SOPHOS

Security made simple.

Sophos Central Help

Document date: December 2016

Contents

1 About Sophos Central Admin Help

Sophos Central is a web-hosted solution which offers seamless protection and policy enforcement for users across all their devices as well as for networks.

This Help file provides additional information 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**.

Tip: 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?** .

Accessing the Help

To open the Help, click **Help** > **Help with ...**. The Help always opens in a separate window. The Help is context-sensitive, so it opens a topic related to the part of the user interface you're using.

Using the Help

The Help consists of a navigation pane on the left side and the topic pane on the right side.

Navigation pane: The navigation pane contains two tabs:

- The **Content** tab gives an overview of all topics covered by the Help.
- The **Search** tab lets you search the whole Help for the word or words you specify. Click the link in a result to open the topic in the topic pane.

Topic pane: The currently selected topic is displayed here.

You can also download a PDF version of the Help by clicking the **PDF** button in the Help.

The **With Frames** button displays the output using HTML frames to render two separate sections: a section that presents the table of contents on the left and a section that presents the content of a topic on the right. The "with frames" layout is displayed if JavaScript is disabled in the browser.

Tips & Tricks

Hidden text: Often you can find additional information by clicking on drop-down arrows.

Closing the navigation pane: You can close the navigation pane by clicking the arrow located on the bar between the navigation and the topic pane.

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 About The User Interface

The user interface of Sophos Central Admin is divided into a header, a main menu, and the main frame. The main frame displays the content of the currently selected menu.

Header

The page header has these links on the right side:

- **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.
- **Help**. Click here for options to see the Help, create a support ticket, give feedback, view knowledgebase articles, or see what's new in the product.

Main Menu

The main menu on the left lets you access the main functions of Sophos Central.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

4 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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, computers, servers, mobiles, or devices protected by web gateway (depending on your licenses).

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 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, phishing sites blocked, websites blocked and total items blocked.

Click on a figure to open a detailed report.

5 Alerts

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

Note: 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

Note: 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.

  Note: This does not resolve threats and does not remove threat details from the quarantine manager on the computer.

- **Mark As Resolved**. Click this if the threat has already been resolved on the endpoint computer. This action clears the alert from the list in Sophos Central and also clears threat details from the quarantine manager on the computer.

  Note: This action does not resolve threats.

  Note: This action is only available for Windows endpoint computers.

- **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 send an email to Sophos Support (page 166). 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 and is not available for mobile devices.

  Note: 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 11).

- **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 and is not available for mobile devices.

- **Send Message** Click this to send a text message to a mobile device when the device is not compliant or when malware or PUA has been detected on the device. This action is available for Android devices that have the Sophos Mobile Security or Sophos Mobile Control app installed and are managed by Sophos Central.

5.1 Alerts for Installation, Updating and Compliance

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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. For information about managing peripherals, see Configure Peripheral Control (page 96).

5.2 Alerts for Threat Protection

There are the following types of threat protection alerts.

Tip: 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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).
- 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.

Note: 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.

5.3 Alerts for Mobile Devices

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

There are the following types of alerts related to mobile device management:

High

- **Your APNs certificate will expire soon**

  If your APNs certificate will expire within the next 7 days, this alert is of high importance. A valid APNs certificate is needed for communication between Sophos Central and iOS mobile devices. Renew it as soon as possible. See Renew APNs Certificate (page 144) for information on how to do that.

- **Your APNs certificate has expired**

  As your certificate has expired, communication between Sophos Central and iOS devices is no longer working. Renew it as soon as possible. See Renew APNs Certificate (page 144) for information on how to do that.

Medium

- **Mobile device decommissioned by user**

  A user has deleted the Sophos Mobile Control app or removed its configuration (this cannot be prevented). The mobile device is now unmanaged. It will lose its connection to the company network if this network connection was specified in a policy (see Configure Wi-Fi (page 101)).

- **Action for mobile device failed**

  The kind of action that failed for the mobile device is specified in the corresponding events.

- **Mobile Exchange settings could not be applied (missing account information)** and **Please add missing Exchange information**

  Exchange settings can only be applied if both the Exchange email and the Exchange login are available. Unless you configured a policy containing specific user information, this account information is taken from the user details. To add missing details, go to the **People** > **Users** page, click on the user to display their details, and click **Edit**.

- **Unable to deploy to iOS devices. Please configure the APNs certificates first.**

  A valid APNs certificate is needed for communication between Sophos Central and iOS mobile devices. See Create APNs Certificate (page 143) for more information on how to get one.

- **Your APNs certificate will expire soon**

  If your APNs certificate will expire in 7-14 days, this alert is of medium importance.

- **User unenrolled Device Management (or Security Management) app**

  The user has unenrolled the Sophos Mobile Control or Sophos Mobile Security app and the respective policy can no longer be applied to the device.

- **The mobile device is now non-compliant**

  The device is not compliant if any compliance rule specified in the policy or policies valid for this device is violated.

- **Malware detected**

  Malware detection is available only with the Sophos Mobile Security app for Android. Automatic cleanup is not possible on Android, so the user needs to remove malware from the device himself.

- **PUA detected**

  A potentially unwanted app has been detected. The user needs to remove it from the device himself.

- **Low reputation app detected**

  A low reputation app has been detected. The user needs to remove it from the device himself.

Low

- **Action for mobile device succeeded**

  The kind of action that succeeded for the mobile device is specified in the corresponding events.

- **Action for mobile device has been canceled**

  The kind of action that was canceled for the mobile device is specified in the corresponding events.

- **Mobile device is not compliant**

  A device is not compliant if any of the requirements specified in the policy valid for this device is not met. For more information, see Configure Compliance Rules (page 101).

- **Mobile device enrolled**

  A mobile device is enrolled.

- **New Device Management (or Security Management) app enrolled**

  The Sophos Mobile Control or Sophos Mobile Security app has been enrolled.

- **Malware cleaned up**

  The user removed malware from the device.

- **PUA cleaned up**

  The user removed PUA from the device.

- **Low reputation app cleaned up**

  The user removed a low reputation app from the device.

Informational

- **Your APNs certificate will expire soon** If your APNs certificate will expire in 14-30 days, this is just an informational alert.
- **Your APNs certificate was renewed** This is to confirm that the certificate was renewed.

5.4 Alerts for Device Encryption

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

- **Recovery key missing**

  A recovery key for an encrypted volume cannot be found in the Sophos Central database.

5.5 Email Alerts

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 9).
- 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.

Note: You cannot change the email alert settings.

6 Logs & Reports

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

6.1 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 19).

Tip: 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).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

6.1.1 Event types

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

- Runtime detections (page 19)
- Application control (page 21)
- Malware (page 21)
- Potentially unwanted application (PUA) (page 22)
- Policy violations (page 23)
- Web control (page 23)
- Updating (page 23)
- Protection (page 24)
- Peripherals (page 25)
- Mobiles (page 25)
- ADSync (page 27)
- Download reputation (page 27)
- Firewall (page 28)
- Device encryption (page 28)

Note: 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 9).

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

Event type	Severity	Action required?	Description
Running malware detected	Medium	No	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

Event type	Severity	Action required?	Description
			the Alerts page, and a "Running malware cleaned up" event will be added to the Events list.
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.
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.
Remotely-run ransomware attack resolved	Low	No	
Ransomware attacking a remote machine detected	High	Yes	This computer has been detected attempting to remotely encrypt applications on another computer.
Safe Browsing detected compromised browser	Medium	Yes	An attempt to exploit a vulnerability in an internet browser has been blocked.

Event type	Severity	Action required?	Description
Exploit prevented	Low	No	An attempt to exploit a vulnerability in an application, on an endpoint computer, has been blocked.
Application hijacking prevented	Low	No	Application hijacking was prevented on an endpoint computer.

Application control

Event type	Severity	Action required?	Description
Controlled application blocked	Medium	No	
Controlled application allowed	Low	No	A controlled application has been detected and then allowed.

Malware

Event type	Severity	Action required?	Description
Malware detected	Medium	No	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.
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.

Event type	Severity	Action required?	Description
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	
Malware alert locally cleared	Low	No	A malware alert has been cleared from the alerts list on an endpoint computer.

Potentially unwanted application (PUA)

Event type	Severity	Action required?	Description
Potentially unwanted application (PUA) blocked	Medium	Yes	A potentially unwanted application has been detected and blocked.
Potentially unwanted application (PUA) not cleaned up	Medium	Yes	The following events may be displayed for this event type: ▪ Manual PUA cleanup required. ▪ Computer scan required to complete PUA cleanup. ▪ Reboot required to complete PUA cleanup. ▪ PUA not cleaned up.
Potentially unwanted application (PUA) cleaned up	Low	No	
Potentially unwanted application (PUA) alert locally cleared	Low	No	A potentially unwanted application alert has been cleared from the alerts list on an endpoint computer.

Policy violations

Event type	Severity	Action required?	Description
Policy non-compliance	Medium	Yes	An alert will be displayed on the Alerts page if a computer remains non-compliant for more than two hours.
Policy in compliance	Low	No	
Real-time protection disabled	High	Yes	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.
Real-time protection re-enabled	Low	No	

Web control

Event type	Severity	Action required?	Description
Web policy events	Low	No	See Web Control Reports (page 38) for detailed information on how users are accessing sites, who is violating policy, and which users have downloaded malware.
Web threat events	Low	No	

Updating

Event type	Severity	Action required?	Description
Computer or server out of date	Medium	Yes	
Update succeeded	Low	No	

Event type	Severity	Action required?	Description
Update failed	Low	No	
Reboot recommended	Low	No	
Reboot required	Medium	Yes	

Protection

Event type	Severity	Action required?	Description
New computer or server registered	Low	No	
Computer or server re-protected	Low	No	
New computer or server protected	Low	No	
Failed to protect computer or server	High	Yes	A computer has started installation of the agent software but has not become protected for one hour.
Error reported	Low	No	
Scan completion	Low	No	
New logins added	Low	No	
New users added automatically	Low	No	

Peripherals

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

Mobiles

Event type	Severity	Action required?	Description
New mobile device enrolled			For information about alerts for mobile devices, see Alerts for Mobile Devices (page 14).
Mobile device decommissioned by user			
Action for mobile device failed			
Action for mobile device succeeded			
Action for mobile device has been canceled			
Your APNs certificate has expired	High	Yes	
Your APNs certificate was renewed	Low	Yes	

Event type	Severity	Action required?	Description
No APNs certificate configured	Medium	Yes	
Your APNs certificate will expire in <n> days	Depends on the time left before expiration	Yes	
Mobile Exchange settings could not be applied (missing account information)	Medium	Yes	
Please add missing Exchange information	Medium	Yes	
New app enrolled (where the app is Device Management or Security Management)	Low	No	
User unenrolled app (where the app is Device Management or Security Management)	Medium	Yes	
The mobile device is now non-compliant	Medium	Yes	
Malware detected	Medium	Yes	
Malware cleaned up	Low	No	
PUA detected	Medium	Yes	
PUA cleaned up	Low	No	
Low reputation app detected	Medium	Yes	
Low reputation app cleaned up	Low	No	

Event type	Severity	Action required?	Description
<URL> blocked due to <threat>	Low	No	
<URL> warned due to <threat>	Low	No	
User bypassed <threat> block to <URL>	Low	No	

ADSync

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

Download reputation

Sophos Central warns end users if a download has a low reputation. This reputation is based on a file's source, how often it is downloaded and other factors. For more information, see Knowledgebase Article 121319.

Event type	Severity	Action required?	Description
User deleted low reputation download	Low	No	A user deleted a download after Sophos Central warned that it had a low reputation.

Event type	Severity	Action required?	Description
User trusted low reputation download	Low	No	A user trusted a download after Sophos Central warned that it had a low reputation.
Low reputation download automatically trusted	Low	No	Sophos Central detected a low reputation download and trusted it automatically. **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	Severity	Action required?	Description
Missing heartbeat reported	High	Yes	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).
Restored heartbeat reported	Low	No	A computer has resumed sending security heartbeat signals to the Sophos Firewall.

Device encryption

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

Event type	Severity	Action required?	Description
Key creation failed	Medium	See Note	A key could not be created (TPM key, TPM+PIN key, USB key, recovery key).

Event type	Severity	Action required?	Description
Encryption failed	Medium	See Note	A volume could not be encrypted.
Encryption info	Low	See Note	Information on various events, for example the user postponed encryption or a PIN/passphrase was reset.
Disk not encrypted	Medium	See Note	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.
Recovery key missing	Medium	See Note	A recovery key for an encrypted volume cannot be found in the Sophos Central database.
Recovery key received	Low	See Note	Sophos Central received a recovery key from an endpoint computer.
Recovery key revoked	Low	See Note	A recovery key has been viewed in Sophos Central, so it has been revoked and will be replaced.

6.2 Audit Logs

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

   Note: Audit reports are exported as audit.csv or audit.pdf.

6.3 User Report

The **User Report** page provides information on users who are active (logged in during the last two weeks), inactive or unprotected.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Click on any of the categories to display a list of those users with more detailed information:

- **Name**: User name. You can click on this to see the user's full details.
- **Email**: The user's email address.
- **Online**: When the user was last logged in.
- **Devices**: The devices associated with the user.
- **Logins**: The user's login name.
- **Groups**: Groups the user belongs to.

You can also display details of particular users by entering a name in the **Search** field.

Print or export reports

You can print or export your reports. Above the list, there are these options:

- **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.

6.4 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 seach 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 Configure Email Security (page 109).

- **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.

6.5 Server Report

The **Server Report** page provides information on servers that are active (updated during the last two weeks), inactive, dormant or unprotected.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Click on any of those categories to display a list of those servers, with more detailed information:

- **Name**: Server name.
- **Online**: When the server last made contact.
- **Real-time scan**
- **Last update**. When the server last updated its Sophos Endpoint Protection agent.
- **Last scheduled scan**. When the server last performed a scheduled scan.
- **Alerts**. Numbers and types of outstanding alerts

Print or export reports

You can print or export your reports. Above the list, there are these options:

- **Search**. In the Search field, enter a term to search for. The list shows only results related to your search term.
- **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.

