Central Admin console. It does not support two-way synchronization between the Sophos Central Admin console 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 the Sophos Central Admin console. 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
Sophos Central Admin

- **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 the Sophos Central Admin console.

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 332).

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

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 cannot...</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><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 cannot:</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.</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></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scan computers.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 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.

---

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role cannot...</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 cannot:  
• 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 cannot:  
• 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. |
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 307).

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.
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.

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.

4.9.1 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 Windows Device Encryption. Click this for an installer for encryption only.
• Windows: Choose Products .... Click this if you want to choose which products will be included in the installer. The choices are:
  — Endpoint Advanced (protection from malware).
  — Intercept X (protection from ransomware and exploits).
  — Device Encryption.
• Send Installers to Users. Click this to go to a page where you can add users and send them installers that they can use.
5 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.

5.1 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.

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.

Messages

Messages shows the number of email messages processed by Email Security for your protected mailboxes for the last 30 days. It also shows the number of spam and malware messages detected.
Click See Report to open the Messages report and review the details of the processed messages, see Messages Report (page 301).

Web Stats

Web Stats 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.

## 5.2 Alerts

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

Alerts that are resolved automatically by Sophos Central are not displayed. For example, if malware is detected and then cleaned up automatically, no alert is displayed. If you want to view all events on your devices, go to the **Logs & Reports > Events** page.

### Alerts

For each alert, the list shows the event that caused the alert, when it occurred, and which user and device are affected.

The list also shows the severity of alerts:

- ![Orange warning sign for medium-priority alerts.](image)
- ![Red warning sign for high-priority alerts.](image)

For information about the different types of alerts, see the other Help pages in this section.

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

### Actions on alerts

There is a checkbox next to each alert. When you select one or more checkboxes, you can apply certain actions on alerts. The action buttons are displayed in the upper right of the page.

The following actions may be available, 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 [Contact Sophos Support](page 368). 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 285).

• **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.

**Related concepts**

- [Events Report](page 289)
- [Email Alerts](page 287)
- [Contact Sophos Support](page 368)

### 5.2.1 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.

### 5.2.2 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.

**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**
**Sophos Central Admin**

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 283).

- 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.

### 5.2.3 Email Alerts

Sophos Central automatically sends email alerts to administrators when events occur (for example, "Potentially Unwanted Application detected").

Sophos Central does as follows:

- Sends alerts for Medium or High severity events that require action. For details of events in these categories, see Alerts (page 283).
- Sends alerts to all administrators. To see details of administrators, go to System Settings > Role Management.
- Does not send alerts if an alert for the same type of event has been sent within the previous 24 hours.

You cannot change the email alert settings.
5.3 Logs & Reports

The Logs & Reports pages provide detailed reports on the security features in Sophos Central.

Some of these reports may be available in Logs & Reports under Overview if you have more than one product.

5.3.1 Logs

The following logs are available for Server Protection:

- **Events.** All events on your devices, see Events Report (page 289).
- **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 300).
- **Data Loss Prevention Events Log.** All events triggered by data loss prevention rules for computers or servers, see Data Loss Prevention Events Log (page 301).

Events Report

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

For information about the different types of event, see Event types (page 290).

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

**Note**

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).

You can find the following features and information on the Events page:

**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.

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

**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:

- **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 283).

After you have taken an action or ignored the alert, it is no longer displayed on the Alerts page, but the event remains in the Events list.

Runtime detections

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running malware detected</td>
<td>Medium</td>
<td>No</td>
<td>A program that was running on a computer and exhibited malicious or suspicious behavior has been detected. Sophos Central will attempt to remove the threat. If it succeeds, no alerts will be displayed on the Alerts page, and a “Running malware cleaned up” event will be added to the Events list.</td>
</tr>
<tr>
<td>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 unauthorised 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

<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 “Malware cleaned up” 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. |
| Malware cleaned up         | Low       | No               | 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. |
| Recurring infection        | High      | Yes              | 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. |
| Threat removed             | Low       | No               | A malware alert has been cleared from the alerts list on an endpoint computer. |
| Malware alert locally cleared | Low       | No               | A malware alert has been cleared from the alerts list on an endpoint computer. |
### 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>
</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>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>
<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>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>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>

**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.

<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>
</tbody>
</table>

**Note**
This occurs only if you change your reputation checking settings to “Log only”.

Firewall

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

---

Copyright © 2017 Sophos Limited
<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 the Sophos Firewall but is still sending network traffic. The computer may be compromised. The Sophos 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 the Sophos 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>
</tbody>
</table>
## Disk not encrypted

- **Event type**: Disk not encrypted
- **Severity**: Medium
- **Action required?**: See Note
- **Description**: The client 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.

## The Device Encryption status changed from Encrypted to Unmanaged

- **Event type**: The Device Encryption status changed from Encrypted to Unmanaged
- **Severity**: Low
- **Action required?**: See Note
- **Description**: Encryption on this computer is no longer managed by Sophos Central. This can happen because a policy is disabled or removed, or because encryption is disabled in the policy. Recovery is still possible at the computer’s details page if recovery keys are available.

## Recovery key missing

- **Event type**: Recovery key missing
- **Severity**: Medium
- **Action required?**: See Note
- **Description**: A recovery key for an encrypted volume cannot be found in the Sophos Central database.

## Recovery key received

- **Event type**: Recovery key received
- **Severity**: Low
- **Action required?**: See Note
- **Description**: Sophos Central received a recovery key from an endpoint computer.

## Recovery key revoked

- **Event type**: Recovery key revoked
- **Severity**: Low
- **Action required?**: See Note
- **Description**: A recovery key has been viewed in Sophos Central, so it has been revoked and will be replaced.

## Data Loss Prevention

### An "allow file transfer on acceptance by user" action was taken

- **Description**: A file containing controlled information was transferred after a user acknowledged they were transferring the information.

### An "allow file transfer" action was taken

- **Description**: A file containing controlled information was transferred.
**Event type** | **Description**
--- | ---
A “block file transfer” action was taken | A transfer of a file containing controlled information was blocked.

**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 in the last 365 days.

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 logged on.
- **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 Admin 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 Admin 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, the last 90 days or the last 365 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.
   - **CSV of past 365 days** or **PDF of past 365 days**: Exports activities from the past 365 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.

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
- **FileName**: 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.

**5.3.2 Reports**

The reports that you can see depend on your license.
If you're new to reports, read this page to find out how reports work. You can customise the information displayed in the report pages by using filters and limiting the time range for the displayed data.

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

### How do I 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.

### How do I 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.

### How do I 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.

## 5.4 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.

### About the servers list

The current servers are listed with these details:

- Name/Operating System.

**Tip**
“Sophos Security VM” indicates a host where Sophos protects the guest VMs.
• IP Address.
• 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).
• Last Updated. This is the last time that the Sophos agent software was updated.
• License. Standard or Advanced license.
• 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, click the drop-down arrow on the filter above the list.

**Tip**
The Virtual Servers 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 323).

### 5.4.1 Server Summary

The Summary tab of a server’s details page lets you see server details and manage the server.

The page includes:
• Server details.
• Actions you can take on the server.
• A summary of recent events on the server.
• A summary of the device status.
• Separate tabs for Events, Exclusions, Lockdown Events and Policies.

The server details and actions buttons are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.
Server details

In the left-hand pane, you can see the server details, such as name and operating system.
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 the Sophos Central Admin console. This does not uninstall the Sophos agent software, but the server will no longer synchronize with the console.
  
  If you deleted the server accidentally, re-install the Sophos agent software to get it back.
- **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.

Device status

The device status summary shows:

- **Last Sophos Central Activity.** The last time the server communicated with Sophos Central.
- **Last Agent Update.** The last time the Sophos agent software on the server was updated.
- **IPv4 Address.**
- **IPv6 Address.**
- **Operating System.**

  If the operating system is shown as "Sophos Security VM", the server is a host with a Sophos security VM installed.
• **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.

  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.

• **Malware policy.** The threat protection policy that applies to the server. Click the policy name to see details.

• **Group.** Shows the group the server belongs to (if it belongs to one). Click **Change Group** to move the server to a different group, or simply to remove it from its current group.

  A server can only be in one group.

• **Tamper Protection.** This shows whether Tamper Protection (page 336) is enabled on the server or not. Click **View Details** to manage the tamper protection password for the server.

### Update cache 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. This is not displayed if a cache has not been set up or if the server is not being used as a cache.

If the server is being used as an update cache this shows:

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

Alternatively this shows that a cache has been set up for the server. It shows which server is being used.

### 5.4.2 Server Events

The **Events** tab in a server’s details page lets you see events (such as threats or policy non-compliance) detected on the server.

**Tip**

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.

### 5.4.3 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 283).

5.4.4 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 156).

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

5.4.5 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.

5.4.6 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.

5.4.7 AWS Instances

On the AWS Instances page, you can view the Amazon Web Services EC2 instances associated with your Sophos Central account. To add AWS accounts, see Amazon Web Services Accounts (page 345).

The AWS instances are listed with these details:
• Instance ID. Click on the ID to view the details of the instance.
• Agent installed. This shows whether a Sophos agent is installed on the instance. Click on the “Server Details” link to view the instances with Sophos agents installed.
• 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.

5.5 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 328).
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 328).

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.

5.5.1 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.

### 5.5.2 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.

### 5.6 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**.

### 5.6.1 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.

### 5.6.2 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.

### 5.6.3 Server Threat Protection Policy

**Attention**

This help page describes policy settings for servers. Different policy settings apply for workstations.

Threat protection keeps you safe from malware, risky file types and websites, and malicious network traffic.
To set up a policy:

- Create a Threat Protection policy. See Create or Edit a Policy (page 228).
- Open the policy’s Settings tab and configure it as described below. Make sure the policy is enabled.

**Recommended settings**

Select Use Recommended Settings if you want to use the settings Sophos recommends. These provide the best protection you can have without complex configuration.

**Note**

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.
- Automatic exclusion of activity by known applications from scanning. See Knowledgebase Article 121461.

**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**.

### 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 Knowledgebase 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.

- **Use Live Protection**. This checks suspicious files against the latest malware in the SophosLabs database.
  - **Automatically submit malware samples to SophosLabs**. This sends a sample of detected malware to Sophos for analysis.

- **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).

### 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.
Advanced security

**Note**
If you enable any Advanced Security features, servers assigned to this policy will use a Server Advanced Protection license.

You can select the following 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).

**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.

**Enable Sophos Security Heartbeat.** This sends regular reports on the security “health” of servers to Sophos XG Firewalls that are registered with Sophos Central. If a report shows that a server might have been compromised, the Firewall can restrict its network access.

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.

**Note**
These instructions give a brief description of exclusions you can use.

You can also exclude applications from detected exploits.

1. Click **Add Exclusion** (on the right of the page).
   
The Add Scanning Exclusion dialog is displayed.

2. In the **Exclusion Type** drop-down list, select a type of item to exclude (file or folder, process, website, or 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, see Virtual Server Scanning Exclusions: Wildcards (page 164)

- **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 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).** Here you can exclude any exploit that’s been detected. Sophos Central will no longer detect it for the affected application. Sophos Central will also no longer block the affected application. Select the detected exploit you want to exclude from the list.

**Note**

This switches off CryptoGuard ransomware protection for this exploit for the affected application on your Windows servers.
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**

**Attention**

This help page describes policy settings for servers.

When you specify the files, folders or processes you want to exclude from scanning, you can use wildcards or variables.

**Note**

This help page applies to Windows servers, but not to Linux. On Linux, only the wildcards * and ? can be used.

**Note**

Some wildcards or variables cannot be used for exclusions from real-time scanning on Windows Server 2003. If you upgrade to Windows Server 2008, you can use all of them.

**Wildcards**

You can use the wildcards shown in this table.
**Note**
Only * and ? can be used on 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 |
| \ [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. | Note that:  
  - *.* matches all files  
  - *. matches all files without an extension  
  - "foo." matches "foo" and "foo." |
| . [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. | |

**Example wildcards**
Here are some examples of the use of wildcards.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Interpreted as</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo</td>
<td>**\foo</td>
<td>Exclude any file named foo (in any location).</td>
</tr>
<tr>
<td>foo\bar</td>
<td>**\foo\bar</td>
<td>Exclude any file named bar in a folder named foo (in any location).</td>
</tr>
<tr>
<td>*.txt</td>
<td>***.txt</td>
<td>Exclude all files named *.txt (in any location).</td>
</tr>
</tbody>
</table>
### 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 Server 2008 + 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>
</tr>
<tr>
<td>%appdata%</td>
<td>C:\Users*\AppData\Roaming</td>
<td>C:\Documents and Settings* \Application Data</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>
</tbody>
</table>

**Note**

Does not work for real-time scanning.

---

**Expression** | **Interpreted as** | **Description**
---|---|---
C: | C: | Exclude drive C: from scanning (including the drive’s master boot record).
C:\ | C:\ | Exclude all files on drive C: from scanning (but scan the drive’s master boot record).
C:\foo\ | C:\foo\ | All files and folders underneath C:\foo, including C:\foo itself.
C:\foo\*.txt | C:\foo\*.txt | All files or folders contained in C:\foo named *.txt
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.

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.

**Note**
If you specify exclusions on specific guest VMs (not on all guest VMs protected by the Sophos security VM), the restrictions are different. See Scanning Exclusions for Specific VMs (page 166).

**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 * (star) and ? as follows:

- You can use wildcards for specifying files, but not for folders.
- You must use * on its own to replace a filename (*.exe), an extension (file.*), or both (*.*). You can’t combine it with other characters (file*.com).
You can use ? to match an exact number of characters and you can combine it with other characters. For example, C:\f???.exe would exclude C:\foo.exe but not C:\fooo.exe.

If you use a wildcard that is invalid, the security VM ignores the exclusion.

### 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 “file”, with any extension, in all locations.</td>
</tr>
<tr>
<td>*.com</td>
<td>Excludes all files with a .com extension in all locations.</td>
</tr>
<tr>
<td>**</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>
Scanning Exclusions for Specific VMs

You can set up scanning exclusions for specific guest VMs that are protected by Sophos Security VM. To do this, you must include the guest VM name when you specify the item you want to exclude, as described below.

**Note**
You can only exclude folders and there must be a local path to the folder when you set up the exclusion.

**Note**
You cannot set up different exclusions for each type of scanning (real-time and scheduled). On guest VMs, exclusions always apply to both types.

To specify exclusions for a guest VM:
1. Go to **Server Protection > Policies** and select the policy that applies to your instance of Sophos Security VM.
2. Select **Scanning options for malware and risky file types**.
3. Click the drop-down arrow next to **Scanning Exclusions**.
4. In **Exclusion for**, select **File and folder (Virtual Server)**.
5. In **Value**, enter the details of the computer and the folder you want to exclude, as follows:
   - Place the guest VM name before the path for the folder you want to exclude. You can use wildcards in the guest VM name.
   - Put a pipe symbol, "|", before and after the guest VM name.
   - Include a backslash after the folder name.

   Example: |Window7_Computer1x64|c:\foo\  
6. Under **Activate for**, select **Real-time and scheduled scanning**.

**How to use wildcards**
You can use the wildcard * in the VM name to apply the exclusion to multiple guest VMs.
You cannot use wildcards in the folder name.
The wildcard is valid at the start or end of the VM name (or both). See examples below.

<table>
<thead>
<tr>
<th>Example</th>
<th>Where the exclusion applies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Window7*</td>
</tr>
<tr>
<td></td>
<td>x64</td>
</tr>
<tr>
<td></td>
<td><em>Computer</em></td>
</tr>
</tbody>
</table>
5.6.4 Server Peripheral Control Policy

Peripheral control lets you control access to peripherals and removable media. You can also exempt individual peripherals from that control.

To set it up:

• Create a Peripheral Control policy. See Create or Edit a Policy (page 228).
• 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.
**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.
5.6.5 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.

To set it up:

• Create an Application control policy. See Create or Edit a Policy (page 228).
• 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:
   • Select Detect controlled applications during scheduled and on-demand scans.
   • 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:
    • Find the applications you want to use and clear the checkbox next to them.
    • 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.

- Click **Save to List**.

11. In **Detection Options**:
- Select **Detect controlled applications when users access them**.
- 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.

### 5.6.6 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.

To set up a policy:
- Create a **Web Control** policy. See **Create or Edit a Policy** (page 228).
- 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:
Sophos Central Admin

- **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**

Select **Control sites tagged in Website Management** if you want to control access to websites that you have "tagged", i.e. put into your own categories, at the **System Settings > Website Management** page.

1. Click **Add New**.
2. Select your **Website Tag** and the **Action** you want to apply to the websites with that tag.

**5.6.7 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.

To set up a policy:

- Create a **Server Lockdown** policy. See **Create or Edit a Policy** (page 228).
- 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.
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**.

### 5.6.8 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 346). 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 226).

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 228).
• 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 an use existing rule or create a new rule, see [Create a Data Loss Prevention Rule](page 347). 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**.

### 5.6.9 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.

To set it up:
• Create a **Updating** policy. See [Create or Edit a Policy](page 228).
• 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 the next time they start.
5.7 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.

5.7.1 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 330). For full details of how it works, see About Active Directory synchronization (page 330). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 329).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 332). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 332).

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 the Sophos Central Admin console. It does not support two-way synchronization between the Sophos Central Admin console 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 the Sophos Central Admin console. 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 the Sophos Central Admin console.

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 332).

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**

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.
5.7.2 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 cannot…</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>
</tbody>
</table>
## Role Permissions

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role cannot...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</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.  
- Update the Sophos agent software on a computer.  
- Scan computers. | Manage roles and role assignments. In addition they cannot:  
- Assign policies.  
- Change settings. | 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 cannot:  
- 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 cannot:  
- 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. |

## 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 307).

**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.
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.

5.7.3 Tamper Protection

You can enable or disable tamper protection for all your servers and users' computers.

To do this, in Settings, open the Tamper Protection page.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer 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.

Note
You can change the settings for an individual device or server. Open its details page and select the Tamper Protection tab. There you can view the password, generate a new one, or temporarily disable tamper protection for that device.

5.7.4 API Token Management

You can generate and manage the API token used for secure access to the Security Information and Event Management (SIEM) Integration API. This enables you to pull new event and alert data from Sophos Central. For further information, click the 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.
5.7.5 Website Management

This page is not available if you do not have a Web Control or Web Gateway license.

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 on the **Policies** page.

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**.
5.7.6 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

Set the bandwidth used

In Settings, on the Bandwidth Usage page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.

This helps to ensure that updating does not cause computers to run slowly.

You can specify a custom bandwidth or unlimited bandwidth.

Note
This setting is for Windows computers only.

Note
This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos Manage Update Cache (page 341).

5.7.7 Manage Update Cache

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.

When you set up a cache on a server, Sophos Central does as follows:

• Installs Sophos caching software.
• Fetches updates from Sophos and puts them in a cache.
• Automatically configures Windows computers in your network to update from a cache.

Using caches doesn’t affect how often or when computers are updated.

Note
Workstations and servers can both update from a cache.

Note
Windows Vista or XP workstations cannot update from a cache.

Set up a cache

Before you set up a cache, ensure that:

• The server has at least 5GB free disk space.
• Port 8191 is available and accessible to computers that will update from the cache.

**Note**
The Update Cache installer will open port 8191 in Windows Firewall. When Update Cache is uninstalled, the port will be closed again.

To set up a cache:
1. In Settings, go to the Manage Update Cache 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. If you have already set up a cache on some servers, to hide them from view, select **Servers without Update Cache**.
3. Select the server or servers where you want to set up a cache.
4. Click **Set Up Cache**.

**Remove a cache**

When you remove a cache:
• Sophos Central uninstalls caching software, removes the cache of downloaded updates, and closes port 8191 in Windows Firewall.
• Computers currently updating from this server are automatically reconfigured to update from another update cache, if you have one.

If you remove all your caches, computers will update directly from Sophos.

To remove a cache:
1. Go to the System Settings > Manage Update Cache 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.
3. Select the server or servers you want to remove a cache from.
4. Click **Remove Cache**.

### 5.7.8 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 342]
• **Controlled Updates** [page 342]
• **Control Updates Manually** [page 343]
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 Updates.

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 Updates.

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 non-test computers 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.

### 5.7.9 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.

When you add an AWS account on this page, Sophos Central will do as follows:

- Display AWS instance details.
- Remove terminated AWS instances automatically.
- Let you apply server policies to Auto Scaling Groups.

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.

5.7.10 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 348).

• **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 347), 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.

You can also export custom rules, click 📄. This creates an xml file containing the rule definition.

Click ✗ to delete a rule and 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 349).

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.

### 5.7.11 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 346).

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 349).

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.](image)

For each custom CCL you can also:

- Click ![on the name of a CCL to edit it.](image)
- Click ![to export a CCL. This creates an XML file containing the definition for the CCL.](image)
- 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.](image)
- Click ![to delete a CCL and click **Delete item** to confirm deletion.](image)

You can also import Content Control Lists:

1. Click **Import**.
2. Select the XML file containing the CCLs.
3. Click **Open**.
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 edits, 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.
5.8 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.

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 on downloading Server Protection installers:
- Server Protection (page 356)
- Server Protection as a Web Service (page 357)
- Virtual Environment Protection (page 357)

5.8.1 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.

Note
For Linux computers, there is an alternative: Sophos Secure OS. See the Server Protection As A Web Service section.

When you protect a server:
- The server is added to the Servers list in Sophos Central.
- Default policies are applied to the server.
5.8.2 Server Protection as a Web Service

You can protect Linux computers with Sophos Secure OS.

Secure OS is a pre-built image of the CentOS Linux operating system and comes with Sophos Anti-Virus for Linux pre-installed.

You can get Secure OS from Amazon Web Services and then enable Sophos Central to manage it.

Set up Sophos Secure OS

Go to Server Protection > Protect Devices.

Under Server Protection as a Web Service, click Set up Sophos Secure OS and follow the instructions. Then register the Secure OS server with your Sophos Central account (click on the link to see the command you need).

5.8.3 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 all the guest VMs on that host.
• 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.

Note

You may also be able to download Sophos Anti-Virus for vShield. However, Sophos has announced this product’s retirement.