6.6 Computer Report

The **Computer Report** page provides information on computers that are active (updated during the last two weeks), inactive or not protected.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Click on any of the categories to display a list of those computers with more detailed information:

- **Name**: Computer name.

- **Online**: When the computer last made contact.
- **Last user**: Last user that logged in to the computer.
- **Real-time scan**: **Yes:** Real-time scan is enabled, **No:** Real-time scan is disabled.
- **Last update**: When the computer last updated.
- **Last scheduled scan**: When the computer last performed a scheduled scan.
- **Alerts**: Numbers and types of outstanding alerts.

You can also display details of particular computers by entering the computer name in the **Search computers** field.

Export and Print

You can print or export your reports. Above the list, there are these options:

- **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.

6.7 Mobile Management Report

The **Mobile Management Reports** page provides information on mobile devices managed by Sophos Central:

- **All** All registered mobile devices.
- **Managed** Mobile Devices under control of Sophos Central.
- **Unmanaged** Mobile Devices not under control of Sophos Central. This covers *Decommissioned*, *Wiping* and *Wiped* (see also below).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Devices that have not yet been enrolled do not appear in the list. The same is true for devices that have been deleted by you as administrator.

Clicking on any of those categories opens a table below with more detailed information:

- **Management Status** An icon showing the management status of the device:
  - *Managed*
  - *Unmanaged*
- **Name** Name of the device.
- **OS** Operating system and version.
- **User** User name.
- **Last Active** The time of the last check-in or synchronization that was performed.

- **Management Status** One of the following:
  - *Managed:* The device is under control.
  - *Not Managed:* The Sophos Mobile Control app is not configured as device administrator.
  - *Enrolling:* The user is enrolling the Sophos Mobile Control app.
  - *Enrolled:* The Sophos Mobile Control app has been enrolled, but no policy has been assigned yet.
  - *Decommissioned* The user removed the Sophos software from the device. It is no longer under control.
  - *Wiping:* You initiated a wipe and the device is resetting itself to factory presets. All data will be deleted.
  - *Wiped:* The device was reset to factory presets. It has lost connection to Sophos Central, but remains in the list so that you can verify that it was wiped successfully. If the device is enrolled again, a new entry will be created for the device. You can safely delete the old entry that lists the device as wiped.
- **Compliance** Compliance status.

You can also display details of particular mobiles by entering a name in the **Search** field.

Print or export reports

You can print or export your reports. Above the list, there are these options:

- **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.

6.8 Mobile Security Report

The **Mobile Security Reports** page provides information on the security status of mobile devices:

- **Android Devices** All registered Android mobile devices.
- **Needs Attention** The number of mobile devices with high-priority security alerts.
- **With Warnings** The number of mobile devices with medium-priority security alerts.
- **In Good Health** The number of mobile devices with low-priority security alerts or no alerts.
- **Not Protected** Mobile devices that do not have a mobile security policy applied.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Clicking on any of those categories opens a table below with more detailed information:

- **Security Status** An icon showing the security status of the device:
  - *Needs Attention*
  - *With Warnings*

- *In Good Health*
- *Not Protected*

- **Name** Name of the device.
- **OS** Operating system and version.
- **User** User name.
- **Last Active** The time of the last check-in or synchronization that was performed.
- **Mobile Security** One of the following:
  - *Managed:* The device is under control.
  - *Not Managed:* The Sophos Mobile Security app is not configured as device administrator.
  - *Decommissioned:* The user removed the Sophos Central software from the device. It is no longer under control.
  - *Enrolling:* The user is enrolling the Sophos Mobile Security app.
  - *Enrolled:* The Sophos Mobile Security app has been enrolled.
  - *Wiping:* You initiated a wipe and the device is resetting itself to factory presets. All data will be deleted.
  - *Wiped:* The device was reset to factory presets. It has lost connection to Sophos Central, but remains in the list so that you can verify that it was wiped successfully. If the device is enrolled again, a new entry will be created for the device. You can safely delete the old entry that lists the device as wiped.

Print or export reports

You can print or export your reports. Above the list, there are these options:

- **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.

6.9 Peripheral Report

The **Peripheral Report** page provides information on monitored peripherals that are allowed, read-only (can be accessed for reading only), or blocked.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Click on any of the categories to display a table below with more detailed information:

- **Type**: Peripheral type.
- **Model**: Peripheral model.
- **ID**: Peripheral ID.

- **Last device**: The last device where the peripheral was attached.
- **Events**: Number of events triggered by the peripheral.
- **Last user**: Last user who caused an event related to the peripheral.
- **Last action**: Last action that was applied on the peripheral
- **When**: Time and date when the peripheral was last used.

Print or export reports

You can print or export your reports. Above the list, there are these options:

- **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.

6.10 Application Control Reports

You can view various reports on the application control feature of Sophos Central.

These reports show which controlled applications are most frequently blocked, which are most frequently allowed, and which users or servers commit policy violations.

To find the reports, go to the **Logs & Reports** page and look for "Application Control".

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

6.10.1 Blocked Applications

The **Applications Most Frequently Blocked** report shows which blocked applications your users or servers try to access most often.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Blocked applications table

The table lists the applications that have been blocked.

For each application, the table shows:

- The category it is in.
- The number of times it has been blocked.
- The top five users or servers that attempted to access it (together with the number of attempts by each user or server).

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.
- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.10.2 Allowed Applications

The **Applications Most Frequently Allowed** report shows the allowed applications that are accessed most often.

Note: An allowed application is an application that is in your controlled list but is not blocked.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Allowed applications table

The table lists controlled applications that users or servers have been allowed to access.

For each application, the table shows:

- The category it is in.
- The number of times it has been allowed.
- The top five users or servers that accessed it (together with the number of times each user or server accessed it).

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.
- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.10.3 Application Control Policy Violators

The **Servers/Users With the Most Application Control Policy Violations** report shows which users or servers try to access blocked applications most often.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Policy violators table

The table list users or servers that have committed policy violations. The user or server with the most violations is at the top.

For each user or server, it shows details of the blocked and allowed applications they attempted to access:

- The number of blocked applications.
- The blocked applications accessed.
- The blocked application categories accessed.
- The number of allowed applications.
- The allowed applications accessed.
- The allowed application categories accessed.

Note: An allowed application is an application that is in the controlled list but is not blocked.

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.
- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.11 Web Control Reports

You can view various reports on the web control feature of Sophos Central.

These reports provide information on how users access sites, which users violate policy, and which users attempt to download malware.

To find the reports, go to the **Logs & Reports** page and look for "Web Control".

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

6.11.1 Blocked Website Categories

The **Top Blocked Categories** report shows which blocked website categories your users try to visit most often.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Blocked categories table

The table lists the categories your users have visited. The most frequently-visited categories are at the top.

For each category, the table shows:

- The number of visits.
- The number of unique visitors who attempted to visit websites in that category.

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.
- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.11.2 Warned Websites

The **Top Warned** report shows the most frequently-visited websites for which we display a warning to the user.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Warned websites table

The table lists the websites your users have visited and been warned about. The most frequently-visited websites are at the top.

For each website, the table shows:

- The categories the website belongs in.
- The number of users who were warned about the website.
- The number of users who proceeded to visit the website anyway.
- The top five users who proceeded to the website (together with the number of visits by each user).

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.

- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.11.3 Blocked Websites

The **Top Blocked Sites** report shows which blocked websites your users try to visit most often.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Blocked websites table

The table lists the blocked websites your users have attempted to visit. The most frequently-visited websites are at the top.

For each website, the table shows:

- The categories the website is in.
- The number of visits.
- The top five users that have attempted to visit the website (together with the number of visits by each user).

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.
- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.11.4 Web Control Policy Violators

The **Policy Violators** report shows which users violate your web control policy most often.

Violations include browsing to blocked sites and attempting to download blocked file types.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Policy violators table

The table lists users who have violated your policy. The users who did so most often are at the top.

For each user, the table shows the number of website visits that triggered a policy violation, the top five website categories that they visited in violation of the policy, and the number of times they visited each category.

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.
- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.11.5 Malware Downloaders

The **Top Malware Downloaders** report shows which users try to download malware most often.

For the purposes of this report, the following incidents are counted:

- Malware is detected in files the user has attempted to download.
- The user visits high risk websites that are known to have hosted malware in the past.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Malware downloaders table

The table lists users who have attempted to download malware or visit high risk websites. The users who did this most often are listed at the top of the table.

For each user, the table shows:

- The computer where the attempt happened.
- The number of website visits in which attempts happened.
- The top five types of malware or risk (together with the number of visits involving each type).

Manage, print and export reports

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:

- **Print**: Send a copy of the report to the printer.
- **Export to CSV**: Export a file of comma separated values (useful for importing to a spreadsheet or processing in other ways).
- **Export to PDF**: Generate and download a PDF file of the report.

6.12 Web Gateway Reports

You can view various reports that provide information on the Web Gateway feature of Sophos Central.

To find the reports, go to the **Logs & Reports** page and look for "Web Gateway".

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

6.12.1 Gateway Activity

This page is only displayed if your license includes Web Gateway.

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.

6.12.2 Gateway Reports

This page is only displayed if your license includes Web Gateway.

The **Gateway Reports** page lets you see all the reports for your Web Gateway protection.

Please note that reports update about once an hour.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

7 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

7.1 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

- **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.

8 People

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

8.1 Users

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

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

Important: Your ability to add and manage users depends on your assigned administrator role, see Administration Roles (page 134).

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

- Add users (page 47).
- Protect existing users (page 48).
- Modify users (page 48).
- Delete users (page 48).

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.
- Exchange login. This is needed if you want users to be able to check their corporate email on mobile devices.

  Note: To give users access to corporate email, configure Exchange Settings (page 145) and then add the settings to the Mobile Device Management section in a user policy (page 99).
- Role. This shows what administration role, if any, the user has, see Administration Roles (page 134).

  Important: 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 49).

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

Add users

You can add users in different ways:

- Add users on the **Users** page manually.
- Import users from Active Directory. Click the **Set up Active Directory Sync** link in the upper right of the page.
- Download an installer and run it yourself (instead of letting users use the setup link). This adds the user automatically. See the **Protect Devices** page.

Note: If you want to protect your users' iOS devices with Sophos Central's Mobile Device Management feature, you'll need an Apple Push (APNs) certificate. Click **Enable iOS for MDM** in the upper right of the page.

This section tells you how to add and protect users on the Users page.

Add and protect a user

1. Click the **Add User** button in the upper right of the page.
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 134).

   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.

   Exchange Login (optional). The Exchange login might be necessary if you want mobile devices to synchronize Exchange information automatically. You configure this by specifying a policy for mobile devices.

   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.

   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 the standard protection. You can install it alongside the standard 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.

Protect existing users

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

1. 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).

   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 the standard protection. You can install it alongside the standard protection or on its own.

Modify users

To modify a user's account, click the user's name to open and edit their user details. For more information, see User Summary (page 49).

Delete users

To delete a user or users, 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 134).

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.

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

Note: 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.

8.1.1 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can find details of each below.

Note: 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.

Note: You can click on the other tabs for more on **Devices**, **Events**, and **Policies**.

Security status

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

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

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

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

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

Note: Role information is only displayed for adminstration roles.

Account details

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

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

Modify the account

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

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

Role. Select a role for the user. Choose from: **SuperAdmin**, **Admin**, **Help Desk**, **Read-only** or **User**. For help on the administration roles, see Administration Roles (page 134).

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

Note: You cannot amend your own administration role.

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

Email Address. Enter the email address of the user.

Exchange Login (optional). The Exchange login might be necessary if you want mobile devices to synchronize Exchange information automatically. You configure this by specifying a policy for mobile devices.

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 the standard protection. You can install it alongside the standard 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 88).

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.

8.1.2 User Devices

The **Devices** tab in a user's details page lets you see the devices associated with the user.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

For each device you can see the device type (an icon shows whether it is a computer or mobile) 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.

8.1.3 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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

Icon	Meaning
	A task (for example, an update) succeeded.
	Warning.
	Action required.
	For information only.

8.1.4 User Policies

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

The icons beside a policy indicate the security settings (such as threat protection or mobile control) included in the policy.

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

Click a policy name to view and edit policy details.

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

8.2 User 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 53).

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 53).

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.

8.2.1 User Group Details

On a group's details page, you can:

- Add or remove members.
- Delete the group.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

8.2.2 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.

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

Note: 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 Computers

On the **Computers** page, you can manage your protected computers. They will appear automatically after Sophos agent software has been installed.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can:

- View details of the computers.
- Delete computers.
- Manage endpoint software.
- Retrieve recovery key 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.

Manage endpoint software

You can select new endpoint software to be installed on computers that are already protected and managed by Central.

1. Click **Manage Endpoint Software** (in the upper right of the page).
2. Select software.
3. Use the picker arrows to select the computers where you want to install the software.

The computers will update to the selected software.

Retrieve recovery key

If users forget their PIN or passphrase or lose the USB drive they use to log on to a BitLocker protected computer, you can get a recovery key which can be used to unlock the computer.

There is a recovery key (password) for each volume. 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.

To get the recovery key, you need to find the recovery key identifier for the computer and use it in the recovery wizard, as described below.

Tip: Alternatively, if you know which computer is affected, you can get the key from the Device Encryption section on that computer's details page. In this case, you don't need the identifier.

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 key 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 with administrator rights can now change the password.

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.

9.1 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.
- Web Gateway summary (if you have Sophos Web Gateway). This agent provides advanced protection against risky or inappropriate web browsing.
- Tamper protection settings.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

Note: 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.

  Note: 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 with administrator rights can now change the password.

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.

9.2 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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

Icon	Meaning
	A task (for example, an update) succeeded.
	Warning.
	Action required.
	For information only.
	Endpoint Agent event.
	Gateway Agent event.

9.3 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 9).

Activity

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

Computer Security Status

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

The computer security status is reported by computers running Windows 7 and later.

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

9.4 Computer Policies

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

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

Note: 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 computer's user.