We recommend you read 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 the Sophos Guest VM Agent and checked it is connected, for each of your guest VMs.
6 Wireless

Use the wireless section of Sophos Central to configure and manage access points, the corresponding wireless networks, and the clients that use wireless access.

**Note**
When the lights on your access point blink rapidly, do not disconnect it from the power outlet! Rapidly blinking lights mean that a firmware flash is currently in progress. For example, a firmware flash takes place after a scheduled firmware update.

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 server is 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 any VLAN to be configured on the AP for this connection.
- Communication on ports 443, 123, 80 to any Internet server is possible.
- No HTTPS proxy on the communication path.

6.1 Wireless Dashboard

This page lets you see the most important Wireless information at a glance. You get information about:

- Access Points
- Alerts which require actions
- Clients
- Traffic generated by applications connected to access points

6.2 Wireless Alerts

There are the following types of 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 your installation (Are the access points well placed? Are there too few?).
**Medium**

- **Access Point is offline**
  The access point has either no connection to the Internet, no power or there is an error with the software. If it is the software, a reboot may help. Otherwise, you should connect to the SOS SSID to get further help [see SSIDs (page 200)].

- **Access Point is not broadcasting any network**
  There is currently no configuration on the AP. Configure the access point under Wireless > Access Points.

- **Access Point has high data packet retries**
  802.11 retries alert is triggered when the data frame retries on the AP goes beyond 20%. It helps you to understand if retries are the reason for a bad network service. WLAN frames are retried by the access point when the acknowledgement frames are not received from the intended recipient. If the retries go beyond the threshold, the overall performance of the network is shown.

- **Access Point command done**
  The reboot is done.

- **Access Point has a DNS timeout**
  DNS requests to the Internet are not answered. This is either caused by the Internet connection or by your network installation.

- **Access Point has high DNS latency**
  The feature triggers alert for high 802.11 retries & DNS delay. This is either caused by the Internet connection or by your network installation.
  - DNS latency alert is triggered if the DNS roundtrip time is above 250 ms.
  - 802.11 retries alert is triggered if the retry percentage is above 20% (conservative).

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

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

In those cases, as first step, reboot the access point. If this does not help, 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**
6.3 Clients

This page provides an overview of currently connected clients and their connectivity.

Client Details

When you click on a client, you can see detailed information.

6.4 Traffic Usage

On this page you can view the traffic on your clients broken down by category, 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 Traffic categorization option in Settings (page 212).

6.5 Access Points

A wireless access point (WAP) is a networking hardware device that allows a Wi-Fi device to connect to a wired network. Use these settings to manage all known access points. To use wireless security in Sophos Central you need to connect an access point to the Internet and register it on Sophos Central. Therefore you need the serial number, which is attached to the access point and its original package.

Note that the country setting of an AP regulates the available channels to be compliant with local law.

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. If you have any trouble with the connection, the access points SOS SSID can help you to fix it. For more information about SOS SSID, see SSIDs (page 200).

Note
For more information on access points, see the Operating Instructions in the Sophos Resource Center.
Register an Access Point

To register an access point, click **Register** in the upper right of the page. A wizard will guide you through the process.

The registration process can take up to 300 seconds. If the registration is successful the access point is displayed in the list.

### 6.5.1 Supported Access Points

All supported access points are listed here with some 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>
</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>
</tr>
<tr>
<td>AP 15C</td>
<td>802.11b/g/n</td>
<td>2.4/5 GHz dual-band/single-radio</td>
<td>2.4 GHz</td>
<td>Channels 1-11</td>
<td>Channels 1-13</td>
</tr>
<tr>
<td>AP 55</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, 100-116, 132-140, 149-165</td>
<td>Channels 1-13, 36-64, 100-116, 132-140</td>
</tr>
<tr>
<td>AP 55C</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, 36-48, 149-165</td>
<td>Channels 1-13, 36-64, 100-116, 132-140</td>
</tr>
<tr>
<td>AP 100</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, 36-48, 149-165</td>
<td>Channels 1-13, 36-64, 100-116, 132-140</td>
</tr>
<tr>
<td>AP 100C</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, 36-48, 149-165</td>
<td>Channels 1-13, 36-64, 100-116, 132-140</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>
</tr>
</thead>
<tbody>
<tr>
<td>AP 100X</td>
<td>802.11a/b/g/n/ac</td>
<td>2.4/5 GHz</td>
<td>2.4 GHz</td>
<td>Channels 1-11, 36-64, 100-116, 132-140</td>
<td>Channels 1-13, 100-116, 132-140</td>
</tr>
</tbody>
</table>

6.5.2 Access Point Details

On this page, you can see access point details and manage access points.

Settings

- **Name**: The default name of an access point is its serial number.
- **Band**: Depending on the access point, 2.4 GHz and 5GHz are available. Adapt them separately.
- **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 to minimize interference. Default: 100 %
- **Channel width**: The higher the channel width the more transmission channels. With more channels, more data can be transmitted, which results in faster wireless speed. If there are lots of neighbouring 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. This improves transmission quality and speed.
- **Dynamic Background Channel Selection**: The access point automatically changes the channel on a regular basis to optimize the network.
- **Enable Airtime Fairness**: The access points try to distribute the airtime for transmission equally to all clients according to their traffic needs.
We recommend that you activate this option if you have several devices connected to your network and/or offer public wireless. Disabling the option makes sense if you want to have better performance on a slower device.

Assign SSIDs

You can use this option to have separate SSIDs accessed 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 AP can have a maximum of eight SSIDs per band.

Tip

You can also add an AP to a network when you create an SSID.

Clients

These graphs show client data of the access point.

6.6 SSIDs

Use the SSID pages to configure and manage your Service Set Identifiers (SSIDs).

About SSIDs

An SSID is a unique identifier which is attached to the header of packets which are sent over a Wireless LAN. 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.

SOS SSID

When an access point is disconnected or not able to reach Sophos Central, the access point will use its wireless capability to create an SOS SSID. When you connect to the SOS SSID with any mobile device you receive information about the current state of an access point which can help you debug the connection issues to Sophos Central.

The SOS SSID is comprised of an open wireless network named “sos” and the access point’s MAC address. After you connected to the SOS SSID, open your web browser and navigate to http://debug.sophos. The SOS SSID debug page provides the technical support to fix the connection issue, for example:

- Serial number and mac address of the access points Ethernet interface
- Link status
- IP of the access points Ethernet interface
• Gateway, DNS server and their reachability
• Reachability of Sophos Central URLs

Note
The SOS SSID is available for a limited time frame of four minutes. After that, the access point reboots and the SOS SSID is available again after one or two minutes. When you are connected to an SOS SSID you have no access to the internet.

6.6.1 Basic Settings

Here you make the basic settings for your SSID.

SSID

Requirements: 1-32 printable characters, name must not begin/end with a space. SSIDs are case-sensitive.

Note
We recommend to use ASCII printable characters to avoid display errors on client devices.

Encryption Mode

We recommend WPA2 instead of WPA. When using an enterprise authentication method, you also need to configure a RADIUS Server for your local network.

Encryption Algorithm

The default algorithm is AES. It is recommended for security reasons.

Passphrase

Protects the SSID from unauthorized access. Requirements: 8-63 ASCII printable characters.

Frequency Band

The access points assigned to this SSID will transmit on the selected frequency band(s).

For VoIP communication, the 5 GHz frequency band should be preferred. It has higher performance, lower latency, and less interference.

Note
For more information on which access point types support the 5 GHz band, see Access Points (page 197).
**6.6.2 Assign Network to SSID**

Here you can assign one or more access points to your SSID. Each AP can have a maximum of eight SSIDs per band.

**Multiple Access Points**

Available and assigned access points.

**Add Access Points later**

Assign the APs later either through editing the SSID or the access point.

---

**6.6.3 Enable SSID**

Enable the SSID you just created.

**Enable SSID**

Deactivate if you do not want to enable the SSID immediately.

---

**6.6.4 Security**

Define settings which make your network more secure.

**Hidden SSID**

When hidden, the SSID is still available but users needs to know the name to connect directly. Even if an SSID is hidden, you can assign the SSID to an access point.

**Note**

This is not a security feature. You still need to protect hidden SSIDs.

**Client isolation**

Clients within the same radio are not allowed to communicate with one another. This could be useful, for example in a guest or hotspot network.

**MAC Filtering**

Provides minimal security by restricting MAC address connections.
• **Blocked List:** All MAC addresses are allowed except those you enter in the MAC addresses field.
• **Allowed List:** All MAC addresses are prohibited except those you enter in the MAC addresses field.

### 6.6.5 Client Connection

#### LAN

Bridges a wireless network into the network of an access point, that means that wireless clients share the same IP address range.

#### VLAN

Connects the access point with an existing VLAN Ethernet interface.

#### 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 goes as untagged if the RADIUS server does not provide VLAN and the default tag is 0.

**Note**

IPv6 is blocked in SSIDs with dynamic VLAN enabled as otherwise devices can end up with multiple IPv6 addresses and gateways from multiple VLANs.

### Enable Guest Network

A guest network provides an isolated network for the clients with some traffic restriction. APs can have one guest network at a given time. There are the following modes:

- **Bridge Mode** uses the DHCP server from the same subnet.

  It will filter all traffic and will only allow communication to the gateway, the DNS server, and external networks. Thus you can add a guest network to an environment without VLAN and still have an isolation. In contrast to NAT mode, the DHCP server is still in your network. By this, roaming between APs works flawlessly.

  **Note**

  By using VLAN for your guest network you can have a separate guest VLAN additional to the guest network.

- **NAT Mode** runs an on-board DHCP server on the access point, which provides local isolated IPs to the guest network clients and clients are unaware of the internal IP scheme.

  For client addressing in NAT mode, a DNS server is optional. If not given, the DNS server of the access point will be taken.
Comparing the modes, bridge mode has a higher throughput, NAT mode has more isolation.

**Creating a guest network**

Guest networks are networks which use the same access points as other networks but are configured to allow only access to the Internet. You can either use an existing SSID or create a new SSID to enable a guest network. This guide 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.</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>Filters all traffic and allows communication to the gateway, the DNS server and the external network. Thereby you can add a guest network to an environment without VLAN and still have an isolation. Roaming between APs works flawlessly.</td>
</tr>
<tr>
<td>NAT Mode</td>
<td>Isolates every guest network on each access point.</td>
</tr>
</tbody>
</table>

6. Save your settings.
7. Provide the passphrase to guest network clients.

**6.6.6 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.

**Scheduled**

Select the weekdays and timeframes for the network to be available.

**6.6.7 Quality of Service**

Optimize your network.
Multicast to unicast conversion

The access point converts multicast packets to unicast packets individually for each client based on the IGMP protocol. This approach is more powerful when few clients are connected to one access point.

Unicast is preferred to multicast in most scenarios where media is streamed as it can operate at higher rates.

Proxy ARP

When this function is activated, the AP can answer ARP queries for network addresses directly and the other clients do not need to take action.

Fast roaming

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 reboot. With this function, clients will still be able to connect to the access point and/or the Internet. If the keep broadcasting function is on, the access point proceeds working with its old configuration.

Note

The SSID will be broadcasted in every other case of connection loss to Sophos Central, regardless if this function is activated or not.

Band Steering

Band steering distributes clients based on the load of the two bands and the clients’ 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 AP, 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 AP level and will affect all SSIDs on that AP.

6.6.8 Captive Portal

Activate and configure a hotspot.
Landing page

Enable Hotspot

Turns the SSID into a hotspot. This allows cafés, hotels, companies, etc. to provide time- and traffic-restricted Internet access to guests.

**Attention**

In many countries, operating a public hotspot is subject to specific national laws, restricting access to websites of legally questionable content (e.g., file sharing sites, extremist websites, etc.).

Page Title

Title which is displayed on the landing page the user will see to accept the terms of service.

Welcome Text

Text you define and which is displayed on the landing page.

Authentication Types

**Terms of Service**

Users have to accept the Terms of Service defined here before authentication.

**Backend Authentication**

With this authentication type, users can authenticate via 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

A new password will be created automatically on a fixed schedule. If the schedule is set to weekly or monthly, you can also select a weekday or week. The former password will become invalid when the scheduled time is reached and current sessions will be cut off. The password will be sent as 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.

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.
6.6.9 About Captive Portals and Hotspots

The hotspot function turns the AP behind the SSID into a hotspot. This allows businesses (for example, cafés and hotels) to provide time- and traffic-restricted Internet access to guests.

Technically, the hotspot feature serves to restrict traffic which is basically allowed by the firewall. Therefore you have to 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**

Before creating a hotspot, you need to have an existing SSID, which then turns into a hotspot.

Creating a hotspot will generate a Wireless node which provides Internet connection and VPN access. Security is crucial when providing hotspots. Select the highest possible security precautions.

You can provide different types of hotspots.

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 200)
- [Basic Settings](page 201)

### 6.6.10 Mesh Networks

Using an AP as a mesh client with 5 GHz effectively reduces the maximum throughput by 50% per hop, because all data sent to the AP needs to be forwarded to the other AP, taking up additional airtime. Therefore we recommend to set the root AP to 5 GHz and the clients to 2.4 GHz.

When an AP boots which is configured to use the mesh network, it tries to connect via cable to Sophos Central. If this does not work, it turns into a repeater AP and scans if the mesh network is visible. If yes, it will join the mesh network as a client. The access points realize by themselves if they are root, repeater (mesh) or bridge access points in the network.

**Deployment possibilities**

Mesh mode enables you to have multiple access points where one is the root AP and the others are repeater APs, called mesh APs. There can be multiple root APs. Mesh APs can broadcast the SSID from the root AP to cover a larger area without cabling each AP.

A mesh network can also be used to bridge Ethernet networks without laying cables. To run a wireless bridge you have to plug 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:

• At least one access point needs a LAN connection.
• Mesh access points need to be on the same channel to make a communication possible.
• Avoid using dynamic channel selection as after a reboot the channels of the APs may differ.
• The mesh network may need up to five minutes to be available after configuration.
• You can have only one mesh SSID.
• There is no automatic takeover of the root AP. The decision to connect to mesh happens during the boot.
• A mesh network can be realized only with Sophos access points.
• For setting up a mesh network you need to create a new SSID.

Create a Mesh Network

Creating a mesh network will generate a WPA2-Personal network with a randomly generated passphrase which will be automatically 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 APs are connected to an SSID.
4. Set the same channel on all APs to the 5 GHz band or set Autochannel.

Note
We recommend to statically set a non-DFS channel, as a channel change which can occur with DFS will interrupt the 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 the name for the SSID.
b) Select a frequency band.

**Note**
We recommend to use the 5 GHz band when the APs are close enough for a good 5 GHz signal as the throughput is higher. For longer distances between the APs 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 **Advanced Settings > Mesh** 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 AP 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 AP and a visible SSID on the repeater AP. 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 APs are on the same channel.
- Ensure that APs which are not part of the mesh network are on a different channel.

There are not all APs in the mesh network:
- Ensure that all APs got the configuration (had been connected via LAN until all configurations were saved and the AP was restarted)
- Ensure that the LAN cable of the repeater APs is unplugged.

**Related concepts**

Access Point Details (page 199)
Basic Settings (page 201)
6.7 Sites

Organize your sites on Google Maps and group the access points to the sites.

Neighborhood SSIDs

The neighborhood SSIDs tab shows every network within the range of the access points of the selected site. This includes also networks which are not provided from Sophos Central. Every neighborhood SSID is classified:

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sanctioned</td>
<td>AP that belongs to your network.</td>
</tr>
<tr>
<td>Unsanctioned</td>
<td>AP that does not belong to your network.</td>
</tr>
<tr>
<td>Rogue</td>
<td>Unsanctioned AP that is connected to your secured wired network.</td>
</tr>
<tr>
<td>SSID Impersonate</td>
<td>AP that spoofs the network name of an access point that belongs to you.</td>
</tr>
<tr>
<td>BSSID Impersonate</td>
<td>AP that spoofs the hardware address of an access point that belongs to you.</td>
</tr>
<tr>
<td>Evil Twin</td>
<td>AP that spoofs the network name and the hardware address of the access point that belongs to you.</td>
</tr>
<tr>
<td>Advanced AP Impersonate</td>
<td>AP that spoofs the network name and unique protection code of the access point that belongs to you.</td>
</tr>
</tbody>
</table>

Every access point scans for neighborhood SSIDs once during the booting process. For example, when you reboot 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 the neighborhood SSIDs, you must switch on Rogue AP detection in the Settings (page 212).

Floorplans

Use floorplans to set detailed locations for access points. Upload a floorplan as an image file (PDF, PNG, JPEG, BMP, GIF or WBMP) and position the APs.

6.7.1 Create a Site

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 AP can be added to one site only.

4. Save your settings.

### 6.7.2 Create a Floorplan

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.

### 6.8 Settings

The Settings pages are used to specify security settings that apply to 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.
6.8.1 Firmware Settings

On this page you can manage the firmware settings for Sophos Central wireless.

Firmware update

You can schedule firmware updates by selecting the frequency and time.

Diagnostics

- **Forward access point logs**: If enabled, your access point logs will be forwarded to Sophos technical support.
- **Remote Login to Access Points for Sophos Support**: If enabled, Sophos technical support will have remote access for the given time. The remaining time is displayed. Deactivate to disable remote access immediately.

Analysis

If the traffic categorization is enabled, the traffic generated by the user will be categorized and listed in Traffic Usage (page 197). This option is enabled by default.

Rogue access point detection

If enabled, every network within the range of an access point is listed as neighborhood SSID in Sites (page 211).
7 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 353).

7.1 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.

Messages

Messages shows the number of email messages processed by Email Security for your protected mailboxes for the last 30 days. It also shows the number of spam and malware messages detected.
Click See Report to open the Messages report and review the details of the processed messages, see Messages Report (page 301).

7.2 Message History Report

This option is only available if your license includes Sophos Email.
The Message History report details the email messages processed by Email Security for your protected mailboxes.
Search: If you want to view email messages with a particular subject line or the messages associated with a sender or recipient, enter the subject, sender or recipient in the search box.
Date range: Use the From and To fields to select the time period for which you want to view the message processing history. You can view email that has been processed in the past 14 days or less. By default the report displays the messages that have been processed during the current day.
You can filter the messages by their Status.
Update Report: Click this to refresh the report if you have changed the date range, entered a search term or filtered the messages.

For each message the report shows:
• Status: Indicates whether it is spam or whether it has been successfully delivered.
  — Success: Message was successfully delivered.
  — Quarantined: Message was marked as spam due to its content or your block list configuration.
  — Deleted: Message was deleted due to its content or your block list configuration.
Note

Whether a message is quarantined or deleted depends on the spam protection settings you have chosen, see Email Security Policy (page 229).

- Date: Date and time the message was processed.
- From: The sender of the message.
- To: The recipient(s) of the message
- Subject: Subject line from the message.

### 7.3 Messages Report

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

The Messages report details the email messages processed by Email Security for your protected mailboxes.

**Date range**: 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.

**Messages**: All scanned messages are shown in the report by default. Use this filter to change the type of message displayed in the report. Choose from:

- Scanned: All messages processed by Email Security.
- Legitimate: All messages that are not spam or malware.
- Spam: All messages that have been classified as spam.
- Malware: All messages that have been classified as containing malware content.

**Graph**: The graph shows you at a glance the number of messages that were processed per day. It reflects the message type selected in the Messages filter.

**Update**: Click this to refresh the report if you changed the type of message in the Messages filter.

**Message table**

The message table shows the number of email messages processed for each date listed. It reflects the message type selected in the Messages filter and the selected Date range.

### 7.4 People

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

#### 7.4.1 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 details including:

- 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 address.
- Role. This shows what administration role, if any, the user has, see Administration Roles (page 333).
  
  This column is only visible if you are an administrator.

To see full details for a user, click on the user’s name. For more information, see User Summary (page 307).
To display different types of user, click the drop-down arrow on the filter above the list.

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 333).

   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.
**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. 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 330).

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 307).

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 333).

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.

**Related concepts**

[Active Directory Sync](#) (page 329)

**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.
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 333).

   **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.

   **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.

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 226).

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.
For each 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 (such as blocked websites or
policy non-compliance) detected on the user’s devices.
You can customize the list by selecting the start and finish dates.
The list shows:
• A description of the event.
• The time and date when the event occurred.
• An icon that indicates the importance of the event.
• The device associated with the event.
To see the events arranged by type, as well as a graph showing events day by day, click View Events
Report.

Key to the icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>⚠</td>
<td>Warning.</td>
</tr>
<tr>
<td>⚠</td>
<td>Action required.</td>
</tr>
<tr>
<td>i</td>
<td>For information only.</td>
</tr>
</tbody>
</table>

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.
7.4.2 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 312).

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 312).

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.

7.5 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 353).

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 225).

7.5.1 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.

### 7.6 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 also release or delete a message in the Message Details dialog.

**Related concepts**
Set up Email Security [page 353]

### 7.7 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.

#### 7.7.1 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.

7.7.2 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.

7.7.3 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 353).

• Edit the Email Security policy. See Create or Edit a Policy (page 228).

   Important
   You can only have one Email Security policy. This is the base policy and applies to all protected mailboxes. You must review the settings to check that they are appropriate.

• 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 226).

Content 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 Confirmed Spam.

You can set the strength of the spam filters. You can use pre-set spam filtering or customize the spam filter settings.

To set the strength of the spam filters:
1. Click on Set spam filter strength with and choose between Pre-set Settings and Custom Settings.
2. Set the options for your chosen spam filter [as described below].

Pre-set Settings

The spam score at which a message is rated as Confirmed Spam varies with the strength of the spam filter. You can choose to automatically delete the Confirmed Spam messages. If you do not choose to delete them these messages are quarantined. Confirmed Spam messages are quarantined by default.

Messages with moderate to high spam scores are quarantined. The spam score at which messages are quarantined varies with the strength of the spam filter.

Users can manage their quarantined messages using the Sophos Self Service Portal.
1. Select a preset spam filter threshold by sliding the control.
2. Choose from:
   • Highest: This is the strictest filter setting. Messages with a low spam score are delivered. Confirmed Spam messages with higher spam scores are quarantined or deleted. The remaining messages are quarantined.