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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

10 Mobile Devices

On the **Mobiles** page, you can manage your mobile devices. They will appear automatically after the Sophos Mobile Device Management app has been installed on the device and enrolled with Sophos Central.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

The devices are listed with details of the operating system, users associated with the device, and the status of the device.

Next to the device name, an icon shows you the health status of the device, which is a combination of the security status and compliance status of the device:

- 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 device, enter the name in the search field above the list.

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

You can click on the entry for a device to see more details, to perform actions on the device like scanning for threats, locking or locating the device, or to delete the device.

10.1 Mobile Device Details

On a mobile device's details page, you can see and manage the full details of the device, including:

- Security and compliance status.
- Device properties and activities details.
- Events created for the device.
- Policies applied to the device.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Device status overview

In the left-hand pane, an icon shows you the health status of the device, which is a combination of the security status and compliance status of the device:

- 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.

For detailed status information, click on the icon to open the **Status** tab of the device's details.

Below the device status icon, the following device information is shown:

- Device name in Sophos Central
- Device model
- Operating system

Device actions

In the left-hand pane, below the device status information, you can edit the device name and interact with the physical device:

- **Edit**: Edit the name under which the device is managed by Sophos Central.

  Although this is not mandatory, we recommend you use unique device names, to easily identify devices in list views.

- **Delete Device**: Removes the device from Sophos Central management. This also deletes the Sophos Central configuration and all associated corporate data from the device (a “corporate wipe”), but leaves personal data untouched. The Sophos Mobile Control app and the Sophos Mobile Security app are not deleted, only decommissioned. In order to get the mobile device back under Sophos Central management, the apps have to be configured again as described in the deployment email sent to the user (for details of how to send the email, see Users (page 46)).
- **Force Check-in**: A check-in synchronizes the Sophos Mobile Control and Sophos Mobile Security apps on the mobile device with Sophos Central. The device and the apps have to be active. For more information on check-in and sync, see Configure Compliance Rules (page 101).
- **AV Scan Now**: Scans the device immediately. This action is available only for Android devices that have the Sophos Mobile Security app installed and managed by Sophos Central. If the device is offline, it will be scanned when it is back online. The scan may take some time. When complete, you can go to **Logs & Reports** > **Events** to see any events resulting from the scan. You can see alerts about malware, PUAs or low reputation apps also on the **Dashboard** page.
- **Send Message**: Allows you to send a text message to the device. This action is not available when neither the Sophos Mobile Control or Sophos Mobile Security app is enrolled.
- **Unlock Device**: Unlocking a device removes the existing password protection on a device so that the user can set a new password. Unlocking works differently on iOS and Android:
  - On iOS devices, unlocking immediately unlocks the device and prompts the user to set a new password. Therefore it is necessary to notify the user in advance (for example, via a phone call), as the device will remain unprotected until a new password is set.
  - On Android devices, unlocking requires a password to be entered on the device. A password is automatically generated and sent to the user via email. The user is requested to unlock the device using that password and set a new one immediately.
- **Lock Device**: Enable the lock screen. The user will need the password that was set for the device in order to be able to use the device again. If no password was set, the lock screen will be enabled, but no password will be necessary.

- **Locate Device**: Locates the device and lets you view the location in Google Maps. This action is available only for devices that have the Sophos Mobile Control app installed and managed by Sophos Central. Also, the user must have "Locate" allowed on the device (you can use a compliance rule (page 101) to ensure this). It can take up to 10 minutes for the most accurate location of this device to be found. If, after 10 minutes, the device has not been located, it is possible that it is off-line or has no power.
- **Wipe Device**: Reset the mobile device to its factory settings. This action is available only for devices that have the Sophos Mobile Control app installed and managed by Sophos Central. Wiping involves the deletion of all user data, which is desirable if the device has been lost or stolen. The Sophos Central software is deleted as well, therefore the device will no longer be managed afterwards. However, it will remain in the list with the management status *wiped*, so that you get feedback that the wipe was successful. You can safely delete the device afterward.

  You can keep the device entry if you plan to re-enroll the device after it has been wiped. When Sophos Central recognizes the device during enrollment, it will update the status of the existing entry instead of creating a new device entry.

Device Summary

This section displays the following details:

- **Associated User**: The user the mobile device belongs to. There is only one user for a mobile device.
- **Management Status**: This shows the status of the Sophos Mobile Control app, or *n/a* if the app is not installed or managed by Sophos Central.
- **Security Status**: For Android devices, this shows the status of the Sophos Mobile Security app, or *n/a* if the app is not installed or managed by Sophos Central.
- **Rooting Status**: This shows if the device is jailbroken (for iOS devices) for rooted (for Android devices).
- **Compliance**: This shows if the device is compliant, according to the compliance rules that you have configured in the policies the device is assigned to. When the Sophos Mobile Control app is not managed by Sophos Central, a device is always shown as *compliant*.

Activity

This section displays the following details:

- **Last Active**: The time of the last check-in or synchronization that was performed.
- **Last Scan**: The last time the Sophos Mobile Security app scanned the device.
- **Last Threat Update**: The last time the Sophos Mobile Security app successfully updated its threat data.

Device Details

This section displays the following details:

- **Telephone Number**: This shows the device's telephone number, if it can be retrieved from the device. Whether the phone number can be retrieved depends on the device model and manufacturer.
- **Enrollment Date**: The time of the first synchronization after installation and configuration of the Sophos Mobile Control app.
- **IMEI / MEID / Device ID**: This shows the device's unique identifier, if it can be retrieved from the device. If the device runs on a GSM network, the IMEI is displayed. If the device runs on a CDMA network, the MEID is displayed. Whether the device identifier can be retrieved depends on the device model and mobile network operator. If the device identifier cannot be retrieved, "n/a" is displayed.
- **Location**: Displays the device's location, or shows if location is not currently available or locating the device is not allowed by the user. (See also the device action **Locate Device** in this topic.)

For Android devices, the following additional information may be shown:

- **Mobile Security App Version**: The status of the Mobile Security app on the device.
- **Samsung SAFE Info**: This shows if the device supports Samsung SAFE features, if these features can be managed by Sophos Central, and the version of Samsung SAFE on the device.
- **Unlock Password**: A temporary password generated when the device is unlocked.

10.2 Mobile Device Events

On the **Events** tab of a mobile device's details page, you can see a list of events related to the device.

These events are a subset of the events that are shown for the assigned user. See User Events (page 52).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

10.3 Mobile Device Status

On the **Status** tab of a mobile device's details page, you can see detailed status information for the device.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Alerts

This section displays all alerts associated with the device. These might be alerts created when malware, potentially unwanted apps (PUAs) or low reputation apps are detected on the device.

(The latter two alerts are displayed if you have enabled PUA and low reputation app detection in the policy). It also lets you take action against alerts. Available actions depend on the type of event and are the same as the actions available in the Dashboard.

Device Status

This section displays the following status information:

- **Activity Status**: This indicates if the device has recently synced with Sophos Central and shows details of the latest activity.
- **Compliance Status**: This indicates the compliance status of the device, according to the compliance rules that you have configured in the policies the device is assigned to, and lists all compliance violations.

  You can take actions against alerts. Available actions depend on the type of event and are the same as the actions available in the Dashboard.

  Note: Compliance violations are reported only if the mobile device is managed by the Sophos Central Mobile Device Management (MDM).

- **Mobile Security Status**: This indicates the security status of the device and lists all security violations. Reported security violations are:
  - The device is jailbroken or rooted.
  - Sophos Mobile Security threat data is outdated.
  - Malware apps are detected.
  - Suspicious apps are detected.
  - Potentially Unwanted Applications (PUA) are detected.

Note: Android does not allow Sophos Mobile Security to uninstall apps automatically, without the user's involvement. Therefore, automatic cleanup of detected threats or questionable apps is not available. You can send a text message to the device asking the user to uninstall the app. See Device actions (page 62).

10.4 Mobile Device Policies

On the **Policies** tab of a mobile device's details page, you can see the policies that are applied to the device.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Policies are not applied to a mobile device directly. Instead, they are applied to the user that is associated with the device.

The icons beside a policy indicate the security settings included in the policy. For a mobile device, only the **Mobile Device Management** and **Mobile Security Settings** parts of a policy are relevant.

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

11 Servers

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

11.1 Servers

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 VMware 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 belong 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 Sophos security VMs on VMware hosts.

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 67).

11.1.1 Server Summary

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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**.

Note: 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.

  Note: 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.

  Note: 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.

  Note: 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**.

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

- **Protected Guest VMs**. You see this only if the server is a host with a Sophos Security VM. It shows the number of guest VMs protected by the Security VM.
- **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.

  Note: A server can only be in one group.

- **Tamper Protection**. This shows whether tamper protection (page 137) is enabled on the server or not. Click **View Details** to manage the tamper protection password for the server.

11.1.2 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

11.1.3 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 Configure Threat Protection for Servers (page 114).

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

11.1.4 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

11.1.5 Server Policies

The **Policies** tab in a server's details page lets you see the policies that are applied to the server.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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

Note: 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.

11.2 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

About the groups list

The current groups are listed and the number of servers in each group is shown.

To see full details for a group, click on the group's name. For more information, see Server Group Summary (page 71).

Add a group

1. Click **Add Server Group** in the upper right of the page.
2. In the **Add Server Group** dialog:

   Enter a **Group name**.

   Enter a **Group description.**

   Select available servers and add them to the **Assigned Servers** list.

   Note: A server can only be in one group. If you select a server that's already in a group, it will be removed from its current group.

   Tip: In the **Search** box you can start typing a name to filter down the displayed entries.

3. Click **Save**.

Edit a group

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

Delete a group

To delete a group, select it and click **Delete** in the upper right of the page.

Deleting a group will not delete its servers.

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

11.2.1 Server Group Summary

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

- Add or remove servers.
- Delete the group.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

11.2.2 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.

Note: 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

12 Wireless

On this page you can configure and manage wireless access points for Sophos Central, 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Network requirements to run Sophos Wireless in Sophos Central

In order to use any access point with Sophos Wireless, the access point has to be able to communicate to Sophos Central. For a successful communication, 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.

12.1 Wireless Dashboard

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

The Dashboard is the overview page of the Sophos Central Wireless section and lets you see the most important information at a glance. It consists of the following areas:

- Access Points: Shows the number of registered Access Points and their current status.
- Alerts: Shows the number of High, Medium and Info wireless alerts. Click a number to see those alerts or click **View All Alerts** to see all alerts.
- Clients: Shows the number of clients connected to access points. You can choose to view the figures for a period of 24 hours or 7 days.
- Usage Insight: Shows the traffic generated by applications connected to access points. You can switch between a time range from 24h or 7d.

You can click **Details** in any pane to see the tab with the full details

12.2 Access Points

On this page you can view your registered 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. To do this you need the serial number, which is on the access point.

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 chapter SSIDs (page 77).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

The sections below tell you about the registered access point list and also how to:

- Delete an access point.
- View full details of an access point and manage it.

About the access point list

The registered access points are listed with these details:

- Name.
- Serial Number.
- Access point state. This is the current state of an access point (up to date, updating, waiting to delete and offline).
- Workload. This shows the current workload of the access point. The workload depends on the traffic generated by the connected clients and applications. The workload increases when the access point updates the firmware.
- Radios. Shows the radio frequency on which the access point is transmitting.

To search for a registered access point, enter the name in the search field above the list.

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.

Enter the serial number of the access point and click **Register**. The registration process can take up to 300 seconds. If registration is successful the access point is displayed in the list.

Note: If you do not have an access point registered or an SSID created in Sophos Central the wizard will automatically start when you go the wireless section.

Delete an Access Point

To delete an access point, select the access point and click **Delete**. You can delete several access points at the same time. The access point's state changes to "waiting to delete". It will stay in this

state until it is connects to Sophos Central. You can click **Force delete** to delete the access point immediately.

List of access points

Currently, Sophos Central provides the following dedicated access points:

Name	Standards	Band	FCC regulatory domain (mainly US)	ETSI regulatory domain (mainly Europe)
AP 15	802.11b/g/n	2.4 GHz	Channels 1-11	Channels 1-13
AP 55	802.11a/b/g/n/ac	2.4/5 GHz dual-band/dual-radio	Channels 1-11, 36-64, 100-116, 132-140, 149-165	Channels 1-13, 36-64, 100-116, 132-140
AP 55C	802.11a/b/g/n/ac	2.4/5 GHz dual-band/dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-64, 100-116, 132-140
AP 100	802.11a/b/g/n/ac	2.4/5 GHz dual-band/dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-64, 100-116, 132-140
AP 100C	802.11a/b/g/n/ac	2.4/5 GHz dual-band/dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-64, 100-116, 132-140

Sophos Central also provides the following dedicated outdoor access points:

Name	Standards	Band	FCC regulatory domain (mainly US)	ETSI regulatory domain (mainly Europe)
AP 100X	802.11a/b/g/n/ac	2.4/5 GHz dual-band/dual-radio	Channels 1-11, 36-64, 100-116, 132-140	Channels 1-13, 100-116, 132-140

12.2.1 Access Point

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

The page includes:

- Access point details
- Radio
- Channel
- Assign SSIDs

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Access point details

- **Name**: Shows the name of the access point. The standard name is a combination of the model and the serial number. You can change the name by clicking on the pen button.
- **Location**: Shows the country where the access point is currently located.
- **Serial number**: Shows the serial number of the access point. The serial number can be found on the access point.
- **IP address**: Shows the IP address of the access point.
- **Model**: Shows the model of the access point.

Reboot Access Point

You can manually reboot the access point by clicking the **Reboot Access Point** button.

Radio

Shows the frequency band of the access points. Depending on the access point 2.4 GHz and/or 5GHz are available.

TX Power: Either keep the default setting (100 %) for the access point to send with maximum power or reduce the power to reduce the operating distance, for example to minimize interference.

Channel

Either keep the default setting **Autochannel**, which will automatically select the least used channel for transmission, or select a fix channel.

Dynamic Background Channel Selection

If enabled the access point will automatically change the channel on a regular basis to optimize the network.

Assign SSIDs

Shows a list of available SSIDs to which the access point should broadcast. You can assign SSIDs to the access point. 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 SSID can have a maximum of 8 access points per band.

To add a SSID select the SSID from the list and enable the check box.

Tip: You can also add an access point to a network when you create a SSID.

Comment

Add a description or other information (optional).

Click **Save** to apply your changes.

12.3 SSIDs

On this page you can view your Service Set Identifier (SSID).

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

- Create a SSID.
- Delete a SSID.
- View full details of a SSID and manage it.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

About the SSID list

The current SSIDs are listed with these details:

- SSID: Shows the SSID for the network.
- Comment.
- Encryption mode: Shows the current encryption mode of the SSID.
- Bands: The access points assigned to this SSID will transmit on the selected frequency band(s). The 5 GHz band generally has higher performance, lower latency, and typically has less interference. This is recommended if the user uses VoIP.
- Status: Shows the current status of the SSID.

Create New SSID

To create a new SSID, click **Create** in the upper right of the page.

Delete a SSID

To delete a SSID, select the SSID and click **Delete**. You can delete several SSIDs at the same time. Click **Confirm** to delete selected SSIDs.

SOS SSID

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

The SOS SSID is comprised of an open wireless network named "sos" and the access point MAC address. After you connect 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 only available for a limited time frame for about 4 minutes. After the time frame, the access point reboots and the SOS SSID will be available again in about 1 or 2 minutes. When you are connected to an SOS SSID you have no access to the internet.

12.3.1 Create SSID

This help page describes how to setup a SSID and advanced settings.

- SSID Configuration (page 78)
- SSID Availability (page 80)
- MAC Filtering (page 80)
- Hotspot (page 80)

SSID Configuration

Click **Create** to create a new SSID and enter the following settings: (you can switch between **Basic Settings** and **Advanced Settings** which gives you more configuration options.)

- **SSID**: Enter the SSID for the network, which clients will see and use to identify the network. The SSID may consist of 1-32 ASCII printable characters. It must not contain a comma and must not begin or end with a space.
- **Encryption Mode**: Select an encryption mode from the drop-down list. We recommend that you select WPA2 rather than WPA, if possible. When using an enterprise authentication method, you also need to configure a RADIUS server on your local network. WEP is not recommended, because this encryption mode is insecure. Create a passphrase to protect the SSID from unauthorized access and confirm it in the next field. The passphrase must consist of 8-63 ASCII printable characters.
- **RADIUS Server** (only for Encryption mode: WPA/WPA2 Enterprise): Enter your IPv4 or hostname and your passphrase for authentication.
- **RADIUS Port** (only for Encryption mode: WPA/WPA2 Enterprise): Select the port for the RADIUS server.
- **Encryption Algorithm** (only available in Advanced Settings and with WPA2 encryption mode): Select an encryption algorithm which can be either AES or TKIP. For security reasons, it is recommended to use AES.

- **Frequency Band**: The access points assigned to this SSID will transmit on the selected frequency band(s). The 5 GHz band generally has higher performance and lower latency, and typically has less interference. Hence it should be preferred for VoIP communication, for example. For more information about which access point types support the 5 GHz band, see Access Points (page 74).
- **Band Steering** (only for Frequency Band: 2.4 GHz and 5 GHz): If enabled, the access point runs on the highest performance and detects clients capability of 2.4 GHz and 5 GHz frequency bands. The access point steers the clients to the frequency band with the best performance. This provides balance between the frequency bands and lowers the latency.
- **Assign Access Point**: Add an access point to the SSID. Select one or several access points from the list which shows the available access points. You can check in the list what frequency band the access points use, 2.4 GHz and/or 5GHz. Each SSID can have a maximum of 8 access points per band.

Optional advanced settings for SSID:

- **VLAN**: VLAN tagging is disabled by default. If you want to connect the access point with an existing VLAN Ethernet interface, you need to enable VLAN tagging by selecting the check-box.
- **RADIUS VLAN Assignment** (Only for Encryption mode: WPA/WPA2 Enterprise): If enabled, user will be tagged to a VLAN provided from a RADIUS server. This way you can separate user without creating multiple SSIDs. Select the default tag number for the RADIUS VLAN assignment.
- **Keep broadcasting when the access point is not connected to the cloud**: If enabled, the access point keeps broadcasting even if the access point is not connected to the internet or Sophos Central. Clients are still able to connect to the access point.
- **Enable mesh mode**: When you enable mesh mode, encryption mode WPA2-Personal will be set and a passphrase will be auto generated. When you add access points to the mesh network, one access point which is connected to the cloud becomes a root access point and the others become repeater access points. The mesh network is not visible for the end user. To get access for the end user you have to create a separate SSID and add access points as well as to the mesh network. Only one band is allowed when using mesh mode. Without a root access point the network is not useable. Repeater access points cannot be reached. Mesh access points will send STP packets. Therefore make sure this complies with your IT rules. In general, in a mesh network multiple access points communicate with each other and broadcast a common SSID. On the one hand, access points connected via a mesh network can broadcast the same SSID to clients, thus working as a single access point, while covering a wider area. On the other hand, a mesh network can be used to bridge ethernet networks without laying cables.

  Note: You can only enable the mesh mode if you create a new SSID and you can only have one SSID with mesh mode enabled. It is not possible to enable the mesh mode in an existing SSID.

- **Hidden SSID** (only available in Advanced Settings): If enabled, the SSID is hidden and cannot be seen. The SSID is still available but the user needs to connect directly. Even if a SSID is hidden you can assign the SSID to an access point. Please note that this is not a security feature and you still need to protect hidden SSIDs.
- **Client isolation** (only available in Advanced Settings): If enabled, clients within a network can not communicate with one another, for example in a guest network.

- **Multicast to unicast conversion** (only available in Advanced Settings): If enabled, the access point tunnels multicast/broadcast packets with unicast packets individually to each client. This approach is faster then multicast and is usefull when several clients are connected to one access point.
- **Fast roaming**: If enabled, SSIDs with WPA2 encryption use the IEEE 802.11r standard to reduce roaming times. Fast roaming between access points provides better a connection experience and also works with several access points which are assigned to different SSIDs. Clients also need to support the IEEE 802.11r standard.
- **Enable Guest Network** (only available in Advanced Settings): If enabled, the SSID connects only to DHCP/DNS server and the internet. Guest user can not reach any internal networks. Choose between two client addressing: the **Bridge Mode** extends the bridged VLANS to the guest user and the **NAT Mode** provides a separate network for the guest user. For the client addressing in NAT mode you need to provide a primary and secondary DNS server.

SSID Availability

You can define SSIDs which are only available for a certain time of a day or certain days in a week. The SSIDs are not visible and are not able to connect with in the meantime. Click **Scheduled** and define the days, the time and the time zone in which the SSID is available.

MAC Filtering

To restrict the MAC addresses allowed to connect to this SSID. Select Blacklist or Whitelist and enter the MAC addresses. With Blacklist, all MAC addresses are allowed except those listed on the MAC address list selected below. With Whitelist, all MAC addresses are prohibited except those listed on the MAC address list selected below.

Hotspot

Click **Enable Hotspot** to turn a SSID into a hotspot. The Hotspot feature 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.).

After you enabled the hotspot function you need to configure the landing page. The landing page is the first page the user will see after connecting to the hotspot.

- **Page Title**: Enter a page title for the landing page.
- **Welcome text**: Enter a welcome text for the landing page.
- **Terms of Service**: Enter the terms of service the user needs to agree before he can connect with the hotspot.

Under **Redirected URL**, select the URL to which the users will be redirected from the landing page. Choose **Redirect to original URL** if user should be redirected to the default website of the mobile device or select **Custom URL** to redirect user to a specific website of your choice. For example, your company page.

Select a authentication type to define how the user is getting access to the hot spot:

- **Backend Authentication**: With this authentication type, the user 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 connection via Sophos Central.

- **Daily Password**: A new password will be created automatically once a day. Select timezone and time of the day at which the new password will be created. At this time the former password will immediately get invalid and current sessions will be cut off. The daily password will be sent as notification to the specified email addresses. You can send a notification to all admin by default when you select **Notify all admins**.
- **Voucher**: With this hotspot type, vouchers with different limitations and properties can be generated, printed and given to customers. After entering the code, the user can directly access the internet. Click **Create Voucher** to define an new voucher. Here you can define the limitations and properties like access time, state date and validation time. You can also choose the amount of vouchers on the PDF output. The PDF output shows all interesting data for the user and shows what to do.

  Note: The authentication type **Voucher** is only available when the SSID already exits and cannot be selected while creating a SSID. You need to save the new SSID fist and select the authentication type afterwards.

12.4 Clients

On this page you can view the clients that are currently connected to an access point on a graph. On a second part of the graph you can view the clients that have poor signal strength.

You can switch between a time span of **24 hours** or **7 days**, and a frequency band of **2.4 GHz and 5 GHz**, **2.4 GHz** or **5 GHz**.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

About the clients list

The clients are listed with the following details:

- Signal: Shows the quality of the connection from the client to the access point.
- Name: Shows the clients connected to the SSID.
- MAC: Shows the clients MAC address.
- IP: Shows the clients IP address.
- Vendor: Shows the vendor of the client and gives information about the device the client uses.
- Access point: Shows the access point the client is connected to.
- SSID: Shows the wireless network.
- Connection speed: Shows the download/upload rate in megabits per second.
- Band.

Note: You can switch between clients which are **Online**, **Offline** or **Online and Offline**.

12.5 Usage Insight

On this page you can view the traffic on your clients. The traffic is listed in different categories such as search engines, social media or advertisements, for example.

You can switch between the categories and a time span of **24 hours** or **7 days**.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

About the usage insight list

The application clients are listed with these details:

- Category: Shows the category of the traffic generated by the users.
- Total: Shows the total amount of traffic in a specific category.
- Download: Shows the download rate in megabits per second.
- Upload: Shows the upload rate in megabits per second.

If you click on a category you can receive 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 under **Usage Insight settings** in Settings (page 84).

12.6 Sites

On this page you can view the locations of your access points. To have a better overview of all your access points around the world you can put them on a Google map.

The sections below tell you about sites and also how to:

- Create a site
- Create a floorplan

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Site

Coordinate the access points to a specific location on Google maps. For information on how to add a site, see Create a Site (page 83).

Access Points

The site overview shows every access point which is assigned to the selected site. The list provides specific details like health, number of clients and workload.

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:

- Sanctioned: Access point that belongs to the customer network.
- Unsanctioned: Access point that does not belong to the customer network.
- Rogue: Unsanctioned access point that is connected to the customer secured wired network.
- SSID Impersonate: Access point that spoofs the network name of the access point that belongs to the customer.
- BSSID Impersonate: Access point that spoofs the hardware address of the access point that belongs to the customer.
- Evil Twin: Access point that spoofs the network name and the hardware address of the access point that belongs to the customer.
- Advanced AP Impersonate: Access point that spoofs the network name and unique protection code of the access point that belongs to the customer.

Every access point scans for neighborhood SSIDs once during the booting process. For example, when you reboot the access point or install a new firmware update. If you activate the access points dynamic background channel selection, the access point will scan for neighborhood SSIDs on a regular basis. For information on reboot the access point and dynamic background channel selection, see Access Point (page 75)

Floorplan

If you added a site for your access points you can use building floorplans to set detailed locations for the access points. You need the floorplan as an image file (supported file types are: PDF, PNG, JPEG, BMP, GIF and WBMP). The file must be smaller than 1 MB. For information on how to add a floorplan, see Create a Floorplan (page 84).

12.6.1 Create a Site

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

1. Click **Create**.
2. Enter the following settings:
   a) **Site name** Enter the name of the site. For example city or company name
   b) **Site location** Enter the exact address of the site.

   Tip: Sophos Central uses Google maps. You must enter a real address.
3. Select the access points from the list or search for it.
4. Click **Save**

The site appears on the list and on the Google map.

12.6.2 Create a Floorplan

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

1. Select a site.
2. Click on **Create a floor**
3. Click **Choose a file** and select the floorplan.

   Note: You need the floorplan as an image file (supported file types are: PDF, PNG, JPEG, BMP, GIF and WBMP). The file must be smaller than 1 MB. You can also use drag and drop to add the floorplan.

4. Click on **Upload** to upload the floorplan to Sophos Central.
5. Use the grid pattern to cut the image and click **crop image**. This can be useful if the image has a lot of white space or you only want a specific area from the image as floorplan.

   Note: Click **proceed without changes** if you want to have the image in the original size.

6. Assign the dimensions.

   Measured dimensions are required to correctly show the network range of access points. Select a location on the floorplan where you know the measured dimensions. For example the distance between two walls. Place two pins on the floorplan and drag them to start and end points of your measured dimension.

7. Set the distance in meters and click **Done**.
8. Drag and drop a access point from the **available** tab and place it on the floorplan.

   Note: You can always move or delete an access point from the floorplan from the **placed** tab.

9. Click **Save**.

The floorplan with the positions of the access points has been added to the site.

12.7 Settings

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Firmware Update

The Firmware section shows the currently installed firmware.

You schedule firmware updates by selecting the frequency and time. You can choose from the following frequencies: daily, weekly, monthly.

Diagnose settings

- **Forward access points logs**: If this is enabled, your access points logs will be forwarded to Sophos technical support.

- **Remote Login for Sophos Support**: If this is enabled, Sophos technical support will have remote access.

Usage Insight settings

If this is enabled, the traffic generated by the user will be categorized and listed in Usage Insight (page 82). This option is enabled by default.

13 Mailboxes

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Email Security provides protection against spam. Set up Email Security, if you have not already done so, see Set up Email Security (page 150).

On the Mailboxes page you can manage Email Security for users, distribution lists and public folders. All protected mailboxes are listed.

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.

13.1 Mailbox

Each mailbox has a set of information associated with it such as name, type, policies or owner. 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Details

You can view the policies, members 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 for a user. A list of aliases is only displayed for a User Email mailbox.
- **Owner**: This is the person that controls the distribution list or public mailbox. An owner is only displayed for distribution list and public folder mailboxes.
- **Members**: This is a list of the email addresses associated with the mailbox. A list of members is only displayed for distribution list and public folder mailboxes. If you are the owner of the mailbox you can block members.