   **Note**
   The filter is set to Highest by default.

   • Higher: This is the moderate filter setting. Messages with a moderate or low spam score are delivered. Confirmed Spam messages with the highest spam scores are quarantined or deleted. The remaining messages are quarantined.

   • High: This is the most lenient filter setting. Messages with a moderate or low spam score are delivered. The remaining messages are quarantined. No messages are deleted.
3. Choose whether you want to delete or quarantine Confirmed Spam messages by selecting the appropriate option in the Confirmed Spam Handling drop-down list.

Custom Settings

Messages are categorized based on their spam score and you can choose how the categories are processed. Messages are split into:

• Confirmed Spam: These are messages that conform to known and verified spam patterns. By default these messages are quarantined.

• Bulk: These are messages that are dubious mass mailings. By default these messages are delivered.

• Suspected Spam: These are messages that have been identified as suspicious. By default these messages are quarantined.

• Non-Spam: These are messages that are confirmed to come from a trusted source and or contain no spam characteristics. By default these messages are delivered.

1. For each category choose an Action from:

   • Quarantine
   • Deliver
   • Delete
Enhanced Email Malware Scan

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.

**Note**
This option may result in some clean email being blocked.

Sender Policy Framework

This is an email validation check. It 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.

You can override the validation check by adding domains and email addresses to the **Allow** list.

Spoofing Protection

A spoofed message is where the From address and the Sender address do not match. These messages are commonly used to initiate phishing attacks. You can control what happens to spoofed messages.

**Note**
Spoofed messages that have been separately identified as spam messages are treated as spam messages. These means that they are deleted or quarantined depending on your **Content Filtering** settings.

Select from:

- **Quarantined**: Message is quarantined. This is the default option.
- **Tagged**: Email Security adds a tag to the message's subject line indicating that it is a spoofed message. The default value is SPOOF.

**Note**
Tagged messages are delivered.

- **Deleted**: Message is deleted.

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. Click **Save**.

### 7.8 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.

### 7.8.1 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 330). For full details of how it works, see *About Active Directory synchronization* (page 330). Once you have set up synchronization you can review its status and other settings, see *Active Directory Sync Status* (page 329).

For instructions on configuring Azure Active Directory synchronization, see *Set up synchronization with Azure Active Directory* (page 332). Once you have set up synchronization you can review its status and other settings, see *Azure AD Sync Status* (page 332).
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 the Sophos Central Admin console. It does not support two-way synchronization between the Sophos Central Admin console 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 the Sophos Central Admin console. 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 the Sophos Central Admin console.

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 332).

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

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.

### 7.8.2 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.
The available administration roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role cannot...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Super Admin</strong></td>
<td>Have access to everything in Sophos Central. In addition they can:</td>
<td>There are no limitations.</td>
<td>None.</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><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 cannot:</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.</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></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scan computers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Read-only</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 cannot:</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 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>
</tbody>
</table>

Anyone with a **User** role only has access to the Self Service Portal.
## 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 307).

**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.

<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role cannot...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td>Have no administration capabilities.</td>
<td>Manage roles and role assignments. In addition they cannot:</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>

### 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.
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.

### 7.8.3 Allow/Block Domains and Addresses

The **Allow/Block** list is part of Email Security and 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 353).
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 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.

In Settings, on the Email Security > 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 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 use the most recent option you chose.

5. Click OK.

   The allowed email address or domain is added to the 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 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 use the most recent option you chose.

5. Click OK.

   The blocked email address or domain is added to the 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 **Allow/Block** list.
3. Click **Yes** to confirm deletion.

### 7.8.4 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 353).

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.

### 7.8.5 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 [Set up Email Security](#) (page 353).

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 the Office 365 link.
   d) Use the information to help you configure your email domain.

2. In the **Email Domain** text field enter your email domain. Example: `example.com`
Domain ownership must be verified before mail will be delivered through Sophos Central. To verify domain ownership, you need to add a TXT record to your domain. Adding this record will not affect your email or other services.

3. Click **Verify Domain Ownership**.

4. Use the details given in **Verify Domain Ownership** to add the TXT record to your Domain Name Server (DNS).

   **Note**
   This can take up to 10 minutes to propagate.

5. Click **Verify**.

   **Note**
   You cannot save an unverified domain. You must correct any issues with the domain ownership verification.

6. 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`.

7. In the **Port** text field enter the port information for your email domain.

8. 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.

9. Click **Save** to validate your settings.

10. Click the Base Policy link to configure spam protection, see **Email Security Policy** (page 229).

    **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.

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 224).

2. Add your protected email domains, see Settings (page 232).
3. Configure spam protection in the email security policy, see Email Security Policy (page 229).
4. Set up global controls on spam using allow and block lists for senders, see Allow/Block Domains and Addresses (page 350).

   **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 330).
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 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.

4. Click **Continue**.

5. Add your email domains, see **Settings** (page 232).
8 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.

8.1 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.
8.2 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.

8.3 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.

8.4 People

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

8.4.1 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 details including:

- **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 address.**

- **Role.** This shows what administration role, if any, the user has, see Administration Roles (page 333).
  
  This column is only visible if you are an administrator.

To see full details for a user, click on the user’s name. For more information, see User Summary (page 307).

To display different types of user, click the drop-down arrow on the filter above the list.

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 333).

   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. 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 330).

**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 307).

---

**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 333).

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.

Related concepts
Active Directory Sync (page 329)

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 333).

   **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.

   **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.

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 226).

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.
For each 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 (such as blocked websites or policy non-compliance) detected on the user’s devices.
You can customize the list by selecting the start and finish dates.
The list shows:
- A description of the event.
- The time and date when the event occurred.
- An icon that indicates the importance of the event.
- The device associated with the event.
To see the events arranged by type, as well as a graph showing events day by day, click View Events Report.

Key to the icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>⚠</td>
<td>Warning.</td>
</tr>
<tr>
<td>🚨</td>
<td>Action required.</td>
</tr>
<tr>
<td>📘</td>
<td>For information only.</td>
</tr>
</tbody>
</table>

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.

8.4.2 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 312).

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 312).

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.

8.5 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.
- Delete computers.
- Install or uninstall software.
- Recover PIN/Password for encrypted computers (if you are using Sophos Device Encryption).

View computer details

The computers are listed with details of the operating system, the last user, the last time they were used, and the security and compliance status of the device.

The security status is indicated by an icon, as follows:

- 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.
To search for a computer, enter the name in the search field above the list.
To display different types of computer, click the drop-down arrow on the filter above the list.
You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

Delete computers

You can delete computers that you no longer need to manage from Sophos Central.
Select the computer or computers you want to delete and click **Delete** (in the upper right of the page).
This deletes the computer from the Sophos Central Admin console. It does not uninstall the Sophos agent software, but the computer will not get updates any more.

**Note**
If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

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.

Retrieve recovery key (Windows computers)

If users are unable to log in to their encrypted computer, you can get a recovery password which used to unlock the computer. There is a recovery key (password) 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 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, you need to find the recovery key identifier for the computer 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.
3. In Sophos Central, go to Computers and click the Retrieve Recovery Key button.
4. Enter the recovery identifier provided by the user and display the recovery key.

Note
If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

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.

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 computer can be unlocked. 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, they can use a recovery key to regain access to their data.

To get the recovery key, you need to find the recovery key identifier for the computer 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.
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 the recovery identifier provided by the user and display the recovery key.

Note
The recovery key ID is displayed for a short time. To display it again, users must restart their computer.

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.

Note
If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

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.

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. They can use it to access the computer and create a new password. Once they have created a new password they can access their computer again.

Note
You can recover access to encrypted non-startup volumes on Mac, see Sophos Central Device Encryption administrator guide.

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.

### 8.5.1 Computer Summary

The Summary tab in a computer’s details page lets you see the following:

- Security status of the computer.
- Recent events on the computer.
- Endpoint Agent summary. This agent provides threat protection and more.
- Device Encryption summary. This is not displayed if the encryption policy has been disabled.
- Web Gateway summary (if you have Sophos Web Gateway). This agent provides advanced protection against risky or inappropriate web browsing.
- Tamper protection settings.
• Update cache status. This is not displayed if a cache has not been set up.

Security status

In the left-hand pane, you can see details of the security status.

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

**Status**

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.

**Delete**
The **Delete** option deletes the computer from the Sophos Central Admin console. This does not uninstall the Sophos agent software, but the computer will not get updates any more.

**Tip**
If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

**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:

- Endpoint Agent (for threat protection and more).
- Web Gateway Agent (advanced web protection).

**Endpoint Agent Summary**

The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.

The summary shows the last activity on the endpoint. It also shows whether the endpoint agent is up to date.

If you need to take action, buttons are displayed:

- **Update**: Updates the Sophos agent software on the computer.
- **Scan Now**: Scans the computer 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 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.

Device Encryption summary

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers.

This summary shows the encryption status and type of authentication used (or "Protector" in BitLocker terms) for each volume.

Retrieve recovery key

You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their PIN or passphrase or lose the USB drive they use to log on.

1. Click Retrieve next to the volume. This displays the recovery key ID and latest recovery key.
2. 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.

3. Give the recovery key to the user.

The computer can be unlocked. 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.

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 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.

This shows that a cache has been set up for the computer. It shows which server is being used.

8.5.2 Computer Events

The Events tab in a computer’s details page displays events (such as blocked websites or policy non-compliance) detected on the computer.

You can customize the list by selecting the start and finish dates.

The list shows:

• A description of the event.
• The time and date when the event occurred.
• An icon that indicates the importance of the event. See the Key to the icons.
• An icon that indicates which Sophos agent reported the event. See the Key to the icons.

To see the events arranged by type, as well as a graph showing events day by day, click View Events Report.

Key to the icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>⚠</td>
<td>Warning.</td>
</tr>
<tr>
<td>⚠</td>
<td>Action required.</td>
</tr>
<tr>
<td>📷</td>
<td>For information only.</td>
</tr>
<tr>
<td>🔍</td>
<td>Endpoint Agent event.</td>
</tr>
<tr>
<td>🔍</td>
<td>Gateway Agent event.</td>
</tr>
</tbody>
</table>

8.5.3 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 283).

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).

8.5.4 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.

8.6 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.

8.6.1 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.

8.6.2 Create or Edit a Policy

You can create or edit a policy as follows.

Create a policy

1. If you have more than one Sophos product, select the one where you want to create a policy.

   Note
   You can’t create policies from the Overview pages.

2. Go to the Policies page.
3. Click Add Policy (in the upper right).
4. If you see an **Add Policy** dialog, select:
   • The feature you want.
   • The policy type (applies only to Endpoint Protection).
5. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users or devices.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.

**Edit a policy**

1. If you have more than one Sophos product, select the one where you want to edit a policy.

   **Note**
   You can't edit policies from the *Overview* pages.

2. Go to the **Policies** page.
   You see a list of policy types.
3. Click on the policy type to open a list of policies.
4. Find the policy you want to edit and click it.
5. On the policy details page, use the tabs to:
   • Assign the policy. For example, assign it to specific users or devices.
   • Enter settings for the policy. See the Help topic for that policy type.
   • Enable or disable the policy.

**8.6.3 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 228).
• 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:
**Sophos Central Admin**

- **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).

8.7 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.

8.7.1 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 330). For full details of how it works, see About Active Directory synchronization (page 330). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 329).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 332). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 332).

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 the Sophos Central Admin console. It does not support two-way synchronization between the Sophos Central Admin console 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 the Sophos Central Admin console. 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 the Sophos Central Admin console.

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 332).
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

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.

8.7.2 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 cannot...</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>
</tbody>
</table>
### 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 307).

**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.
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.

8.7.3 Tamper Protection

You can enable or disable tamper protection for all your servers and users' computers.

To do this, in Settings, open the Tamper Protection page.

When tamper protection is enabled, a local administrator cannot make any of the following changes on their computer 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.

Note
You can change the settings for an individual device or server. Open its details page and select the Tamper Protection tab. There you can view the password, generate a new one, or temporarily disable tamper protection for that device.

8.7.4 API Token Management

You can generate and manage the API token used for secure access to the Security Information and Event Management (SIEM) Integration API. This enables you to pull new event and alert data from Sophos Central. For further information, click the 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.
8.7.5 Website Management

This page is not available if you do not have a Web Control or Web Gateway license.

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 on the Policies page.
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**.
8.7.6 Global Scanning Exclusions

You can exclude files, websites and applications from scanning for threats. You can also exclude applications from detected exploits.

For example, you might exclude activity by some commonly-used applications to reduce the impact of scanning on performance.

You can do this in Settings, on the Global Scanning 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 scanning exclusions in the policies instead.

1. On the Global Scanning Exclusions page, click Add Exclusion (on the right of the page). The Add Scanning 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 detected exploit).
3. Specify the item or items you want to exclude. The following rules apply:
   - **File or folder (Windows).** You can exclude a drive, folder or file by full path. For file title or extension the wildcard * may be used, though *.* 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 of exclusions for Windows servers, see Scanning exclusions (page 159).
   - **File or folder (Mac/Linux).** You can exclude a folder or file. You can use the wildcards ? and *.
   
   Examples:
   - `/Volumes/excluded` *(Mac)*
   - `/mnt/hgfs/excluded` *(Linux)*
   - **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 164).
   - **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 11111111.11111111.11111111.00000000. 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’s been detected. Sophos Central will no longer detect it for the affected application. Sophos Central will also no longer block the affected application.

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**.

### 8.7.7 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 Cache (page 341).
8.7.8 Manage Update Cache

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.

When you set up a cache on a server, Sophos Central does as follows:
- Installs Sophos caching software.
- Fetches updates from Sophos and puts them in a cache.
- Automatically configures Windows computers in your network to update from a cache.

Using caches doesn't affect how often or when computers are updated.

**Note**
Workstations and servers can both update from a cache.

**Note**
Windows Vista or XP workstations cannot update from a cache.

Set up a cache

Before you set up a cache, ensure that:
- The server has at least 5GB free disk space.
- Port 8191 is available and accessible to computers that will update from the cache.

**Note**
The Update Cache installer will open port 8191 in Windows Firewall. When Update Cache is uninstalled, the port will be closed again.

To set up a cache:
1. In Settings, go to the Manage Update Cache 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. If you have already set up a cache on some servers, to hide them from view, select Servers without Update Cache.
3. Select the server or servers where you want to set up a cache.
4. Click Set Up Cache.

Remove a cache

When you remove a cache:
- Sophos Central uninstalls caching software, removes the cache of downloaded updates, and closes port 8191 in Windows Firewall.
• Computers currently updating from this server are automatically reconfigured to update from another update cache, if you have one.

If you remove all your caches, computers will update directly from Sophos.

To remove a cache:
1. Go to the System Settings > Manage Update Cache 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.
3. Select the server or servers you want to remove a cache from.
4. Click Remove Cache.

8.8 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.

8.8.1 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.
9 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.

9.1 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.

Messages

Messages shows the number of email messages processed by Email Security for your protected mailboxes for the last 30 days. It also shows the number of spam and malware messages detected.

Click See Report to open the Messages report and review the details of the processed messages, see Messages Report (page 301).

Web Stats

Web Stats 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.

9.2 Alerts

The Alerts page lists all the alerts that require your action.
Alerts that are resolved automatically by Sophos Central are not displayed. For example, if malware is detected and then cleaned up automatically, no alert is displayed. If you want to view all events on your devices, go to the Logs & Reports > Events page.

Alerts

For each alert, the list shows the event that caused the alert, when it occurred, and which user and device are affected.
The list also shows the severity of alerts:

⚠️ Orange warning sign for medium-priority alerts.
⚠️ Red warning sign for high-priority alerts.
For information about the different types of alerts, see the other Help pages in this section.
The alert event time is not updated if the same event occurs repeatedly.

Actions on alerts

There is a checkbox next to each alert. When you select one or more checkboxes, you can apply certain actions on alerts. The action buttons are displayed in the upper right of the page.
The following actions may be available, 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.
9.2.1 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.

9.2.2 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.

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 283).

- 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.

9.2.3 Email Alerts

Sophos Central automatically sends email alerts to administrators when events occur (for example, "Potentially Unwanted Application detected").

Sophos Central does as follows:

• Sends alerts for Medium or High severity events that require action. For details of events in these categories, see Alerts (page 283).
• Sends alerts to all administrators. To see details of administrators, go to System Settings > Role Management.
• Does not send alerts if an alert for the same type of event has been sent within the previous 24 hours.

You cannot change the email alert settings.
9.2.4 Wireless Alerts

There are the following types of 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 your installation (Are the access points well placed? Are there too few?).

Medium

- **Access Point is offline**
  The access point has either no connection to the Internet, no power or there is an error with the software. If it is the software, a reboot may help. Otherwise, you should connect to the SOS SSID to get further help (see SSIDs (page 200)).
- **Access Point is not broadcasting any network**
  There is currently no configuration on the AP. Configure the access point under Wireless > Access Points.
- **Access Point has high data packet retries**
  802.11 retries alert is triggered when the data frame retries on the AP goes beyond 20%. It helps you to understand if retries are the reason for a bad network service. WLAN frames are retried by the access point when the acknowledgement frames are not received from the intended recipient. If the retries go beyond the threshold, the overall performance of the network is shown.
- **Access Point command done**
  The reboot is done.
- **Access Point has a DNS timeout**
  DNS requests to the Internet are not answered. This is either caused by the Internet connection or by your network installation.
- **Access Point has high DNS latency**
  The feature triggers alert for high 802.11 retries & DNS delay. This is either caused by the Internet connection or by your network installation.
  - DNS latency alert is triggered if the DNS roundtrip time is above 250 ms.
  - 802.11 retries alert is triggered if the retry percentage is above 20% (conservative).

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

- **Access Point configuration failed**
- **Access Point(s) failed to update to the new firmware**
  In those cases, as first step, reboot the access point. If this does not help, call Sophos Support. They will need remote access to investigate the issue (Wireless > Settings > Remote Login to Access Points for Sophos Support).
9.3 Logs & Reports

The Logs & Reports pages provide detailed reports on the security features in Sophos Central. To find out what logs are available, see Logs (page 289). To find out how reports work and how you can customize them, see Reports (page 302).

9.3.1 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 289).

**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 300).

**Data Loss Prevention Events Log.** All events triggered by data loss prevention rules for computers or servers, see Data Loss Prevention Events Log (page 301).

**Message History.** The email messages processed by Email Security for your protected mailboxes, see Message History Report (page 303).

**Gateway Activity Logs.** All the network activity logs associated with your Web Gateway protection, see Gateway Activity (page 302).

Events Report

The Events Report page provides information about all events on your devices. For information about the different types of event, see Event types (page 290).

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

**Note**

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).

You can find the following features and information on the Events page:
**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.

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

**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:

- **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 283).

After you have taken an action or ignored the alert, it is no longer displayed on the Alerts page, but the event remains in the Events list.
## Runtime detections

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running malware detected</td>
<td>Medium</td>
<td>No</td>
<td>A program that was running on a computer and exhibited malicious or suspicious behavior has been detected. Sophos Central will attempt to remove the threat. If it succeeds, no alerts will be displayed on the Alerts page, and a “Running malware cleaned up” event will be added to the Events list.</td>
</tr>
</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. |
| 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. |
## Event type

<table>
<thead>
<tr>
<th>Event type</th>
<th>Severity</th>
<th>Action required?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 unauthorised 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></td>
</tr>
</tbody>
</table>
## Controlled application allowed

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

<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 “Malware cleaned up” 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. |
| Malware cleaned up       | Low      | No               | 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. |
| Recurring infection      | High     | Yes              | 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. |
| Threat removed           | Low      | No               |              |
### Malware alert locally cleared

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

<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>

**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>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>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>
<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>
</tbody>
</table>

**Firewall**

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

Note
This occurs only if you change your reputation checking settings to “Log only”.

Copyright © 2017 Sophos Limited
### Event type

<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 the Sophos Firewall but is still sending network traffic. The computer may be compromised. The Sophos 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 the Sophos 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>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>Disk not encrypted</td>
<td>Medium</td>
<td>See Note</td>
<td>The client 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.</td>
</tr>
<tr>
<td>The Device Encryption status changed from Encrypted to Unmanaged</td>
<td>Low</td>
<td>See Note</td>
<td>Encryption on this computer is no longer managed by Sophos Central. This can happen because a policy is disabled or removed, or because encryption is disabled in the policy. Recovery is still possible at the computer’s details page if recovery keys are available.</td>
</tr>
<tr>
<td>Recovery key missing</td>
<td>Medium</td>
<td>See Note</td>
<td>A recovery key for an encrypted volume cannot be found in the Sophos Central database.</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>
</tbody>
</table>
Event type | Description
---|---
A “block file transfer” action was taken | A transfer of a file containing controlled information was blocked.

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 in the last 365 days.

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 logged on.
• **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 Admin 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 Admin 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, the last 90 days or the last 365 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.
   - **CSV of past 365 days** or **PDF of past 365 days**: Exports activities from the past 365 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.

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.

### Messages Report

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

**Date range**: 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.

**Messages**: All scanned messages are shown in the report by default. Use this filter to change the type of message displayed in the report. Choose from:

- **Scanned**: All messages processed by Email Security.
- **Legitimate**: All messages that are not spam or malware.
- **Spam**: All messages that have been classified as spam.
- **Malware**: All messages that have been classified as containing malware content.

**Graph**: The graph shows you at a glance the number of messages that were processed per day. It reflects the message type selected in the **Messages** filter.

**Update**: Click this to refresh the report if you changed the type of message in the **Messages** filter.

**Message table**

The message table shows the number of email messages processed for each date listed. It reflects the message type selected in the **Messages** filter and the selected **Date range**.

**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.

### 9.3.2 Reports

The reports that you can see depend on your license.

If you're new to reports, read this page to find out how reports work.

You can customise the information displayed in the report pages by using filters and limiting the time range for the displayed data.
How do I 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.

How do I 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.

How do I 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.

Message History Report

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

The Message History report details the email messages processed by Email Security for your protected mailboxes.