  Tip: Click on an email address in the **Members** list to view the details for that user.

14 Policies

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

Users and servers have separate policies.

To find out how policies work and how you can use them to customize security settings for different users or servers, see About Policies (page 88).

For detailed information on setting up policies, see User Policies (page 90) or Server Policies (page 112).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

14.1 About Policies

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

What is a policy?

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

Users and servers have separate policies.

What is the Base policy?

The Base policy is the default policy. Sophos provide it and configure it with the best practise settings. The Base policy applies to all users (or servers) initially. You can leave it unchanged or edit it to suit your needs.

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 servers), you can simply use the Base policy or adapt it for your needs.

If you want to use different settings for different groups of users or servers, 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 or servers. You can also use them to make it easier to switch the settings applied to users or groups quickly.

The order in which you put the policies on the page matters, as this decides the priority given to a policy. See “How do you prioritize policies?" below.

What is in each policy?

A policy lets you:

- Configure one or more of the features that you have licensed, such as threat protection.
- Specify which users (or servers) the policy applies to.
- Specify whether the policy is enabled and whether it expires.

Each policy for workstations or servers contains all the settings for a 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.

Note: The features for mobiles have sub-features, such as Exchange email settings or Wi-Fi settings, that are treated separately. So a user can get their Exchange email settings from one policy and their Wi-Fi settings from another.

How do you prioritize policies?

The order in which you arrange the policies determines which settings are applied for each security feature.

To find the policy to apply for a user, Sophos Central looks through the policies from the top down. The first policy that applies to that user and includes settings for a feature (such as malware protection), will be applied for this feature.

The settings for another feature might be taken from another policy. Sophos Central will search again for the first policy that applies to that user and includes that feature.

The Base Policy is always at the bottom, and therefore applied last.

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.

Example: Using two policies

In a simple scenario, you might want to use different threat protection settings for one user or group of users.

You can create a new policy, customize the settings for threat protection, and apply the policy to selected users.

When Sophos Central applies policies to those selected users, it will:

- Check the new, additional policy first.
- Find the threat protection settings in the additional policy and apply them to the selected users.
- Check the basic policy.
- Find the settings for the other features, such as Peripheral Control, and apply them to the selected users. The threat protection settings in the Base policy are ignored because the settings in the additional policy have already been used.

Other users, who are not covered by this additional policy, will get all their settings, for threat protection and for the other security features, from the Base policy.

Example: Using three policies

Assume that you have three policies, Base Policy, Policy A and Policy B, and that:

- Policy A and Policy B are both assigned to a user.
- Policy A is the higher one in the policies list.
- Policy A specifies threat protection. It also specifies the Exchange email settings for mobiles.
- Policy B specifies threat protection and peripheral control. It also specifies the Wi-Fi settings for mobiles.

In this case, the settings for threat protection and Exchange email are taken from Policy A, settings for peripheral control and Wi-Fi are taken from Policy B if specified there. This is shown in the table.

Policy	Threat Protection	Peripheral Control	Exchange Email Settings	Wi-Fi Settings
Policy A	Yes	No	Yes	No
Policy B	Yes	Yes	No	Yes
Base Policy	Yes	Yes	Yes	No
Policy that is applied:	**Policy A**	**Policy B**	**Policy A**	**Policy B**

14.2 User Policies

User policies define the security measures that will be used for your users' devices.

If you're new to policies, see About Policies (page 88).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

On the **User Policies** page, you can view, add, and edit policies.

View a policy

In the policies list, you can see:

- Whether a policy is enabled or not. If it is enabled, the settings in the policy are enforced on users.
- Which security features, for example threat protection, are included in the policy.

To see which users the policy applies to, and which options have been set, click on the policy name.

Add a policy

To add a new policy, do the following:

1. Click the **Add Policy** button above the Policies list.
2. Enter a name for the new policy.
3. Select available users or groups the policy should apply to.

   Tip: To switch between the list of users and the list of groups, click the tabs above the **Available** and **Assigned** lists.

4. Enable or disable this policy. By default, you see **Policy is Enabled**. Click on this tab to see the options. You can:
   - Disable the policy if you want to preconfigure the policy now and activate it later.
   - Set an expiry date if the policy needs to be deactivated automatically in future
5. Configure the features in the policy. Click on a tab, e.g. Threat Protection, and enter your settings. For information on specific features, see the other pages in this section of the Help.

   Note: You can open tabs in any order.

6. When you have finished setting options, click **Save**.

Edit a policy

To edit a policy:

1. In the policies list, click on a policy name .

   The **Edit Policy** page is displayed.

2. Select the tab for the feature that you want to edit.

   Tip: You can open panels in any order to edit them.

3. When you have finished your edits, click **Save**.

Delete, disable, clone or reset a policy

You can make changes to a policy with the action buttons in the upper right of the page. The actions available depend on the policy you select.

- **Enable** or **Disable**. Enabling a policy makes it active so that it is applied to users or servers.

  Note: You can disable any active policy except for the Base Policy.

- **Clone**. This creates a copy of the policy.This is useful if you need a similar policy and do not want to configure it from scratch.
- **Delete** You can delete any policy except the Base Policy. If you try to delete an active policy, you are asked to confirm.
- **Reset** This is only available with the Base Policy. You can reset the Base Policy to its initial configuration if you want to revert changes.

Action buttons that cannot be applied on a certain policy are grayed out.

14.2.1 Configure Threat Protection

Attention: This help page describes policy settings for workstation users. Different policy settings apply for servers (page 114).

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can configure this feature if you create or open a user policy and click the **Threat Protection** tab.

You can either use the recommended settings or change them. If you want to change them, you can configure these options, which are described in detail below:

Enable Threat Protection

Ensure **Threat Protection** is enabled.

Tip: You can disable this option any time if you want to stop enforcing this part of the policy.

Use Recommended Settings

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

If we change our recommendations in future, we'll automatically update your policy with new settings.

The recommended settings offer:

- Detection of known malware.
- In-the-cloud checks to enable detection of the latest malware known to Sophos.
- Proactive detection of malware that has not been seen before.
- Automatic cleanup of malware.

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 43).

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.

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. In the **Value** text field, enter the desired entry. 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.

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**.

14.2.2 Configure Peripheral Control

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

You can configure this feature if you create or open a user policy and click the **Peripheral Control** tab.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Enable Peripheral Control

Ensure **Peripheral Control** is enabled.

You can disable this option any time if you want to stop enforcing this part of the policy.

Manage Peripherals

In Manage Peripherals, select how you want to control peripherals:

- **Monitor but do not block**. If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you cannot set access rules for them.
- **Control access by peripheral type and add exemptions**. If you select this, you can go on to set access policies for peripheral types and for individual detected peripherals.

Set Access Policies

Set access policies in the table.

The table displays detected peripheral types, the number of each type detected, and the current access policy.

Note: The totals include all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent policies for all devices.

Note: The **MTP/PTP** category includes devices such as phones, tablets, cameras and media players that connect using the MTP or PTP protocols.

For each peripheral type, you can change the access policy:

- **Allow**: Peripherals are not restricted in any way.
- **Block** : Peripherals are not allowed at all.
- **Read Only**: Peripherals can be accessed only for reading.

Note: The Bluetooth, Infrared, and Modem categories do not have the **Read Only** option.

Note: The Wireless Network Adaptor category has a **Block Bridged** option. This prevents bridging of two networks.

Peripheral Exemptions

Click the **Peripheral Exemptions** fold-out if you want to exempt individual peripherals from the control settings, or apply less restrictive controls.

1. Click **Add Exemptions**.
2. In the **Add Peripheral Exemptions** dialog, you'll see a list of detected peripherals.

   Note: Peripherals are detected when you are in monitoring mode or if there is an access restriction for that type of peripheral.

   Note: This list shows all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent exemptions for all devices.

3. Select a peripheral.
4. In the **Policy** column, you can optionally use the drop-down list to assign a specific access policy to an exempt peripheral.

   Restriction: Do not set a stricter access policy for an individual peripheral than for its peripheral type. If you do, the setting for the individual policy is ignored and a warning icon is displayed beside it.

5. In the **Enforce by** column, you can optionally use the drop-down menu to apply the policy to all peripherals of that model or to ones with the same ID (the list shows you the model and ID).
6. Click **Add Exemption(s)**.

14.2.3 Configure Application Control

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.

You can configure this feature if you create or open a policy and select **Application control**.

Note: If you want to use application control, ensure that the Threat Protection feature is also enabled in the policy.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

We recommend that you detect the applications being used on your network and then decide which to block, as follows.

1. Ensure **Application Control** is enabled.

   Tip: You can disable this option any time if you want to stop enforcing this part of the policy.

2. 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.

3. Click an application category, for example **Browser Plugin**.

   A full list of the applications in that category is displayed in the right-hand table.

4. We recommend that you select the option **Select all applications**. You'll refine your selection later.
5. 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.

6. 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.

7. Allow time for all your computers to run a scheduled scan.
8. Go to the **Logs & Reports** > **Events** page.
9. 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.

10. Return to your policy page.
11. 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**.

12. 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.

14.2.4 Configure Mobile Device Management

The mobile device management policy allows you to manage the Sophos Mobile Control app on mobile devices—smartphones and tablets. Sophos Mobile Control helps you to keep corporate data safe by managing apps and security settings. It allows configuration and software distribution as well as many other device management operations on mobile devices.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can configure this feature if you create or open a user policy and click the **Mobile Device Management** tab.

1. Choose the sub-features you want to specify settings for in the policy you are working on. These sub-features might be, for example, Disable/Hide Feature Access, Exchange Email Settings or Wi-Fi Settings.
2. Specify settings for each sub-feature as described on the following pages.

14.2.4.1 Configure Password Policy

A mobile device can be locked by the user or also remotely by you as Sophos Central administrator. In order to be able to lock a device effectively, the user must set a password.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To ensure that users do not set weak passwords, use the following settings:

1. **Password complexity:**

   The following choices are available:

   - **PIN**: Passwords may only contain numbers; using repeated numbers or sequences (1234, 4444, 9876,...) is not allowed.
   - **Alphanumeric**: Passwords must contain characters between a-z or A-Z as well as numbers.
   - **Complex**: Passwords must contain characters as well as numbers and at least one special character (%, &, $,...).
   - **None**: There are no restrictions, passwords may contain characters, numbers and/or special characters.

2. **Minimum Password length**: The minimum number of digits or characters a password must have.
3. Click **Advanced** for more options for password settings.

4. **Maximum number of login attempts**: The user can try to enter the password as many times as specified here.

Warning: If the user has no more attempts to enter the password left, the device will wipe itself. All data will be lost. The reason is that we assume that the device has been stolen. If the password has just been forgotten, you can unlock the device on the details page for a mobile device. For more information, see Mobile Device Details (page 61).

5. **Maximum password age (days)**: After the period of time specified here the user will be asked to change the password. The new password must not match the one that has been used before.
6. **Maximum auto lock (minutes)**: Auto lock means that after a period of time the device will lock itself, if there has been no user interaction. The user can unlock it by entering the password. The actual value for the auto lock can be changed by the user, but it cannot exceed the period of time specified here. For example, you can set the value to 15 minutes, but the user can choose to set it to 5 minutes instead.

14.2.4.2 Configure Device Features

Enable **Device Features** to disable or hide access to certain features on all mobile devices.

Some restrictions are not available on all mobile platforms. This is due to functionality differences between iOS and Android. The icons beside each restriction show which platforms it is for.

Note: When you see the Android icon, you can hover over it to see which specific Android devices the restriction is for.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

The following features can be restricted:

1. **App Store**: If you select this, the App Store can no longer be used on the device.
2. **Camera**: If you select this, the camera can no longer be used on the device.
3. **Taking screenshots**: If you select this, the user will no longer be able to take screenshots on the device.
4. **Native browser**: If you select this, the user will no longer be able to use the native browser (for example Safari) for surfing the Internet.
5. **Sending diagnostics data to device vendor**: If you select this, the device will no longer send diagnostics data about app crashes to Apple, Samsung or LG.
6. **Backup to iCloud**: If you select this, backup to iCloud will no longer be possible on the device.
7. **Touch ID usage to unlock device**: If you select this, fingerprint recognition cannot be used on the device.
8. **Sharing docs from managed to unmanaged accounts or apps**: We recommend that you select this option. Otherwise sensitive company data might be disclosed.
9. **Sharing docs from unmanaged to managed accounts or apps**: We recommend that you select this option. Otherwise malware or unwanted content might find its way into the company network.
10. **Control center/Widgets on lock screen (e.g. Wi-Fi, Volume, Bluetooth...)**: We recommend that you select this option. Otherwise settings such as Wi-Fi or Bluetooth might be displayed on the lock screen. It is not necessary to know the password and unlock the device in order to carry out changes of these settings.

11. **Notifications on lock screen (e.g. SMS, emails, calls...)**: We recommend that you select this option. Otherwise messages or missed calls might be shown on the lock screen. It is not necessary to know the password and unlock the device in order to read this information.

14.2.4.3 Configure Email

Enable **Email** to add Exchange email settings to the policy. These settings configure access to corporate Exchange email servers. When you assign the policy to your users, email access on their devices is automatically configured.

You must configure Exchange email settings before you can assign them to a policy. See Exchange Settings (page 145).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

- To add an Exchange email setting to the policy:
- Select a setting in the **Available Settings** list and then click the **>** button to move it to the **Selected Settings** list. Or click **>>** to move all available settings to the **Selected Settings** list.

  Tip: You can also double-click a setting to move it from one list to the other.

After the policy is assigned to a user, all Exchange email settings in the **Selected Settings** list are applied to the user's mobile devices.

14.2.4.4 Configure Wi-Fi

Enable **Wi-Fi** to add Wi-Fi settings to the policy. These settings configure the connection of mobile devices with Wi-Fi networks. When you apply the policy to your users, the Wi-Fi networks are automatically configured on their devices.

You must configure Wi-Fi settings before you can assign them to a policy. See Wi-Fi Settings (page 146).