Search: If you want to view email messages with a particular subject line or the messages associated with a sender or recipient, enter the subject, sender or recipient in the search box. Date range: Use the From and To fields to select the time period for which you want to view the message processing history. You can view email that has been processed in the past 14 days or less. By default the report displays the messages that have been processed during the current day. You can filter the messages by their Status. Update Report: Click this to refresh the report if you have changed the date range, entered a search term or filtered the messages.

For each message the report shows:

- Status: Indicates whether it is spam or whether it has been successfully delivered.
  - Success: Message was successfully delivered.
  - Quarantined: Message was marked as spam due to its content or your block list configuration.
  - Deleted: Message was deleted due to its content or your block list configuration.
Note
Whether a message is quarantined or deleted depends on the spam protection settings you have chosen, see Email Security Policy (page 229).

• Date: Date and time the message was processed.
• From: The sender of the message.
• To: The recipient(s) of the message
• Subject: Subject line from the message.

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.

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 details including:
• 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.
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 333).

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. 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 330).
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 307).

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 333).

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.

Related concepts

Active Directory Sync (page 329)

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.
Sophos Central Admin

- 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 333).
**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.

**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.

**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 226).

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.
For each 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 (such as blocked websites or policy non-compliance) detected on the user’s devices.

You can customize the list by selecting the start and finish dates.

The list shows:

- A description of the event.
- The time and date when the event occurred.
- An icon that indicates the importance of the event.
- The device associated with the event.

To see the events arranged by type, as well as a graph showing events day by day, click **View Events Report**.

#### Key to the icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Checkmark]</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>![Warning]</td>
<td>Warning.</td>
</tr>
<tr>
<td>![Exclamation]</td>
<td>Action required.</td>
</tr>
<tr>
<td>![Information]</td>
<td>For information only.</td>
</tr>
</tbody>
</table>

### 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 312).

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 312).

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 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.

9.5.1 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.
- Delete computers.
- Install or uninstall software.
- Recover PIN/Password for encrypted computers (if you are using Sophos Device Encryption).

**View computer details**

The computers are listed with details of the operating system, the last user, the last time they were used, and the security and compliance status of the device.

The security status is indicated by an icon, as follows:

- Green check mark if there are low-priority alerts or no alerts.
- Orange warning sign if there are medium-priority alerts.
Sophos Central Admin

Red warning sign if there are high-priority alerts.

To search for a computer, enter the name in the search field above the list.
To display different types of computer, click the drop-down arrow on the filter above the list.
You can click on a computer name to see more details of that computer, to take action against the alerts, or to update, scan or delete the computer.

Delete computers

You can delete computers that you no longer need to manage from Sophos Central.
Select the computer or computers you want to delete and click Delete (in the upper right of the page).
This deletes the computer from the Sophos Central Admin console. It does not uninstall the Sophos agent software, but the computer will not get updates any more.

Note
If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

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.

Retrieve recovery key [Windows computers]

If users are unable to log in to their encrypted computer, you can get a recovery password which used to unlock the computer. There is a recovery key (password) for each volume of a BitLocker protected computer. It is created and backed up in Sophos Central before the computer is encrypted.
When Sophos encryption is installed, existing BitLocker recovery keys are replaced automatically and can no longer be used.

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, you need to find the recovery key identifier for the computer 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.
3. In Sophos Central, go to Computers and click the Retrieve Recovery Key button.
4. Enter the recovery identifier provided by the user and display the recovery key.

If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

Click the Show key button to display the recovery key.

Make sure that the user is authorized to access the encrypted device before you provide the recovery key.

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.

Give the recovery key to the user.

The computer can be unlocked. 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.

If users forget their login password, they can use a recovery key to regain access to their data.

To get the recovery key, you need to find the recovery key identifier for the computer 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.
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 the recovery identifier provided by the user and display the recovery key.

Note
If the recovery password has already been used to unlock a computer, a hint informs you that a newer recovery key identifier is available for this computer.

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.

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. They can use it to access the computer and create a new password. Once they have created a new password they can access their computer again.

Note
You can recover access to encrypted non-startup volumes on Mac, see Sophos Central Device Encryption administrator guide.

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.

Computer Summary
The Summary tab in a computer’s details page lets you see the following:

- Security status of the computer.
- Recent events on the computer.
- Endpoint Agent summary. This agent provides threat protection and more.
- Device Encryption summary. This is not displayed if the encryption policy has been disabled.
- Web Gateway summary (if you have Sophos Web Gateway). This agent provides advanced protection against risky or inappropriate web browsing.
- Tamper protection settings.
- Update cache status. This is not displayed if a cache has not been set up.
Security status

In the left-hand pane, you can see details of the security status.

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

Status
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.

Delete
The Delete option deletes the computer from the Sophos Central Admin console. This does not uninstall the Sophos agent software, but the computer will not get updates any more.

Tip
If you deleted the computer accidentally, re-install the Sophos agent software to get it back.

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:

- Endpoint Agent (for threat protection and more).
- Web Gateway Agent (advanced web protection).

Endpoint Agent Summary

The Endpoint Agent provides threat protection and other features like peripheral control, application control and web control.

The summary shows the last activity on the endpoint. It also shows whether the endpoint agent is up to date.

If you need to take action, buttons are displayed:

- Update: Updates the Sophos agent software on the computer.
- Scan Now: Scans the computer 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 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.

Device Encryption summary

Device Encryption allows you to manage BitLocker Drive Encryption on Windows computers. This summary shows the encryption status and type of authentication used (or "Protector" in BitLocker terms) for each volume.

Retrieval recovery key

You can also retrieve a recovery key here. This can be used to unlock the computer if users forget their PIN or passphrase or lose the USB drive they use to log on.

1. Click Retrieve next to the volume. This displays the recovery key ID and latest recovery key.
2. 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.

3. Give the recovery key to the user.

The computer can be unlocked. 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.

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 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.

This shows that a cache has been set up for the computer. It shows which server is being used.

Computer Events

The Events tab in a computer’s details page displays events (such as blocked websites or policy non-compliance) detected on the computer.

You can customize the list by selecting the start and finish dates.

The list shows:

• A description of the event.
• The time and date when the event occurred.
• An icon that indicates the importance of the event. See the Key to the icons.
• An icon that indicates which Sophos agent reported the event. See the Key to the icons.

To see the events arranged by type, as well as a graph showing events day by day, click View Events Report.

Key to the icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>A task (for example, an update) succeeded.</td>
</tr>
<tr>
<td>⚠</td>
<td>Warning.</td>
</tr>
<tr>
<td>⚠</td>
<td>Action required.</td>
</tr>
<tr>
<td>i</td>
<td>For information only.</td>
</tr>
<tr>
<td>🌐</td>
<td>Endpoint Agent event.</td>
</tr>
<tr>
<td>🌐</td>
<td>Gateway Agent event.</td>
</tr>
</tbody>
</table>

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:
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.
   
   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.

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.

**9.5.2 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.

**About the servers list**

The current servers are listed with these details:

- Name/Operating System.

  **Tip**

  “Sophos Security VM” indicates a host where Sophos protects the guest VMs.

- IP Address.
- 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).
• Last Updated. This is the last time that the Sophos agent software was updated.
• License. Standard or Advanced license.
• 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, click the drop-down arrow on the filter above the list.

Tip
The Virtual Servers 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 323).

Server Summary

The Summary tab of a server’s details page lets you see server details and manage the server.
The page includes:
• Server details.
• Actions you can take on the server.
• A summary of recent events on the server.
• A summary of the device status.
• Separate tabs for Events, Exclusions, Lockdown Events and Policies.
The server details and actions buttons are in the left-hand pane. This pane is always shown, even when you click the other tabs on this page.

Server details

In the left-hand pane, you can see the server details, such as name and operating system.
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 the Sophos Central Admin console. This does not uninstall the Sophos agent software, but the server will no longer synchronize with the console.
  
  If you deleted the server accidentally, re-install the Sophos agent software to get it back.

- **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.

Device status

The device status summary shows:

- **Last Sophos Central Activity**: The last time the server communicated with Sophos Central.
- **Last Agent Update**: The last time the Sophos agent software on the server was updated.
- **IPv4 Address**.
- **IPv6 Address**.
- **Operating System**.
  
  If the operating system is shown as "Sophos Security VM", the server is a host with a Sophos security VM installed.

- **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.

  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.
Sophos Central Admin

- **Malware policy.** The threat protection policy that applies to the server. Click the policy name to see details.
- **Group.** Shows the group the server belongs to (if it belongs to one). Click Change Group to move the server to a different group, or simply to remove it from its current group.
  
  A server can only be in one group.
- **Tamper Protection.** This shows whether Tamper Protection [page 336] is enabled on the server or not. Click View Details to manage the tamper protection password for the server.

**Update cache 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. This is not displayed if a cache has not been set up or if the server is not being used as a cache.

If the server is being used as an update cache this shows:

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

Alternatively this shows that a cache has been set up for the server. It shows which server is being used.

**Server Events**

The Events tab in a server’s details page lets you see events (such as threats or policy non-compliance) detected on the server.

**Tip**

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.

**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 283).

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 156).

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.
**AWS Instances**

On the **AWS Instances** page, you can view the Amazon Web Services EC2 instances associated with your Sophos Central account. To add AWS accounts, see [Amazon Web Services Accounts](page 345).

The AWS instances are listed with these details:

- **Instance ID**. Click on the ID to view the details of the instance.
- **Agent installed**. This shows whether a Sophos agent is installed on the instance. Click on the "Server Details" link to view the instances with Sophos agents installed.
- **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](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.

**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 328).

**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 328).

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.
9.6 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.

9.6.1 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 330). For full details of how it works, see About Active Directory synchronization (page 330). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 329).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 332). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 332).

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 the Sophos Central Admin console. It does not support two-way synchronization between the Sophos Central Admin console 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 the Sophos Central Admin console. 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 the Sophos Central Admin console.

   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 332).

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**

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.

### 9.6.2 Role Management

You can use pre-defined administration roles to divide up security tasks according to the administrators’ responsibility level.

In Settings, the **Role Management** page shows a list of administration roles and the number of users assigned to each role.

**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 cannot</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. | There are no limitations. | None. |
|           | In addition they can:         |                                      |                             |
|           | • Manage roles and role assignments |                                      |                             |
| **Admin** | Have access to everything in Sophos Central. | Manage roles and role assignments. | No Role Management options are displayed. |

Copyright © 2017 Sophos Limited
<table>
<thead>
<tr>
<th>Role</th>
<th>Administrators with this role...</th>
<th>Administrators with this role cannot...</th>
<th>User Interface Restrictions</th>
</tr>
</thead>
</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.  
• Update the Sophos agent software on a computer.  
• Scan computers. | Manage roles and role assignments. In addition they cannot:  
• Assign policies.  
• Change settings. | 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 cannot:  
• 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 other 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 cannot:  
• 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. |

**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 307).

**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.

9.6.3 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.

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 x to the right of the exclusion you wish to remove.

9.6.4 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.

**Note**
You can change the settings for an individual device or server. Open its details page and select the **Tamper Protection** tab. There you can view the password, generate a new one, or temporarily disable tamper protection for that device.

### 9.6.5 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.

### 9.6.6 Website Management

**This page is not available if you do not have a Web Control or Web Gateway license.**

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.
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 on the Policies page.

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**.

### 9.6.7 Registered Firewall Appliances

In Settings, on the **Registered Firewall Appliances** page, you can view Sophos Firewalls that have been registered with Sophos Central. You can also deregister (or "disconnect") them.

**Note**

You can only register a Sophos Firewall from the Firewall console (Go to **System > System Services > Security Heartbeat**).

### About registered Firewalls

When a Sophos Firewall is registered with Sophos Central, your computers can send regular reports on their security status or "health" to the Firewall. These reports are known as "Security Heartbeats".

If more than one 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 Firewall can restrict its network access. The Firewall admin and the 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 Firewalls that are registered with Sophos Central:

- Name
- IP address
• Active. This indicates whether the Firewall has received Security Heartbeats within the previous hour.

To find a Firewall, start to enter the name in the Search for a Firewall field. As you type, the list is filtered to show only Firewalls that match.

Deregister Firewalls

You can deregister Firewalls from Sophos Central. For example, if you no longer use a Firewall, you could deregister it so that it is no longer shown here.

When you deregister a 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 the Firewall or Firewalls 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 the Firewalls.

The selected Firewalls are removed from the list.

If you deregister all the 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.

9.6.8 Global Scanning Exclusions

You can exclude files, websites and applications from scanning for threats. You can also exclude applications from detected exploits.

For example, you might exclude activity by some commonly-used applications to reduce the impact of scanning on performance.

You can do this in Settings, on the Global Scanning 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 scanning exclusions in the policies instead.

1. On the Global Scanning Exclusions page, click Add Exclusion [on the right of the page]. The Add Scanning 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 detected exploit).
3. Specify the item or items you want to exclude. The following rules apply:

   • File or folder [Windows]. You can exclude a drive, folder or file by full path. For file title or extension the wildcard * may be used, though ** 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 of exclusions for Windows servers, see Scanning exclusions (page 159).

   • File or folder [Mac/Linux]. You can exclude a folder or file. You can use the wildcards ? and *. Examples:
     - /Volumes/excluded (Mac)
• **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 164).

• **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 11111111.11111111.11111111.00000000. 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’s been detected. Sophos Central will no longer detect it for the affected application. Sophos Central will also no longer block the affected application.

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**.

### 9.6.9 Bandwidth Usage

You can configure the bandwidth used for updating the Sophos agent software on your endpoint computers.

**Set the bandwidth used**

In Settings, on the **Bandwidth Usage** page, you can limit the bandwidth used. Currently the default limit is 256 Kbps.
This helps to ensure that updating does not cause computers to run slowly. You can specify a custom bandwidth or unlimited bandwidth.

**Note**  
This setting is for Windows computers only.

**Note**  
This setting does not apply to the initial installation of Sophos agent software or to updates downloaded by Sophos Manage Update Cache (page 341).

### 9.6.10 Manage Update Cache

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.

When you set up a cache on a server, Sophos Central does as follows:

- Installs Sophos caching software.
- Fetches updates from Sophos and puts them in a cache.
- Automatically configures Windows computers in your network to update from a cache.

Using caches doesn't affect how often or when computers are updated.

**Note**  
Workstations and servers can both update from a cache.

**Note**  
Windows Vista or XP workstations cannot update from a cache.

### Set up a cache

Before you set up a cache, ensure that:

- The server has at least 5GB free disk space.
- Port 8191 is available and accessible to computers that will update from the cache.

**Note**  
The Update Cache installer will open port 8191 in Windows Firewall. When Update Cache is uninstalled, the port will be closed again.

To set up a cache:

1. In Settings, go to the **Manage Update Cache** 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. If you have already set up a cache on some servers, to hide them from view, select **Servers without Update Cache**.
3. Select the server or servers where you want to set up a cache.
4. Click **Set Up Cache**.

### Remove a cache

When you remove a cache:

- Sophos Central uninstalls caching software, removes the cache of downloaded updates, and closes port 8191 in Windows Firewall.
- Computers currently updating from this server are automatically reconfigured to update from another update cache, if you have one.

If you remove all your caches, computers will update directly from Sophos.

To remove a cache:

1. Go to the **System Settings > Manage Update Cache** 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.
3. Select the server or servers you want to remove a cache from.
4. Click **Remove Cache**.

### 9.6.11 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 342]
- **Controlled Updates** [page 342]
- **Control Updates Manually** [page 343]

#### 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 Updates.

**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 Updates.

**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 non-test computers 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.

### 9.6.12 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.

When you add an AWS account on this page, Sophos Central will do as follows:

- Display AWS instance details.
- Remove terminated AWS instances automatically.
- Let you apply server policies to Auto Scaling Groups.

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.**
9.6.13 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 348).

- **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 347), 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.

You can also export custom rules, click 🔄. This creates an xml file containing the rule definition.

Click ✗ to delete a rule and 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 348).
      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.

### 9.6.14 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 346).

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 349).

You can filter the CCLs by:

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

You also can search the list of CCLs.

Click **i** to view details of a CCL.

For each custom CCL you can also:

- Click on the name of a CCL to edit it.
- Click **p** to export a CCL. This creates an XML file containing the definition for the CCL.
- Click **c** 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 **x** to delete a CCL and 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 edits, 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>
</tbody>
</table>
**Expression** | **Score** | **Max Count**
--- | --- | ---
Expression B | 3 | 1
Expression C | 1 | 5

### 9.6.15 Allow/Block Domains and Addresses

The **Allow/Block** list is part of Email Security and 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 353).

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 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.

In Settings, on the **Email Security > 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 **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** use the most recent option you chose.

5. Click **OK**.

The allowed email address or domain is added to the **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 **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** use the most recent option you chose.

5. Click **OK**.

The blocked email address or domain is added to the 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 Allow/Block list.
3. Click **Yes** to confirm deletion.

**9.6.16 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 353).

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.

**9.6.17 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 [Set up Email Security](#) (page 353).

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 the Office 365 link.

d) Use the information to help you configure your email domain.

2. In the **Email Domain** text field enter your email domain. Example: `example.com`.

   Domain ownership must be verified before mail will be delivered through Sophos Central. To verify domain ownership, you need to add a TXT record to your domain. Adding this record will not affect your email or other services.

3. Click **Verify Domain Ownership**.

4. Use the details given in **Verify Domain Ownership** to add the TXT record to your Domain Name Server (DNS).

   **Note**

   This can take up to 10 minutes to propagate.

5. Click **Verify**.

   **Note**

   You cannot save an unverified domain. You must correct any issues with the domain ownership verification.

6. 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` of `mymail@example.com`.

   b) If you selected **MX** enter a FQDN in the **FQDN** text field. Example: `mymail@example.com`.

7. In the **Port** text field enter the port information for your email domain.

8. 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.

9. Click **Save** to validate your settings.
10. Click the Base Policy link to configure spam protection, see Email Security Policy (page 229).

**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.
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 224).

2. Add your protected email domains, see Settings (page 232).
3. Configure spam protection in the email security policy, see Email Security Policy (page 229).
4. Set up global controls on spam using allow and block lists for senders, see Allow/Block Domains and Addresses (page 350).

**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 330).
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 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.

4. Click Continue.
5. Add your email domains, see Settings (page 232).
9.7 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.

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.

9.7.1 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.

• Windows: Endpoint Advanced Installer. Click this for an installer with all endpoint products your license covers.
• Windows: Choose Products .... Click this if you want to choose which products will be included in the installer. The choices are:
  — Endpoint Advanced (protection from malware).
  — Intercept X (protection from ransomware and exploits).
  — Device Encryption.
• Download Mac OS X installer. Click this for an installer for Macs.
• 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, DOMAINE\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.

9.7.2 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 Windows Device Encryption.** Click this for an installer for encryption only.
- **Windows: Choose Products ...** Click this if you want to choose which products will be included in the installer. The choices are:
  - Endpoint Advanced (protection from malware).
  - Intercept X (protection from ransomware and exploits).
  - Device Encryption.
- **Send Installers to Users.** Click this to go to a page where you can add users and send them installers that they can use.

9.7.3 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.
Note
For Linux computers, there is an alternative: Sophos Secure OS. See the Server Protection As A Web Service section.

When you protect a server:
• The server is added to the Servers list in Sophos Central.
• Default policies are applied to the server.

9.7.4 Server Protection as a Web Service

You can protect Linux computers with Sophos Secure OS.
Secure OS is a pre-built image of the CentOS Linux operating system and comes with Sophos Anti-Virus for Linux pre-installed.
You can get Secure OS from Amazon Web Services and then enable Sophos Central to manage it.

Set up Sophos Secure OS

Go to Server Protection > Protect Devices.
Under Server Protection as a Web Service, click Set up Sophos Secure OS and follow the instructions. Then register the Secure OS server with your Sophos Central account [click on the link to see the command you need].

9.7.5 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 all the guest VMs on that host.
• 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.
Note
You may also be able to download Sophos Anti-Virus for vShield. However, Sophos has announced this product’s retirement.

We recommend you read 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 the Sophos Guest VM Agent and checked it is connected, for each of your guest VMs.

9.7.6 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.
10 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.
11 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.

11.1 Account Details

The Account Details page lets you change 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**
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**

You cannot turn this feature off once you have enabled it. See Create an Enterprise Admin (page 362).

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 SuperAdmin 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 administrator'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.

**11.1.1 Create an Enterprise Admin**

Before you begin:
You need to be a SuperAdmin administrator, see Administration Roles (page 333).
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 cannot turn on Enterprise Management from Sophos Central Trial accounts.

After you enable Enterprise Management:

You cannot turn the Enterprise Management option off once you have enabled it.

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 SuperAdmin 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.

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.
   a) If you need further information read the knowledge base article. Click Continue.

   Important
   You cannot turn this option off once you have enabled it.

3. Enter the account details to create the Enterprise Admin. Choose from:
   a) Use your Sophos Central login credentials.
      To do this, click Use my Sophos Central login credentials to create the first Sophos Central Enterprise admin.
      If you do use your Sophos Central login credentials you won't be able to log in to Sophos Central Admin with that account.
   b) Create a new account.
      To do this, enter new account information.
      You must use a unique email that is not already used in any other Sophos Central account.
4. Click Enable Enterprise Management and Save.
   The Account Preferences tab now shows that Enterprise Management has been enabled and the name of Enterprise Admin. The Enterprise Admin receives the password setup link in an email.
5. Click the link in the set up 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 login page and enter your Enterprise Admin credentials.
   This opens Sophos Central Enterprise.
11.2 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 360).
- **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. In the Apply Activation Code field, enter the Activation Key shown on the License Schedule that Sophos has emailed you and click Apply. 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.

## 11.3 Early Access Programs

Early access programs let you try out new product features before we release them to all customers. You can take part in more than one program at the same time.

There are two types of early access program:

- **Open.** Anyone can take part.
- **Invitation only.** We invite you to take part in the program and send you the code you need for access.

### 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.
12 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://cloud.sophos.com/unsupported.
13 Contact Sophos Support

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.
14 Legal notices

Copyright © 2013–2017 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.