Important: Your assigned adminstrator role affects what you can do, see Administration Roles (page 134).

- To add a Wi-Fi setting to the policy:
- Select a setting in the **Available Settings** list and then click the **>** button to move it to the **Selected Settings** list. Or click **>>** to move all available settings to the **Selected Settings** list.

  Tip: You can also double-click a setting to move it from one list to the other.

After the policy is applied to a user, all Wi-Fi settings in the **Selected Settings** list are applied to the user's mobile devices.

14.2.4.5 Configure Compliance Rules

Users might connect mobile devices to the company network that do not meet essential security criteria. As administrator, you want to be notified, and maybe you also want to exclude the devices from receiving email or even from network access.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To configure compliance rules, enable **Compliance**. Then select the respective checkbox on the left, if you want to get notified, and select the respective checkboxes in the columns on the right, if you also want to remove email or Wi-Fi settings.

You can configure the following compliance settings:

1. **Jailbroken or rooted device:** Choose your settings for devices that are jailbroken or rooted. Jailbroken or rooted devices are devices modified to allow extended access to OS functionality not intended by the originator. This may expose a high security risk.
2. **Overdue check in:** Choose your settings for devices that have not checked in recently. A check-in synchronizes the iOS built-in mobile device management (MDM) and the Sophos Mobile Control app on Android with Sophos Central. This will be done each time the device restarts and every 24 hours (if the device is not turned off).
3. **iOS version too low:** Choose your setting for devices with an iOS version that is too low. This will be relevant for example if there are known security issues in older iOS versions.
4. **iOS version too high:** Choose your setting for devices with an iOS version that is too high. This might be relevant if you use custom apps that have not been tested or are not running on a newer iOS version.
5. **Android version too low:** Choose your setting for devices with an Android version that is too low.
6. **Android version too high:** Choose your setting for devices with an Android version that is too high.
7. **Overdue sync:** Choose your setting for iOS devices on which the Sophos Mobile Control app has not synchronized recently. A sync synchronizes the Sophos Mobile Control app on iOS with Sophos Central. This will be done each time the app is started and every 24 hours (if the app is active). Data exchanged include model, OS version and jailbreak detection status.
8. **Sideloading:** Choose your setting for Android devices that allow the sideloading of apps. "Sideloading" is a setting on Android devices that, when activated, allows the user to install apps from sources other than the Google Play Store (.apk-files, other store apps). Installing apps from sources other than the Google Play Store exposes higher security risks.
9. **Disabled location data:** Choose your setting for iOS devices on which locating the device is not allowed. The "Locate" feature in Sophos Central will only work if you ensure that users have allowed the Sophos Mobile Control app to locate their device.
10. **Security risks:** Choose your setting for devices with the mobile security status showing that the device is at risk (for example, when the status is red).

14.2.5 Configure Mobile Security for Android

The Sophos Mobile Security app can protect Android phones and tablets (running Android 4.0 or later) against malicious apps and other threats.

You can use it either with or without Sophos Mobile Device Management (MDM).

By default, Sophos Mobile Security scans the mobile device for malicious apps and checks whether the device is rooted. You can also configure it to detect potentially unwanted and low reputation apps, and malicious websites, as described below.

Note: To use Sophos Mobile Security, users must enroll their device.

- If you're already using the MDM policy, and the Sophos Mobile Control app is installed on the device, you don’t need to do anything. The enrollment will be done automatically.

- If you're not using MDM, go to the **People** > **Users** page and send users a setup link that enables them to enroll their device.

Note: If you don't want to apply a mobile security policy to all your Sophos Central users, disable mobile security in the Base policy, and then set up a new policy and apply it only to users who will be using it. If the number of your Sophos Central users exceeds your Sophos Mobile Security license limit, you must do this to ensure that your usage doesn't exceed the license limit.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can configure Mobile Security if you create or open a user policy and click the **Mobile Security Settings** tab.

1. Ensure **Mobile Security** is enabled.

   You can disable this option any time if you want to stop enforcing this part of the policy.
2. Specify settings for Scanning (page 103).
3. Specify settings for Allowed Apps (page 104). These are apps that you want your users to have.

14.2.5.1 Configure Scanning

Sophos Mobile Security scans the mobile device for malware and reports any malicious apps. It automatically scans apps when they are installed. In addition, you can schedule scanning of the entire device, including system apps, SD cards and external USB devices, as well as configure scanning for potentially unwanted apps (PUA) and low reputation apps.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Under **Scanning**, the following features can be configured:

1. **Enable scheduled scan every**: If you select this and also select a time interval, a scheduled scan of the entire device will be performed.
2. **Detect potentially unwanted applications**: If you select this, the Sophos Mobile Security app will detect potentially unwanted applications (PUAs) during scans and notify the device user. The user can choose to allow a detected PUA.

   An event will be logged in the Sophos Central Admin console when a PUA is detected and when a detected PUA is uninstalled by the user.

   Note: PUAs are apps that, while not malicious, are generally considered unsuitable for business networks. The major PUA classifications are adware, dialer, system monitor, remote administration tools and hacking tools. However, certain apps that fall into the PUA category might be considered useful by some users.
3. **Detect low reputation applications**:If you select this, the Sophos Mobile Security app will detect low reputation apps during scans and notify the device user. The user can choose to allow a detected low reputation app.

   An event will be logged in the Sophos Central Admin console when a low reputation app is detected and when a detected low reputation app is uninstalled by the user.

   Note: Sophos calculates an app's reputation based on its source, age, prevalence, and feedback on its trustworthiness.
4. **Include SD cards and external USB devices in scans**: If you select this, all Android apps and files on those devices will be checked.

5. **Monitor files on the SD card**: If you select this, Sophos Mobile Security scans all new apps and files that are written to the SD card or USB storage devices.

   For all newly attached storage devices a scan is initiated automatically.

14.2.5.2 Configure Allowed Apps

Enable **Allowed Apps** to add allowed apps to the policy. These are apps that users are allowed to use and are not reported during a mobile device scan.

You must configure allowed apps before you can assign them to a policy. See Allowed App Settings (page 152).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To add an allowed app to the policy:

1. Select an app in the **Available Apps** list and then click the **>** button to move it to the **Selected Apps** list. Or click **>>** to move all available apps to the **Selected Apps** list.

   Tip: You can also double-click an app to move it from one list to the other.

After the policy is assigned to a user, all apps in the **Selected Apps** list are not reported during scans of the user's mobile devices.

14.2.6 Configure Web Control

You can configure this feature if you create or open a user policy and click the **Web Control** tab.

Note: If you enable web control in a policy you created, options which you don't configure will be handled by the next policy that applies and has web control enabled.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Enable Web Control

Ensure **Web Control** is enabled.

Tip: You can disable this option any time if you want to stop enforcing this part of the policy.

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.

14.2.7 Configure 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To use Web Gateway:

1. Create or edit a user policy and click the **Web Gateway** tab.
2. Configure the Web Gateway settings (all are described below).
3. Install the Sophos Web Gateway agent on devices. See the **Protect Devices** page.

You can configure any of the following options.

Enable Web Gateway

Click **Web Gateway** to include the web gateway settings in the policy and enforce them on users.

Tip: You can disable this option any time if you want to stop enforcing this part of the policy.

Web Filtering by Categories

Use this to control which websites your users are allowed to visit. You can set options for security categories or productivity categories.

Security Categories

Use this section to configure access to websites that are known to be high-risk. You can choose these options:

- **Block risky downloads**: This will block all high-risk websites.
- **Block**: This blocks all traffic categorized as security.
- **Custom**: Lets you choose which categories you want to Allow, Audit, Warn or Block. (page 109)

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. (page 109)

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. (page 109)

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 Audit, Warn or Block (page 109) 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).

14.2.8 Configure Email Security

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 150).

You use the Email Security settings in the Base user policy to configure spam protection.

Important: Spam protection applies to all protected mailboxes by default. You must review the settings to check that they are appropriate.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To configure spam protection:

1. Edit the Base policy and click the **Email Security** tab.
2. Configure the Email Security settings (as described below).
3. Click **Save**.

If you're new to policies, see About Policies (page 88).

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, see Managing Quarantined Email (page 151).

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.

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.

14.2.9 Configure 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Encryption is set up as follows:

1. The Device Encryption agent is installed on computers automatically when you use the standard Windows agent installer (if you have the required license).
2. You enable encryption in a policy and apply the policy to users.
3. Computers are encrypted when those users log in.

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.

Enable encryption

To manage BitLocker Drive Encryption on computers, you need to enable the function in the base policy or create a separate Device Encryption policy.

Note: If you want to enable Device Encryption for some users only, you need to create a separate Device Encryption policy and apply it to specific users.

A computer will be encrypted as soon as one of the users the policy is applied to logs in. It will stay encrypted even if a different user who is not included in the policy logs in.

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 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.

14.3 Server Policies

Server policies define the security measures that will be used for your servers.

If you're new to policies, see About Policies (page 88).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

On the **Server Policies** page, you can:

- See policy details (page 113)
- Add a policy (page 113)
- Edit a policy (page 113)
- Delete, disable, clone or reset a policy (page 114)

See policy details

In the policies list, you can see:

- Whether a policy is enabled or not. If it is enabled, the settings in the policy are enforced on servers.
- Which security features, for example threat protection, are included in the policy

To see which servers the policy applies to, and which options have been set, click on the policy name.

Add a policy

To add a new policy, do the following:

1. Click the **Add Policy** button above the Policies list.
2. Enter a name for the new policy.
3. Select servers the policy should apply to.
4. Enable or disable this policy. By default, you see **Policy is Enabled**. Click on this tab to see the options. You can:
   - Disable the policy if you want to preconfigure the policy now and activate it later.
   - Set an expiry date if the policy needs to be deactivated automatically in future
5. Configure the features in the policy. Click on a tab, e.g. Threat Protection, and enter your settings.

   Note: For information on specific features, see Configure Threat Protection for Servers (page 114) and Configure Server Lockdown (page 124).
6. When you have finished setting options, click **Save**.

Edit a policy

To edit a policy:

1. In the policies list, click on a policy name.

   The **Edit Policy** page is displayed.
2. Select the tab for the feature that you want to edit.

   Tip: You can open tabs in any order to edit them.
3. When you have finished your edits, click **Save**.

Delete, disable, clone, or reset a policy

You can manage a policy using the action buttons in the upper right of the page.

- **Enable** or **Disable** Enabling a disabled policy makes it active so that it is applied in your network.

  Note: You can disable any active policy except for the Base Policy.

- **Edit** Click this button to edit the settings of a policy. You can change every aspect of the configuration.
- **Clone** This is useful if you need a similar policy and do not want to start configuring from scratch.
- **Delete** You can delete any policy except for the Base Policy. When you try to delete an active policy, you need to confirm a warning message first.
- **Reset** This is only available with the Base Policy. You can reset the Base Policy to its initial configuration if you want to revert changes made on that policy.

Action buttons that cannot be applied on a certain policy are grayed out.

14.3.1 Configure Threat Protection for Servers

Attention: This help page describes policy settings for servers. Different policy settings apply for workstation users (page 92).

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can configure this feature if you create or open a server policy and click the **Threat Protection** tab.

You can either use the Recommended settings (page 115) or change them

If you want to change the settings, you can configure:

- Real-time scanning (Local files and network shares). (page 115)
- Real-time scanning (Internet) (page 115)
- Real-time scanning (Options) (page 116)
- Scheduled scanning. (page 116)
- Scanning exclusions. (page 117)

Note: Some options are only for Windows servers. The columns on the right of the page show you which server type each option is for.

Enable Threat Protection

Ensure **Threat Protection** is enabled.

Tip: You can disable this option any time if you want to stop enforcing this part of the policy.

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 (page 117) 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.

Note: This option may not be available for all users yet.

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. For full details of wildcards and variables you can use, see Windows Scanning Exclusions: Wildcards and Variables (page 118) or Virtual Server Scanning Exclusions: Wildcards (page 121).

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

   The Add Scanning Exclusiondialog 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. In the **Value** text field, 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 Scanning Exclusions for Specific VMs (page 123)
   - **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.

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**.

14.3.1.1 Windows Scanning Exclusions: Wildcards and Variables

Attention: This help page describes policy settings for servers. These settings do not apply to workstations.

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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Wildcards

You can use the wildcards shown in this table.

Note: Only * and ? can be used on Windows Server 2003.

Token	Matches	Comments
***** (Star)	Zero or more of any character except \ or /	
****** (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.	
. (Period)	A period OR the empty string at the end of a filename, if the pattern ends in a period and the filename does not have an extension.	Note that: ▪ ***.*** matches all files ▪ ***.*** matches all files without an extension ▪ "foo." matches "foo" and" "foo."

Examples

Here are some examples of the use of wildcards.

Expression	Interpreted as	Description
foo	**\foo	Exclude any file named foo (in any location).
foo\bar	**\foo\bar	Exclude any file named bar in a folder named foo (in any location).
*.txt	***.txt	Exclude all files named *.txt (in any location).

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

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.

Variable	Windows Server 2008 + later	Windows Server 2003
%allusersprofile%	C:\ProgramData	C:\Documents and Settings\All Users
%appdata%	C:\Users*\AppData\Roaming	C:\Documents and Settings*\Application Data **Note:** Does not work for real-time scanning.
%commonprogramfiles%	C:\Program Files\Common Files	C:\Program Files\Common Files
%commonprogramfiles(x86)%	C:\Program Files (x86)\Common Files	C:\Program Files (x86)\Common Files
%localappdata%	C:\Users*\AppData\Local	C:\Documents and Settings*\Local Settings\Application Data **Note:** Does not work for real-time scanning.
%programdata%	C:\ProgramData	C:\Documents and Settings\All Users\Application Data

Variable	Windows Server 2008 + later	Windows Server 2003
%programfiles%	C:\Program Files	C:\Program Files
%programfiles(x86)%	C:\Program Files (x86)	C:\Program Files (x86)
%systemdrive%	C:	C:
%systemroot%	C:\Windows	C:\Windows
%temp% or %tmp%	C:\Users*\AppData\Local\Temp	C:\Documents and Settings*\Local Settings\Temp **Note:** Does not work for real-time scanning.
%userprofile%	C:\Users*	C:\Documents and Settings*
%windir%	C:\Windows	C:\Windows

14.3.1.2 Virtual Server Scanning Exclusions: Wildcards

Virtual Server exclusions let you exclude items from scanning on Windows guest VMs that are protected by a Sophos security VM.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 123).

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.

Exclusion	Notes
D:	Excludes the entire drive.
C:\programdata\adobe\photoshop\	Excludes the folder (you must include the final slash).
C:\program files\program*.com	Excludes files with a .com extension in the specified folder.
file.com	Excludes files with this name in any location (full path not needed).
file.*	Excludes all files called "file", with any extension, in all locations.
*.com	Excludes all files with a .com extension in all locations.
.	Excludes all files in all locations.
C:\file??.docx	Excludes C:\file12.exe (but not C:\file123.exe).

Exclusions that do NOT work

The expressions shown in this table are not valid for Virtual Server exclusions.

Exclusion	Notes
file	Cannot specify a file without a file extension.
\folder	Cannot specify a folder without the full path.
file*	Cannot use * within a filename.
file*.com	Cannot use * within a filename.
file*.*	Cannot use * within a filename.

Exclusion	Notes
C:\?\	Cannot replace the folder name with a wildcard.
C:\folder*\	Cannot use * within a folder name.

14.3.1.3 Scanning Exclusions for Specific VMs

You can set up scanning exclusions for specific guest VMs that are protected by a 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. This is because the VMware software doesn't currently support file exclusions for individual guest VMs. 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To specify exclusions for a guest VM:

1. Go to **Policies** > **Server Policies** and select the policy that applies to your 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. This is because the VMware software doesn't currently support this option for exclusions on individual guest VMs.

The wildcard is valid at the start or end of the VM name (or both). See examples below.

Example	Where the exclusion applies
|Window7*|c:\foo\	All guest VMs where the name starts with Windows 7.
|*x64|c:\foo\	All guest VMs where the name ends with x64.
|*Computer*|c:\foo\	All guest VMs where the name contains Computer.

14.3.2 Configure Server Lockdown

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.

The settings let you:

- Allow software to run and modify other files.
- Block software that is currently allowed to run.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Allowed files/folders

This option lets you allow software (such as updaters) to run and modify other applications. It also lets you add new software to a locked-down server without unlocking it.

Caution: This option “trusts” the software, so that any files it creates or changes are also allowed. This is different from the process when you lock down a server, which only allows the software itself to run.

You can specify files that are allowed, or a folder in which all the files are allowed.

Tip: You can specify a folder where you always download installers for use on the server.

1. Click **Add allowed file/folder**.
2. Select the type of item to allow (file or folder).
3. Enter the path of the file or folder.

   Note: You can use the wildcard *
4. Click **Save**.

Blocked files/folder

This lets you block software that is currently allowed to run.

You can specify files that are blocked, or a folder in which all the files are blocked.

Tip: You can block a folder used for applications, such as installers, that you want to make available to other users on the network, but don't want to run on your server.

1. Click **Add blocked file/folder**.
2. Select the type of item to block (file or folder).
3. Enter the path of the file or folder.

   Note: You can use the wildcard *
4. Click **Save**.

14.3.3 Configure Peripheral Control for Servers

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can configure this feature if you create or open a server policy and click the **Peripheral Control** tab.

Enable Peripheral Control

Ensure **Peripheral Control** is enabled.

You can disable this option any time if you want to stop enforcing this part of the policy.

Manage Peripherals

In Manage Peripherals, select how you want to control peripherals:

- **Monitor but do not block**. If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you cannot set access rules for them.
- **Control access by peripheral type and add exemptions**. If you select this, you can go on to set access policies for peripheral types and for individual detected peripherals.

Set Access Policies

Set access policies in the table.

The table displays detected peripheral types, the number of each type detected, and the current access policy.

Note: The totals include all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent policies for all devices.

Note: The **MTP/PTP** category includes devices such as phones, tablets, cameras and media players that connect using the MTP or PTP protocols.

For each peripheral type, you can change the access policy:

- **Allow**: Peripherals are not restricted in any way.
- **Block** : Peripherals are not allowed at all.
- **Read Only**: Peripherals can be accessed only for reading.

Note: The Bluetooth, Infrared, and Modem categories do not have the **Read Only** option.

Note: The Wireless Network Adaptor category has a **Block Bridged** option. This prevents bridging of two networks.

Peripheral Exemptions

Click the **Peripheral Exemptions** fold-out if you want to exempt individual peripherals from the control settings, or apply less restrictive controls.

1. Click **Add Exemptions**.
2. In the **Add Peripheral Exemptions** dialog, you'll see a list of detected peripherals.

   Note: Peripherals are detected when you are in monitoring mode or if there is an access restriction for that type of peripheral.

   Note: This list shows all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent exemptions for all devices.

3. Select a peripheral.
4. In the **Policy** column, you can optionally use the drop-down list to assign a specific access policy to an exempt peripheral.

   Restriction: Do not set a stricter access policy for an individual peripheral than for its peripheral type. If you do, the setting for the individual policy is ignored and a warning icon is displayed beside it.

5. In the **Enforce by** column, you can optionally use the drop-down menu to apply the policy to all peripherals of that model or to ones with the same ID (the list shows you the model and ID).
6. Click **Add Exemption(s)**.

14.3.4 Configure Application Control for Servers

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.

You can configure this feature if you create or open a policy and select **Application control**.

Note: If you want to use application control, ensure that the Threat Protection feature is also enabled in the policy.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

We recommend that you detect the applications being used on your network and then decide which to block, as follows.

1. Ensure **Application Control** is enabled.

   Tip: You can disable this option any time if you want to stop enforcing this part of the policy.

2. 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.

3. Click an application category, for example **Browser Plugin**.

   A full list of the applications in that category is displayed in the right-hand table.

4. We recommend that you select the option **Select all applications**. You'll refine your selection later.
5. 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.

6. 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.

7. Allow time for all your computers to run a scheduled scan.
8. Go to the **Logs & Reports** > **Events** page.
9. 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.

10. Return to your policy page.
11. 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**.

12. 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.

14.3.5 Configure Web Control for Servers

Attention: This help page describes policy settings for servers. Different policy settings apply for workstation users (page 104).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can configure this feature if you create or open a server policy and click the **Web Control** tab.

Note: Web Control settings apply only to Windows servers.

Note: All servers to which this policy applies will use a Server Advanced license.

Enable Web Control

Ensure **Web Control** is enabled.

Tip: You cannot disable this option in the Base policy. However, you can disable it in any other policy if you want to stop enforcing this part of the policy.

Website Controls

Select **Website controls** to control access to websites that may be inappropriate.

For each website category, you can select:

- **Allow**: Allows all websites in this category.
- **Warn**: Warns the user that a website may be inappropriate.
- **Block**: Blocks all websites in this category.

Log web control events

Select **Log web control events** to log attempts to visit blocked websites or websites for which we display a warning.

Note: If you do not enable logging, only attempts to visit infected sites will be logged.

Control sites tagged in Website Management

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.

15 System Settings

The System 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

15.1 Active Directory Sync

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 131). For full details of how it works, see About Active Directory synchronization (page 131). Once you have set up synchronization you can review its status and other settings, see Active Directory Sync Status (page 130).

For instructions on configuring Azure Active Directory synchronization, see Set up synchronization with Azure Active Directory (page 133). Once you have set up synchronization you can review its status and other settings, see Azure AD Sync Status (page 133).

15.1.1 Active Directory Sync Status

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

On this page, once you set up Active Directory synchronization, you can view:

- 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

By default the Active Directory federation service is switched off. If you want your users to access the Self Service Portal with Active Directory credentials, you can enable this option.

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

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 and groups containing at least one active user.
- 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.

  You cannot edit groups imported from Active Directory. For users imported from Active Directory:

  - You *cannot* modify their name, email, or Exchange login, or add or remove associated groups or logins managed by Active Directory.
  - You *can* add 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 when an existing Sophos Central user is matched to an Active Directory user. If a match is found, then the existing user is updated with any new or changed information. 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.

15.1.1.1 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To set up synchronization with Active Directory:

1. 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. On the last page, select the **Launch Sophos Cloud AD Sync Utility** checkbox and click **Finish**.

   Alternatively, go to the **Windows Start menu** > **All Programs** > **Sophos** > **Central** > **AD Sync**. If you are running Windows 8 or later, in the Apps list, find the app **AD Sync** listed under **Sophos**.

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

3. On the **Sophos Credentials** page, enter your Sophos Central account credentials.
4. On the **AD Configuration** page, specify your Active Directory LDAP server and credentials for a user account that has read access to the entire Active Directory forest with which you want to synchronize. To stay secure, use an account with the least rights that will give this access.

   We recommend that you use a secure LDAP connection, encrypted via SSL, and leave the **Use LDAP over an SSL connection (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.

5. If you don't want to synchronize the entire forest, on the **AD Filters** page, you can specify which domains to include in the synchronization. You can also specify additional search options—search bases and LDAP query filters—for each domain. Distinct options can be specified for users and groups.

   Note: AD Sync will only create groups that have members which include discovered users, regardless of group filter settings.

   - **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.

6. On the **Sync Schedule** page, define the times at which the synchronization will be performed automatically.

   Note: A scheduled synchronization is performed by a background service. The AD Sync utility does not need to be running for the scheduled synchronizations to occur.

   If you want to synchronize manually by running the AD Sync utility and don't want the synchronization to run automatically on a regular basis, select **Never. Only sync when manually initiated.**

7. To synchronize immediately, click **Preview and Sync**. Review the changes that will be made during the synchronization. If you are happy with the changes, click **Approve Changes and Continue**.

   The Active Directory users and groups are imported from the Active Directory to the Sophos Central Admin console.

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

15.1.2 Azure AD Sync Status

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

On this 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 133).

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.

15.1.2.1 Set up synchronization with Azure Active Directory

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To configure Azure Active Directory synchronization:

1. 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 a 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.

15.2 Role Management

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

The **System Settings** > **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.

15.2.1 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:

Role	Administrators with this role...	Administrators with this role cannot...	User Interface Restrictions
Super Admin **Important:** There must be at least one administrator with a SuperAdmin role.	Have access to everything in Sophos Central . In addition they can: ▪ Manage roles and role assignments	There are no limitations.	None.
Admin	Have access to everything in Sophos Central.	Manage roles and role assignments.	No Role Management options are displayed.
Help Desk	Have read only access for all settings in Sophos Central. In addition they can: ▪ 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. ▪ Look at sensitive logs or reports. ▪ Change settings.	No Role Management options are displayed. In addition: ▪ Sensitive reports and logs are not displayed. ▪ 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.	Has access only to the Self Service Portal.

Role	Administrators with this role...	Administrators with this role cannot...	User Interface Restrictions
		▪ Update the Sophos agent software on a computer. ▪ Scan computers. ▪ Look at sensitive logs or reports.	

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 49).

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.

15.3 Tamper Protection

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

15.4 API Token Management

On the **System Settings** > **API Token Management** page, 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. Click **Add Token**.
2. 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

15.5 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

On the **System Settings** > **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.

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**.

15.6 Registered Firewall Appliances

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**).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

15.7 Global Scanning Exclusions

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

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

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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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. In the **Value** text field, enter the desired entry. 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 Windows Scanning Exclusions: Wildcards and Variables (page 118).
   - **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 121).
   - **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.

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**.

15.8 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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

15.9 Bandwidth Usage

You can configure the updating of Sophos agent software on your endpoint computers.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Set the bandwidth used

Sophos Central limits the bandwidth used for updating. 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 Update Caches (page 142).

15.10 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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. Go to the **System Settings** > **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**.

15.11 iOS Settings for MDM

If you want to protect mobile iOS devices with MDM (Mobile Device Management), a valid Apple Push (APNs) certificate is necessary for communication between Sophos Central and the iOS devices.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You can create a certificate (page 143) or renew an existing certificate (page 144) at the **System Settings** > **iOS Settings for MDM** page.

Note: If your APNs certificate is about to expire, renew it as soon as possible so that communication between Sophos Central and your iOS devices will be possible at all times.

Note: If you only want to protect Android devices, you do not need an APNs certificate.

15.11.1 Create APNs Certificate

This procedure assumes that you have not uploaded an Apple Push (APNs) certificate to Sophos Central yet. To renew an existing APNs certificate, see Renew APNs Certificate (page 144).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

1. On the **iOS Settings for MDM** page, click **Enable iOS support now**.

   The **iOS Support Setup** dialog is displayed.

2. In the **Download Certificate Signing** step, click **Download the certificate signing request**.

   This saves the certificate signing request file `apple.csr` to your local computer.

3. You need an Apple ID. Even if you already have an ID, we recommend that you create a new one for use with Sophos Central. In the **Create Apple ID** step, click **Create Apple ID**.

   This opens an Apple web page where you can create an Apple ID for your company.

   Note: Store the credentials in a safe place where your colleagues can access them. Your company will need these credentials to renew the certificate each year.

4. In the **Create/Renew APNs Certificate** step, click **Apple Push Certificates Portal**.

   This opens the Apple Push Certificates Portal.

5. Log in with your Apple ID and upload the certificate signing request file `apple.csr` you prepared before. Download the .pem APNs certificate file and save it to your computer.
6. In the **Upload APNs Certificate** step, enter your Apple ID. Then click **Browse**. Select the .pem file that you received from the Apple Push Certificates Portal.
7. Click **Save** to add the APNs certificate to Sophos Central and to close the dialog.

After you have created an APNs certificate, the page shows the certificate details.

15.11.2 Renew APNs Certificate

This procedure assumes that you already have uploaded an Apple Push (APNs) certificate to Sophos Central that is about to be expire and needs to be renewed. To create and upload an APNs certificate initially, see Create APNs Certificate (page 143).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

1. On the **iOS Settings for MDM** page, make a note of the Apple ID that is displayed in the **Details** section.

   That Apple ID was used for creating the initial APNs certificate. You need to use the same Apple ID for the renewal.

2. In the left-hand pane, click **Renew**.

   The **Renew APNs Certificate** dialog is displayed.

3. Skip the steps **Download Certificate Signing** and **Create Apple ID**. These steps are only required if you are creating an APNs certificate for Sophos Central for the first time.
4. In the **Create/Renew APNs Certificate** step, click **Apple Push Certificates Portal**.

   This opens the Apple Push Certificates Portal.

5. Log in to the Apple Push Certificates Portal with your Apple ID and then do as follows:
   a) If you have more than one certificate in your overview, find the one you need to renew. You can do this by using the certificate information you saw earlier.
   b) Click **Download** next to the certificate to save the .pem APNs certificate file to your computer.
6. In the **Upload APNs Certificate** step of the Sophos Central dialog, verify that the displayed Apple ID matches the one you used for the certificate and then click **Browse**. Select the .pem file that you received from the Apple Push Certificates Portal.
7. Click **Save** to add the APNs certificate to Sophos Central and to close the dialog.

Note: What to do if you cannot renew your certificate

If you cannot renew your certificate, you will have to create and upload a new APNs certificate. However, this means that you must re-enroll all your devices. There are two ways to do so:

- Go to **Mobile Devices** and delete the devices from Sophos Central. Then send a new setup email to your users so that they will re-enroll their devices. As the app is still installed, it is not necessary to do the first step described in the setup mail.
- Alternatively, the users can delete the Sophos Central profile from their devices manually and repeat the configuration as described in the setup mail. They can even use their original deployment mail. The device will change its state from **Decommissioned by user** back to **Managed**.

15.12 Exchange Settings

On the **System Settings** > **Exchange Settings** page, you enter Microsoft Exchange email settings that enable users to check their corporate email on their mobile devices.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

The settings that you enter here can later be added to a user policy. The settings will then apply to all users (and their mobile devices) to whom that policy is assigned to.

Note: Due to OS limitations, you can only set up these settings on iOS devices and on these Android devices:

- Samsung SAFE version 2 or above
- LG GATE version 1.0 or above
- SONY Enterprise API version 4 or above

To add a new Exchange setting:

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

   The **Add Exchange Settings** dialog is displayed.

2. In the **Server Address** text field, enter the address of your Microsoft Exchange server. Example: `mail.mycompany.com`

   Note: If required, you can configure several Exchange settings with the same server address.

3. In the **Domain** text field, optionally enter your domain name if this is necessary for authentication at the Exchange server.
4. In the **Sync Period** drop-down list, select the time period for email synchronization. Only emails from within the specified period will be synchronized to the mobile device. For example, if you select **Two weeks**, only emails from the latest two weeks will be synchronized.
5. Enable **Use SSL** to use a secure connection (https) for communication with the Exchange server. It must also be configured on the Exchange server in order to work.
6. In the **Account Information** drop-down list, select if you want to configure the Exchange settings for a specific user account. You have the following options:
   - **Take information from Sophos Central user details**. This uses the email address and Exchange login supplied when the user was added. To check these details, go to the **Users** page and click the user's name.
   - **Take information from Sophos Central user details with email as login**. This uses the email address supplied when the user was added for both the login name and the email address of the Exchange account.
   - **Define information for one user here**. This lets you enter specific account information for a single user. The same account information is used for all users to whom the Exchange settings are applied to.

When you have selected **Define information for one user here**, use the following two fields to specify the account information.

7. In the **Exchange Login** text field, enter the login name of the Exchange account.
8. In the **Exchange E-Mail** text field, enter the email address of the Exchange account.
9. Click **Save**. The settings are added to the Exchange settings list.

To edit an Exchange setting later, click the server address in the Exchange Settings list, enter new settings and click **Save**.

To apply the settings to your users, add them to the **Mobile Device Management** section of a user policy. The settings will then apply to all users (and their mobile devices) to whom that policy is assigned to.

15.13 Wi-Fi Settings

On the **System Settings** > **Wi-Fi Settings** page, you configure the connection of mobile devices to Wi-Fi networks. No manual configuration on the devices is necessary and the devices can connect automatically to the respective networks.

The settings you enter here can be added to a user policy. The settings then apply to all users (and their mobile devices) that the policy is assigned to.

Note: Wi-Fi settings that can only be applied to iOS devices are indicated with the iOS icon.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To add a new Wi-Fi setting:

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

   The **Add Wi-Fi Settings** dialog is displayed.

2. In the **Network Name (SSID)** text field, enter the ID of the wireless network. Example: **`MyCompanyWiFi`**

   Note: If required, you can configure several Wi-Fi settings with the same SSID.

3. In the **Security Type** drop-down list, select the security type used by the network.
4. When you have selected a different security type than **None**, in the **Password** text field enter the password to connect with the network.
5. Enable **Connect automatically** to let the mobile devices connect to the network as soon as the network becomes available.
6. Enable **Hidden network** if the network is configured as hidden. Hidden networks cannot be found by devices when they perform a scan for networks.
7. In the **Proxy Settings** section, you can configure a proxy that is used for the Wi-Fi connection. In the **Type** drop-down list, select the configuration type. You have the following options:

   - **None**. Do not use a proxy.
   - **Automatic**. Use a proxy and configure it automatically using proxy auto-configuration (PAC).

     When you select this option, you must also enter the URL of the proxy server's PAC file.

   - **Manual**. Use a proxy and configure it manually.

     When you select this option, you must also enter the server address and port of the proxy and, if authentication is required to connect to the proxy, a user name and password.

8. Click **Save**. The settings are added to the Wi-Fi settings list.

To edit Wi-Fi settings later, click the SSID in the Wi-Fi Settings list, enter new settings and click **Save**.

To apply the settings to your users, add them to the **Mobile Device Management** section of a user policy. The settings will then apply to all users (and their mobile devices) to whom that policy is assigned to.

15.14 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 150).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

On the **System Settings** > **Email Security** > **Allow/Block** page you can:

- Add an allowed domain or address (page 148)

- Add a blocked domain or address (page 148)
- Remove a domain or address (page 148)

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. Click **OK**.

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

Note: If the domain or email address is present in the list as a blocked domain or email address you can override the setting. This changes the blocked status for the email domain or address to allowed.

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. Click **OK**.

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

Note: If the domain or email address is present in the list as an allowed domain or email address you can override the setting. This changes the allowed status for the email domain or address to blocked

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.

15.15 Email Security Settings

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 150).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

You configure and manage protected email domains, on the **System Settings** > **Email Security** > **Settings** page, using the options described below.

- Add a domain (page 149).
- Delete a domain (page 150).
- Edit a domain (page 150)

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:

   1. Expand **Information to configure External Dependencies**.
   2. Click **Instructions for Common Providers**.
   3. Click the Office 365 link.
   4. 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 Configure Email Security (page 109).

    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**.

15.15.1 Set up Email Security

Email Security provides protection against spam.

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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 (page 150)or Add users and email addresses (page 151) below.
2. Add your protected email domains, see Email Security Settings (page 148)
3. Configure spam protection in the Base user policy, see Configure Email Security (page 109).
4. Set up global controls on spam using allow and block lists for senders, see Allow/Block Domains and Addresses (page 147).

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. On the **System Settings** > **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 131).
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. On the **System Settings** > **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 Email Security Settings (page 148).

15.15.2 Managing Quarantined Email

You can use the Sophos Self Service Portal to manage your quarantined email. Quarantined email consists of messages that have been marked as spam. You can review these messages and either release or delete them. Releasing messages delivers them.

1. Sign in to the Sophos Self Service Portal.

2. Click on **Email**.

   This opens the **Email Security** page and shows the number of quarantined messages you have.

3. Click on **Quarantine**.

   This displays a list of your quarantined email messages. The sender, recipient, subject, time and date are shown for each email.

4. You can either release (deliver) or delete a quarantined message.

   - Select a message and click **Release** to deliver it.
   - Select a message and click **Delete** to remove it.

     Note: Quarantined messages are deleted after 14 days.

5. Log out when you have finished reviewing your quarantined email.

15.16 Allowed App Settings

On the **System Settings** > **Allowed App Settings** page, you can define apps that the users are allowed to use and are not reported as potentially unwanted apps (PUAs) or low reputation apps during a mobile device scan.

Important: Your assigned adminstrator role affects what you can do, see Administration Roles (page 134).

The settings that you enter here can later be added to a user policy. The settings will then apply to all users (and their mobile devices) to whom that policy is assigned to.

Note:

- Allowed App settings can only be applied to Android devices.
- If an allowed app is subsequently reclassified as a greater risk, for example from a PUA to malware, it will be reported again.

To add a new allowed app setting:

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

   The **Add Allowed App Settings** dialog is displayed.

2. In the **App Name** text field, enter the name of the app. The name is arbitrary and is only used to identify the app setting.
3. In the **Package Name** text field, enter the package name that uniquely identifies the app.

   Tip: The package name can be retrieved from the app's URL in Google Play Store. For example for the Sophos Mobile Control Android app, the Play Store URL is https://play.google.com/store/apps/details?id=com.sophos.mobilecontrol.client.android and the package name is **`com.sophos.mobilecontrol.client.android`**.

4. Click **Save**. The app settings are added to the Allowed App Settings list.

To edit Allowed App settings later, click the app name in the Allowed App Settings list, enter new settings and click **Save**.

To apply the settings to your users, add them to the **Mobile Security Settings** section of a user policy. The settings will then apply to all users (and their mobile devices) to whom that policy is assigned to.

15.17 Amazon Web Services Accounts

This feature may not be available for all customers yet.

On the **System Settings** > **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.

Note: You can only add AWS accounts if you are a SuperAdmin or Admin administrator, see Administration Roles (page 134).

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 with a Sophos agent installed are listed on the **Servers** page.
- AWS Auto Scaling Groups are listed on the **Server Groups** page.
- Policies assigned to AWS Auto Scaling Groups are automatically assigned to instances that are in that group and have a Sophos agent installed.

16 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.

Note: You cannot download installers for Mobile Device Management or Mobile Security here. Instead, go to the **Users** page and send users a setup link that lets them enroll their mobile.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

16.1 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).

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Download and run installers

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

For **Windows**, you have a choice of downloads:

- Click **Download Windows Installer** for an installer with all components your license covers.
- Click **Choose Windows Installer Components** if you want to choose the components included in the installer. The components are Endpoint Advanced (protection from malware), Intercept X (protection from ransomware and exploits), and Device Encryption.

For **Linux**, look in the "Server Protection" list. Sophos Central treats all Linux computers as servers.

When you protect a workstation:

- Each user who logs in is added to the users list in Sophos Central automatically.
- A user policy is applied to each user (by default, this is the Base Policy).
- 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.

16.2 Server Protection

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

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.
- A server policy is applied to the server (by default, this is the Base Policy).

16.3 Server Protection As A Web Service

You can protect Linux computers with Sophos Secure OS.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

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.

To use it, click on **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).

16.4 Mobile Management and Security

You can protect your mobile devices with one or both of the following apps:

- **Sophos Mobile Control** helps you to keep corporate data safe by managing apps and security settings.
- **Sophos Mobile Security** scans the mobile device for malicious apps and checks whether the device is rooted. You can also configure it to detect potentially unwanted and low reputation apps, and malicious websites.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

To send a personalized email with deployment instructions for these apps to selected users, go to the **Users** page and click **Email Setup Link** in the upper right of the page. Then select one or both of these options:

- For **Sophos Mobile Control**, under **Mobile Device Management** select **iOS and Android mobile devices**.
- For **Sophos Mobile Security**, under **Endpoint Protection** select **Android mobile devices**.

The device will be automatically associated with the user in Sophos Central when deployed.

16.5 Virtual Environment Protection

You can use Sophos Central to protect your virtual machines (VMs).

To do this, you must install a "Sophos security VM" on your host to provide central anti-virus scanning for all the guest VMs on that host.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Click **Download Sophos Security Host VM Installer** and then run the installer on your host. We recommend you read the startup guide.

Click **Download Sophos Guest VM Installer** to get the optional Sophos agent and install it on your guest VMs. This agent enables automatic cleanup of threats.

When you install a Sophos security VM on your host:

- The Sophos security VM is added to the **Servers** list in Sophos Central.
- A server policy is applied to the security VM (by default, this is the Base Policy).

16.6 Web Gateway

The Sophos Web Gateway installers are available only if you are licensed for 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.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Install Web Gateway on workstations

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 and a user policy is applied to them.
- If the computer is not already in the Computers list, it is added.
- If you have Web Gateway enabled in a user policy that applies to the computer, it starts protecting the computer.

Install Web Gateway on mobile 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.

17 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.

18 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** .

Important: Your ability to manage your account details depends on your assigned administrator role, see Administration Roles (page 134).

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**.

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**.

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.

19 Licensing

You can activate and manage your Sophos licenses from the Sophos Central Admin console.

Important: Your assigned administrator role affects what you can do, see Administration Roles (page 134).

Click your account name (upper right of the user interface), select **Licensing**.

You can:

- Activate a license (page 161)
- Buy a license (page 161)
- Review end-user license agreement (page 161)
- View your licenses and usage (page 161)

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 6).

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.
- **Expires**. The date when the license expires.
- **License#**. License number.

20 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**.

21 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.

22 Contact Sophos Support

Get help

To get help from Sophos Support:

1. Click **Help** in the top right of the user interface and select **Create Support Ticket**.
2. Fill in the form. Be as precise as possible so that Support can help you effectively.
3. Optionally, select **Enable Remote Assistance**. This enables Support to directly access your Sophos Central session to be better able to help you.
4. Click **Send**.

Sophos will contact you within 24 hours.

Note: If you selected Remote Assistance, this function is enabled when you click **Send**. Remote Assistance will automatically be disabled after 72 hours. To disable it sooner, click on your account name (upper right of the user interface), select **Licensing & Administration**, and click the **Sophos Support** tab.

Submit feedback

To submit feedback or a suggestion to Sophos Support:

1. Click **Help** in the top right of the user interface and select **Give Feedback**.
2. Fill in the form.
3. Click **Send**.

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.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.

23 Legal notices